



# ASP

CITTÀ DI BOLOGNA

*Azienda pubblica  
di servizi alla persona*

## **MANUALE DI GESTIONE DEL PROTOCOLLO INFORMATICO, DEI FLUSSI DOCUMENTALI E DEGLI ARCHIVI DI ASP CITTÀ DI BOLOGNA**

(APPROVATO CON DETERMINAZIONE DEL DIRETTORE AREA AMMINISTRATIVA N. 440 DEL 10.06.2025)

**Allegato n. 1** Linee Guida di Agid sulla formazione, gestione e conservazione dei documenti informatici comprensive dei seguenti allegati:

- a) Allegato 1 – Glossario dei termini e degli acronimi
- b) Allegato 2 – Formati di File e Riversamento
- c) Allegato 3 – Certificazione di processo
- d) Allegato 4 – Standard e specifiche tecniche
- e) Allegato 5 – Metadati
- f) Allegato 6 – Comunicazione tra AOO di Documenti Amministrativi Protocollati

# Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Maggio 2021

## Sommario

CAPITOLO 1	Introduzione, strumenti di lettura e disposizioni comuni	5
1.1.	Scopo del documento	5
1.2.	Ambito soggettivo di applicazione	5
1.3.	Ambito oggettivo di applicazione	6
1.4.	Abrogazioni e norme transitorie	6
1.5.	Principali riferimenti normativi	7
1.6.	Linee guida AGID richiamate	8
1.7.	Gruppo di lavoro	8
1.8.	Allegati	9
1.9.	Premessa metodologica	9
1.10.	Natura vincolante delle Linee Guida	10
1.11.	Principi generali della gestione documentale	10
CAPITOLO 2	Formazione dei documenti informatici	12
2.1.	Documento informatico	12
2.1.1.	Formazione del documento informatico	12
2.2.	Copie per immagine su supporto informatico di documenti analogici	14
2.3.	Duplicati, copie ed estratti informatici di documenti informatici	15
2.4.	Il documento amministrativo informatico	16
2.4.1.	Formazione del documento amministrativo informatico	16
2.5.	Copie su supporto informatico di documenti amministrativi analogici	17
CAPITOLO 3	Gestione documentale	18
3.1.	Registrazione informatica dei documenti	18
3.1.1.	Ambito di applicazione	18
3.1.2.	Adeguamento organizzativo e funzionale	18
3.1.3.	Registrazione di protocollo e altre forme di registrazione	19

3.1.4.	Formato della registrazione e della segnatura di protocollo	20
3.1.5.	Annullamento delle informazioni registrate in forma immodificabile	21
3.1.6.	Requisiti minimi di sicurezza dei sistemi di protocollo informatico	21
3.2.	Classificazione dei documenti informatici	22
3.3.	Aggregazioni documentali informatiche	22
3.3.1.	Fascicoli informatici	22
3.3.2.	Altre aggregazioni documentali informatiche	23
3.3.3.	Registri e repertori informatici	24
3.4.	Compiti del responsabile della gestione documentale	24
3.5.	Manuale di gestione documentale	25
3.6.	Formati di file	27
3.7.	Riversamento	28
3.8.	Trasferimento al sistema di conservazione	28
3.9.	Misure di sicurezza	29
CAPITOLO 4 Conservazione		31
4.1.	Sistema di conservazione	31
4.2.	Pacchetti informativi	32
4.3.	Modelli organizzativi della conservazione	32
4.4.	Ruoli e responsabilità	33
4.5.	Responsabile della conservazione	33
4.6.	Manuale di conservazione	35
4.7.	Processo di conservazione	36
4.8.	Infrastrutture	37
4.9.	Modalità di esibizione	38
4.10.	Misure di sicurezza	38
4.11.	Selezione e scarto dei documenti informatici	39

Questo documento raccoglie il testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

## CAPITOLO 1 Introduzione, strumenti di lettura e disposizioni comuni

---

### 1.1. Scopo del documento

Lo scopo delle presenti linee guida è duplice:

- a) aggiornare le attuali regole tecniche in base all'art. 71 del Codice dell'amministrazione digitale<sup>1</sup> (da ora in avanti CAD), concernenti la formazione, protocollazione, gestione e conservazione dei documenti informatici;
- b) incorporare in un'unica linea guida le regole tecniche e le circolari in materia, addivenendo ad un "unicum" normativo che disciplini gli ambiti sopracitati, nel rispetto della disciplina in materia di Beni culturali.

### 1.2. Ambito soggettivo di applicazione

Le presenti Linee Guida sono applicabili ai soggetti indicati nell'art. 2 commi 2 e 3 del CAD<sup>2</sup>, fatti salvi gli specifici riferimenti alla Pubblica Amministrazione.

---

<sup>1</sup> L'art. 71, comma 1, del CAD prevede che "L'AgID, previa consultazione pubblica da svolgersi entro il termine di trenta giorni, sentiti le amministrazioni competenti e il Garante per la protezione dei dati personali nelle materie di competenza, nonché acquisito il parere della Conferenza unificata, adotta Linee guida contenenti le regole tecniche e di indirizzo per l'attuazione del presente Codice".

<sup>2</sup> L'art. 2, comma 2, del CAD prevede che le disposizioni del Codice si applicano:

"a) alle pubbliche amministrazioni di cui all'articolo 1, comma 2, del decreto legislativo 30 marzo 2001, n. 165, nel rispetto del riparto di competenza di cui all'articolo 117 della Costituzione, ivi comprese le autorità di sistema portuale, nonché alle autorità amministrative indipendenti di garanzia, vigilanza e regolazione;

b) ai gestori di servizi pubblici, ivi comprese le società quotate, in relazione ai servizi di pubblico interesse;

c) alle società a controllo pubblico, come definite nel decreto legislativo 19 agosto 2016, n. 175, escluse le società quotate di cui all'articolo 2, comma 1, lettera p), del medesimo decreto che non rientrino nella categoria di cui alla lettera b)".

Il successivo comma 3 prevede che le disposizioni del Codice e le relative Linee guida "concernenti il documento informatico, le firme elettroniche e i servizi fiduciari di cui al Capo II, la riproduzione e conservazione dei documenti di cui agli articoli 43 e 44, il domicilio digitale e le comunicazioni elettroniche di cui all'articolo 3-bis e al Capo IV, l'identità digitale di cui agli articoli 3-bis e 64 si applicano anche ai privati, ove non diversamente previsto".

### 1.3. Ambito oggettivo di applicazione

Le presenti Linee Guida contengono le regole tecniche sugli ambiti disciplinati dalle seguenti disposizioni del CAD:

- Art. 20, *Validità ed efficacia probatoria dei documenti informatici*, fatte salve le norme in materia di generazione, apposizione e verifica di qualsiasi tipo di firma elettronica
- Art. 21, *Ulteriori disposizioni relative ai documenti informatici, sottoscritti con firma elettronica avanzata, qualificata o digitale*
- Art. 22, commi 2 e 3, *Copie informatiche di documenti analogici*
- Art. 23, *Copie analogiche di documenti informatici*
- Art. 23-bis, *Duplicati e copie informatiche di documenti informatici*
- Art. 23-ter, *Documenti amministrativi informatici*
- Art. 23-quater, *Riproduzioni informatiche*
- Art. 34, *Norme particolari per le Pubbliche Amministrazioni*
- Art. 40, *Formazione di documenti informatici*
- Art. 40-bis, *Protocollo informatico*
- Art. 41, *Procedimento e fascicolo informatico*
- Art. 42, *Dematerializzazione dei documenti delle Pubbliche Amministrazioni*
- Art. 43, *Conservazione ed esibizione dei documenti*
- Art. 44, *Requisiti per la conservazione dei documenti informatici*
- Art. 45, *Valore giuridico della trasmissione*
- Art. 46, *Dati particolari contenuti nei documenti trasmessi*
- Art. 47, *Trasmissione dei documenti tra le Pubbliche Amministrazioni*
- Art. 49, *Segretezza della corrispondenza trasmessa per via telematica*
- Art. 50, *Disponibilità dei dati delle Pubbliche Amministrazioni*
- Art. 51, *Sicurezza e disponibilità dei dati, dei sistemi e delle infrastrutture delle Pubbliche Amministrazioni*
- Art. 64-bis, *Accesso telematico ai servizi della Pubblica Amministrazione*
- Art. 65, *Istanze e dichiarazioni presentate alle Pubbliche Amministrazioni per via telematica*

### 1.4. Abrogazioni e norme transitorie

Le presenti Linee Guida entrano in vigore il giorno successivo a quello della loro pubblicazione sul sito istituzionale di AGID, di cui si darà notizia sulla Gazzetta Ufficiale.

Esse si applicano a partire dal duecento settantesimo giorno successivo alla loro entrata in vigore.

A partire da questo termine i soggetti di cui all' art. 2 commi 2 e 3 del CAD formano i loro documenti esclusivamente in conformità alle presenti Linee Guida.

A partire dalla data di applicazione delle presenti Linee Guida, sono abrogati:

- il DPCM 13 novembre 2014, contenente “Regole tecniche in materia di formazione, trasmissione, copia, duplicazione, riproduzione e validazione temporale dei documenti informatici”;
- il DPCM 3 dicembre 2013, contenente “Regole tecniche in materia di sistema di conservazione”.

Per quanto concerne il DPCM 3 dicembre 2013, contenente “Regole tecniche per il protocollo informatico”, a partire dalla data di applicazione delle presenti Linee guida sono abrogate tutte le disposizioni fatte salve le seguenti:

- art. 2 comma 1, *Oggetto e ambito di applicazione*;
- art. 6, *Funzionalità*;
- art. 9, *Formato della segnatura di protocollo*;
- art. 18 commi 1 e 5, *Modalità di registrazione dei documenti informatici*;
- art. 20, *Segnatura di protocollo dei documenti trasmessi*;
- art. 21, *Informazioni da includere nella segnatura*.

Sempre a far data dalla data di applicazione delle presenti Linee guida, la circolare n. 60 del 23 gennaio 2013 dell'AgID in materia di “Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni” è abrogata e sostituita dall'allegato 6 “Comunicazione tra AOO di documenti amministrativi protocollati” del presente documento.

### 1.5. Principali riferimenti normativi

I principali riferimenti normativi presi in considerazione ai fini della redazione delle presenti Linee Guida sono i seguenti:

- a) RD 1163/1911, *Regolamento per gli archivi di Stato*;
- b) DPR 1409/1963, *Norme relative all'ordinamento ed al personale degli archivi di Stato*;
- c) Legge 241/1990, *Nuove norme sul procedimento amministrativo*;
- d) DPR 445/2000, *Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*;
- e) DPR 37/2001, *Regolamento di semplificazione dei procedimenti di costituzione e rinnovo delle Commissioni di sorveglianza sugli archivi e per lo scarto dei documenti degli uffici dello Stato*;
- f) D.lgs 196/2003 *recante il Codice in materia di protezione dei dati personali*;
- g) D.lgs 42/2004, *Codice dei beni culturali e del paesaggio, ai sensi dell'articolo 10 della legge 6 luglio 2002, n. 137*;
- h) Legge 9 gennaio 2004, n. 4 aggiornata dal decreto legislativo 10 agosto 2018, n. 106, *Disposizioni per favorire e semplificare l'accesso degli utenti e, in particolare, delle persone con disabilità agli strumenti informatici*;
- i) D.lgs 82/2005 e ss.mm.ii., *Codice dell'amministrazione digitale*;
- j) D.lgs 33/2013, *Riordino della disciplina riguardante il diritto di accesso civico e gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni*;
- k) DPCM 22 febbraio 2013, *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71*;
- l) DPCM 21 marzo 2013, *Individuazione di particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente*

*ed allegata al documento informatico, ai sensi dell'art. 22, comma 5, del Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni;*

- n) Reg. UE 910/2014, *in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE - Regolamento eIDAS;*
- o) Circolare 40 e 41 del 14 dicembre 2015 della Direzione generale degli archivi, *Autorizzazione alla distruzione di originali analogici riprodotti secondo le regole tecniche di cui al DPCM 13.11.2014 e conservati secondo le regole tecniche di cui al DPCM 13.12.2013;*
- p) Reg. UE 679/2016 (GDPR), *relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;*
- q) Circolare 18 aprile 2017, n. 2/2017 dell'Agenzia per l'Italia Digitale, *recante le misure minime di sicurezza ICT per le pubbliche amministrazioni;*
- r) Circolare n. 2 del 9 aprile 2018, *recante i criteri per la qualificazione dei Cloud Service Provider per la PA;*
- s) Circolare n. 3 del 9 aprile 2018, *recante i criteri per la qualificazione di servizi SaaS per il Cloud della PA;*
- t) Reg. UE 2018/1807, *relativo a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione europea;*
- u) DPCM 19 giugno 2019, n. 76, *Regolamento di organizzazione del Ministero per i beni e le attività culturali, degli uffici di diretta collaborazione del Ministro e dell'Organismo indipendente di valutazione della performance.*

### 1.6. Linee guida AGID richiamate

- a) Linee guida del 15 aprile 2019 *dell'indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi;*
- b) Linee guida del 6 giugno 2019 *contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.*
- c) Linee guida del 09/01/2020 *sull'Accessibilità degli strumenti informatici.*

### 1.7. Gruppo di lavoro

Il presente documento è stato redatto dal Tavolo di lavoro dell'Agenzia per l'Italia Digitale, istituito con determinazione del Direttore Generale n. 137 del 2 maggio 2018. Al Tavolo di lavoro, coordinato da Patrizia Gentili, hanno partecipato Alessandra Antolini, Gaetano Bruno, Matteo Carabellese, Antonio Florio, Enrica Massella Ducci Teri, Guido Pera, Vincenzo Travascio, Cristina Valiante. A titolo di esperti hanno partecipato inoltre Walter Arrighetti, Pietro Falletta Giacomo Massi e Luigi Avena, sentito anche il MIC come da art. 23 ter comma 4 del CAD<sup>3</sup>.

---

<sup>3</sup> L'art. 23 ter comma 4 del CAD prevede che "In materia di formazione e conservazione di documenti informatici delle pubbliche amministrazioni, le Linee guida sono definite anche sentito il Ministero dei beni e delle attività culturali e del turismo".

## 1.8. Allegati

Costituiscono parte integrante delle presenti Linee Guida i seguenti allegati:

1. Glossario dei termini e degli acronimi
2. Formati di file e riversamento
3. Certificazione di processo
4. Standard e specifiche tecniche
5. Metadati
6. Comunicazione tra AOO di Documenti Amministrativi Protocollati, che sostituisce la circolare 60/2013 dell'AgID.

## 1.9. Premessa metodologica

Le presenti linee guida costituiscono la nuova versione aggiornata delle regole tecniche in materia di formazione, protocollazione, gestione e conservazione del documento, già precedentemente regolate nei DPCM del 2013 e 2014. Obiettivo generale del documento è che la gestione complessiva del documento informatico risulti semplificata attraverso una visione d'insieme che aggrega in un "corpo unico" materie prima disciplinate separatamente.

L'approccio utilizzato è di tipo olistico, ossia diretto a mettere in evidenza e a rappresentare le interdipendenze funzionali tra le varie fasi della gestione documentale dal momento della formazione fino alla selezione per lo scarto o la conservazione permanente.

La tecnica redazionale – stante la natura prescrittiva del testo - ha privilegiato uno stile chiaro e fruibile per il lettore, indipendentemente dalla natura pubblica o privata di quest'ultimo e dalle sue competenze in materia.

Considerata la velocità dell'innovazione, le linee guida devono garantire un adattamento costante ai cambiamenti imposti dall'incessante rivoluzione digitale. Di qui la scelta di prevedere un testo "statico" che contenga la base normativa della materia e una serie di "allegati" i cui contenuti più "flessibili" potranno adeguarsi agevolmente all'evoluzione tecnologica. Tale processo di costante adeguamento degli "allegati" è realizzato in coerenza con il quadro normativo e attuativo in materia di digitalizzazione. Relativamente ai temi della trasmissione di contenuti digitali tra e con le pubbliche amministrazioni si assicura la conformità al Modello di interoperabilità definito da AgID e alle tecnologie introdotte dallo stesso.

## 1.10. Natura vincolante delle Linee Guida

Come precisato dal Consiglio di Stato - nell'ambito del parere reso sullo schema di decreto legislativo del correttivo al CAD, n. 2122/2017 del 10.10.2017 - le Linee Guida adottate da AGID, ai sensi dell'art. 71 del CAD, hanno carattere vincolante e assumono valenza *erga omnes*.

Ne deriva che, nella gerarchia delle fonti, anche le presenti Linee Guida sono inquadrate come un atto di regolamentazione, seppur di natura tecnica, con la conseguenza che esse sono pienamente azionabili davanti al giudice amministrativo in caso di violazione delle prescrizioni ivi contenute. Nelle ipotesi in cui la violazione sia posta in essere da parte dei soggetti di cui all'art. 2, comma 2 del CAD, è altresì possibile presentare apposita segnalazione al difensore civico, ai sensi dell'art. 17 del CAD<sup>4</sup>.

## 1.11. Principi generali della gestione documentale

La gestione documentale è un processo che può essere suddiviso in tre fasi principali: formazione, gestione e conservazione. Nell'ambito di ognuna delle suddette fasi si svolgono una serie di attività che si distinguono per complessità, impatto, natura, finalità e/o effetto, anche giuridico, alle quali corrispondono approcci metodologici e prassi operative distinte.

Il sistema di gestione informatico dei documenti, la cui tenuta può anche essere delegata a terzi, affinché possa essere efficiente e sicuro deve essere necessariamente presidiato da specifiche procedure e strumenti informatici, in grado di governare con efficacia ogni singolo accadimento che coinvolge la vita del documento ed effettuata secondo i principi generali applicabili in materia di trattamento dei dati personali anche mediante un'adeguata analisi del rischio.

Una corretta gestione dei documenti sin dalla loro fase di formazione rappresenta inoltre la migliore garanzia per il corretto adempimento degli obblighi di natura amministrativa, giuridica e archivistica tipici della gestione degli archivi pubblici.

Dal punto di vista archivistico, si distinguono tradizionalmente tre fasi di gestione in ragione delle diverse modalità di organizzazione ed utilizzo dei documenti:

- archivio corrente: riguarda i documenti necessari alle attività correnti;
- archivio di deposito: riguarda i documenti ancora utili per finalità amministrative o giuridiche, ma non più indispensabili per la trattazione delle attività correnti;
- archivio storico: riguarda i documenti storici selezionati per la conservazione permanente.

Nella fase di formazione devono essere perseguiti obiettivi di qualità, efficienza, razionalità, sistematicità, accessibilità e coerenza alle regole tecniche che presidiano la formazione dei documenti

---

<sup>4</sup> L'art. 17 comma 1-quater del CAD prevede che "È istituito presso l'AgID l'ufficio del difensore civico per il digitale, a cui è preposto un soggetto in possesso di adeguati requisiti di terzietà, autonomia e imparzialità. Chiunque può presentare al difensore civico per il digitale, attraverso apposita area presente sul sito istituzionale dell'AgID, segnalazioni relative a presunte violazioni del presente Codice e di ogni altra norma in materia di digitalizzazione ed innovazione della pubblica amministrazione da parte dei soggetti di cui all'articolo 2, comma 2. Ricevuta la segnalazione, il difensore civico, se la ritiene fondata, invita il soggetto responsabile della violazione a porvi rimedio tempestivamente e comunque non oltre trenta giorni".

informatici, tenendo in debito conto le esigenze e i bisogni pratici del lavoro quotidiano. Al tal fine, risulta decisivo avvalersi di un valido e completo manuale di gestione documentale, di workflow documentali e sistemi di Document & Content Management e di applicativi informatici, per la PA ai sensi degli articoli 68<sup>5</sup> e 69<sup>6</sup> del CAD, che si basino su elevati livelli di automazione ed interoperabilità in grado di operare nel web. In un contesto in continua trasformazione, il manuale di gestione documentale deve essere sottoposto a continuo aggiornamento, in ragione dell'evoluzione tecnologica e dell'obsolescenza degli oggetti e degli strumenti digitali utilizzati. Allo stesso modo, anche i processi e le attività che governano la fase di formazione dei documenti informatici devono essere sottoposti ad un costante lavoro di valutazione, monitoraggio, riprogettazione e reingegnerizzazione. L'adozione del manuale di gestione documentale e del manuale di conservazione non risponde solo ad esigenze pratico-operative, ma rappresenta un preciso obbligo come specificato ai paragrafi 3.5 e 4.7, al quale per la PA fa seguito l'ulteriore obbligo della loro pubblicazione sul sito istituzionale dell'ente.

La gestione dei documenti informatici prosegue con il suo trasferimento in un sistema di conservazione da realizzarsi in ottemperanza a quanto disposto dal CAD e dalle presenti Linee guida.

La conservazione dei documenti è tipicamente svolta all'interno di un sistema di conservazione dedicato a questa funzione.

Tuttavia, l'attenzione al profilo conservativo deve essere posta fin dal momento della formazione del documento, al fine di garantirne la tenuta all'interno del sistema di gestione informatica dei documenti e di eventuale conservazione a lungo termine all'interno di sistemi dedicati.

Nell'ambito della gestione documentale possono essere necessarie attività di riversamento dei documenti in altro formato diverso da quello originale, come specificato al paragrafo 3.7. Tale riversamento può avvenire più volte nella gestione del documento informatico e in diversi momenti per finalità gestionali o conservative.

In ambito digitale, infine, gli obblighi di pubblicazione di atti e provvedimenti amministrativi aventi effetto di pubblicità legale o comunque derivanti dalla normativa in materia di trasparenza devono essere assolti con la pubblicazione nei rispettivi siti web istituzionali. Affinché il processo di pubblicazione on line possa generare un prodotto atto ad assolvere i predetti obblighi è necessario che esso garantisca la conformità di quanto pubblicato all'originale, l'autorevolezza dell'ente emanatore e del sito web, la validità giuridica dei documenti e quindi la loro veridicità, efficacia e perdurabilità nel tempo.

---

<sup>5</sup> L'art. 68 del CAD prevede che "Le pubbliche amministrazioni acquisiscono programmi informatici o parti di essi nel rispetto dei principi di economicità e di efficienza, tutela degli investimenti, riuso e neutralità tecnologica, a seguito di una valutazione comparativa di tipo tecnico ed economico tra le seguenti soluzioni disponibili sul mercato:

- a) software sviluppato per conto della pubblica amministrazione;
- b) riutilizzo di software o parti di esso sviluppati per conto della pubblica amministrazione;
- c) software libero o a codice sorgente aperto;
- d) software fruibile in modalità cloud computing;
- e) software di tipo proprietario mediante ricorso a licenza d'uso;
- f) software combinazione delle precedenti soluzioni".

<sup>6</sup> L'art. 69 del CAD prevede che "Le pubbliche amministrazioni che siano titolari di soluzioni e programmi informatici realizzati su specifiche indicazioni del committente pubblico, hanno l'obbligo di rendere disponibile il relativo codice sorgente, completo della documentazione e rilasciato in repertorio pubblico sotto licenza aperta, in uso gratuito ad altre pubbliche amministrazioni o ai soggetti giuridici che intendano adattarli alle proprie esigenze, salvo motivate ragioni di ordine e sicurezza pubblica, difesa nazionale e consultazioni elettorali".

## CAPITOLO 2    Formazione dei documenti informatici

---

### 2.1.    Documento informatico

#### 2.1.1.    Formazione del documento informatico

Il contenuto del presente capitolo si applica, salvo ove diversamente specificato, ai soggetti di cui all'art. 2 commi 2 e 3 del CAD.

Il documento informatico è formato mediante una delle seguenti modalità:

- a) creazione tramite l'utilizzo di strumenti software o servizi cloud qualificati che assicurino la produzione di documenti nei formati e nel rispetto delle regole di interoperabilità di cui all'allegato 2;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.

Il documento informatico deve essere identificato in modo univoco e persistente. Nel caso della Pubblica Amministrazione<sup>7</sup>, l'identificazione dei documenti oggetto di registrazione di protocollo è rappresentata dalla segnatura di protocollo univocamente associata al documento. L'identificazione dei documenti non protocollati è affidata alle funzioni del sistema di gestione informatica dei documenti. In alternativa l'identificazione univoca può essere realizzata mediante associazione al documento di una sua impronta crittografica basata su funzioni di *hash* che siano ritenute crittograficamente sicure, e conformi alle tipologie di algoritmi previsti nell'allegato 6 delle linee guida nella tabella 1 del paragrafo 2.2 regole di processamento.

---

<sup>7</sup>Si fa riferimento ai soggetti di cui all'art. 2 comma 2, lettera a) del CAD.

## Linee Guida sulla formazione, gestione e conservazione dei documenti informatici

Il documento informatico è immodificabile se la sua memorizzazione su supporto informatico in formato digitale non può essere alterata nel suo accesso, gestione e conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera a), l'immodificabilità e l'integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- il trasferimento a soggetti terzi attraverso un servizio di posta elettronica certificata o un servizio elettronico di recapito certificato qualificato, come definito dal regolamento (UE) 23 luglio 2014 n. 910 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (regolamento eIDAS), valido ai fini delle comunicazioni elettroniche aventi valore legale;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo la sopracitata lettera b) l'immodificabilità ed integrità sono garantite da una o più delle seguenti operazioni mediante:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata;
- memorizzazione su sistemi di gestione documentale che adottino idonee misure di sicurezza in accordo con quanto riportato al § 3.9;
- versamento ad un sistema di conservazione.

Nel caso di documento informatico formato secondo le sopracitate lettere c) e d) le caratteristiche di immodificabilità e di integrità sono garantite da una o più delle seguenti operazioni:

- apposizione di una firma elettronica qualificata, di una firma digitale o di un sigillo elettronico qualificato o firma elettronica avanzata
- registrazione nei log di sistema dell'esito dell'operazione di formazione del documento informatico, compresa l'applicazione di misure per la protezione dell'integrità delle basi di dati e per la produzione e conservazione dei log di sistema;
- produzione di una estrazione statica dei dati e il trasferimento della stessa nel sistema di conservazione.

Al momento della formazione del documento informatico immodificabile, devono essere generati e associati permanentemente ad esso i relativi metadati. L'insieme dei metadati del documento informatico è definito nell'allegato 5 "Metadati" alle presenti linee guida. Potranno essere individuati ulteriori metadati da associare a particolari tipologie di documenti informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

La disponibilità e la riservatezza delle informazioni contenute nel documento informatico sono garantite attraverso l'adozione di specifiche politiche e procedure predeterminate dall'ente, in

conformità con le disposizioni vigenti in materia di accesso e protezione dei dati personali. Nel caso della Pubblica Amministrazione, tali politiche e procedure sono contenute nel manuale di gestione documentale di cui al paragrafo 3.5. L'evidenza informatica corrispondente al documento informatico immutabile è prodotta in uno dei formati contenuti nell'Allegato 2 "Formati di file e riversamento" alle presenti linee guida ove sono specificate, anche, le caratteristiche e i criteri di scelta del formato stesso.

## 2.2. Copie per immagine su supporto informatico di documenti analogici

La copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurino che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o, nel caso di esigenze di dematerializzazione massiva di documenti analogici, attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 "Certificazione di Processo".

Fermo restando quanto previsto dall'art. 22 comma 3 del CAD<sup>8</sup> nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia per immagine ad un documento analogico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata o altro tipo di firma ai sensi dell'art. 20 comma 1bis, ovvero del sigillo elettronico qualificato o avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico può essere inserita nel documento informatico contenente la copia per immagine o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

La distruzione degli originali analogici potrà essere effettuata in accordo con le previsioni di cui all'art. 22, commi 4 e 5 del CAD<sup>9</sup>.

---

<sup>8</sup> L'art. 22 comma 4 del CAD prevede "Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico nel rispetto delle regole tecniche di cui all'articolo 71 hanno la stessa efficacia probatoria degli originali da cui sono tratte se la loro conformità all'originale non è espressamente disconosciuta."

<sup>9</sup> L'art. 22 commi 4 e 5 del CAD prevedono "4. Le copie formate ai sensi dei commi 1, 1 bis, 2 e 3 sostituiscono ad ogni effetto di legge gli originali formati in origine su supporto analogico, e sono idonee ad assolvere gli obblighi di conservazione previsti dalla legge, salvo quanto stabilito dal comma 5.

5. Con decreto del Presidente del Consiglio dei Ministri possono essere individuate particolari tipologie di documenti analogici originali unici per le quali, in ragione di esigenze di natura pubblicistica, permane l'obbligo della conservazione dell'originale analogico oppure, in caso di conservazione sostitutiva, la loro conformità all'originale deve essere autenticata da un notaio o da altro pubblico ufficiale a ciò autorizzato con dichiarazione da questi firmata digitalmente ed allegata al documento informatico."

## 2.3. Duplicati, copie ed estratti informatici di documenti informatici

Un duplicato informatico ha lo stesso valore giuridico del documento informatico da cui è tratto se è ottenuto mediante la memorizzazione della medesima evidenza informatica, sullo stesso dispositivo o su dispositivi diversi; ad esempio, effettuando una copia da un PC ad una pen-drive di un documento nel medesimo formato.

La copia di un documento informatico è un documento il cui contenuto è il medesimo dell'originale ma con una diversa evidenza informatica rispetto al documento da cui è tratto, come quando si trasforma un documento con estensione “.doc” in un documento “.pdf”. L'estratto di un documento informatico è una parte del documento con una diversa evidenza informatica rispetto al documento da cui è tratto. Tali documenti hanno lo stesso valore probatorio dell'originale da cui hanno origine se la stessa conformità non viene espressamente disconosciuta. In particolare, la validità del documento informatico per le copie e/o estratti di documenti informatici è consentita mediante uno dei due metodi:

- raffronto dei documenti;
- certificazione di processo.

I requisiti tecnici per la certificazione di processo sono individuati nell'allegato 3 “Certificazione di Processo”.

Il ricorso ad uno dei due metodi sopracitati assicura la conformità del contenuto della copia o dell'estratto informatico alle informazioni del documento informatico di origine.

Fatto salvo quanto previsto dall'art. 23bis comma 2 del CAD<sup>10</sup> nel caso in cui non vi è l'attestazione di un pubblico ufficiale, la conformità della copia o dell'estratto informatico ad un documento informatico è garantita mediante l'apposizione della firma digitale o firma elettronica qualificata o firma elettronica avanzata, nonché del sigillo elettronico qualificato e avanzato da parte di chi effettua il raffronto.

Laddove richiesta dalla natura dell'attività, l'attestazione di conformità delle copie o estratti informatici di documenti informatici può essere inserita nel documento informatico contenente la copia o l'estratto. L'attestazione di conformità delle copie o dell'estratto informatico di uno o più documenti informatici può essere altresì prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia o estratto informatico. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del notaio o del pubblico ufficiale a ciò autorizzato.

---

<sup>10</sup> Le copie e gli estratti informatici del documento informatico, se prodotti in conformità alle vigenti regole tecniche di cui all'articolo 71, hanno la stessa efficacia probatoria dell'originale da cui sono tratte se la loro conformità all'originale, in tutti le sue componenti, è attestata da un pubblico ufficiale a ciò autorizzato o se la conformità non è espressamente disconosciuta. Resta fermo, ove previsto, l'obbligo di conservazione dell'originale informatico.

## 2.4. Il documento amministrativo informatico

### 2.4.1. Formazione del documento amministrativo informatico

Al documento amministrativo informatico si applicano le stesse regole valide per il documento informatico, salvo quanto specificato nel presente paragrafo.

La Pubblica Amministrazione forma gli originali dei propri documenti attraverso gli strumenti informatici riportati nel manuale di gestione documentale oppure acquisendo le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5 -bis<sup>11</sup>, 40 -bis<sup>12</sup> e 65<sup>13</sup> del CAD.

Il documento amministrativo informatico è identificato e trattato nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Le istanze, le dichiarazioni e le comunicazioni di cui agli articoli 5-bis, 40-bis e 65 del CAD sono identificate e trattate come i documenti amministrativi informatici. Se soggette a norme specifiche che prevedono la sola tenuta di estratti per riassunto sono memorizzate in specifici archivi informatici dettagliatamente descritti nel manuale di gestione documentale.

Il documento amministrativo informatico assume le caratteristiche di immutabilità e di integrità, oltre che con le modalità di cui al paragrafo 2.1.1, anche con la sua registrazione nel registro di protocollo, negli ulteriori registri, nei repertori, negli albi, negli elenchi, negli archivi o nelle raccolte di dati contenute nel sistema di gestione informatica dei documenti con le modalità descritte nel manuale di gestione documentale.

Al documento amministrativo informatico viene associato l'insieme dei metadati previsti per la registrazione di protocollo ai sensi dell'art 53 del TUDA<sup>14</sup>, nonché i metadati relativi alla

---

<sup>11</sup> L'art. 5-bis, comma 1, del CAD prevede che "La presentazione di istanze, dichiarazioni, dati e lo scambio di informazioni e documenti, anche a fini statistici, tra le imprese e le amministrazioni pubbliche avviene esclusivamente utilizzando le tecnologie dell'informazione e della comunicazione. Con le medesime modalità le amministrazioni pubbliche adottano e comunicano atti e provvedimenti amministrativi nei confronti delle imprese".

<sup>12</sup> L'art. 40-bis del CAD prevede che "Formano comunque oggetto di registrazione di protocollo ai sensi dell'articolo 53 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, le comunicazioni che provengono da o sono inviate a domicili digitali eletti ai sensi di quanto previsto all'articolo 3-bis, nonché le istanze e le dichiarazioni di cui all'articolo 65 in conformità alle regole tecniche di cui all'articolo 71".

<sup>13</sup> L'art. 65 del CAD disciplina "Le istanze e le dichiarazioni presentate per via telematica alle pubbliche amministrazioni e ai gestori dei servizi pubblici".

<sup>14</sup> L'art. 53, comma 1, del TUDA prevede che "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni: a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile; b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile; c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile; d) oggetto del documento, registrato in forma non modificabile; e) data e protocollo del documento ricevuto, se disponibili; f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

classificazione, ai sensi dell'articolo 56 del TUDA<sup>15</sup>, e ai tempi di conservazione, in coerenza con il piano di conservazione, e quelli relativi alla relazione con l'aggregazione documentale informatica d'appartenenza.

Al documento amministrativo informatico sono associati ulteriori metadati rilevanti ai fini amministrativi o per finalità gestionali o conservative, definiti, per ogni tipologia di documento, nell'ambito del contesto a cui esso si riferisce, secondo quanto previsto dall'Allegato 5 alle presenti Linee guida.

Sarà cura dell'Amministrazione individuare ulteriori metadati (ad es. metadati relativi al Registro giornaliero di protocollo ecc.) da associare a particolari tipologie di documenti amministrativi informatici. A tal proposito si ricorda che nel manuale di gestione devono essere riportati i metadati definiti per ogni tipologia di documento.

Sono inclusi i documenti soggetti a registrazione particolare, come identificati nel manuale di gestione documentale, che comunque devono contenere al proprio interno o avere associati l'insieme minimo dei metadati previsti per il documento amministrativo informatico.

In applicazione dell'art.23-ter comma 5-bis del CAD<sup>16</sup>, i documenti amministrativi informatici devono essere accessibili secondo le regole previste dall'art. 11 della legge n. 4/2004.

## 2.5. Copie su supporto informatico di documenti amministrativi analogici

Alle copie su supporto informatico di documenti amministrativi analogici si applicano le disposizioni di cui al paragrafo 2.2.

L'attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

---

<sup>15</sup> L'art. 56 del TUDA prevede che "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

<sup>16</sup> L'art. 23-ter comma 5-bis prevede che "I documenti di cui al presente articolo devono essere fruibili indipendentemente dalla condizione di disabilità personale, applicando i criteri di accessibilità definiti dai requisiti tecnici di cui all'articolo 11 della legge 9 gennaio 2004, n. 4".

## CAPITOLO 3 Gestione documentale

---

### 3.1. Registrazione informatica dei documenti

#### 3.1.1. Ambito di applicazione

Il presente capitolo individua le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo, di cui agli articoli da 50 a 57 e da 61 a 66 del TUDA<sup>17</sup>.

Il presente capitolo stabilisce inoltre le regole tecniche, i criteri e le specifiche delle informazioni previste nelle operazioni di registrazione e segnatura di protocollo di cui agli articoli 40-bis, 41 e 47 del CAD<sup>18</sup>.

#### 3.1.2. Adeguamento organizzativo e funzionale

Le Pubbliche Amministrazioni, nell'ambito del proprio ordinamento, provvedono a:

- A. individuare le aree organizzative omogenee (di seguito AOO) e i relativi uffici di riferimento ai sensi dell'art. 50, comma 4, del TUDA<sup>19</sup>;
- B. nominare, in ciascuna delle AOO, il responsabile della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;

---

<sup>17</sup> Gli articoli da 50 a 57 e da 61 a 66 del TUDA sono compresi nel Capo IV "Sistemi di gestione informatica del documento".

<sup>18</sup> Gli articoli 40-bis, 41 e 47 del CAD disciplinano, rispettivamente, in materia di protocollo informatico, procedimento e fascicolo informatico, trasmissione dei documenti tra le pubbliche amministrazioni.

<sup>19</sup> L'art. 50, comma 4, del TUDA prevede che "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

- C. per le amministrazioni con più AOO, nominare il coordinatore della gestione documentale e un suo vicario, in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
- D. adottare per ogni AOO il manuale di gestione documentale, su proposta del responsabile della gestione documentale oppure, ove nominato, dal coordinatore della gestione documentale.

Secondo quanto previsto dal CAD e dalle Linee guida AGID del 15 aprile 2019<sup>20</sup>, l'Indice dei domicili digitali delle Pubbliche Amministrazioni e dei gestori di pubblici servizi, di seguito indicato con l'acronimo IPA, include, tra gli indirizzi telematici degli Enti ivi iscritti, il domicilio digitale da cui provengono, o sono inviate, comunicazioni, istanze, dichiarazioni e notifiche che formano oggetto di registrazione di protocollo.

### 3.1.3. Registrazione di protocollo e altre forme di registrazione

La registrazione informatica dei documenti è rappresentata dall'insieme di dati in forma elettronica allegati o connessi al documento informatico al fine dell'identificazione univoca di tutti i documenti prodotti e acquisiti. Per la Pubblica Amministrazione vale quanto disposto ai sensi dell'articolo 53 comma 5 del TUDA<sup>21</sup>.

Al termine della registrazione, il documento è identificato da un insieme di dati in forma elettronica che può includere sin da questa fase la classificazione e si integra con il piano di organizzazione delle aggregazioni documentali, definito dal Responsabile della gestione documentale di cui al paragrafo 3.4, nell'ambito del manuale di gestione.

La Pubblica Amministrazione, al fine di dare attuazione alle disposizioni introdotte dal CAD stesso in materia di sistema di gestione informatica dei documenti realizza le funzionalità di gestione dell'archivio corrente, dell'archivio di deposito, dei flussi documentali, automatizzazione dei procedimenti amministrativi sulla base dei propri obiettivi di miglioramento dei servizi e di incremento dell'efficienza operativa, tenuto conto del rapporto costi e benefici, nel rispetto degli articoli 53 e 55 del TUDA<sup>22</sup> e dei requisiti del sistema di gestione informatica dei documenti e dei flussi documentali" definiti negli articoli 52, 65 e 67 del TUDA<sup>23</sup>, applicando ove possibile i requisiti fissati per la registrazione di protocollo anche alle altre forme di registrazione informatica dei documenti, fatto salvo quanto disposto per esse da eventuali norme vigenti".

---

<sup>20</sup> Linee Guida dell'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi.

<sup>21</sup> L'art. 53, comma 5, del TUDA prevede che "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

<sup>22</sup> Gli articoli 53 e 55 del TUDA disciplinano, rispettivamente, in materia di registrazioni di protocollo e segnatura di protocollo.

<sup>23</sup> Gli articoli 52, 65 e 67 del TUDA disciplinano, rispettivamente, in materia di sistema di gestione informatica dei documenti, requisiti del sistema per la gestione dei flussi documentali e trasferimento dei documenti all'archivio di deposito.

### 3.1.4. Formato della registrazione e della segnatura di protocollo

La registrazione di protocollo è l'insieme dei metadati che il registro di protocollo deve memorizzare, per tutti i documenti ricevuti o spediti dalla Pubblica Amministrazione e per tutti i documenti informatici che non rientrano tra le tipologie specificate dall'art. 53, comma 5 del TUDA<sup>24</sup> e che non sono oggetto di registrazione particolare da parte dell'amministrazione, al fine di garantirne l'identificazione univoca e certa. In merito, l'articolo 53, comma 1, del TUDA indica le informazioni che caratterizzano il registro di protocollo<sup>25</sup>, a cui si aggiungono le informazioni inerenti l'assegnazione interna all'amministrazione e la eventuale classificazione.

La segnatura di protocollo è l'associazione ai documenti amministrativi informatici in forma permanente e non modificabile di informazioni riguardanti i documenti stessi, in ingresso e in uscita al sistema di protocollo, utile alla sua identificazione univoca e certa.

In merito l'articolo 55, comma 1, del TUDA individua le informazioni che caratterizzano la segnatura di protocollo<sup>26</sup>.

Le operazioni di segnatura e registrazione di protocollo sono effettuate contemporaneamente.

Gli "standard, le modalità di trasmissione, il formato e le definizioni dei tipi di informazioni minime ed accessorie comunemente scambiate tra le Pubbliche Amministrazioni e associate ai documenti protocollati" sono definiti nell'allegato 6 "Comunicazione tra AOO di Documenti Amministrativi Protocollati".

---

<sup>24</sup> L'art. 53, comma 5 del TUSA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

<sup>25</sup> L'art. 53, comma 1, del TUDA prevede che: "La registrazione di protocollo per ogni documento ricevuto o spedito dalle pubbliche amministrazioni è effettuata mediante la memorizzazione delle seguenti informazioni:

- a) numero di protocollo del documento generato automaticamente dal sistema e registrato in forma non modificabile;
- b) data di registrazione di protocollo assegnata automaticamente dal sistema e registrata in forma non modificabile;
- c) mittente per i documenti ricevuti o, in alternativa, il destinatario o i destinatari per i documenti spediti, registrati in forma non modificabile;
- d) oggetto del documento, registrato in forma non modificabile;
- e) data e protocollo del documento ricevuto, se disponibili;
- f) l'impronta del documento informatico, se trasmesso per via telematica, costituita dalla sequenza di simboli binari in grado di identificarne univocamente il contenuto, registrata in forma non modificabile".

<sup>26</sup> L'art. 55, comma 1, del TUDA prevede che: "La segnatura di protocollo è l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, delle informazioni riguardanti il documento stesso. Essa consente di individuare ciascun documento in modo inequivocabile. Le informazioni minime previste sono:

- a) il progressivo di protocollo, secondo il formato disciplinato all'articolo 57;
- b) la data di protocollo;
- c) l'identificazione in forma sintetica dell'amministrazione o dell'area organizzativa individuata ai sensi dell'articolo 50, comma 4".

### 3.1.5. Annullamento delle informazioni registrate in forma immutabile

Il protocollo informatico deve assicurare il tracciamento e la storicizzazione di ogni operazione, comprese le operazioni di annullamento, e la loro attribuzione all'operatore. Il sistema di protocollo informatico assicura che:

- le informazioni relative all'oggetto, al mittente e al destinatario di una registrazione di protocollo, non possano essere modificate, ma solo annullate con la procedura prevista dall'art. 54 del TUDA<sup>27</sup>;
- le uniche informazioni modificabili di una registrazione di protocollo siano l'assegnazione interna all'amministrazione e la classificazione;
- le azioni di annullamento provvedano alla storicizzazione dei dati annullati attraverso le informazioni oggetto della stessa;
- per ognuno di questi eventi, anche nel caso di modifica di una delle informazioni di cui al punto precedente, il sistema storicizzi tutte le informazioni annullate e modificate rendendole entrambe visibili e comparabili, nel rispetto di quanto previsto dall'art. 54, comma 2 del TUDA.

### 3.1.6. Requisiti minimi di sicurezza dei sistemi di protocollo informatico

Il sistema di protocollo informatico, eventualmente integrato in un sistema di gestione informatica dei documenti, assicura il rispetto delle disposizioni in materia di sicurezza predisposte dall'AgID di cui al paragrafo 3.9 e dagli altri organismi preposti e delle disposizioni in materia di protezione dei dati personali.

In particolare, il sistema di protocollo informatico deve garantire:

- a) l'univoca identificazione ed autenticazione degli utenti;
- b) la garanzia di accesso alle risorse esclusivamente agli utenti abilitati e/o a gruppi di utenti secondo la definizione di appositi profili;
- c) il tracciamento permanente di qualsiasi evento di modifica delle informazioni trattate e l'individuazione del suo autore.

Il registro giornaliero di protocollo è trasmesso entro la giornata lavorativa successiva al sistema di conservazione, garantendone l'immutabilità del contenuto.

---

<sup>27</sup> L'art. 54, comma 2, del TUDA prevede che: "La procedura per indicare l'annullamento riporta, secondo i casi, una dicitura o un segno in posizione sempre visibile e tale, comunque, da consentire la lettura di tutte le informazioni originarie unitamente alla data, all'identificativo dell'operatore ed agli estremi del provvedimento d'autorizzazione".

## 3.2. Classificazione dei documenti informatici

La classificazione ha il fine di organizzare logicamente tutti i documenti amministrativi informatici prodotti o ricevuti da un ente nell'esercizio delle sue funzioni. L'attività di classificazione si avvale del piano di classificazione che mappa, su più livelli gerarchici, tutte le funzioni dell'ente.

La classificazione è un'attività obbligatoria nel sistema di gestione informatica dei documenti dell'AOO e si applica a tutti i documenti prodotti e acquisiti dalla stessa AOO sottoposti o meno alla registrazione di protocollo, ai sensi degli articoli 56<sup>28</sup> e 64, comma 4<sup>29</sup>, del TUDA. Le informazioni relative alla classificazione nei casi dei documenti amministrativi informatici costituiscono parte integrante dei metadati previsti per la formazione dei documenti medesimi.

Il Responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, verifica periodicamente la rispondenza del piano di classificazione ai procedimenti amministrativi e agli affari in essere e procede al suo aggiornamento.

Nel sistema di gestione informatica dei documenti dell'AOO l'attività di classificazione guida la formazione dell'archivio mediante il piano di organizzazione delle aggregazioni documentali.

## 3.3. Aggregazioni documentali informatiche

La Pubblica Amministrazione documenta la propria attività tramite funzioni del sistema di gestione informatica dei documenti finalizzate alla produzione, alla gestione e all'uso delle aggregazioni documentali informatiche, corredate da opportuni metadati, così come definiti nell'allegato 5 "Metadati" alle presenti Linee guida.

### 3.3.1. Fascicoli informatici

Nelle Pubbliche Amministrazioni l'AOO gestisce i flussi documentali mediante fascicoli informatici predisposti secondo il piano di classificazione e relativo piano di organizzazione delle aggregazioni documentali ai sensi dell'art. 64 del TUDA, anche con riferimento a fascicoli non afferenti a procedimenti.

---

<sup>28</sup> L'articolo 56 del TUDA prevede che: "Le operazioni di registrazione indicate all'articolo 53 e le operazioni di segnatura di protocollo di cui all'articolo 55 nonché le operazioni di classificazione costituiscono operazioni necessarie e sufficienti per la tenuta del sistema di gestione informatica dei documenti da parte delle pubbliche amministrazioni".

<sup>29</sup> L'articolo 64, comma 4, del TUDA prevede che: "Le amministrazioni determinano autonomamente e in modo coordinato per le aree organizzative omogenee, le modalità di attribuzione dei documenti ai fascicoli che li contengono e ai relativi procedimenti, definendo adeguati piani di classificazione d'archivio per tutti i documenti, compresi quelli non soggetti a registrazione di protocollo".

La produzione, il mantenimento e l'uso dei fascicoli informatici sono conformi a quanto stabilito dall'art. 65<sup>30</sup> del TUDA e dell'art 41<sup>31</sup> del CAD.

### 3.3.2. Altre aggregazioni documentali informatiche

All'interno del sistema di gestione informatica dei documenti la Pubblica Amministrazione forma, gestisce e utilizza tipologie di aggregazioni documentali informatiche diverse dai fascicoli: serie che aggregano documenti e serie che aggregano fascicoli.

Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.

Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.

I fascicoli appartenenti a serie diverse possono essere collegati tra loro.

---

<sup>30</sup>L'articolo 65 del TUDA prevede che: "Oltre a possedere i requisiti indicati all'articolo 52, il sistema per la gestione dei flussi documentali deve:

- a) fornire informazioni sul legame esistente tra ciascun documento registrato, il fascicolo ed il singolo procedimento cui esso è associato;
- b) consentire il rapido reperimento delle informazioni riguardanti i fascicoli, il procedimento ed il relativo responsabile, nonché la gestione delle fasi del procedimento;
- c) fornire informazioni statistiche sull'attività dell'ufficio;
- d) consentire lo scambio di informazioni con sistemi per la gestione dei flussi documentali di altre amministrazioni al fine di determinare lo stato e l'iter dei procedimenti complessi".

<sup>31</sup> L'art. 41, comma 2-ter, del CAD prevede che: "Il fascicolo informatico reca l'indicazione:

- a) dell'amministrazione titolare del procedimento, che cura la costituzione e la gestione del fascicolo medesimo;
  2. delle altre amministrazioni partecipanti;
  3. del responsabile del procedimento;
  4. dell'oggetto del procedimento;
- e) dell'elenco dei documenti contenuti, salvo quanto disposto dal comma 2-quater;
- e-bis) dell'identificativo del fascicolo medesimo apposto con modalità idonee a consentirne l'indicizzazione e la ricerca attraverso il sistema di cui all'articolo 40-ter nel rispetto delle Linee guida".

Il successivo comma 2-quater prevede che: "Il fascicolo informatico può contenere aree a cui hanno accesso solo l'amministrazione titolare e gli altri soggetti da essa individuati; esso è formato in modo da garantire la corretta collocazione, la facile reperibilità e la collegabilità, in relazione al contenuto ed alle finalità, dei singoli documenti. Il fascicolo informatico è inoltre costituito in modo da garantire l'esercizio in via telematica dei diritti previsti dalla citata legge n. 241 del 1990 e dall'articolo 5, comma 2, del decreto legislativo 14 marzo 2013, n. 33, nonché l'immediata conoscibilità anche attraverso i servizi di cui agli articoli 40-ter e 64-bis, sempre per via telematica, dello stato di avanzamento del procedimento, del nominativo e del recapito elettronico del responsabile del procedimento. AgID detta, ai sensi dell'articolo 71, Linee guida idonee a garantire l'interoperabilità tra i sistemi di gestione dei fascicoli dei procedimenti e i servizi di cui agli articoli 40-ter e 64-bis".

Il sistema di gestione informatica dei documenti dell'AOO, individuata ai sensi dell'art. 50, comma 4, del TUDA<sup>32</sup>, permette la gestione, formazione, utilizzo di serie secondo il piano di classificazione o di fascicolatura, sulla base delle indicazioni contenute nel manuale di gestione.

### 3.3.3. Registri e repertori informatici

Il registro di protocollo e i registri dei documenti soggetti a registrazione particolare, i repertori, gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti realizzati dalle amministrazioni su supporto informatico in luogo dei registri cartacei sono formati attraverso la generazione o il raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti che operano fra loro, secondo una struttura logica predeterminata e memorizzata in forma statica.

## 3.4. Compiti del responsabile della gestione documentale

Le Pubbliche Amministrazioni definiscono le attribuzioni del responsabile della gestione documentale ovvero, ove nominato, del coordinatore della gestione documentale.

Il responsabile della gestione documentale è preposto al servizio di cui all'articolo 61 del TUDA<sup>33</sup> e, d'intesa con il responsabile della conservazione, il responsabile per la transizione digitale di cui

---

<sup>32</sup> L'art. 50, comma 4, del TUDA, prevede che: "Ciascuna amministrazione individua, nell'ambito del proprio ordinamento, gli uffici da considerare ai fini della gestione unica o coordinata dei documenti per grandi aree organizzative omogenee, assicurando criteri uniformi di classificazione e archiviazione, nonché di comunicazione interna tra le aree stesse".

<sup>33</sup> L'articolo 61 del TUDA prevede che "1. Ciascuna amministrazione istituisce un servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi in ciascuna delle grandi aree organizzative omogenee individuate ai sensi dell'articolo 50. Il servizio è posto alle dirette dipendenze della stessa area organizzativa omogenea.

2. Al servizio è preposto un dirigente ovvero un funzionario, comunque in possesso di idonei requisiti professionali o di professionalità tecnico archivistica acquisita a seguito di processi di formazione definiti secondo le procedure prescritte dalla disciplina vigente. 3. Il servizio svolge i seguenti compiti:

- a) attribuisce il livello di autorizzazione per l'accesso alle funzioni della procedura, distinguendo tra abilitazioni alla consultazione e abilitazioni all'inserimento e alla modifica delle informazioni;
- b) garantisce che le operazioni di registrazione e di segnatura di protocollo si volgano nel rispetto delle disposizioni del presente testo unico;
- c) garantisce la corretta produzione e la conservazione del registro giornaliero di protocollo di cui all'articolo 53;
- d) cura che le funzionalità del sistema in caso di guasti o anomalie siano ripristinate entro ventiquattro ore dal blocco delle attività e, comunque, nel più breve tempo possibile;
- e) conserva le copie di cui agli articoli 62 e 63, in luoghi sicuri differenti;
- f) garantisce il buon funzionamento degli strumenti e dell'organizzazione delle attività di registrazione di protocollo, di gestione dei documenti e dei flussi documentali, incluse le funzionalità di accesso di cui agli articoli 59 e 60 e le attività di gestione degli archivi di cui agli articoli 67, 68 e 69;
- g) autorizza le operazioni di annullamento di cui all'articolo 54;
- h) vigila sull'osservanza delle disposizioni del presente testo unico da parte del personale autorizzato e degli incaricati.

all'art.17 del CAD<sup>34</sup> e acquisito il parere del responsabile della protezione dei dati personali, di cui agli artt. 37 “Designazione del responsabile della protezione dei dati” e 39 “Compiti del responsabile della protezione dei dati” del Regolamento UE 679/2016, predisporre:

- il manuale di gestione documentale relativo alla formazione, alla gestione, alla trasmissione, all'interscambio, all'accesso ai documenti informatici nel rispetto della normativa in materia di trattamenti dei dati personali ed in coerenza con quanto previsto nel manuale di conservazione;

Tale manuale conterrà inoltre, come parte integrante dello stesso, il piano per la sicurezza informatica, per la quota parte di competenza, nel rispetto delle:

- misure di sicurezza predisposte dall'AgID e dagli altri organismi preposti;
- delle disposizioni in materia di protezione dei dati personali in linea con l'analisi del rischio fatta;
- indicazioni in materia di continuità operativa dei sistemi informatici predisposti dall'AGID.

Per l'Amministrazione con più AOO il coordinatore della gestione, sentiti i responsabili della gestione documentale, assicura l'adozione di criteri uniformi per la gestione informatica dei documenti.

Il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, verifica l'avvenuta eliminazione dei protocolli di settore, dei protocolli multipli e, più in generale, dei protocolli diversi dal protocollo informatico previsto dal TUDA.

### 3.5. Manuale di gestione documentale

Il manuale di gestione documentale descrive il sistema di gestione informatica dei documenti e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.

Nel manuale di gestione documentale sono riportati, in particolare:

1. relativamente agli aspetti organizzativi:
  - a) le modalità di utilizzo degli strumenti informatici per la formazione dei documenti informatici e per lo scambio degli stessi all'interno ed all'esterno dell'AOO, applicando le modalità di trasmissione indicate nell'allegato 6 “Comunicazione tra AOO di Documenti Amministrativi Protocollati”;
  - b) l'indicazione delle unità organizzative responsabili (UOR) delle attività di registrazione di protocollo, di archiviazione dei documenti all'interno dell'AOO;
  - c) l'indicazione delle regole di assegnazione dei documenti ricevuti con la specifica dei criteri per l'ulteriore eventuale inoltro dei documenti verso aree organizzative omogenee della stessa amministrazione o verso altre amministrazioni;
  - d) i criteri e le modalità per il rilascio delle abilitazioni di accesso, interno ed esterno all'Amministrazione, al sistema di gestione informatica dei documenti;

---

<sup>34</sup> L'art. 17 del CAD prevede che: “...ciascuna pubblica amministrazione affida a un unico ufficio dirigenziale generale, fermo restando il numero complessivo di tali uffici, la transizione alla modalità operativa digitale”.

2. relativamente ai formati dei documenti:
  - a) l'individuazione dei formati utilizzati per la formazione del documento informatico, come introdotti nel paragrafo 3.6, tra quelli indicati nell'Allegato 2 "Formati di file e riversamento";
  - b) la descrizione di eventuali ulteriori formati utilizzati per la formazione di documenti in relazione a specifici contesti operativi che non sono individuati nell'Allegato 2 "Formati di file e riversamento";
  - c) le procedure per la valutazione periodica di interoperabilità dei formati e per le procedure di riversamento previste come indicato al paragrafo 3.7 e nell'Allegato 2 "Formati di file e riversamento";
3. relativamente al protocollo informatico e alle registrazioni particolari:
  - a) le modalità di registrazione delle informazioni annullate o modificate nell'ambito delle attività di registrazione;
  - b) la descrizione completa e puntuale delle modalità di utilizzo della componente «sistema di protocollo informatico» del sistema di gestione informatica dei documenti;
  - c) le modalità di utilizzo del registro di emergenza ai sensi dell'art. 63 del TUDA<sup>35</sup>, inclusa la funzione di recupero dei dati protocollati manualmente;
  - d) l'elenco dei documenti esclusi dalla registrazione di protocollo, per cui è prevista registrazione particolare ai sensi dell'art. 53, comma 5, del TUDA<sup>36</sup>;
  - e) determinazione dei metadati da associare ai documenti soggetti a registrazione particolare individuati, assicurando almeno quelli obbligatori previsti per il documento informatico dall'Allegato 5 alle presenti Linee Guida;
  - f) i registri particolari individuati per la gestione del trattamento delle registrazioni particolari informatiche anche associati ad aree organizzative omogenee definite dall'amministrazione sull'intera struttura organizzativa e gli albi, gli elenchi e ogni raccolta di dati concernente stati, qualità personali e fatti, riconosciuti da una norma;
4. relativamente alle azioni di classificazione e selezione:
  - a) il piano di classificazione adottato dall'Amministrazione, con l'indicazione delle modalità di aggiornamento, integrato con le informazioni relative ai tempi, ai criteri e alle regole di selezione e conservazione, con riferimento alle procedure di scarto;
5. relativamente alla formazione delle aggregazioni documentali
  - a) le modalità di formazione, gestione e archiviazione dei fascicoli informatici e delle aggregazioni

---

<sup>35</sup> L'art. 63 del TUDA prevede che: "1. Il responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi autorizza lo svolgimento anche manuale delle operazioni di registrazione di protocollo su uno o più registri di emergenza, ogni qualvolta per cause tecniche non sia possibile utilizzare la normale procedura informatica. Sul registro di emergenza sono riportate la causa, la data e l'ora di inizio dell'interruzione nonché la data e l'ora del ripristino della funzionalità del sistema. 2. Qualora l'impossibilità di utilizzare la procedura informatica si prolunghi oltre ventiquattro ore, per cause di eccezionale gravità, il responsabile per la tenuta del protocollo può autorizzare l'uso del registro di emergenza per periodi successivi di non più di una settimana. Sul registro di emergenza vanno riportati gli estremi del provvedimento di autorizzazione. 3. Per ogni giornata di registrazione di emergenza è riportato sul registro di emergenza il numero totale di operazioni registrate manualmente. 4. La sequenza numerica utilizzata su un registro di emergenza, anche a seguito di successive interruzioni, deve comunque garantire l'identificazione univoca dei documenti registrati nell'ambito del sistema documentario dell'area organizzativa omogenea. 5. Le informazioni relative ai documenti protocollati in emergenza sono inserite nel sistema informatico, utilizzando un'apposita funzione di recupero dei dati, senza ritardo al ripristino delle funzionalità del sistema. Durante la fase di ripristino, a ciascun documento registrato in emergenza viene attribuito un numero di protocollo del sistema informatico ordinario, che provvede a mantenere stabilmente la correlazione con il numero utilizzato in emergenza".

<sup>36</sup> L'art. 53, comma 5, del TUDA prevede che: "Sono oggetto di registrazione obbligatoria i documenti ricevuti e spediti dall'amministrazione e tutti i documenti informatici. Ne sono esclusi le gazzette ufficiali, i bollettini ufficiali e i notiziari della pubblica amministrazione, le note di ricezione delle circolari e altre disposizioni, i materiali statistici, gli atti preparatori interni, i giornali, le riviste, i libri, i materiali pubblicitari, gli inviti a manifestazioni e tutti i documenti già soggetti a registrazione particolare dell'amministrazione".

documentali informatiche con l'insieme minimo dei metadati ad essi associati;

6. relativamente ai flussi di lavorazione dei documenti in uso:
  - a) la descrizione dei flussi di lavorazione interni all'Amministrazione, anche mediante la rappresentazione formale dei processi attraverso l'uso dei linguaggi indicati da AgID, applicati per la gestione dei documenti ricevuti, inviati o ad uso interno;
7. relativamente alla organizzazione dei documenti informatici, dei fascicoli informatici e delle serie informatiche:
  - a) la definizione della struttura dell'archivio all'interno del sistema di gestione informatica dei documenti. L'archivio informatico - formato ai sensi del capo IV "Sistema di gestione informatica dei documenti" del DPR 445/2000 - deve essere progettato in modo da assicurare certezza e trasparenza all'attività giuridico amministrativa;
8. relativamente alle misure di sicurezza e protezione dei dati personali adottate:
  - a) le opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio anche in materia di protezione dei dati personali;
9. relativamente alla conservazione:
  - a) per le Pubbliche Amministrazioni il piano di conservazione è allegato al manuale di gestione documentale, con l'indicazione dei tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate;
  - b) per i soggetti diversi dalle Pubbliche Amministrazioni che sono sprovvisti di piano di conservazione, qualora si renda necessario redigere un Manuale di gestione per la complessità della struttura organizzativa e della documentazione prodotta, dovrebbero essere definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione dei documenti, ivi compresi i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate.

La Pubblica Amministrazione è tenuta a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di gestione documentale. La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013<sup>37</sup>.

### 3.6. Formati di file

I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti dall'Allegato 2 "Formati di file e riversamento". Nello scegliere i formati di file di cui sopra, da utilizzare per i propri documenti informatici, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD possono effettuare una valutazione di interoperabilità che tenga conto dei seguenti fattori: formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo.

---

<sup>37</sup> L'art. 9, comma 1, del d.lgs. 33/2013, prevede che: "Ai fini della piena accessibilità delle informazioni pubblicate, nella home page dei siti istituzionali è collocata un'apposita sezione denominata «Amministrazione trasparente», al cui interno sono contenuti i dati, le informazioni e i documenti pubblicati ai sensi della normativa vigente. Le amministrazioni non possono disporre filtri e altre soluzioni tecniche atte ad impedire ai motori di ricerca web di indicizzare ed effettuare ricerche all'interno della sezione «Amministrazione trasparente»".

Le pubbliche amministrazioni garantiscono sempre la gestione dei formati classificati nell'Allegato 2 "Formati di file e riversamento" come "generici", secondo la distinzione introdotta nell'Allegato 2 tra formati di file generici e specifici.

Qualora l'ordinamento giuridico preveda, per particolari categorie di documenti elettronici, degli obblighi relativamente all'uso di formati di file specifici ovvero di vincoli aggiuntivi su formati generici (quali, ad esempio, l'uso di particolari dialetti o specializzazioni per formati generici), le pubbliche amministrazioni, assolvendo tali obblighi, accettano i suddetti documenti elettronici solo se prodotti nei formati o con i vincoli aggiuntivi obbligatori.

È possibile utilizzare formati diversi da quelli elencati nell'Allegato 2 "Formati di file e riversamento", effettuando una valutazione di interoperabilità.

La valutazione di interoperabilità è effettuata in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento". La valutazione di interoperabilità, in quanto parte della gestione informatica dei documenti, viene effettuata periodicamente e, comunque, ogni anno, allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati.

Il manuale di gestione documentale contiene l'elenco dei formati utilizzati e la valutazione di interoperabilità.

### 3.7. Riversamento

A seguito della valutazione di interoperabilità, i soggetti di cui all'art. 2 comma 2 e comma 3 del CAD valutano l'esigenza o l'opportunità di effettuare o pianificare il riversamento dei file da un formato di file ad un altro formato, sempre tenendo in considerazione quanto previsto nel punto precedente. Il riversamento è effettuato in base alle indicazioni previste nell'Allegato 2 "Formati di file e riversamento".

### 3.8. Trasferimento al sistema di conservazione

I termini entro cui i documenti informatici e le aggregazioni documentali informatiche devono essere trasferiti in conservazione sono stabiliti in conformità alla normativa vigente e al piano di conservazione.

Coerentemente con quanto stabilito dal Codice dei beni culturali, il trasferimento a un sistema di conservazione di documenti e aggregazioni documentali informatiche, appartenenti ad archivi pubblici e privati dichiarati di interesse storico particolarmente importante, è assoggettato all'obbligo di cui all'art. 21 del Codice dei Beni Culturali<sup>38</sup> di comunicazione agli organi competenti in materia di tutela dei beni archivistici o, nel caso di affidamento esterno, alla loro autorizzazione.

---

<sup>38</sup> L'art. 21, comma 1, del Codice dei beni culturali prevede che: "Sono subordinati ad autorizzazione del Ministero: a) la rimozione o la demolizione, anche con successiva ricostituzione, dei beni culturali; b) lo spostamento, anche temporaneo, dei beni culturali mobili, salvo quanto previsto ai commi 2 e 3; c) lo smembramento di collezioni, serie e raccolte; d) lo scarto dei documenti degli archivi pubblici e degli archivi privati per i quali sia intervenuta la dichiarazione ai sensi

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di gestione informatica dei documenti nel rispetto della normativa sui beni culturali.

### 3.9. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della gestione documentale ovvero, ove nominato, il coordinatore della gestione documentale, in accordo con il responsabile della conservazione di cui al paragrafo 4.6, con il responsabile per la transizione digitale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016 (GDPR)<sup>39</sup>, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art. 28 "Responsabile del trattamento" del Regolamento.

Il piano conterrà altresì la descrizione della procedura da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016<sup>40</sup>, e sarà redatto nell'ambito del

---

dell'articolo 13, nonché lo scarto di materiale bibliografico delle biblioteche pubbliche, con l'eccezione prevista all'articolo 10, comma 2, lettera c), e delle biblioteche private per le quali sia intervenuta la dichiarazione ai sensi dell'articolo 13; e) il trasferimento ad altre persone giuridiche di complessi organici di documentazione di archivi pubblici, nonché di archivi privati per i quali sia intervenuta la dichiarazione ai sensi dell'articolo 13".

Il successivo comma 3 prevede che: "Lo spostamento degli archivi correnti dello Stato e degli enti ed istituti pubblici non è soggetto ad autorizzazione, ma comporta l'obbligo di comunicazione al Ministero per le finalità di cui all'articolo 18".

<sup>39</sup> L'art. 32 del Regolamento (UE) 2016/679 prevede che: "1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri".

<sup>40</sup> Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.

In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è eventualmente delegata la tenuta del sistema di gestione informatica dei documenti sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici possono adottare misure di sicurezza per garantire la tenuta del documento informatico. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento Reg. UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

## CAPITOLO 4 Conservazione

---

### 4.1. Sistema di conservazione

Nella Pubblica Amministrazione, il sistema di gestione informatica dei documenti trasferisce al sistema di conservazione, ai sensi dell'art. 44, comma 1-bis, del CAD<sup>41</sup>:

- a) i fascicoli informatici chiusi e le serie informatiche chiuse, trasferendoli dall'archivio corrente o dall'archivio di deposito;
- b) i fascicoli informatici e le serie non ancora chiuse trasferendo i documenti in essi contenuti sulla base di specifiche esigenze dell'ente, con particolare attenzione per i rischi di obsolescenza tecnologica.

Il sistema di conservazione assicura, dalla presa in carico fino all'eventuale scarto, la conservazione dei seguenti oggetti digitali in esso conservati, tramite l'adozione di regole, procedure e tecnologie, garantendone le caratteristiche di autenticità, integrità, affidabilità, leggibilità, reperibilità:

- a) i documenti informatici e i documenti amministrativi informatici con i metadati ad essi associati;
- b) le aggregazioni documentali informatiche (fascicoli e serie) con i metadati ad esse associati contenenti i riferimenti che univocamente identificano i singoli oggetti documentali che costituiscono le aggregazioni medesime, nel rispetto di quanto indicato per le Pubbliche Amministrazioni nell'articolo 67, comma 2, del DPR 445/2000<sup>42</sup> e art. 44, comma 1-bis, CAD.

Il sistema di conservazione garantisce l'accesso all'oggetto conservato per il periodo previsto dal piano di conservazione del titolare dell'oggetto della conservazione e dalla normativa vigente, o per un tempo superiore eventualmente concordato tra le parti, indipendentemente dall'evoluzione del contesto tecnologico.

Il sistema di conservazione è almeno logicamente distinto dal sistema di gestione informatica dei documenti.

Gli elenchi degli standard, delle specifiche tecniche e dei formati utilizzabili quali riferimento per il

---

<sup>41</sup> L'art. 44, comma 1-bis, del CAD prevede che: "Il sistema di gestione dei documenti informatici delle pubbliche amministrazioni è gestito da un responsabile che opera d'intesa con il dirigente dell'ufficio di cui all'articolo 17 del presente Codice, il responsabile del trattamento dei dati personali di cui all'articolo 29 del decreto legislativo 30 giugno 2003, n. 196, ove nominato, e con il responsabile del sistema della conservazione dei documenti informatici delle pubbliche amministrazioni, nella definizione e gestione delle attività di rispettiva competenza. Almeno una volta all'anno il responsabile della gestione dei documenti informatici provvede a trasmettere al sistema di conservazione i fascicoli e le serie documentarie anche relative a procedimenti non conclusi".

<sup>42</sup> L'art. 67, comma 2, del TUDA prevede che: "Il trasferimento deve essere attuato rispettando l'organizzazione che i fascicoli e le serie avevano nell'archivio corrente".

sistema di conservazione sono riportati negli allegati 2 “Formati di file e riversamento” e 4 “Standard e specifiche tecniche”.

### 4.2. Pacchetti informativi

Gli oggetti della conservazione sono trattati dal sistema di conservazione in pacchetti informativi che si distinguono in:

- a) pacchetti di versamento;
- b) pacchetti di archiviazione;
- c) pacchetti di distribuzione.

L'interoperabilità tra i sistemi di conservazione dei soggetti che svolgono attività di conservazione è garantita dall'applicazione delle specifiche tecniche del pacchetto di archiviazione definite dalla norma UNI 11386 - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

Il Titolare dell'oggetto della conservazione utilizza, già al momento della formazione, le modalità e i formati individuati nel manuale di gestione e nel manuale di conservazione in conformità con le presenti Linee Guida.

### 4.3. Modelli organizzativi della conservazione

Le Pubbliche Amministrazioni realizzano il processo di conservazione ai sensi dall'art. 34, comma 1-bis, del CAD<sup>43</sup>, fatte salve le competenze del Ministero per i beni e le attività culturali e del turismo ai sensi del decreto legislativo 22 gennaio 2004, n. 42.

Il processo di conservazione può essere pertanto svolto all'interno o all'esterno della struttura organizzativa dell'ente.

I requisiti del processo di conservazione, le responsabilità e i compiti del responsabile della conservazione e del responsabile del servizio di conservazione, e le loro modalità di interazione sono formalizzate nel manuale di conservazione del Titolare dell'oggetto della conservazione e nelle specifiche del contratto di servizio o dell'accordo. Tali modalità trovano riscontro anche nel manuale di conservazione del conservatore.

---

<sup>43</sup> L'art. 34, comma 1-bis, del CAD prevede che: “Le pubbliche amministrazioni possono procedere alla conservazione dei documenti informatici:

- a) all'interno della propria struttura organizzativa;
- b) affidandola, in modo totale o parziale, nel rispetto della disciplina vigente, ad altri soggetti, pubblici o privati che possiedono i requisiti di qualità, di sicurezza e organizzazione individuati, nel rispetto della disciplina europea, nelle Linee guida di cui all'art 71 relative alla formazione, gestione e conservazione dei documenti informatici nonché in un regolamento sui criteri per la fornitura dei servizi di conservazione dei documenti informatici emanato da AgID, avuto riguardo all'esigenza di assicurare la conformità dei documenti conservati agli originali nonché la qualità e la sicurezza del sistema di conservazione”.

Al fine di garantire l'autenticità, l'integrità, l'affidabilità, la leggibilità e la reperibilità dei documenti, i fornitori di servizi di conservazione devono possedere requisiti di elevato livello in termini di qualità e sicurezza in aderenza allo standard ISO/IEC 27001 (*Information security management systems - Requirements*) del sistema di gestione della sicurezza delle informazioni nel dominio logico, fisico e organizzativo nel quale viene realizzato il processo di conservazione e ISO 14721 OAIS (*Open Archival Information System - Sistema informativo aperto per l'archiviazione*), e alle raccomandazioni ETSI TS 101 533-1 v. 1.2.1, *Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni*.

### 4.4. Ruoli e responsabilità

I ruoli individuati nel processo di conservazione sono:

- a) titolare dell'oggetto della conservazione;
- b) produttore dei PdV;
- c) utente abilitato;
- d) responsabile della conservazione
- e) conservatore.

Nelle Pubbliche Amministrazioni, il ruolo di produttore del PdV è svolto da persona interna alla struttura organizzativa.

L'utente abilitato può richiedere al sistema di conservazione l'accesso ai documenti per acquisire le informazioni di interesse nei limiti previsti dalla legge e nelle modalità previste dal manuale di conservazione.

Nelle Pubbliche Amministrazioni il responsabile della gestione documentale o il coordinatore della gestione documentale, ove nominato, svolge il ruolo di produttore di PdV e assicura la trasmissione del pacchetto di versamento al sistema di conservazione, secondo le modalità operative definite nel manuale di conservazione.

Nel caso di affidamento a terzi, il produttore di PdV provvede a generare e trasmettere al sistema di conservazione i pacchetti di versamento nelle modalità e con i formati concordati con il conservatore e descritti nel manuale di conservazione del sistema di conservazione. Provvede inoltre a verificare il buon esito della operazione di trasferimento al sistema di conservazione tramite la presa visione del rapporto di versamento prodotto dal sistema di conservazione stesso.

### 4.5. Responsabile della conservazione

Il responsabile della conservazione opera secondo quanto previsto dall'art. 44, comma 1-quater, del CAD<sup>44</sup>.

---

<sup>44</sup> L'art. 44, comma 1-quater, del CAD prevede che: "Il responsabile della conservazione, che opera d'intesa con il responsabile del trattamento dei dati personali, con il responsabile della sicurezza e con il responsabile dei sistemi informativi, può affidare, ai sensi dell'articolo 34, comma 1-bis, lettera b), la conservazione dei documenti informatici ad

Nella Pubblica Amministrazione, il responsabile della conservazione:

- a) è un ruolo previsto dall'organigramma del Titolare dell'oggetto di conservazione;
- b) è un dirigente o un funzionario interno formalmente designato e in possesso di idonee competenze giuridiche, informatiche ed archivistiche;
- c) può essere svolto dal responsabile della gestione documentale o dal coordinatore della gestione documentale, ove nominato.

Per i soggetti diversi dalla Pubblica Amministrazione, il ruolo del responsabile della conservazione può essere svolto da un soggetto esterno all'organizzazione, in possesso di idonee competenze giuridiche, informatiche ed archivistiche, purché terzo rispetto al Conservatore al fine di garantire la funzione del Titolare dell'oggetto di conservazione rispetto al sistema di conservazione.

Il responsabile della conservazione definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.

Il responsabile della conservazione, sotto la propria responsabilità, può delegare lo svolgimento delle proprie attività o parte di esse a uno o più soggetti, che all'interno della struttura organizzativa, abbiano specifiche competenze ed esperienze. Tale delega, riportata nel manuale di conservazione, deve individuare le specifiche funzioni e competenze delegate.

In particolare, il responsabile della conservazione:

- a) definisce le politiche di conservazione e i requisiti funzionali del sistema di conservazione, in conformità alla normativa vigente e tenuto conto degli standard internazionali, in ragione delle specificità degli oggetti digitali da conservare (documenti informatici, aggregazioni informatiche, archivio informatico), della natura delle attività che il Titolare dell'oggetto di conservazione svolge e delle caratteristiche del sistema di gestione informatica dei documenti adottato;
- b) gestisce il processo di conservazione e ne garantisce nel tempo la conformità alla normativa vigente;
- c) genera e sottoscrive il rapporto di versamento, secondo le modalità previste dal manuale di conservazione;
- d) genera e sottoscrive il pacchetto di distribuzione con firma digitale o firma elettronica qualificata, nei casi previsti dal manuale di conservazione;
- e) effettua il monitoraggio della corretta funzionalità del sistema di conservazione;
- f) effettua la verifica periodica, con cadenza non superiore ai cinque anni, dell'integrità e della leggibilità dei documenti informatici e delle aggregazioni documentarie degli archivi;
- g) al fine di garantire la conservazione e l'accesso ai documenti informatici, adotta misure per rilevare tempestivamente l'eventuale degrado dei sistemi di memorizzazione e delle registrazioni e, ove necessario, per ripristinare la corretta funzionalità; adotta analoghe misure con riguardo all'obsolescenza dei formati;
- h) provvede alla duplicazione o copia dei documenti informatici in relazione all'evolversi del contesto tecnologico, secondo quanto previsto dal manuale di conservazione;
- i) predispose le misure necessarie per la sicurezza fisica e logica del sistema di conservazione come previsto dal par. 4.11;
- j) assicura la presenza di un pubblico ufficiale, nei casi in cui sia richiesto il suo intervento, garantendo allo stesso l'assistenza e le risorse necessarie per l'espletamento delle attività al medesimo attribuite;
- k) assicura agli organismi competenti previsti dalle norme vigenti l'assistenza e le risorse necessarie per l'espletamento delle attività di verifica e di vigilanza;
- l) provvede per le amministrazioni statali centrali e periferiche a versare i documenti

---

altri soggetti, pubblici o privati, che offrono idonee garanzie organizzative, e tecnologiche e di protezione dei dati personali. Il responsabile della conservazione della pubblica amministrazione, che opera d'intesa, oltre che con i responsabili di cui al comma 1-bis, anche con il responsabile della gestione documentale, effettua la conservazione dei documenti informatici secondo quanto previsto all'articolo 34, comma 1-bis”.

informatici, le aggregazioni informatiche e gli archivi informatici, nonché gli strumenti che ne garantiscono la consultazione, rispettivamente all'Archivio centrale dello Stato e agli archivi di Stato territorialmente competenti, secondo le tempistiche fissate dall'art. 41, comma 1, del Codice dei beni culturali<sup>45</sup>;

- m) predisporre il manuale di conservazione di cui al par. 4.7 e ne cura l'aggiornamento periodico in presenza di cambiamenti normativi, organizzativi, procedurali o tecnologici rilevanti.

Nel caso in cui il servizio di conservazione venga affidato ad un conservatore, le attività suddette o alcune di esse, ad esclusione della lettera m), potranno essere affidate al responsabile del servizio di conservazione, rimanendo in ogni caso inteso che la responsabilità giuridica generale sui processi di conservazione, non essendo delegabile, rimane in capo al responsabile della conservazione, chiamato altresì a svolgere le necessarie attività di verifica e controllo in ossequio alle norme vigenti sui servizi affidati in outsourcing dalle PA.

Si precisa che il nominativo ed i riferimenti del responsabile della conservazione devono essere indicati nelle specifiche del contratto o della convenzione di servizio con il Conservatore nel quale sono anche riportate le attività affidate al responsabile del servizio di conservazione.

### 4.6. Manuale di conservazione

Il manuale di conservazione è un documento informatico che deve illustrare dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture utilizzate, le misure di sicurezza adottate e ogni altra informazione utile alla gestione e alla verifica del funzionamento, nel tempo, del sistema di conservazione.

Il manuale di conservazione, inoltre, deve riportare:

- a) i dati dei soggetti che nel tempo hanno assunto la responsabilità del sistema di conservazione, descrivendo in modo puntuale, in caso di delega, i soggetti, le funzioni e gli ambiti oggetto della delega stessa;
- b) la struttura organizzativa comprensiva delle funzioni, delle responsabilità e degli obblighi dei diversi soggetti che intervengono nel processo di conservazione;
- c) la descrizione delle tipologie degli oggetti digitali sottoposti a conservazione, comprensiva dell'indicazione dei formati gestiti, dei metadati da associare alle diverse tipologie di oggetti e delle eventuali eccezioni;
- d) la descrizione delle modalità di presa in carico di uno o più pacchetti di versamento, comprensiva della predisposizione del rapporto di versamento;
- e) la descrizione del processo di conservazione e del trattamento dei pacchetti di archiviazione;
- f) la modalità di svolgimento del processo di esibizione e di esportazione dal sistema di conservazione con la produzione del pacchetto di distribuzione;
- g) la descrizione del sistema di conservazione, comprensivo di tutte le componenti tecnologiche, fisiche e logiche, opportunamente documentate e delle procedure di gestione

---

<sup>45</sup> L'art. 41, comma 1, del Codice dei beni culturali prevede che: "Gli organi giudiziari e amministrativi dello Stato versano all'archivio centrale dello Stato e agli archivi di Stato i documenti relativi agli affari esauriti da oltre trent'anni, unitamente agli strumenti che ne garantiscono la consultazione. Le liste di leva e di estrazione sono versate settant'anni dopo l'anno di nascita della classe cui si riferiscono. Gli archivi notarili versano gli atti notarili ricevuti dai notai che cessarono l'esercizio professionale anteriormente all'ultimo centennio".

- e di evoluzione delle medesime;
- h) la descrizione delle procedure di monitoraggio della funzionalità del sistema di conservazione e delle verifiche sull'integrità degli archivi con l'evidenza delle soluzioni adottate in caso di anomalie;
- i) la descrizione delle procedure per la produzione di duplicati o copie;
- j) i tempi entro i quali le diverse tipologie di oggetti digitali devono essere trasferite in conservazione ed eventualmente scartate, qualora, nel caso delle Pubbliche Amministrazioni, non siano già indicati nel piano di conservazione allegato al manuale di gestione documentale;
- k) le modalità con cui viene richiesta la presenza di un pubblico ufficiale, indicando anche quali sono i casi per i quali è previsto il suo intervento;
- l) le normative in vigore nei luoghi dove sono conservati gli oggetti digitali.

Le Pubbliche Amministrazioni sono tenute a redigere, adottare con provvedimento formale e pubblicare sul proprio sito istituzionale il Manuale di conservazione.

La pubblicazione è realizzata in una parte chiaramente identificabile dell'area "Amministrazione trasparente" prevista dall'art. 9 del d.lgs. 33/2013.

In caso di affidamento del servizio di conservazione ad un conservatore esterno, le Pubbliche Amministrazioni possono descrivere nel proprio manuale anche le attività del processo di conservazione affidate al conservatore, in conformità con il contenuto del manuale di conservazione predisposto da quest'ultimo, o rinviare, per le parti di competenza, al manuale del conservatore esterno.

Resta fermo l'obbligo in carico alla Pubblica Amministrazione di individuare e pubblicare i tempi di versamento, le tipologie documentali trattate, i metadati, le modalità di trasmissione dei PdV e le tempistiche di selezione e scarto dei propri documenti informatici.

Resta ferma inoltre la competenza del Ministero dei beni e delle attività culturali e del Turismo in materia di tutela dei sistemi di conservazione sugli archivi pubblici e privati che rivestono interesse storico particolarmente importante, così come disciplinato dalla normativa sui beni culturali.

### 4.7. Processo di conservazione

Il trasferimento dell'oggetto di conservazione nel sistema di conservazione avviene generando un PdV nelle modalità e con il formato previsti dal manuale di conservazione di cui al paragrafo 4.6.

Il processo di conservazione prevede:

- a) l'acquisizione da parte del sistema di conservazione del PdV per la sua presa in carico;
- b) la verifica che il PdV e gli oggetti digitali contenuti siano coerenti con le modalità previste dal manuale di conservazione e con quanto indicato nell'allegato 2 "Formati di file e riversamento" relativo ai formati;
- c) il rifiuto del PdV, nel caso in cui le verifiche di cui alla lettera b) abbiano evidenziato delle anomalie. Il numero massimo di rifiuti è stabilito nell'ambito di un contratto o convenzione;
- d) la generazione, anche in modo automatico, del rapporto di versamento relativo ad uno o più pacchetti di versamento, univocamente identificato dal sistema di conservazione e contenente un riferimento temporale, specificato con riferimento al Tempo universale coordinato (UTC), e una o più impronte, calcolate sull'intero contenuto del pacchetto di versamento, secondo le modalità descritte nel manuale di conservazione;
- e) la sottoscrizione del rapporto di versamento con la firma digitale o firma elettronica

- qualificata o avanzata apposta dal responsabile della conservazione o dal responsabile del servizio di conservazione, ove prevista nel manuale di conservazione;
- f) la preparazione, la sottoscrizione con firma digitale o firma elettronica - qualificata o avanzata - del responsabile della conservazione o del responsabile del servizio di conservazione o con il sigillo elettronico - qualificato o avanzato – apposto dal conservatore esterno, nonché la gestione del pacchetto di archiviazione sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
  - g) ai fini dell'esibizione richiesta dall'utente la preparazione e la sottoscrizione con firma digitale o firma elettronica qualificata o avanzata del responsabile della conservazione o del responsabile del servizio di conservazione, oppure l'apposizione del sigillo elettronico qualificato o avanzato, secondo le modalità indicate nel manuale di conservazione, di pacchetti di distribuzione che possono contenere parte, uno o più pacchetti di archiviazione;
  - h) ai soli fini della interoperabilità tra sistemi di conservazione, la produzione di pacchetti di distribuzione coincidenti con i pacchetti di archiviazione o comunque contenenti pacchetti di archiviazione generati sulla base delle specifiche della struttura dati indicate dallo standard UNI 11386 e secondo le modalità riportate nel manuale di conservazione;
  - i) la produzione di duplicati informatici o di copie informatiche effettuati su richiesta degli utenti in conformità a quanto previsto dalle presenti linee guida;
  - j) la produzione di copie informatiche tramite attività di riversamento al fine di adeguare il formato alle esigenze conservative di leggibilità nel tempo in base alle indicazioni previste dall'allegato 2 “Formati di file e riversamento”;
  - k) l'eventuale scarto del pacchetto di archiviazione dal sistema di conservazione alla scadenza dei termini di conservazione previsti dalla norma o secondo quanto indicato dal piano di conservazione del Titolare dell'oggetto di conservazione e le procedure descritte nel successivo paragrafo 4.12;
  - l) nel caso degli archivi pubblici o privati, che rivestono interesse storico particolarmente importante, l'eventuale scarto del pacchetto di archiviazione avviene previa autorizzazione del MIC rilasciata al Titolare dell'oggetto della conservazione secondo quanto previsto dalla normativa vigente in materia e al successivo paragrafo 4.12.

Nel caso di affidamento a terzi del servizio di conservazione le modalità sono indicate nei manuali del Titolare dell'oggetto di conservazione e del conservatore e concordate tra le parti.

## 4.8. Infrastrutture

Fatto salvo quanto previsto dal Codice dei beni culturali, nel rispetto del principio di libera circolazione dei dati all'interno dell'Unione europea<sup>46</sup>, si sottolinea l'obbligo, in capo al fornitore del servizio di conservazione, di conservare e rendere disponibili le descrizioni del sistema di conservazione all'interno del territorio nazionale. I conservatori devono altresì garantire alle amministrazioni l'accesso elettronico effettivo e tempestivo ai dati conservati, indipendentemente dallo Stato membro nel cui territorio i dati sono conservati.

Le componenti tecnologiche hardware e software utilizzate dai sistemi di conservazione delle Pubbliche Amministrazioni e dei conservatori sono segregate logicamente. Qualora i servizi di conservazione siano erogati in modalità cloud, il servizio deve essere qualificato come previsto dalla Circolare Agid n. 3 del 9 aprile 2018 e, conseguentemente, essere presente nel “Catalogo dei servizi

---

<sup>46</sup> Reg. (UE) 2018/1807 all'articolo 4, paragrafo 1 recita: “Gli obblighi di localizzazione di dati sono vietati a meno che siano giustificati da motivi di sicurezza pubblica nel rispetto del principio di proporzionalità.”

Cloud per la PA qualificati” pubblicato sul sito di Agid.

I sistemi di conservazione devono essere realizzati nel rispetto del principio di integrità e riservatezza, nonché dei principi di protezione fin dalla progettazione e per impostazione predefinita, e dei conseguenti adempimenti previsti dagli artt. 25<sup>47</sup> e 32 del citato Regolamento UE 679/2016.

### 4.9. Modalità di esibizione

Fermi restando gli obblighi previsti in materia di esibizione dei documenti dalla normativa vigente, il sistema di conservazione permette ai soggetti autorizzati l'accesso diretto, anche da remoto, agli oggetti digitali conservati, attraverso la produzione di pacchetti di distribuzione secondo le modalità descritte nel manuale di conservazione, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio e modalità di accesso diverse, in funzione delle tipologie di dati personali trattati, nonché delle operazioni di trattamento consentite.

Nel caso di affidamento esterno del servizio di conservazione tali modalità sono concordate tra le parti e indicate nei rispettivi manuali.

### 4.10. Misure di sicurezza

Nell'attuazione delle presenti Linee Guida, le Pubbliche Amministrazioni sono tenute ad ottemperare alle misure minime di sicurezza ICT emanate dall'AgID con circolare del 18 aprile 2017, n. 2/2017. In tale ottica, il responsabile della conservazione, di concerto con il responsabile per la transizione digitale, con il responsabile della gestione documentale e acquisito il parere del responsabile della protezione dei dati personali, predispone il piano della sicurezza del sistema di gestione informatica dei documenti, prevedendo opportune misure tecniche e organizzative per garantire un livello di sicurezza adeguato al rischio in materia di protezione dei dati personali, ai sensi dell'art. 32 del Regolamento UE 679/2016<sup>48</sup>, anche in funzione delle tipologie di dati trattati, quali quelli riferibili alle categorie particolari di cui agli artt. 9-10 del Regolamento stesso.

---

<sup>47</sup> L'art. 25 del Regolamento “Protezione dei dati fin dalla progettazione e protezione per impostazione predefinita”

<sup>48</sup> L'art. 32 del Regolamento (UE) 2016/679 prevede che: “1. Tenendo conto dello stato dell'arte e dei costi di attuazione, nonché della natura, dell'oggetto, del contesto e delle finalità del trattamento, come anche del rischio di varia probabilità e gravità per i diritti e le libertà delle persone fisiche, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio, che comprendono, tra le altre, se del caso:

- a) la pseudonimizzazione e la cifratura dei dati personali;
- b) la capacità di assicurare su base permanente la riservatezza, l'integrità, la disponibilità e la resilienza dei sistemi e dei servizi di trattamento;
- c) la capacità di ripristinare tempestivamente la disponibilità e l'accesso dei dati personali in caso di incidente fisico o tecnico;
- d) una procedura per testare, verificare e valutare regolarmente l'efficacia delle misure tecniche e organizzative al fine di garantire la sicurezza del trattamento.

2. Nel valutare l'adeguato livello di sicurezza, si tiene conto in special modo dei rischi presentati dal trattamento che derivano in particolare dalla distruzione, dalla perdita, dalla modifica, dalla divulgazione non autorizzata o dall'accesso, in modo accidentale o illegale, a dati personali trasmessi, conservati o comunque trattati. 3. L'adesione a un codice di condotta approvato di cui all'articolo 40 o a un meccanismo di certificazione approvato di cui all'articolo 42 può essere

L'adozione delle predette misure è in capo al titolare o, in caso di trattamento effettuato per suo conto, al responsabile del trattamento, individuato sulla base dell'art.28 del Regolamento.

Il piano conterrà altresì la descrizione della procedura da adottarsi in caso di violazione dei dati personali ai sensi degli artt. 33-34 del Regolamento UE 679/2016<sup>49</sup>, e sarà redatto nell'ambito del piano generale della sicurezza, in coerenza con quanto previsto dal Piano Triennale per l'Informatica nella Pubblica Amministrazione vigente.

Le misure di sicurezza sono descritte nel manuale di conservazione di cui al par. 4.7.

Nel caso di affidamento esterno del servizio di conservazione le misure di sicurezza sono concordate tra le parti e indicate nei rispettivi manuali. In conformità all'art. 28 del Regolamento UE 679/2016, i soggetti esterni a cui è delegata la tenuta del sistema di conservazione sono individuati come Responsabili del trattamento dei dati e devono presentare garanzie sufficienti per mettere in atto misure tecniche e organizzative adeguate in modo tale che il trattamento soddisfi i requisiti del Regolamento e garantisca la tutela dei diritti dell'interessato.

I soggetti privati appartenenti ad organizzazioni che applicano particolari regole di settore per la sicurezza dei propri sistemi informatici adeguano il sistema di conservazione a tali regole. Le citate misure di sicurezza ICT emanate dall'AGID possono costituire, a tal fine, un modello di riferimento, fermo restando gli obblighi previsti dal citato Regolamento UE 679/2016.

I servizi devono sempre organizzati nel rispetto dei principi e dei requisiti previsti in materia di sicurezza dei dati e dei sistemi dagli artt.32 e 34 del Regolamento, avuto riguardo anche alla notifica delle violazioni dei dati personali di cui all'art.33 del Regolamento stesso.

### 4.11. Selezione e scarto dei documenti informatici

I documenti informatici e le aggregazioni documentali informatiche possono essere oggetto di selezione e scarto nel sistema di conservazione nel rispetto della normativa sui beni culturali.

Nel sistema di conservazione, la selezione e lo scarto dei pacchetti di archiviazione sono definiti dal Titolare dell'oggetto di conservazione e, nel caso delle Pubbliche Amministrazioni, secondo quanto indicato dal piano di conservazione. Nel caso di affidamento esterno del servizio di conservazione le modalità operative sono concordate dal Titolare dell'oggetto di conservazione e dal Conservatore.

Il responsabile della conservazione genera l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto e, dopo aver verificato il rispetto dei termini temporali stabiliti dal piano di conservazione, lo comunica al responsabile della gestione documentale o del coordinatore della gestione documentale, ove nominato. In caso di affidamento esterno del servizio di conservazione l'elenco dei pacchetti di archiviazione contenenti i documenti destinati allo scarto è generato dal responsabile del servizio di conservazione e trasmesso al responsabile della conservazione che a sua volta, verificato il rispetto dei termini temporali stabiliti dal piano di

---

utilizzata come elemento per dimostrare la conformità ai requisiti di cui al paragrafo 1 del presente articolo. 4. Il titolare del trattamento e il responsabile del trattamento fanno sì che chiunque agisca sotto la loro autorità e abbia accesso a dati personali non tratti tali dati se non è istruito in tal senso dal titolare del trattamento, salvo che lo richieda il diritto dell'Unione o degli Stati membri”.

<sup>49</sup> Gli artt. 33 e 34 del Regolamento (UE) 2016/679 prevedono, rispettivamente, la procedura di notifica di una violazione dei dati personali all'autorità di controllo e quella di comunicazione di una violazione dei dati personali all'interessato.

conservazione, lo comunica al responsabile della gestione documentale o al coordinatore della gestione documentale.

Nel caso degli archivi pubblici e degli archivi privati con il solo riferimento a quelli dichiarati di interesse storico particolarmente importante l'autorizzazione è rilasciata ai sensi della normativa vigente in materia di beni culturali.

Il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, procede alla distruzione dei pacchetti di archiviazione.

Nel caso di affidamento esterno del servizio di conservazione, il Titolare dell'oggetto di conservazione, una volta ricevuta l'autorizzazione, che può essere concessa anche solo su una parte dell'elenco proposto, provvede a trasmetterlo al conservatore affinché provveda alla distruzione dei pacchetti di archiviazione.

L'operazione di scarto viene tracciata sul sistema mediante la produzione delle informazioni essenziali sullo scarto, inclusi gli estremi della richiesta di nulla osta allo scarto e il conseguente provvedimento autorizzatorio.

Al termine delle operazioni di distruzione dal sistema di conservazione dei pacchetti di archiviazione scartati, il Titolare dell'oggetto di conservazione notifica l'esito della procedura di scarto agli organi preposti alla tutela come già indicato in precedenza. Analoga comunicazione è inviata al Ministero dell'interno in caso di eliminazione di pacchetti di archiviazione contenenti documenti e/o dati di carattere riservato.

Tale operazione avrà completa efficacia solo al momento del completo aggiornamento delle copie di sicurezza del sistema.

I documenti e le aggregazioni documentali informatiche sottoposti a scarto nel sistema di conservazione devono essere distrutti anche in tutti i sistemi gestiti dal Titolare dell'oggetto di conservazione.

## **Glossario dei termini e degli acronimi**

***Allegato 1 al documento “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.***

## Sommario

Indice.....	2
CAPITOLO 1 .....	4
Premessa .....	4
1.1    Scopo e campo di applicazione del documento .....	4
1.2    Glossario dei termini.....	4
1.3    Glossario degli Acronimi .....	14

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

---

# CAPITOLO 1

Premessa

## 1.3 Scopo e campo di applicazione del documento

Lo scopo del presente allegato è il seguente:

- esplicitare il significato dei termini maggiormente utilizzati nel documento *linea guida sulla formazione, gestione e conservazione dei documenti informatici*, che necessitano una spiegazione.

## 1.4 Glossario dei termini

TERMINE	DEFINIZIONE
<b>Accesso</b>	Operazione che consente di prendere visione dei documenti informatici.
<b>Affidabilità</b>	Caratteristica che, con riferimento a un sistema di gestione documentale o conservazione, esprime il livello di fiducia che l'utente ripone nel sistema stesso, mentre con riferimento al documento informatico esprime la credibilità e l'accuratezza della rappresentazione di atti e fatti in esso contenuta.
<b>Aggregazione documentale informatica</b>	Insieme di documenti informatici o insieme di fascicoli informatici riuniti per caratteristiche omogenee, in relazione alla natura e alla forma dei documenti o in relazione all'oggetto e alla materia o in relazione alle funzioni dell'ente.
<b>Archivio</b>	Complesso dei documenti prodotti o acquisiti da un soggetto pubblico o privato durante lo svolgimento della propria attività.
<b>Archivio informatico</b>	Archivio costituito da documenti informatici, organizzati in aggregazioni documentali informatiche.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Area Organizzativa Omogenea</b>	Un insieme di funzioni e di uffici individuati dall'ente al fine di gestire i documenti in modo unitario e coordinato, secondo quanto disposto dall'art. 50 comma 4 del D.P.R. 28 dicembre 2000, n. 445. Essa rappresenta il canale ufficiale per l'invio di istanze e l'avvio di procedimenti amministrativi.
<b>Attestazione di conformità delle copie per immagine su supporto informatico di un documento analogico</b>	Dichiarazione rilasciata da notaio o altro pubblico ufficiale a ciò autorizzato allegata o asseverata al documento informatico.
<b>Autenticità</b>	Caratteristica in virtù della quale un oggetto deve considerarsi come corrispondente a ciò che era nel momento originario della sua produzione. Pertanto un oggetto è autentico se nel contempo è integro e completo, non avendo subito nel corso del tempo o dello spazio alcuna modifica non autorizzata. L'autenticità è valutata sulla base di precise evidenze.
<b>Certificazione</b>	Attestazione di terza parte relativa alla conformità ai requisiti specificati di prodotti, processi, persone e sistemi.
<b>Classificazione</b>	Attività di organizzazione di tutti i documenti secondo uno schema costituito da un insieme di voci articolate in modo gerarchico e che individuano, in astratto, le funzioni, competenze, attività e/o materie del soggetto produttore.
<b>Cloud della PA</b>	Ambiente virtuale che consente alle Pubbliche Amministrazioni di erogare servizi digitali ai cittadini e alle imprese nel rispetto di requisiti minimi di sicurezza e affidabilità.
<b>Codec</b>	Algoritmo di codifica e decodifica che consente di generare flussi binari, eventualmente imbustarli in un file o in un <i>wrapper</i> (codifica), così come di estrarli da esso (decodifica).
<b>Conservatore</b>	Soggetto pubblico o privato che svolge attività di conservazione dei documenti informatici.
<b>Conservazione</b>	Insieme delle attività finalizzate a definire ed attuare le politiche complessive del sistema di conservazione e a governarne la gestione in relazione al modello organizzativo

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
	adottato, garantendo nel tempo le caratteristiche di autenticità, integrità, leggibilità, reperibilità dei documenti
<b>Convenzioni di denominazione del file</b>	Insieme di regole sintattiche che definisce il nome dei file all'interno di un filesystem o pacchetto.
<b>Coordinatore della Gestione Documentale</b>	Soggetto responsabile della definizione di criteri uniformi di classificazione ed archiviazione nonché di comunicazione interna tra le AOO ai sensi di quanto disposto dall'articolo 50 comma 4 del DPR 445/2000 nei casi di amministrazioni che abbiano istituito più AOO.
<b>Destinatario</b>	Soggetto o sistema al quale il documento informatico è indirizzato.
<b><i>Digest</i></b>	Vedi Impronta crittografica.
<b>Documento amministrativo informatico</b>	Ogni rappresentazione, grafica, fotocinematografica, elettromagnetica o di qualunque altra specie, del contenuto di atti, anche interni, formati dalle pubbliche amministrazioni, o, comunque, da queste ultime utilizzati ai fini dell'attività amministrativa
<b>Documento elettronico</b>	Qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva
<b>Documento informatico</b>	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
<b>Duplicato informatico</b>	Vedi art. 1, comma 1, lett) i quinquies del CAD.
<b><i>eSeal</i></b>	Vedi sigillo elettronico.
<b>Esibizione</b>	operazione che consente di visualizzare un documento conservato
<b><i>eSignature</i></b>	Vedi firma elettronica.
<b>Estratto di documento informatico</b>	Parte del documento tratto dal documento originale
<b>Estratto per riassunto di documento informatico</b>	Documento nel quale si attestano in maniera sintetica fatti, stati o qualità desunti da documenti informatici.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Estrazione statica dei dati</b>	Estrazione di informazioni utili da grandi quantità di dati (es. database, datawarehouse ecc...), attraverso metodi automatici o semi-automatici
<b>Evidenza informatica</b>	Sequenza finita di <i>bit</i> che può essere elaborata da una procedura informatica.
<b>Fascicolo informatico</b>	Aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.
<b>File</b>	Insieme di informazioni, dati o comandi logicamente correlati, raccolti sotto un unico nome e registrati, per mezzo di un programma di elaborazione o di scrittura, nella memoria di un computer.
<b>File container</b>	Vedi Formato contenitore.
<b>File wrapper</b>	Vedi Formato contenitore.
<b>File-manifesto</b>	File che contiene metadati riferiti ad un file o ad un pacchetto di file.
<b>Filesystem</b>	Sistema di gestione dei file, strutturato mediante una o più gerarchie ad albero, che determina le modalità di assegnazione dei nomi, memorizzazione e organizzazione all'interno di uno storage.
<b>Firma elettronica</b>	Vedi articolo 3 del Regolamento eIDAS.
<b>Firma elettronica avanzata</b>	Vedi articoli 3 e 26 del Regolamento eIDAS.
<b>Firma elettronica qualificata</b>	Vedi articolo 3 del Regolamento eIDAS.
<b>Flusso (binario)</b>	Sequenza di bit prodotta in un intervallo temporale finito e continuativo che ha un'origine precisa ma di cui potrebbe non essere predeterminato il suo istante di interruzione.
<b>Formato contenitore</b>	Formato di file progettato per consentire l'inclusione ("imbustamento" o <i>wrapping</i> ), in uno stesso file, di una o più

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
	evidenze informatiche soggette a differenti tipi di codifica e al quale possono essere associati specifici metadati.
<b>Formato del documento informatico</b>	Modalità di rappresentazione della sequenza di bit che costituiscono il documento informatico; comunemente è identificato attraverso l'estensione del file.
<b>Formato "deprecato"</b>	Formato in passato considerato ufficiale il cui uso è attualmente sconsigliato a favore di una versione più recente.
<b>Funzioni aggiuntive del protocollo informatico</b>	Nel sistema di protocollo informatico, componenti supplementari rispetto a quelle minime, necessarie alla gestione dei flussi documentali, alla conservazione dei documenti nonché alla accessibilità delle informazioni.
<b>Funzioni minime del protocollo informatico</b>	Componenti del sistema di protocollo informatico che rispettano i requisiti di operazioni ed informazioni minime di cui all'articolo 56 del D.P.R. 28 dicembre 2000, n. 445.
<b>Funzione di <i>hash</i> crittografica</b>	Funzione matematica che genera, a partire da una evidenza informatica, una impronta crittografica o <i>digest</i> (vedi) in modo tale che risulti computazionalmente difficile (di fatto impossibile), a partire da questa, ricostruire l'evidenza informatica originaria e generare impronte uguali a partire da evidenze informatiche differenti.
<b>Gestione Documentale</b>	Processo finalizzato al controllo efficiente e sistematico della produzione, ricezione, tenuta, uso, selezione e conservazione dei documenti.
<b><i>hash</i></b>	Termine inglese usato, impropriamente, come sinonimo d'uso di "impronta crittografica" o " <i>digest</i> " (vedi).
<b>Identificativo univoco</b>	Sequenza di numeri o caratteri alfanumerici associata in modo univoco e persistente ad un'entità all'interno di uno specifico ambito di applicazione.
<b>Impronta crittografica</b>	Sequenza di bit di lunghezza predefinita, risultato dell'applicazione di una funzione di <i>hash</i> crittografica a un'evidenza informatica.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Integrità</b>	Caratteristica di un documento informatico o di un'aggregazione documentale in virtù della quale risulta che essi non hanno subito nel tempo e nello spazio alcuna alterazione non autorizzata. La caratteristica dell'integrità, insieme a quella della completezza, concorre a determinare la caratteristica dell'autenticità.
<b>Interoperabilità</b>	Caratteristica di un sistema informativo, le cui interfacce sono pubbliche e aperte, e capaci di interagire in maniera automatica con altri sistemi informativi per lo scambio di informazioni e l'erogazione di servizi.
<b>Leggibilità</b>	Caratteristica di un documento informatico che garantisce la qualità di poter essere decodificato e interpretato da un'applicazione informatica.
<b>Manuale di conservazione</b>	Documento informatico che descrive il sistema di conservazione e illustra dettagliatamente l'organizzazione, i soggetti coinvolti e i ruoli svolti dagli stessi, il modello di funzionamento, la descrizione del processo, la descrizione delle architetture e delle infrastrutture.
<b>Manuale di gestione</b>	Documento informatico che descrive il sistema di gestione, anche ai fini della conservazione, dei documenti informatici e fornisce le istruzioni per il corretto funzionamento del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi.
<b>Metadati</b>	Dati associati a un o documento informatico, a un fascicolo informatico o a un'aggregazione documentale per identificarli, descrivendone il contesto, il contenuto e la struttura - così da permetterne la gestione del tempo - in conformità a quanto definito nella norma ISO 15489-1:2016 e più nello specifico dalla norma ISO 23081-1:2017.
<b><i>Naming convention</i></b>	Vedi Convenzioni di denominazione
<b>Oggetto di conservazione</b>	Oggetto digitale versato in un sistema di conservazione.
<b>Oggetto digitale</b>	Oggetto informativo digitale, che può assumere varie forme tra le quali quelle di documento informatico, fascicolo informatico, aggregazione documentale informatica o archivio informatico.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Pacchetto di archiviazione</b>	Pacchetto informativo generato dalla trasformazione di uno o più pacchetti di versamento coerentemente con le modalità riportate nel manuale di conservazione.
<b>Pacchetto di distribuzione</b>	Pacchetto informativo inviato dal sistema di conservazione all'utente in risposta ad una sua richiesta di accesso a oggetti di conservazione.
<b>Pacchetto di file (<i>file package</i>)</b>	Insieme finito di più file (possibilmente organizzati in una struttura di sottoalbero all'interno di un filesystem) che costituiscono, collettivamente oltre che individualmente, un contenuto informativo unitario e auto-consistente.
<b>Pacchetto di versamento</b>	Pacchetto informativo inviato dal produttore al sistema di conservazione secondo il formato descritto nel manuale di conservazione.
<b>Pacchetto informativo</b>	Contenitore logico che racchiude uno o più oggetti di conservazione con i relativi metadati, oppure anche i soli metadati riferiti agli oggetti di conservazione.
<b><i>Path</i></b>	Percorso ( <i>vedi</i> ).
<b><i>Pathname</i></b>	Concatenazione ordinata del percorso di un file e del suo nome.
<b><i>Percorso</i></b>	Informazioni relative alla localizzazione virtuale del file all'interno del filesystem espressa come concatenazione ordinata del nome dei nodi del percorso.
<b>Piano della sicurezza del sistema di conservazione</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di conservazione dei documenti informatici da possibili rischi.
<b>Piano della sicurezza del sistema di gestione Informatica dei documenti</b>	Documento che, nel contesto del piano generale di sicurezza, descrive e pianifica le attività volte a proteggere il sistema di gestione informatica dei documenti da possibili rischi.
<b>Piano di classificazione (Titolario)</b>	Struttura logica che permette di organizzare documenti e oggetti digitali secondo uno schema desunto dalle funzioni e dalle attività dell'amministrazione interessata.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Piano di conservazione</b>	Documento, allegato al manuale di gestione e integrato con il sistema di classificazione, in cui sono definiti i criteri di organizzazione dell'archivio, di selezione periodica e di conservazione ai sensi dell'articolo 68 del D.P.R. 28 dicembre 2000, n. 445.
<b>Piano di organizzazione delle aggregazioni documentali</b>	Strumento integrato con il sistema di classificazione a partire dai livelli gerarchici inferiori di quest'ultimo e finalizzato a individuare le tipologie di aggregazioni documentali (tipologie di serie e tipologie di fascicoli) che devono essere prodotte e gestite in rapporto ai procedimenti e attività in cui si declinano le funzioni svolte dall'ente
<b>Piano generale della sicurezza</b>	Documento che pianifica le attività volte alla realizzazione del sistema di protezione e di tutte le possibili azioni indicate dalla gestione del rischio nell'ambito dell'organizzazione di appartenenza.
<b>Preso in carico</b>	Accettazione da parte del sistema di conservazione di un pacchetto di versamento in quanto conforme alle modalità previste dal manuale di conservazione e, in caso di affidamento del servizio all'esterno, dagli accordi stipulati tra il titolare dell'oggetto di conservazione e il responsabile del servizio di conservazione.
<b>Processo</b>	Insieme di attività correlate o interagenti che trasformano elementi in ingresso in elementi in uscita.
<b>Produttore dei PdV</b>	Persona fisica, di norma diversa dal soggetto che ha formato il documento, che produce il pacchetto di versamento ed è responsabile del trasferimento del suo contenuto nel sistema di conservazione. Nelle pubbliche amministrazioni, tale figura si identifica con il responsabile della gestione documentale.
<b><i>qSeal</i></b>	Sigillo elettronico qualificato, come da art. 35 del Regolamento eIDAS.
<b><i>qSignature</i></b>	Firma elettronica qualificata, come da art. 25 del Regolamento eIDAS.
<b>Rapporto di versamento</b>	Documento informatico che attesta l'avvenuta presa in carico da parte del sistema di conservazione dei pacchetti di versamento inviati dal produttore.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Registro di protocollo</b>	Registro informatico ove sono memorizzate le informazioni prescritte dalla normativa per tutti i documenti ricevuti e spediti da un ente e per tutti i documenti informatici dell'ente stesso.
<b>Registro particolare</b>	Registro informatico individuato da una pubblica amministrazione per la memorizzazione delle informazioni relative a documenti soggetti a registrazione particolare-
<b>Regolamento eIDAS</b>	electronic IDentification Authentication and Signature, Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
<b>Repertorio</b>	Registro su cui vengono annotati con un numero progressivo i fascicoli secondo l'ordine cronologico in cui si costituiscono all'interno delle suddivisioni del piano di classificazione.
<b>Responsabile dei sistemi informativi per la conservazione</b>	Soggetto che coordina i sistemi informativi all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID.
<b>Responsabile del servizio di conservazione</b>	soggetto che coordina il processo di conservazione all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile della conservazione</b>	Soggetto che definisce e attua le politiche complessive del sistema di conservazione e ne governa la gestione con piena responsabilità ed autonomia.
<b>Responsabile della funzione archivistica di conservazione</b>	soggetto che coordina il processo di conservazione dal punto di vista archivistico all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile della gestione documentale</b>	Soggetto responsabile della gestione del sistema documentale o responsabile del servizio per la tenuta del protocollo informatico, della gestione dei flussi documentali e degli archivi, ai sensi dell'articolo 61 del D.P.R. 28 dicembre 2000, n. 445.

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
<b>Responsabile della protezione dei dati</b>	Persona con conoscenza specialistica della normativa e delle prassi in materia di protezione dei dati, in grado di assolvere i compiti di cui all'articolo 39 del Regolamento (UE) 2016/679.
<b>Responsabile della sicurezza dei sistemi di conservazione</b>	soggetto che assicura il rispetto dei requisiti di sicurezza all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Responsabile dello sviluppo e della manutenzione del sistema di conservazione</b>	soggetto che assicura lo sviluppo e la manutenzione del sistema all'interno del conservatore, in possesso dei requisiti professionali individuati da AGID
<b>Riferimento temporale</b>	Insieme di dati che rappresenta una data e un'ora con riferimento al Tempo Universale Coordinato (UTC).
<b>Riversamento</b>	Procedura mediante la quale uno o più documenti informatici sono convertiti da un formato di file (ovvero di busta, ovvero di pacchetto di file) ad un altro, lasciandone invariato il contenuto per quanto possibilmente permesso dalle caratteristiche tecniche del formato (ovvero dei formati) dei file e delle codifiche di destinazione.
<b>Scarto</b>	Operazione con cui si eliminano definitivamente, secondo quanto previsto dalla normativa vigente, i documenti ritenuti non più rilevanti ai fini giuridico-amministrativo e storico-culturale.
<b>Serie</b>	Raggruppamento di documenti con caratteristiche omogenee (vedi anche aggregazione documentale informatica).
<b>Sidecar (file)</b>	File-manifesto ( <i>vedi</i> ).
<b>Sigillo elettronico</b>	Dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica, per garantire l'origine e l'integrità di questi ultimi.
<b>Sistema di conservazione</b>	Insieme di regole, procedure e tecnologie che assicurano la conservazione dei documenti informatici in attuazione a quanto previsto dall'art. 44, comma 1, del CAD.
<b>Sistema di gestione informatica dei documenti</b>	Insieme delle risorse di calcolo, degli apparati, delle reti di comunicazione e delle procedure informatiche utilizzati dalle organizzazioni per la gestione dei documenti. Nell'ambito

## Allegato 1 - Glossario dei termini e degli acronimi

TERMINE	DEFINIZIONE
	della pubblica amministrazione è il sistema di cui all'articolo 52 del D.P.R. 28 dicembre 2000, n. 445
<b>Timeline</b>	Linea temporale virtuale su cui sono disposti degli eventi relativi ad un sistema informativo o a un documento informatico. Costituiscono esempi molto diversi di <i>timeline</i> un file di log di sistema, un flusso multimediale contenente essenze audio\video sincronizzate.
<b>Titolare dell'oggetto di conservazione</b>	Soggetto produttore degli oggetti di conservazione.
<b>Trasferimento</b>	Passaggio di custodia dei documenti da una persona o un ente ad un'altra persona o un altro ente.
<b>TUDA</b>	Testo Unico della Documentazione Amministrativa, Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, e successive modificazioni e integrazioni.
<b>Ufficio</b>	Riferito ad un'area organizzativa omogenea, un ufficio dell'area stessa che utilizza i servizi messi a disposizione dal sistema di protocollo informatico.
<b>Utente abilitato</b>	Persona, ente o sistema che interagisce con i servizi di un sistema di gestione informatica dei documenti e/o di un sistema per la conservazione dei documenti informatici, al fine di fruire delle informazioni di interesse.
<b>Versamento</b>	Passaggio di custodia, di proprietà e/o di responsabilità dei documenti. Nel caso di un organo giudiziario e amministrativo dello Stato operazione con la quale il responsabile della conservazione trasferisce agli Archivi di Stato o all'Archivio Centrale dello Stato della documentazione destinata ad essere ivi conservata ai sensi della normativa vigente in materia di beni culturali.

### 1.5 Glossario degli Acronimi

ACRONIMO	DEFINIZIONE
<b>AGID</b>	Agenzia per l'Italia digitale

## Allegato 1 - Glossario dei termini e degli acronimi

ACRONIMO	DEFINIZIONE
<b>AOO</b>	Area Organizzativa Omogenea
<b>CAD</b>	Codice dell'Amministrazione Digitale - Decreto legislativo 7 marzo 2005, n. 82 e successive modificazioni e integrazioni.
<b>eIDAS</b>	Regolamento (UE) № 910/2014 del Parlamento Europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
<b>FEA</b>	Vedi firma elettronica avanzata.
<b>FEQ</b>	Vedi firma elettronica qualifica.
<b>GDPR</b>	Regolamento (UE) № 679/2016 del Parlamento Europeo e del Consiglio, del 27 aprile 2016 ( <i>"General Data Protection Regulation"</i> ), relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE.
<b>PdA (AiP)</b>	Pacchetto di Archiviazione.
<b>PdD (DiP)</b>	Pacchetto di Distribuzione.
<b>PdV (SiP)</b>	Pacchetto di Versamento.
<b>UOR</b>	Unità Organizzativa Responsabile

## **Formati di file e riversamento**

**Allegato 2 al documento  
“*Linee Guida sulla  
formazione, gestione e  
conservazione dei documenti  
informatici*”.**

# Sommario

1	Introduzione	3
1.1	Definizioni fondamentali	3
1.1.1	File, flussi digitali e buste-contenitori	4
1.1.2	Filesystem e metadati	5
1.1.3	Metadati e identificazione del formato	8
1.2	Tassonomia	9
1.2.1	Tipologie di formati	9
1.2.2	Classificazione di formati	11
1.2.3	Formati generici e specifici	14
2.	Tipi di file	16
2.1	Documenti impaginati	21
2.1.1	Raccomandazioni per la produzione di documenti	33
2.2	Ipertesti	34
2.2.1	Raccomandazioni per la produzione di documenti	41
2.3	Dati strutturati	42
2.3.1	Raccomandazioni per la produzione di documenti	52
2.4	Posta elettronica	53
2.4.1	Raccomandazioni per la produzione di documenti	55
2.5	Fogli di calcolo e presentazioni multimediali	55
2.5.1	Raccomandazioni per la produzione di documenti	59
2.6	Immagine raster	60
2.6.1	Raccomandazioni per la produzione di documenti	74
2.7	Immagine vettoriale e modellazione digitale	77
2.7.1	Raccomandazioni per la produzione di documenti	84
2.8	Caratteri tipografici	84
2.8.1	Raccomandazioni per la produzione di documenti	86
2.9	Audio e musica	87
2.9.1	Raccomandazioni per la produzione di documenti	92
2.10	Video	93
2.10.1	Raccomandazioni per la produzione di documenti	102
2.11	Sottotitoli, didascalie e dialoghi	103
2.11.1	Raccomandazioni per la produzione di documenti	108
2.12	Contenitori e pacchetti di file multimediali	108
2.12.1	Raccomandazioni per la produzione di documenti	131
2.13	Archivi compressi	132
2.13.1	Raccomandazioni per la produzione di documenti	138
2.14	Documenti amministrativi	138
2.15	Applicazioni e codice sorgente	142
2.16	Applicazioni crittografiche	142
3	Raccomandazioni sui formati di file	146
3.1	Valutazione di interoperabilità	147
3.2	Indice di interoperabilità	149
3.3	Riversamento	150

## 1 Introduzione

1. Il presente documento fornisce indicazioni iniziali sui formati dei file con cui vengono rappresentati i documenti informatici oggetto delle presenti linee guida. I termini indicati in azzurro, alla prima occorrenza all'interno di questo testo, sono definiti nel Glossario delle presenti Linee guida.
2. I formati descritti sono stati scelti tra quelli che possono maggiormente garantire il principio dell'interoperabilità tra i sistemi di gestione documentale e conservazione e in base alla normativa vigente riguardante specifiche tipologie di documenti. Va tuttavia segnalato che non tutti i formati di file nel presente documento sono leggibili da qualsivoglia elaboratore, a seconda della configurazione degli applicativi installati. Questo perché, nel caso di finalità specifiche e settoriali (come avviene ad esempio per i file multimediali), alcuni formati di file sono utilizzabili solo dopo l'installazione di software applicativi specifici per l'attuazione delle suddette finalità.
3. È bene precisare che, rispettando il principio di interoperabilità e cercando di mitigare il rischio di "obsolescenza tecnologica", i formati consigliati tra quelli elencati –inclusi quelli per finalità specifiche, cfr. §1.2.3– sono quanto più possibile "aperti", liberamente utilizzabili e non coperti da brevetto. Sono inoltre reperibili online diversi software applicativi open-source in grado di leggere tali file. Tra i formati elencati
4. Tra i formati elencati nel presente Allegato, vi sono anche quelli non consigliati per finalità di interoperabilità, archiviazione o conservazione; essi sono presenti nell'elenco perché formati già ampiamente diffusi nella pubblica amministrazione e quindi non ignorabili per quanto riguarda il loro trattamento e il riversamento da questi formati verso formati più interoperabili.
5. Il presente Allegato, per la natura stessa dell'argomento trattato, viene periodicamente aggiornato sulla base dell'evoluzione tecnologica e dell'obsolescenza dei formati e potrà essere pubblicato online sotto forma di Avvisi, ovvero di un registro dei formati sul sito istituzionale dell'Agenzia per l'Italia Digitale<sup>1</sup>.

### 1.1 Definizioni fondamentali

Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questa sezione.

---

<sup>1</sup> Qui di seguito indicata anche, per brevità, come Agenzia, ovvero come AGID.

### 1.1.1 File, flussi digitali e buste-contenitori

1. Dal punto di vista tecnologico un documento informatico è rappresentato da un file, ovvero da un flusso binario (*stream*); in linea di principio un flusso binario di dimensione finita può essere contenuto in un file. Il parametro progettuale più importante associato a un file è la sua dimensione (espressa in byte o suoi multipli). Per un flusso binario, che invece può non avere una dimensione predeterminata, si parla invece del suo *data-rate* (ovvero *bit-rate*, quando espresso in bit o suoi multipli), cioè la media temporale dei bit contenuti dal flusso nell'arco di un secondo.

2. La capacità di poter produrre, elaborare o trasmettere flussi entro un data-rate massimo attraverso un canale di comunicazione digitale costituisce la banda dell'elaboratore ovvero del canale — in inglese *bandwidth*. In questo capitolo ci interessiamo prevalentemente ai documenti informatici rappresentati mediante file, mentre sarà presa in considerazione la rappresentazione mediante flussi binari nel caso di alcuni file multimediali (cfr. §§2.9–2.12).

3. In alcuni casi il documento informatico è rappresentato da un insieme di file distinti, organizzati in un pacchetto di file, in inglese (*file*) *package*.

4. L'algoritmo che permette di rappresentare un documento informatico mediante un'evidenza quale un file tramite un'operazione di codifica, o *encoding*, definisce dunque il formato del file; l'operazione inversa, per estrapolare dai dati binari di un file —codificato in un dato formato— nel contenuto informativo del documento, è chiamata decodifica (*decoding*). Formati diversi necessitano di codificatori e decodificatori specifici, che in una parola (soprattutto quando entrambi, per un formato specifico, sono implementati da una singola componente applicativa) sono abbreviati in codec.

5. Esistono una moltitudine di formati di file per rappresentare i documenti informatici ma, a seconda del contenuto del documento e delle esigenze specifiche di gestione e conservazione dello stesso, alcuni formati sono più adatti di altri. Alcuni formati possono essere utilizzati per codificare documenti di una sola tipologia (ad es. formati di file per immagini, generalmente, non possono codificare documenti audio); altri formati, invece, vengono usati per una o più finalità di codifica tra le seguenti:

- codificare documenti di tipologie diverse (ad es. sia testi, che immagini, che audio);
- codificare più documenti insieme nel medesimo file (ad es. scopo principale dei formati di archiviazione);
- codificare documenti di una medesima tipologia (ad es. video) usando però algoritmi di codifica diversa.

I formati di file che assolvono ad una o più delle suddette funzioni sono chiamati (formati) busta, o (formati) contenitori — in inglese, rispettivamente, (*file*) *wrappers* o *containers*. Le due tipologie di documento si utilizzano prevalentemente formati contenitori sono i documenti che richiedono funzioni crittografiche avanzate (cfr. §2.16) e i file multimediali (immagini, suono, video, cfr. §§2.6–2.12).

6. Alcuni formati contenitori, infine, imbustano al loro interno, in un unico file-busta, pacchetti di più file precostituiti secondo un determinato formato di pacchetto di file. È questo il caso, ad esempio, dei formati OpenDocument e Microsoft® OOXML (cfr. §2.1 e §2.5), ovvero delle immagini virtuali di filesystem (cfr. §2.13).

## 1.1.2 Filesystem e metadati

1. I file sono solitamente archiviati una base di dati chiamata **filesystem**, ove i file con maggiore parentela fra loro (altrimenti detta *locality of reference*, ovvero “affinità per referenza”) sono collocati nel medesimo nodo dell’albero: la cartella (ovvero *folder* o *directory* in inglese).

2. All’interno di un filesystem, ai file possono essere associate altre informazioni che ne completano l’esistenza all’interno dello stesso, anche se tali informazioni non fanno parte del contenuto binario del file propriamente detto; tali informazioni sono chiamate per questo motivo metadati (in inglese *metadata*) “esterni” del file.

3. Esistono molteplici formati di filesystem, che variano a seconda delle tecnologie di stoccaggio, di specifiche finalità. Alcuni di questi formati sono open-source; altri sono codificati in standard; altri ancora sono protetti da brevetti e/o copyright.

4. I metadati esterni rappresentabili in un dato filesystem possono differire anch’essi —per qualità, numero, sintassi e funzionalità— a seconda del formato di filesystem, ma di solito comprendono almeno:

- il nome del file, cioè una stringa di caratteri (di lunghezza variabile entro un limite massimo finito) che identifica univocamente il file all’interno della medesima cartella. Sussistono limitazioni differenti circa i caratteri ammessi nel nome e la sua lunghezza massima, a seconda dei diversi formati di filesystem considerati;
- la posizione virtuale del file all’interno del filesystem, chiamato “percorso del file” (**path**) — “locale” in quanto relativo al filesystem che lo ospita;
- la dimensione del file sopra definita, espressa da un numero intero di byte (o suoi multipli);

- la data e l’ora relativa all’ultimo istante in cui il sistema informatico che gestisce il filesystem ha rilevato una modifica del file — chiamata “data di modifica” del file.
5. La concatenazione ordinata del percorso di un file e del suo nome prende il nome di percorso completo del file (*pathname*). Invece la parte, opzionale, del nome del file costituita, scorrendo i caratteri del nome da sinistra a destra, a partire dall’ultima occorrenza del carattere punto ‘.’ in poi (codice ASCII 2E<sub>16</sub> in esadecimale) è chiamata —quando esiste— “estensione” del file.
6. A titolo esemplificativo, fanno parte dei metadati esterni di un file anche i seguenti:
- la data e l’ora creazione del file (che, a seconda della tipologia di filesystem può, con diversi gradi di ambiguità, coincidere con il momento di prima comparsa del file sul filesystem specifico, ovvero il momento della creazione del file sul suo filesystem di origine, o altro);
  - la data e l’ora relativa al più recente accesso in lettura sul file avvenuto nel filesystem specifico;
  - un identificativo più o meno univoco dell’utente informatico che è il proprietario virtuale del file (rispetto agli altri utenti virtuali del sistema) — chiamato l’*owner* del file;
  - una serie di attributi che istruiscono i sistemi informativi che gestiscono l’intero filesystem di appartenenza circa la possibilità di autorizzare determinate operazioni sullo specifico file, a seconda sia dell’operazione da compiere che dell’utenza informatica che presenta tale richiesta; per ogni file, tali metadati costituiscono o sono una parte del cosiddetto insieme dei suoi permessi (*permissions*), ovvero una vera e propria lista dei controlli d’accesso (*ACL*);
  - un’etichetta che stabilisce il tipo di formato file (o container) impiegato per la codifica del documento; una cui codifica universalmente riconosciuta *MIME type* – cfr. [RFC-2046](#) e [RFC-3023](#)).
7. È importante esplicitare che le “date” sopra descritte, pur non assolvono a requisiti di integrità, precisione e immutabilità nel tempo solo per il fatto di rappresentare una data e un’ora in un filesystem, non producendo dunque, a priori, la stessa validità giuridica di marcature temporali elettroniche qualificate ai sensi del Regolamento (UE) N°910/2014.
8. Come anticipato in §1.1.1, il documento informatico può essere rappresentato da un insieme di file distinti, organizzati in un **pacchetto di file** –in inglese (*file package*)– ove l’affinità per referenza tra di essi è realizzata, a seconda del formato del pacchetto, mediante *una o più* delle seguenti tecniche:

- Parentela stretta dei file all'interno del filesystem realizzata definendo un sottoalbero riservato a contenere l'intero pacchetto. I file del pacchetto sono tutti contenuti nella cartella-radice del pacchetto ovvero in sue sottocartelle e, tipicamente, è escluso da tale sottoalbero qualunque file non appartenente al pacchetto. Esempi di formati che utilizzano questa tecnica sono le firme elettroniche avanzate nel formato ASiC (§2.16), il formato di master interoperabile (IMF), i pacchetti per il cinema digitale (DCP), e i pacchetti XDCAM (per tutti, §2.12).
- Sintassi dei nomi –rigida o parziale– per file ed eventuali sottocartelle costituenti il pacchetto. Formati che utilizzano esclusivamente questa tecnica sono le impronte crittografiche *detached* (§2.16) e i pacchetti video organizzati in sequenze di fotogrammi (quali ad esempio i master per la distribuzione del cinema digitale, DCDM, §2.12).
- Presenza di un “indice di pacchetto”, generalmente rappresentato da un file che ha sia un nome che una posizione controllate e che contiene i *pathname* degli altri file costituenti il pacchetto. Tale indice assolve spesso a scopi aggiuntivi, come ad esempio consolidare in un unico punto i metadati esterni del pacchetto o dei singoli file (§1.1.3), che altrimenti potrebbero essere accidentalmente alterati (o persi) spostando il pacchetto da un filesystem ad un altro. In questi casi il file indice prende anche il nome di file-*manifesto*, ovvero *sidecar file*. Formati che utilizzano esclusivamente questo metodo sono i pacchetti di siti web (indice con nome *non* obbligatorio *index.html*, §2.2), alcuni tipi di firme elettroniche avanzate ASiC (tramite la cartella-indice META-INF, §2.16), i già menzionati pacchetti IMF e DCP (che utilizzano più di un file con funzioni di indice, §2.12).
- Riferimento mediante **identificativi unici (UID)** assegnati a ciascun file del pacchetto, quali ad esempio le loro impronte crittografiche. Esempi di formati che utilizzano questo metodo sono le firme elettroniche avanzate CADES e XADES *detached* (§2.16), le marche temporali *detached* e i già menzionati pacchetti IMF e DCP.
- Consolidamento di tutti e soli i file del pacchetto in un file-archivio (§2.13). Esempi che utilizzano questo metodo sono i documenti nei formati OpenDocument e Microsoft® OOXML (cfr. §2.1 e §2.5), gli applet Java e i pacchetti applicativi per dispositivi mobili con sistemi operativi Android e iOS® (§2.15), le firme elettroniche ASiC (§2.16) e, in senso lato, i file PDF (versione 1.7 e successive) quando imbustano altri documenti al loro interno sotto forma di “allegati PDF” (§2.1).

9. La tipologia di regole sintattiche che stabilisce come implementare i primi due metodi sopra elencati costituisce la *naming convention* del formato di pacchetto. La sua efficacia è ridotta quando non coadiuvata da ulteriori controlli di integrità del

pacchetto, in quanto l'affinità per referenza è generalmente difficile da far rispettare tecnicamente (a meno di usare uno stretto controllo dei permessi di “sola-lettura”, ovvero archiviare su dispositivi logicamente immutabili). Per questo motivo la *naming convention* si affianca spesso ad altri metodi quali quelli ai punti dal 3 al 5 del sopracitato elenco.

### 1.1.3 Metadati e identificazione del formato

1. Abbiamo già parlato in §1.1.2 dei metadati esterni, che servono a descrivere meglio un file ma sono fortemente dipendenti dal filesystem ove il file è archiviato in un dato momento. Inoltre, tali metadati possono essere soggetti a modifiche che non pregiudicano l'integrità del file stesso.

2. Più importanti ancora sono perciò i cosiddetti metadati “interni” di un file, cioè informazioni descrittive del file che sono codificate nel suo formato stesso. A seconda del formato impiegato, la presenza di questi metadati interni può essere obbligatoria o facoltativa. Facendo parte del contenuto binario di un file, la modifica di tali metadati compromette l'integrità del documento informatico.

3. Il riconoscimento (in modalità automatica o manuale) del formato di file impiegato per rappresentare un documento informatico può avvenire attraverso alcune modalità, tra cui le più diffuse sono tramite metadati interni ovvero esterni:

a) L'estensione nel nome del file, anche se tale associazione:

- non è resiliente — è solitamente banale rinominare un file cambiandone l'estensione [ovvero crearne direttamente il nome] con un'estensione non corrispondente al formato utilizzato (es. un file di testo semplice con codifica ASCII denominato con estensione .doc, che invece è prerogativa dei documenti di Microsoft® *Word*);
- non è biunivoca — una medesima estensione può essere usata nel nome di file codificati in formati diversi (es. l'estensione .log, usata per rappresentare file di registro codificati in maniera diversa), ovvero un dato formato viene associato a file con una molteplicità di estensioni (es. i certificati elettronici in formato X.509 con codifica DER, rappresentati con diverse estensioni tra cui .crt ovvero .cer).

b) La “tipologia MIME” (*MIME type*) del formato di file, anche se tale associazione gode di svantaggi simili all'estensione, in quanto:

- soprattutto se espressa come metadato esterno (si veda §1.1.2), non è resiliente a variazioni o rimozioni del medesimo in maniera non controllata;

- sia nel caso in cui sia espressa come metadato interno che come metadato esterno del file, potrebbe descrivere il formato in modo comunque ambiguo.
- c) La presenza di metadati interni al file, espressi in “campi” che si trovano in posizioni specifiche (prefissate ovvero ricalcolabili) all’interno del file<sup>2</sup>. La lettura di tali campi permette di dedurre il formato del file in maniera più diretta e affidabile. Molti formati impiegano, specificatamente a questo scopo, una stringa prefissata di pochi caratteri (generalmente dai 2 ai 6), posta all’inizio del file, chiamata *magic number* e che ne identifica univocamente<sup>3</sup> il tipo di file.

## 1. 2 Tassonomia

### 1.2.1 Tipologie di formati

1. L’evolversi delle tecnologie e la crescente disponibilità e complessità dell’informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità specializzate per renderne più facile la creazione e la modifica.

2. Questo fenomeno porta all’aumento del numero di formati disponibili e dei corrispondenti programmi necessari per codificarli, decodificarli e gestirli in ogni modo.

3. Segue una sommaria e non esaustiva catalogazione dei più diffusi formati di file e pacchetti, secondo il loro specifico utilizzo (“tipologia”). A fianco di ogni tipologia di formati sono indicati i formati pertinenti oggetto del presente Allegato; qualora l’estensione di file associata al formato sia diversa –a meno di maiuscole/minuscole– dall’eventuale acronimo del nome del formato stesso, essa sarà indicata affiancata al nome tra parentesi (e.g., il formato PDF non avrà un’estensione indicata tra parentesi in quanto la sua estensione predefinita è già .pdf).

- **Documenti impaginati** (§2.1) — PDF, Microsoft® OOXML (.docx) e *Word* (.doc), OpenDocument Text (.odt), Rich-Text Format (.rtf), EPUB, PostScript™ (.ps), Adobe® *InDesign*® Markup Language (.idml);

---

<sup>2</sup> La parte iniziale ovvero quella terminale di un file contengono spesso gran parte dei campi utili a contenere i metadati interni (e quindi anche a identificare il formato) del file; quando presenti, queste parti sono chiamate, rispettivamente, *header* (impropriamente tradotto come “intestazione”) e *footer* del file.

<sup>3</sup> Il magic number può anche identificare l’allineamento delle *word*, che le architetture dei microprocessori e i sistemi operativi implementano diversamente per varie ragioni. Alcuni magic number notevoli sono indicati, per i rispettivi formati, nel §2.

- **Ipertesti** (§2.2) — XML, dialetti e schemi XML (.xsd, .xsl), HTML (.html, .htm), fogli di stile per XML/HTML (.xsl, .xslt, .css), Markdown (.md);
- **Dati strutturati** (§2.3) — SQL, CSV, Microsoft® OOXML (.accdb) e *Access* (.mdb), OpenDocument Database (.odb), JSON, Linked OpenData (.json-ld), JWT<sup>4</sup>;
- **Posta elettronica** (§2.4) — .eml, .mbox;
- **Fogli di calcolo** (§2.5) — Microsoft® OOXML (.xlsx) e *Excel* (.xls), OpenDocument Spreadsheet (.ods);
- **Presentazioni multimediali** (§2.5) — Microsoft® OOXML (.pptx) e *PowerPoint* (.ppt), OpenDocument Presentation (.odp);
- **Immagini raster** (§2.6) — JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), PNG, GIF, OpenEXR (.exr), JPEG2000 (.jp2k, .jp2c, .jp2), DICOM, Adobe® DNG, Adobe® *Photoshop*® (.psd), DPX, ARRIRAW (.ari);
- **Immagini vettoriali e modellazione digitale** (§2.7) — SVG, Adobe® *Illustrator*® (.ai), Encapsulated PostScript™ (.eps);
- **Modelli digitali** (§2.7) — StereoLithography (.stl); Autodesk® DWG™, DXF™, DWF™, FBX™.
- **Caratteri tipografici** (§2.8) — OpenType (.otf), TrueType (.ttf), Web Open Font (.woff, .woff2);
- **Suono** (§2.9) — Waveform RIFF / Broadcast Wave (.wav, .bwf), MP3, audio RAW (.pcm, .raw, .snd), AIFF (.aiff, .aifc, .aif), FLAC, MusicXML™ (.music.xml), MIDI (.mid); molteplici codec audio;
- **Video** (§2.10) — formati video delle famiglie MPEG2 e MPEG4; molteplici codec video;
- **Sottotitoli** (§2.11) — TTML/IMSC/EBU-TT (.ttml, .dfxp, .xml), EBU STL;
- **Contenitori multimediali** (§2.12) — MP4, MXF, MPEG2 Transport/Program Stream (.vob, .ts, .ps), AVI RIFF (.avi), Matroska (.mkv), QuickTime (.mov, .qt), WebM;
- **Pacchetti multimediali** (§2.12) — pacchetto di master interoperabile (IMF, IMP); pacchetto per il cinema digitale (DCP); master per la distribuzione cinematografica (DCDM); pacchetti Digital Intermediate basati su sequenze di fotogrammi (.exr/.dpx; .wav), ACES metadata file (.amf); pacchetto XDCAM;
- **Archivi compressi** (§2.13) — TAR, ZIP, GZIP, 7-Zip (.7z), RAR, TAR compresso (.tgz, .t7z, ...), ISO9660 (.iso), VMware® Disk (.vmdk), Apple Disk Image (.dmg);
- **Documenti amministrativi** (§2.14) — fattura elettronica, fascicolo sanitario elettronico, *response* SAML SPID, segnatrice di protocollo;

---

<sup>4</sup> Il *Java Web Token* (JWT) è in realtà un formato di flusso digitale, che può essere banalmente contenuto in un file, cfr. §2.3.

- **Applicazioni e codice sorgente** (§2.15) — eseguibili Microsoft® (.exe, .com), *applet* Java (.jar); pacchetti applicativi *Windows*® (.msi), Android (.apk), macOS® (.pkg), iOS® (.ipa); librerie statiche (.a, .lib) e dinamiche (.so, .dll, .dylib); script interpretabili (.sh, .?sh, .bat, .cmd, .py, .perl, .js, .go, .r, ...); codice sorgente in vari linguaggi di programmazione (.c, .cpp, .h, .java, .asm, ...).
- **Applicazioni crittografiche** (§2.16) — certificati elettronici (.cer, .crt, .pem), chiavi crittografiche (.pkix, .pem), marcature temporali elettroniche (.tsr, .tsd, .tst), impronte crittografiche (.sha1, .sha2, .md5, ...); per le firme e i sigilli elettronici avanzati: buste crittografiche XAdES (.xml), CADES (.p7m, .p7s), PAdES (.pdf), contenitori ASiC (.zip); KDM (.kdm.xml).

## 1.2.2 Classificazione di formati

1. L'evolversi delle tecnologie e la crescente disponibilità e complessità dell'informazione digitale ha indotto la necessità di gestire sempre maggiori forme di informazione digitale (testo, immagini, filmati, ecc.) e di disporre di funzionalità specializzate per renderne più facile la creazione e la modifica.
2. Gli *standard* tecnologici vengono incontro a tali esigenze, permettendo di definire regole di codifica e decodifica di un documento informatico, affinché sia rappresentato tramite un file, un flusso digitale, ovvero un pacchetto di file (tutti oggetti del presente allegato). Gli standard tendono a stabilizzare le specifiche tecniche dei formati di file –sia nel tempo che rispetto alle tecnologie di produzione, trasmissione e archiviazione– ma la loro importanza nel cristallizzare tali specifiche in una forma precisa serve ad impedire la nascita di varianti “esotiche” o dialetti non controllati del medesimo formato che, alla lunga, ne riducano l'interoperabilità (cfr. più avanti).
3. Un esempio su tutti: la mancata standardizzazione dei codec usati nei formati-busta multimediali (§2.12), specialmente dei file video, che spesso conduce all'impossibilità di riprodurre un filmato ritenuto compatibile con il sistema informativo a causa del riconoscimento della sola estensione del file da parte di svariate applicazioni (che al massimo può servire a identificare il formato contenitore), senza invece un'adeguata verifica del possesso dei codec adatti a riprodurre le essenze.
4. Gli standard migliori sono quelli che possono essere facilmente estesi, rivisti o aggiornati nel tempo per adattarsi all'imminente obsolescenza tecnologica. Tra questi inoltre, eccellono gli standard che sono *ab initio* disegnati con il preciso scopo di evolvere a lungo termine; per questo motivo essi sono detti formati “compatibili in avanti” o anche “*future-proof*”.

5. Esempi di questi standard “virtuosi”, sono l’XML e il JSON; il PDF e l’OpenDocument per i documenti impaginati; il TIFF (e il DNG), il PNG e il DPX per le immagini *raster*; l’SVG e il DXF per i modelli vettoriali; il TTML per i dialoghi; l’MXF e l’MP4 come contenitori multimediale; l’IMF come pacchetto di file multimediali.
6. I formati di file sono soggetti a revisioni allo scopo di includere caratteristiche evolutive; a questo scopo gli standard corrispondenti vengono “versionati” con diverse tassonomie, cioè incrementandone progressivamente i numeri delle revisioni (possibilmente in gerarchie di non più di 2-4 componenti numeriche— ovvero utilizzando l’anno o una data più precisa di riferimento, ovvero mediante sia numeri progressivi che date).
7. Quando non sono più fatti evolvere in favore di un formato differente (e quindi vengono progressivamente abbandonati), il formato diventa quiescente ed eventualmente viene “deprecato” in favore di un altro standard.
8. Sebbene sia tecnicamente possibile continuare a produrre e riprodurre file in un formato deprecato, il progresso tecnologico, o per meglio dire l’*obsolescenza tecnologica*, condannerà tali file a non essere più definitivamente leggibili, a causa della mancanza di applicativi che ne implementino la decodifica (a meno di non coinvolgere risorse economiche solitamente sproporzionate al bisogno di accesso ai dati contenuti). Quando ciò accade ed è riconosciuto in maniera manifesta, si parla di formati “obsoleti”.
9. Esistono varie classificazioni per le tipologie di formati, le quali sono spesso determinanti —ancor più delle loro peculiarità tecniche— per la scelta d’uso di un formato in favore di altri, ovvero per prendere decisioni ragionate circa il riversamento da un formato verso un altro (cfr. §3.3).
10. Tali classificazioni, elencate brevemente qui sotto, sono per lo più dicotomiche (cioè del tipo presenza o assenza di una determinata caratteristica) e indipendenti fra loro. Accanto ad ogni classificazione è riportato un modificatore in grassetto, il cui significato è riferito all’[indice di interoperabilità](#) introdotto nel §3.2. Un formato può essere:
- a) uno standard *de facto* (+2) quando questioni contingenti (anche fa loro correlate), quali l’efficienza in casi d’uso reali, l’autoregolazione dei mercati di riferimento, l’efficacia tecnica, ne hanno determinato una larghissima e non trascurabile diffusione, per lo meno in settori di riferimento. Un formato può essere invece uno standard *de iure* (+3), quando esistono normative che ne obblighino, o per lo meno ne raccomandino, l’uso in determinati contesti amministrativo-legali e settori di riferimento. Rappresentano esempi di tali normative le Linee guida di cui il presente Allegato è parte integrante (in quanto già Regole Tecniche) ovvero, a livello comunitario, alcune Decisioni di Esecuzione (UE). Sono standard *de iure*, inoltre, tutti i formati codificati come tali dalle organizzazioni nazionali, comunitarie e internazionali che hanno il compito di definire standard e linee guida nei settori di riferimento

dei formati stessi (come, ad esempio, ISO, ITU, UNI, CEN, SMPTE, ecc.). Infine, un formato può anche non rappresentare alcuno standard (0), ma tale caratteristica tendenzialmente lo esclude dall'elenco dei formati virtuali contenuti nel presente Allegato.

- b) **aperto (+3)** ovvero **chiuso (0)** a seconda che esista o meno, e sia resa pubblicamente disponibile, una “specifica tecnica” del medesimo: la documentazione che descrive dettagliatamente, come minimo, la procedura di formazione e di lettura di file in quel formato e, possibilmente, l'elaborazione e i suoi possibili scenari di utilizzo, spesso descritti organicamente mediante *operational patterns* (in italiano: schemi operativi).
- c) **proprietario** (variabile) o **non proprietario (+4)**, a seconda che sia stato creato da un'organizzazione privata –che dunque ne detenga la proprietà intellettuale– ovvero quando la gestione delle sue specifiche non è controllata in tale ambito (quindi possibilmente rilasciata al pubblico dominio, o comunque gestita da un organismo di standardizzazione). In particolare, i formati proprietari possono essere **liberi (+3)** ovvero **limitati**; in quest'ultimo caso la limitazione potrebbe permettere soltanto l'utilizzo libero di file già codificati in tale formato ma non la produzione di nuovi file (+2), ovvero limitare anche la lettura dei file formattati secondo tale formato (0); potrebbero essere possibili anche altri tipi di vincoli (pagamento di *royalty*, sottoscrizione di contratti di riservatezza o contratti vincolanti relativamente a particolari utilizzi quali lo sfruttamento commerciale, ecc.).
- d) **estendibile (+2)** o **non estendibile (0)** qualora esso sia stato concepito *ab initio* per ammettere revisioni che ne aumentino progressivamente le funzionalità. I formati *non* estendibili, quindi, possono comunque essere soggetti a revisioni, che però potrebbero, per tali formati, richiedere una re-ingegnerizzazione o un adattamento più difficoltoso rispetto a formati estendibili, probabilmente anche a scapito delle compatibilità di cui al punto precedente.
- e) **livello del modello per i metadati** (da 0 a +3) che segue l'analoga classificazione emanata nelle *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico*, emanate dall'Agenzia per l'Italia Digitale, ove al livello 1 vengono attribuiti 0 punti e così via fino al livello 4 cui sono attribuiti 3 punti. Tale valore è indicato, per i formati descritti al §1.2.3, nelle loro tabelle riassuntive.
- f) **non robusto (0)** ovvero **parzialmente robusto (+1)** a seconda che il file comprenda meccanismi per verificare l'eventuale perdita di *integrità* di un file (o pacchetto di file); **completamente robusto (+2)**, invece, qualora tale meccanismo sia presente e consenta, inoltre, di leggere correttamente le parti integre del file.

- g) **dependente (0)** ovvero **indipendente dal dispositivo (+4)** a seconda che esso richieda o meno specifici componenti hardware, firmware o software per essere creato o letto.
- h) i formati il cui standard prevede *by design* che un applicativo in grado di interpretare una data revisione possa anche leggere file formattati con revisioni precedenti (eventualmente entro un limite massimo) si dicono **retro-compatibili**. Quelli per cui gli applicativi disegnati al momento in cui una data revisione sia corrente possano leggere anche file formattati in base a revisioni successive del medesimo standard si dicono invece “**compatibili in avanti**”<sup>5</sup> **(0)**.
- i) **testuale (0)** se, rappresentando ogni **word** di un file come caratteri testuali, sia possibile estrapolarne il contenuto informativo tramite lettura manuale e non automatizzata di tali caratteri — a seguito di uno sforzo di interpretazione di entità variabile, ma comunque proporzionato alle capacità intellettive di un tecnico di settore. Si parla, in alternativa, di formato **binario (binary) (0)** quando il processo è generalmente possibile solo mediante interpretazione automatizzata, “bit a bit”, del contenuto digitale del file da parte di un algoritmo di **parsing**.

### 1.2.3 Formati generici e specifici

1. In ottica di interoperabilità è necessario, per le PPA.A., individuare un elenco di formati di file (e, *mutatis mutandis*, di formati di contenitori, pacchetti di file, flussi digitali e codec) per i quali vi siano obblighi o raccomandazioni in merito al riconoscimento o alla produzione in tali formati. Tale elenco non può presentare un unico tipo di obblighi e raccomandazioni, in quanto le organizzazioni di categoria, avendo necessità amministrative e operative differenti, utilizzano tecnologie digitali — e di conseguenza formati di file e applicazioni che li elaborano — estremamente variegate.

2. È auspicabile che i formati raccomandati nel presente Allegato siano adottati con modalità analoghe anche dagli enti privati — quando non già obbligatori per effetto di altre leggi — allo scopo di incrementare l’interoperabilità nello scambio di documenti informatici tra settore pubblico e privato. Per questo motivo queste Linee guida individuano, dall’insieme di formati di cui al §2:

---

<sup>5</sup> A titolo di esempio, un formato potrebbe essere progettato affinché, in uno schema di versionamento del tipo “*m.n*” (ove *m* sia il numero ‘maggiore’ della versione e *n* il numero ‘minore’) vi sia retrocompatibilità totale in scrittura di almeno *k* versioni precedenti, nonché estendibilità (in lettura) per tutte le revisioni minori della stessa versione. Ad esempio, per *k*=2, questo significa che un file codificato nella versione 3.12 di un dato formato, ad esempio, potrà essere prodotto anche da applicativi che producano file codificati con le versioni 4 e 5; inoltre ad un applicativo in grado di leggere la versione 3.12 sarà richiesto di poter leggere file di qualunque versione 3 (anche se eventuali funzionalità aggiuntive introdotte in revisioni minori successive alla 3.12, pur non “onorabili” dall’applicativo, non dovranno pregiudicarne la possibilità di aprire il file).

- a) una **categoria generale** di formati, rispetto ai quali *tutte* le P.P.A.A. e le organizzazioni sul territorio nazionale,
  - a. sono in grado di leggere file prodotti in questi formati,
  - b. seguono le indicazioni riportate nella tabella riassuntiva del formato per quanto concerne la produzione di nuovi documenti in questi formati;
- b) diverse **categorie specifiche** o **speciali**, diversificate in base al settore merceologico o alla natura del documento informatico rappresentabile, verso le quali sono identificati ulteriori obblighi e raccomandazioni solo verso le P.P.A.A. che, in quanto utenti professionali,<sup>6</sup> trattano documenti di quella tipologia nell'ambito ristretto, o comunque delimitato, di quella categoria specifica. Tali categorie possono essere di riferimento anche per soggetti privati che trattano professionalmente i medesimi documenti informatici.

3. L'appartenenza di un formato di file alla categoria generale piuttosto che a una o più categorie speciali è indicata nelle tabelle riassuntive dei formati contenute nel §2, possibilmente differenziata per la lettura ovvero la scrittura (cioè la formazione) di documenti in tali formati.

4. Come indicato nelle Linee guida di cui il presente Allegato è parte integrante, qualora un formato di file sia indicato come generico, ma una sua particolare applicazione in un determinato settore specialistico fornisca anche un formato di file specifico, ovvero una variazione strutturale del medesimo formato generico (ad es. dialetti, specializzazioni, varianti, schemi operativi, profili, specifiche tecniche particolari o aggiuntive), la specializzazione del formato prevale su quella generale.

5. Ad esempio, nel caso di un documento informatico contenente informazioni fiscali relative a una prestazione, cessazione di beni o servizi, le organizzazioni non devono produrlo in un qualsiasi tipo di file XML (che è altresì un formato generico per dati strutturati, anche di codesto tipo, cfr. §2.3); ne è garantita, invece la produzione sotto forma di **fattura elettronica** nello specifico formato FatturaPA (cfr. §2.14), individuato dal legislatore come il dialetto XML per quell'utilizzo specifico.

6. Si precisa che, sempre in analogia con l'indice di interoperabilità introdotto nel §3.2, il caso di pacchetti e contenitori di file va sempre considerato congiuntamente con tutte le sue parti costituenti: cioè, per i pacchetti di file, il formato del pacchetto in se, insieme ai formati di tutti i file costituenti il pacchetto stesso; per i contenitori di file, il formato della busta in se, insieme ai formati di tutti i flussi e i codec di tutte le essenze imbustate nel contenitore.

---

<sup>6</sup> Il termine "utente professionale" va inteso ai sensi del Regolamento (UE) N° 1807/2018 ([regolamento "FFnpD"](#)) del Parlamento europeo e del Consiglio relativa a un quadro applicabile alla libera circolazione dei dati non personali nell'Unione Europea.

7. Ad esempio, si consideri un contenitore multimediale<sup>7</sup> i cui formati della busta (e.g. MP4, §2.12) e quello delle essenze audio e sottotitoli (e.g., rispettivamente, WAVE e EBU STL, §2.9) sono contenute nella categoria generale, mentre il codec usato nell'essenza video (e.g. XDCAM EX) non è presente in nessun elenco, trattandosi di un codec chiuso e proprietario. In effetti un documento elettronico così formato non è riproducibile integralmente, a meno di non avere a disposizione nell'applicativo d'utilizzo (riproduttore multimediale) il codec proprietario XDCAM, la cui disponibilità pubblica è, ad oggi, limitata e potrebbe ridursi sensibilmente in futuro, a causa dell'obsolescenza del codec rispetto alle tecnologie degli applicativi, della scadenza di licenze d'uso e brevetti, nonché delle sorti dell'organizzazione che li detiene. In questo esempio, dunque, il documento elettronico non può considerarsi un file codificato, nella sua interezza, in un formato interoperabile: lo sono le tracce audio, sottotitoli e il contenitore che le imbusta, ma non lo è la traccia video e, quindi, non lo è il documento informatico nella sua interezza.

## 2. Tipi di file

1. Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questa sezione.

La sezione mantiene la medesima suddivisione per tipologie di formato delineata in §1.2.1. Per ciascun formato di file, pacchetto di file, busta o codec, ne vengono ricapitolate le caratteristiche principali in una tabella sinottica, recante:

- **nome abbreviato, acronimo** ovvero **pseudonimo** del formato (in alto a sinistra).
- **TIPOLOGIA DI FORMATO** (in alto a destra) — in particolare se si tratti di un formato di file, di busta/contenitore, di pacchetto di file, di flusso, ovvero un codec per essenze multimediali.
- icona del formato (in alto a destra) — riferimento visivo, a scopo di mera indicazione o suggestione, della riproduzione grafica di un'icona specifica per

---

<sup>7</sup> Questi file sono, comunemente ma in maniera inesatta, chiamati «file video», perché l'essenza più importante contenuta al loro interno è quella video, ovvero in questo caso «file 'MP4'» in quanto si esplicita il solo formato della busta, ignorando i codec delle essenze al suo interno, perché la busta è spesso —impropriamente— il solo oggetto cui venga una visibilità tecnica, verso l'utente, da parte del sistema operativo e di archiviazione che conserva e processa il file. Tuttavia, tali contenitori possono avere più tracce video, audio, sottotitoli — talvolta persino file di altri formati in allegato. L'integrità di tali file, che ne consente un utilizzo pieno sotto ogni aspetto tecnico, amministrativo e giuridico, è legata perciò alla possibilità di aprire e decodificare non solo la busta e una traccia video, ma tutte le essenze ivi contenute. Per questo motivo è importante sottolineare la presenza di essenze di più tipologie diverse al suo interno, ciascuna potenzialmente codificata con un codec diverso, da cui l'esigenza di nominare correttamente questi file come «contenitori multimediali».

la tipologia in oggetto (così come implementata nelle GUI dei principali sistemi operativi o software applicativi, per la riproduzione di detto formato).

- **nome completo del formato.**
- **estensione di file** — se più di una, la prima è da considerarsi raccomandata per la generazione dei file, mentre le altre sono estensioni meno comunemente usate, per le quali si raccomanda la capacità di lettura in tale formato. Nel caso dei pacchetti di file, sono invece indicate le estensioni dei formati di file che compongono obbligatoriamente il pacchetto (escludendo tutte le tipologie di formati ammessi dal pacchetto ma che non devono essere obbligatoriamente presenti all'interno).
- **Tipologia MIME** (*per i formati di file e busta*) — per i formati di file vengono indicati i possibili tipi MIME, come definiti in [RFC-6838](#), per l'identificazione del formato a prescindere dall'estensione; qualora presenti più di un tipo MIME, il primo è sempre da intendersi quale preferenziale (e dunque raccomandato per la creazione di file in questo formato). Nel caso di pacchetti di file, sono invece indicati i tipi MIME usati dai file che compongono il pacchetto. Una lista aggiornata di tipi MIME registrati si può trovare al seguente indirizzo internet: [www.digipres.org/formats/mime-types](http://www.digipres.org/formats/mime-types).
- **Derivato da** (*opzionale*) — eventuali formati di file, buste, pacchetti o codec di cui il formato è un'evoluzione ovvero, come nel caso di XML, ne rappresenti un dialetto. Possono essere indicati qui, per contenitori e pacchetti di file multimediali, l'applicabilità a uno o più schemi operativi.
- **Magic number** (*per i formati di file e busta*) — L'eventuale codice, definito nel Glossario e in §1.1.3, viene indicato nella sua codifica ASCII **così**; qualora i caratteri del *magic number* contengano caratteri speciali non alfanumerici e non diacritici, essi potranno essere indicati, *in toto* o in parte, in notazione esadecimale, come ad esempio `0x1A3F` (2 byte).
- **Profili** (*per i soli codec*) — Molti codec posseggono parametri di compressione che sono usati per “tarare” l'algoritmo a diverse esigenze. Alcuni di questi parametri possono essere impostati—in maniera più o meno rigida— su valori determinati *a priori*, andando a costituire delle pre-selezioni che prendono il nomi di “profili”, “livelli” o altro (a seconda del tipo di codec). Se rilevante o vincolante a livello di codec, può essere indicata qui la compatibilità di un codec con uno più schemi operativi (anche se uno schema operativo viene tecnicamente rafforzato al livello di contenitore o di pacchetto di file). Quando utile per distinguere ulteriormente i tipi di profilo fra loro, da un punto di vista puramente grafico, possono essere usati **anche** alcuni **colori**.
- **Codice FourCC** (*per i soli codec*) — definito in [RFC-2361](#) (oltre che in [www.fourcc.org](http://www.fourcc.org)) e nel Glossario, è usato per indicare una stringa identificativa di al più 4 caratteri alfanumerici minuscoli, indicata **così**, per distinguere i

codec audio e video usati nelle essenze per alcuni tipi di formati di busta multimediale (§2.12).

- **Sviluppato da** — Nome dell'organizzazione di standardizzazione, azienda, dicasterio governativo di competenza, società o comunità che ne detiene la proprietà intellettuale (formati proprietari), ovvero che ne mantiene lo sviluppo (formati non proprietari).
- **Tipologia di standard** — viene brevemente elencato se il formato sia codificato in qualche tipo di standard, se sia o meno aperto, proprietario (con eventuali licenze d'uso), testuale/binario, retrocompatibile, estendibile, robusto e dipendente dal dispositivo. Qualora non espressamente indicato in tale casella (rispetto alla classificazione delle tipologie di formato di cui al §1.2.1), viene implicitamente assunto che il formato sia:
  - a) non codificato in alcuno standard, né *de iure* né *de facto*,
  - b) chiuso,
  - c) proprietario con licenza d'uso vincolante sia in lettura che in scrittura,
  - d) non estendibile,
  - e) possenga modello per i metadati di livello 1,
  - f) non robusto,
  - g) *indipendente* dal dispositivo.
- **Livello metadati** — Il “livello del modello per i metadati”, come introdotto nelle *Linee guida nazionali per la valorizzazione del patrimonio informativo pubblico* emesse dall'Agenzia per l'Italia Digitale, che si riferisce alla classificazione dei metadati supportati nativamente dal formato. Si precisa che la classificazione di ciascun formato in un dato livello si riferisce all'opportunità di valorizzare *tutti* i metadati, obbligatori e facoltativi, come previsti dalle specifiche tecniche del formato stesso riportate nella tabella, alla sezione Riferimenti). Qualora non vengano valorizzati tutti i metadati facoltativi, la classificazione può attestarsi a un livello inferiore. Altresì, non viene considerata, ai fini di tale classificazione, la valorizzazione *custom* di eventuali metadati “riservati” a casi d'uso non riportati dalle specifiche (quali, ad esempio, campi riempiti da singoli fornitori con metadati di loro propria rilevanza e sintassi). Nel caso di pacchetti di file, la classificazione si riferisce ai metadati complessivamente presenti nell'insieme di file minimi costituenti il pacchetto.
- **Revisione** — viene indicata qui la versione dello standard di riferimento per le PP.AA.; la “versione di riferimento” va intesa, salvo indicazione contraria in Revisione, come la versione più recente tra quelle supportate, nel senso che:

- ◆ per le organizzazioni che *leggono* file in questo formato, è obbligatoria la leggibilità di file creati con questa versione e, con tutte le precedenti con cui tale versione è descritta come retrocompatibile (cfr. §1.2.2);<sup>8</sup>
  - ◆ per le organizzazioni che *producono* documenti in tale formato, è obbligatoria la produzione di nuovi documenti in tale versione *ovvero* – qualora non tecnicamente praticabile– con una qualunque versione precedente rispetto alla quale la versione indicata in Revisione sia descritta come retrocompatibile (cfr. §1.2.2<sup>9</sup>), *ovvero* –qualora non tecnicamente praticabile neanche ciò– con una qualunque versione successiva rispetto alla quale, però, la quella indicata in Revisione sia descritta come compatibile in avanti.
- **Riferimenti** — sono qui elencate tutte le normative di riferimento (sotto forma di leggi, regolamenti tecnici, linee guida o standard) nonché –in mancanza o a complemento di altro– *best practices* e indirizzi di siti web ove sia resa disponibile altra utile documentazione ufficiale;
  - **Conservazione** — Sono date indicazioni in merito all’utilizzo del formato per la conservazione di cui alle presenti Linee guida. In alcuni casi, il formato può essere adottato per la conservazione dei documenti informatici purché siano adottate specifiche configurazioni, eventualmente indicate qui. Infine, è indicato in questo campo (con la dicitura “cfr. §2.8”), l’eventuale attenzione all’uso di caratteri tipografici non interoperabili.
  - **Racc. per la lettura** — raccomandazioni per le PPA.A. relativamente alla capacità di leggere documenti informatici nel dato formato, oltre che eventuali obblighi normati dalle Linee guida di cui questo Allegato è parte integrante;
  - **Racc. per la scrittura** — raccomandazioni per le PPA.A. relativamente alla capacità di formare documenti informatici nel dato formato, oltre che eventuali obblighi previsti dalle Linee guida di cui questo Allegato è parte integrante. In tale sezione sono collocate anche indicazioni in merito all’uso di tale formato per la conservazione, così come trattata nelle presenti Linee guida.

Ciascun formato può essere ulteriormente descritto, particolarmente riguardo alle raccomandazioni e agli eventuali obblighi, in una parte discorsiva successiva alla tabella sinottica.

---

<sup>8</sup> Se, ad esempio, è raccomandata la versione 3.0 di un dato formato di file, che è definito come una variante della versione 2.0 tale che qualunque lettore in grado di leggere la 3.0 leggerà anche la 2.0, l’obbligo in lettura si applica anche alla versione 2.0.

<sup>9</sup> Se, utilizzando il precedente esempio, è raccomandata la versione 3.5 di un dato formato di file ma qualunque applicazione in grado

2. Si rimanda al Regolamento (UE) N°679/2016 (“GDPR”) del Parlamento europeo e del Consiglio in materia di trattamento dei dati personali che, rappresentati in un documento informatico, possono essere soggetti a *pseudonimia*, come metodologia atta a proteggerli, aggiornarli, cancellarli. La scelta dei formati di file da utilizzare può discendere anche dall’implementazione di tecnologie e procedure allo scopo di ottemperare agli obblighi imposti in capo al GDPR.

3. Si rimanda al Regolamento (UE) N° 1807/2018 (regolamento “FFnpD”) del Parlamento europeo e del Consiglio relativa a un quadro applicabile alla libera circolazione dei dati non personali nell’Unione Europea, per quanto riguarda ulteriori considerazioni in merito sia alla localizzazione geografica dei documenti informatici, alla loro portabilità e alle distinzioni tra utilizzo e utenti professionali di dati non personali.

4. Si rimanda alle *Linee guida sull’accessibilità* e alle *Linee guida di design* per le considerazioni sulla rappresentazione di elementi testuali e grafici nei documenti elettronici, cui le P.P.AA. si attengono per la produzione di documenti informatici. Come mero esempio, tali considerazioni possono riguardare i criteri di scelta:

- delle famiglie di caratteri tipografici (§2.8) e del loro corpo;
- dell’inclusione di un elemento grafico come immagine vettoriale (§2.6) ovvero *raster* (§2.7).

5. Il primo criterio di scelta è di particolare pertinenza con la formazione dei documenti informatici, in quanto in moltissime tipologie elencate nel §2 (non solo i documenti impaginati, bensì anche le pagine web, i fogli di calcolo, le presentazioni multimediali, le immagini vettoriali e la modellazione digitale, nonché i sottotitoli) il tipo di carattere è parte integrante del documento perciò, qualora il carattere tipografico non sia presente o non sia interpretabile dal sistema informativo che visualizza il documento, ciò può comportare una difformità o addirittura l’impossibilità di leggere lo stesso.

6. Nel caso di documenti la cui rappresentazione o utilizzo (si pensi, ad esempio, non soltanto a documenti impaginati, bensì a documenti multimediali) dipendano dalle caratteristiche tecniche del formato scelto e delle modalità con cui il documento viene specificatamente formato, le considerazioni di cui alle sopracitate Linee guida saranno valutate allo scopo di incrementare l’interoperabilità e l’accessibilità dei documenti.

7. Proprio in considerazione dei precedenti 2, 4, 5 e 6, le P.P.AA. possono includere nella valutazione di interoperabilità (cfr. §3.1) le considerazioni relative alla scelta dei formati dei file, delle modalità con cui i documenti vengono formati usando determinati formati (profili, impostazioni o configurazione del sistema di formazione del file, ecc.).

8. Nel caso di formati di file che permettano di scegliere i caratteri tipografici da utilizzare salvando tali scelte come parte del documento informatico stesso, qualora

i caratteri tipografici non facciano anch'essi parte del documento informatico, le PP.AA. adotteranno tutte le misure necessarie per la scelta di caratteri tipografici di uso comune, affinché la visualizzazione del documento sia il più possibile indipendente dai caratteri tipografici.

9. La raccomandazione di cui al punto 8 viene richiamata, nelle successive schede tecniche dei formati di file, mediante l'indicazione del capitolo sui caratteri tipografici, cioè con la semplice dicitura “cfr. §2.8”, alla voce “Livello metadati”.

## 2.1 Documenti impaginati

1. I formati “orientati alla pagina”, o “impaginati”, suddividono un documento informatico in unità separate chiamate *fogli*, in quanto il loro utilizzo primario è la carta stampata, come mezzo di origine (tramite scansione di documento cartaceo) ovvero di destinazione (tramite stampa). Non tutti i documenti impaginati sono però concepiti per la stampa, esibendo anzi caratteristiche tipiche del mondo digitale, quale la possibilità di allegare contenuti multimediali o anche di altro genere, così come di collegamenti di tipo URL a altre posizioni nella rete internet, intranet o in altro sistema di gestione dei documenti, in modo che l'utente possa accedervi tipicamente dopo aver attivato il collegamento di riferimento.

2. La pagina va inoltre considerata come un'entità virtuale — dunque non legata alla bidimensionalità e staticità di una superficie fisica di stampa. Con l'eccezione di alcuni formati nati ed evoluti esclusivamente nell'ambito della stampa tradizionale, e.g. il formato PostScript<sup>®</sup>, che dunque sono tecnicamente vincolati a rappresentare esclusivamente elementi direttamente stampabili (quali testi, disegni, immagini statiche), i formati più evoluti quali il PDF possono rappresentare dati multimediali, elementi interattivi o persino includere altri file all'interno di un documento impaginato (si legga la sezione corrispondente).

3. In formati di questo tipo viene descritta anche la “presentazione” (cioè la rappresentazione visuale) dei contenuti informativi all'interno delle pagine, utilizzando stili di visualizzazione di ipertesti (cfr. §2.2), immagini (raster o vettoriali, cfr. §2.6 e §2.7) e altre tecniche tipografiche, quali i caratteri tipografici (§0), che possono essere riferiti sia internamente nel medesimo file e che contiene dunque, al suo interno, un insieme completo o parziale di glifi.

PDF		FORMATO DI FILE
Nome completo	Portable Document Format	
Estensione/i	.pdf	
Magic number	%PDF	
Tipo MIME	application/pdf	
Sviluppato da	Adobe Systems	

Tipologia di standard	aperto (2.0)/proprietario (libero 1.7), estendibile, <i>de jure</i>
Livello metadati	4
Derivato da	Adobe® PostScript®
Revisione	2.0 (2017)
Riferimenti	Famiglie di standard <b>32000</b> e <b>19005</b> della ISO/IEC: <ul style="list-style-type: none"> <li>• <a href="#">32000-2:2017</a>, <i>PDF v2.0</i></li> <li>• <a href="#">32000-1:2008</a>, <i>PDF v1.7</i></li> <li>• <a href="#">19005-1:2005</a>, <i>PDF/A-1</i> (v1.4)</li> <li>• <a href="#">19005-2:2011</a>, <i>PDF/A-2</i> (v1.7)</li> <li>• <a href="#">19005-3:2012</a>, <i>PDF/A-3</i> (v1.7)</li> <li>• Adobe, <a href="#">Supplement to PDF v1.7 Extension 3</a>, ©2008</li> <li>• Adobe, <a href="#">Document management - PDF 1.7</a>, ©2008</li> <li>• ISO <a href="#">24517-1:2008</a>, <i>PDF/E-1</i> (v1.6)</li> <li>• ISO <a href="#">15930-1:2001</a>, <i>PDF/X-1</i> e <i>PDF/X-1a</i> (v1.4)</li> <li>• ISO <a href="#">15930-8:2010</a>, <i>PDF/X-5</i> (v1.6)</li> <li>• ISO <a href="#">14289-1:2014</a>, <i>PDF/UA-1</i> (v1.4)</li> <li>• ISO/CD <a href="#">14289-2</a>, <i>PDF/UA-2</i> (v2.0)</li> <li>• ISO <a href="#">16612-2:2010</a>, <i>PDF/VT-1</i> e <i>PDF/VT-2</i> (<i>PDF/X-4</i> e <i>/X-5</i>)</li> <li>• ISO/CD <a href="#">16612-3</a>, <i>PDF/VT-3</i> (<i>PDF/X-6</i>) (v2.0)</li> </ul>
Conservazione	Sì, solo profili PDF/A e PDF/B; altrimenti, cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio (v1.x).
Racc. per la scrittura	Raccomandata: v1.7+. Obbligatoria: v1.4+. Profili raccomandati (leggere raccomandazioni più sotto): PDF/A-2a, PDF/A-2u, PDF/A-2b, PDF/A-1a, PDF/A-1b. Profili PDF/A e PDF/B adatti alla conservazione.

4. Il formato PDF è il “principe” dei formati per documenti impaginati. Nato come formato proprietario (sviluppato da Adobe Corporation), è stato rapidamente adottato come standard *de facto* per la produzione digitale del cartaceo; nel 2008 è diventato uno standard *de iure*, con il nome di ISO [32000-1](#) (PDF versione 1.7); successivamente rivisto nel 2017, con il nome di ISO [32000-2](#) (PDF versione 2.0). Il formato PDF è estremamente versatile in quanto è stato continuamente aggiornato nel tempo aggiungendo nuove funzionalità. Allo stato attuale (PDF versione 2.0) è possibile includere nel documento evidenze di vario tipo (incluse immagini, audio, video, modelli tridimensionali animati), imbustare all’interno del file di qualsivoglia formato sotto forma di “allegati”, sovraimprimere graficamente alle pagine moduli interattivi che permettono all’utente compilazione libera o vincolata (per poi salvarne un’istanza con i campi riempiti). È anche possibile proteggere un documento PDF con password o firme elettroniche e usare la crittografia per

limitarne la lettura o la modifica, anche se tale protezione è aggirabile con appositi strumenti software.

5. L'apposizione di firme e sigilli elettronici su documenti in formato PDF è effettuata mediante la busta crittografica PAdES (cfr. §2.16), mentre il servizio fiduciario elettronico costituito dalla convalida di documenti in formato PAdES è sancito dalla normativa comunitaria.

6. Il PDF è uno standard “modulare”, nel senso che sono stati definiti **profili** diversi che introducono insiemi aggiuntivi di nuove funzionalità (quali quelle sopra elencate), ovvero vincolano alcune di esse allo scopo di migliorare l'interoperabilità del documento PDF in specifici ambiti. I profili possono prevedere sotto-profili con ulteriori specifiche (additive o vincolanti), chiamati **livelli di conformità**. Si noti inoltre che un file PDF può essere conforme a più livelli (profili o sotto-profili) contemporaneamente. I profili e sotto-profili ufficialmente riconosciuti sono i seguenti:

- **PDF/A** (*archival*) — Profilo particolarmente adatto alla creazione di documenti di cui deve essere garantita la leggibilità in caso di archiviazione a lungo termine e conservazione. Si divide in due sotto-profili:
  - **PDF/A-1** — Basato su PDF versione 1.4, impedisce al file di contenere (graficamente o come allegati) niente altro che testi, ipertesti, immagini *raster* o vettoriali; sono in particolar modo vietati i moduli con contenuti variabili (e.g. codice Java eseguibili). Infine, il formato contenere al suo interno tutti i caratteri tipografici utilizzati.
    - **PDF/A-1a** (*accessible*) — Specifica “forte” del sotto-profilo PDF/A-1, ove ad ogni contenuto non testuale del file è garantita piena coerenza semantica e accessibilità (p.es. ogni immagine deve avere un commento, ed ogni glifo un codice UNICODE); questo consente non solo una visualizzazione del file a lungo termine, ma anche un suo utilizzo da parte di *parser* e di lettori del documento per persone diversamente abili.
    - **PDF/A-1b** (*basic*) — Specifica “debole” del sotto-profilo PDF/A-1, ove non è richiesta la presenza di dati semantici come in PDF/A-1a.
  - **PDF/A-2** — Basato su PDF versione 1.7, è dotato di tre livelli di conformità:
    - **PDF/A-2a** — analogo a PDF/A-1a.
    - **PDF/A-2b** — analogo a PDF/A-1b.
    - **PDF/A-2u** — analogo a PDF/A-2b, ma con il vincolo aggiuntivo che tutti i caratteri impiegati devono essere codificati in base alla mappatura UNICODE.

- **PDF/A-3** — Sotto-profilo poco usato che aggiunge, rispetto a PDF/A-2, la possibilità di allegare file di qualsiasi tipo.
- **PDF/E** (*engineering*) — Profilo dedicato all'inclusione di disegni e altri dati tecnici nel PDF (versione 1.6), quali informazioni geografiche, e modelli grafici tridimensionali interattivi.
- **PDF/H** (*health*) — Inclusione di dati sanitari (sotto forma di XML) quali referti, sondaggi, testi di laboratorio o altri sistemi diagnostici.
- **PDF/X** (*graphics exchange*) — Interscambio professionale di contenuti grafici (sia *raster* che vettoriali, cfr. §2.6 e §2.7 rispettivamente)
  - **PDF/X-1** — Sotto-profilo basato su PDF versione 1.3.
    - **PDF/X-1a** — Variante in cui devono essere incluse tutte le fonti tipografiche, mentre i colori sono codificati in spazio-colore CMYK o come colori *spot*<sup>10</sup>.
  - **PDF/X-3** — Sotto-profilo (basato su PDF versione 1.3) che include capacità colorimetriche avanzate, come ad esempio ammettere, oltre a colori *spot*, spazi-colore CMYK, CIELAB, RGB (calibrati o meno), profili ICC.
  - **PDF/X-4** — Ulteriore evoluzione del sotto-profilo PDF/X-3 (basato su PDF versione 1.4) che include anche le trasparenze.
  - **PDF/X-5** — Ulteriore evoluzione del sotto-profilo PDF/X-5 (basato su PDF versione 1.6), con una ulteriore distinzione: **PDF/X-5g**, **PDF/X-5pg** e **PDF/X-5n**.
- **PDF/UA** (*universal accessibility*) — Profilo dedicato all'accessibilità universale, che comprende ad esempio l'ordine con cui devono comparire commenti e note, le didascalie per i contenuti extra meno accessibili (ad es. foto o video), i requisiti per permettere a tecnologie di accessibilità di gestire tutte le parti del documento (incluse quelle criptate).
- **PDF/VT** (*variable and transactional printing*) — Profilo dedicato a PDF che andranno stampati con parti variabili da tiratura a tiratura (ad es. il numero seriale progressivo in ogni esemplare a tiratura limitata).
  - **PDF/VT-1** — Variante in cui tutte le parti sono auto-contenute in un singolo file PDF (compatibile con PDF/X-4).
  - **PDF/VT-2** — Variante in cui è contemplato l'uso di elementi grafici contenuti in file esterni (compatibile con PDF/X-5)

---

<sup>10</sup> Un colore *spot* è indicato digitalmente da un semplice codice corrispondente, nei plotter e stampanti professionali, ad un particolare inchiostro che viene inserito appositamente. I colori *spot* possono prevedere qualità colorimetriche non visibili digitalmente (p.es. colori lucidi, opachi, metallizzati, perlati, ruvidi), così come essere associati, in particolari processi di stampa, a lavorazioni completamente diverse nella zona dell'impaginazione digitalmente indicata come da stampare con un dato color *spot*.

- **PDF/VT-2s** — Ulteriore variante in cui sono ammessi contenuti presi da flussi digitali esterni al PDF stesso (p.es. dati provenienti da un sensore).

7. Come riportato nella scheda tecnica del formato PDF, a prescindere dalla tipologia di contenuto (e quindi dall'eventuale conformità con altri profili), la produzione di file in formato PDF privilegia, ove disponibile, la più recente versione conforme allo ISO [32000-2](#), adottando preferenzialmente i suoi i profili di accessibilità, con il seguente ordine di preferenza: PDF/A-2a, PDF/A-2u, PDF/A-2b. Qualora non siano disponibili strumenti per la produzione di documenti PDF conformi alla versione 2.0, si utilizza la versione più recente disponibile, preferendo le versioni conformi allo ISO [32000-1](#) (PDF versione 1.7 e successive), in nessun caso inferiori al PDF versione 1.4, adottando i profili di accessibilità con il seguente ordine di preferenza: PDF/A-1a, PDF/A-1b. La ragione principale di tale ordine di preferenza risiede nella maggiore versatilità del PDF versione 1.7 e successive nel:

- includere documenti (anche non in formato PDF), come *allegati* al PDF stesso;
- permettere l'utilizzo di campi modulo senza incidere sulla validità di firme o sigilli elettronici senza invalidare l'integrità del documento stesso, né tantomeno delle firme o sigilli elettronici PAdES eventualmente apposti;

8. L'obbligo di cui al precedente capoverso può essere disatteso per i documenti PDF prodotti per essere specificatamente modificati ovvero “compilabili” in un momento successivo alla loro produzione, come ad “modelli” o *template* per procedimenti amministrativi di varia natura. Tuttavia, le P.P.AA. producono il documento compilabile e modificabile in formato PDF, usando versioni e profili adeguati, tenendo conto che una volta compilati o redatti in forma definitiva, tali file costituiranno documenti informatici (nel senso della rilevanza degli atti, fatti o dati giuridicamente rilevanti contenuti nella versione modificata o compilata). Si raccomanda, ad esempio, di utilizzare per file PDF compilabili o modificabili, solamente caratteri tipografici tra quelli interoperabili “standard” definiti nel §2.8.

9. I documenti che sono imm modificabili salvo per la compilazione di campi vuoti o l'apposizione di firme o sigilli elettronici devono essere prodotti in formato PDF versione almeno pari a 1.7, sfruttando i campi modulo e la loro robustezza, come già esposto al punto 7.

WORD® 2007		FORMATO DI FILE
Nome completo	WordProcessingML OOXML Extension	
Estensione/i	.docx, .dotx	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.openxmlformats-officedocument.wordprocessingml.document application/vnd.openxmlformats-officedocument.wordprocessingml.template	

Sviluppato da	Microsoft Corporation; ISO; ECMA
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , <i>testuale</i>
Livello metadati	3
Derivato da	Office Open XML; Microsoft® Word®
Revisione	11.1 (2018)
Riferimenti	<ul style="list-style-type: none"> <li>• Microsoft, <a href="#">Word extensions to OOXML (.docx) file format v11.1</a> (2018)</li> <li>• <a href="#">officeopenxml.com</a>, <i>Anatomy of a WordProcessingML file</i></li> </ul>
Conservazione	Sì, solo profilo <b>Strict</b> ; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Vedasi capoversi 10 e 11 per la conservazione.

9. La suite di applicativi Microsoft® Office®, dalla versione 2007 in poi, utilizza un formato di file unico per i suoi applicativi principali, chiamato Open Office XML (OOXML, descritto più genericamente in §2.5). Il formato consiste in un pacchetto di file, suddiviso in più cartelle, imbustato e compresso con un algoritmo ZIP e presentato come un unico file. I file all'interno del pacchetto compresso sono prevalentemente in formato XML e utilizzano il dialetto WordprocessingML, riservato ai documenti di videoscrittura elaborati dall'applicativo Word® per definire l'intera struttura e il contenuto del documento. Eventuali documenti allegati (p.es. immagini, video, audio o altri file) sono inseriti, all'interno di opportune cartelle, nel loro formato nativo. L'estensione del documento compresso per gli impaginati normali (*senza macro* attive) è .docx, mentre altri tipi di documenti (p.es. modelli di documento, impaginati con *macro* attive) sono indicati semplicemente con estensioni diverse.

10. Come per altri formati basati su OOXML, si consiglia la produzione di documenti con il profilo Strict, che è più restrittivo ma consente di eliminare alcune estensioni “proprietarie” che possono ridurre l'interoperabilità del formato stesso.

11. Il documento è adatto alla conservazione solo se:

- sono utilizzati esclusivamente caratteri tipografici “standard” (cfr. §2.8 capoverso 2),
- è privo di contenuti dinamici ad eccezione di campi compilabili o campi-firma,
- è privo di contenuti audiovisivi (suoni, video),
- eventuali immagini o altri contenuti multimediali sono contenute direttamente nel documento e non mediante collegamenti a file esterni al documento.

Si consiglia inoltre di effettuare un controllo sull'intera accessibilità del documento.

MS-DOC		FORMATO DI FILE
Nome completo	Microsoft® <i>Word</i> ® Binary File Format	
Estensione/i	.doc, .dot	
Magic number	0xD0CF11E0A1B11AE1	
Tipo MIME	application/msword	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , binario, deprecato	
Livello metadati	3	
Derivato da	Microsoft® Compound File Binary format; Corel® <i>WordPerfect</i> ™	
Revisione	8.1 (2018)	
Riferimenti	• Microsoft, <a href="#">[MS-DOC]: Word (.doc) binary file format v8.1 (2018)</a>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Obbligatorio con riversamento raccomandato	
Racc. per la scrittura	Sconsigliato	

12. Il formato binario *Word*®, utilizzato come formato principale fino alle versione 2003 da codesto applicativo di videoscrittura, è una variante specializzata del formato Compound File Binary, proprietario di Microsoft Corporation (cfr. §2.5); utilizza l'estensione .doc per il documenti impaginati normale, e la cambia in caso di varianti, quali ad esempio i modelli di documento (estensione .dot). Il formato contiene in un unico file i metadati, i contenuti testuali, ipertestuali e gli allegati dell'impaginato, senza offrire efficaci meccanismi di controllo dell'integrità. Inoltre, le revisioni al documento vengono in generale salvate come modifiche differenziali in coda al file, contribuendo ad ingrandire la dimensione del file e, al tempo stesso, renderne più complessa l'apertura e l'interpretazione da parte degli applicativi di videoscrittura. Per questa mancanza di robustezza (soprattutto in caso di documenti di dimensioni molto grandi a causa di contenuti multimediali allegati), l'azienda proprietaria del formato decide di cambiare strategia, adottando un nuovo formato per tutti i documenti della suite applicativa *Office*®, a partire dalla versione 2007, anche se il "formato .doc" è pienamente supportato dalle nuove versioni. In caso di produzione di nuovi documenti impaginati tramite *Word*® si raccomanda l'uso del nuovo, sopra descritto formato basato su Open Office XML.

ODT		FORMATO CONTENITORE
Nome completo	Open Document Text	
Estensione/i	.odt	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.oasis.opendocument.text	
Sviluppato da	Organization for the Advancement of Structured Information Standards	

Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC: <ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">26300-1:2015</a>, <i>ODF for Office Applications v1.2 – Part 1: OpenDocument Schema</i></li> <li>• ISO/IEC <a href="#">26300-3:2015</a>, <i>ODF for Office Applications v1.2 – Part 3: Packages</i></li> <li>• OASIS, <a href="#">Open Document Format for Office Applications (OpenDocument)</a>, v1.2 (2015)</li> </ul>
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Fortemente raccomandato

13. Il formato OpenDocument Text (ODT) è una particolare implementazione del più generale formato OpenDocument (cfr. §2.5). Esso è il formato di default usato dall'applicazione di videoscrittura *Writer* della suite open source *LibreOffice*, ma è ampiamente supportato da molti altri applicativi di videoscrittura. Come per l'Open Office XML, anche tale formato è costituito da una busta compressa ZIP contenente un pacchetto di file che descrive la composizione del documento, cui componenti principali sono in formato XML.

RICHTEXT	FORMATO DI FILE	
Nome completo	Rich Text Format	
Estensione/i	.rtf	
Magic number	{\rtf1	
Tipo MIME	text/rtf, application/rtf	
Sviluppato da	Microsoft	
Tipologia di standard	proprietario (libero), <i>de facto</i> , binario, deprecato	
Livello metadati	1	
Derivato da	Rich-Text; Enriched Text	
Revisione	1.9.1 (2008)	
Riferimenti	<ul style="list-style-type: none"> <li>• Microsoft, <i>Word 2007: Rich Text Format (RTF) Specification</i> v1.9.1 (2008)</li> <li>• <a href="#">RFC-1521</a></li> </ul>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Generico con riconoscimento consigliato	
Racc. per la scrittura	Non raccomandato	

14. Rich Text Format (RTF) è un formato di proprietà di Microsoft utilizzato come formati interoperabile di documenti impaginati. Il formato supporta un numero molto ridotto di caratteristiche grafiche e tipografiche, e una possibilità limitata relativamente a ipertesti e allegati multimediali, a fronte di una semplicità strutturale conforme con lo scopo della sua introduzione. Nonostante sia ancora supportato dai principali applicativi di videoscrittura (inclusi quelli installati di default nei principali sistemi operativi), ma seguito della standardizzazione e apertura di formati ben più evoluti e completi (cfr. quelli basati su OOXML e OpenDocument) e, se ne sconsiglia l'uso per la produzione di nuovi documenti.

EPUB		FORMATO DI FILE
Nome completo	EPUB	
Estensione/i	.epub	
Specializzazione di	HTML, CSS, XML, SVG, ... imbustati dentro ZIP	
Tipo MIME	application/epub+zip	
Sviluppato da	International Digital Publishing Forum	
Tipologia di standard	aperto, estendibile, <i>de facto</i>	
Livello metadati	3; cfr. §2.8	
Derivato da	Open eBook publication structure; XHTML; CSS	
Revisione	3.1 (2017)	
Riferimenti	Famiglia di standard <b>30135</b> della ISO/IEC: <ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">30135-1:2014</a>, <i>EPUB Part 1: EPUB3 overview</i></li> <li>• ISO/IEC <a href="#">30135-3:2014</a>, <i>EPUB Part 3: content documents</i></li> <li>• ISO/IEC <a href="#">30135-5:2014</a>, <i>EPUB Part 5: media overLay</i></li> <li>• <a href="http://www.idpf.org/epub">www.idpf.org/epub</a></li> </ul>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Generico con riconoscimento consigliato	
Racc. per la scrittura	Raccomandato nell'editoria digitale	

15. Il formato EPUB è costituito da un pacchetto di file che descrivono, complessivamente, una documento paginato comprensivo dei suoi allegati multimediali, compressi con compressione ZIP in un unico file con estensione .epub. I documenti prediletti da questo formato si chiamano anche eBook, in quanto si prestano ad una visualizzazione prevalentemente elettroica su dispositivi con diverse

capacità di visualizzazione grafica, anche notevolmente ridotta, come ad esempio *smartphone* e *tablet* (inclusi gli *eBook reader* specializzati).<sup>11</sup>

All'interno di questo pacchetto, i metadati interni del documento sono contenuti in file XML, il contenuto testuale in uno o più file HTML, le sue impostazioni tipografiche in uno o più file CSS, e gli eventuali elementi grafici in file immagini di vari formati aperti (PNG, SVG, ecc.). La versatilità grafica dell'*eBook* è ottenuta da questo formato sfruttando le caratteristiche di adattamento ed "elasticità" dei contenuti HTML dotati di opportuni "stili" CSS (cfr. §2.2) basati su profili di dispositivo apposito.

INDESIGNML		FORMATO DI FILE
Nome completo	Adobe® <i>InDesign</i> ® Markup Language	
Estensione/i	.idml	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/x-indesign+xml	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario (libero), <i>de facto</i> , testuale	
Livello metadati	4	
Derivato da	Adobe® <i>InDesign</i> ® file format (.indd)	
Revisione	8.0 (2012)	
Riferimenti	<ul style="list-style-type: none"> <li>• Adobe, <a href="#">IDML File Format Specification, v8.0 (2012)</a></li> <li>• Adobe, <a href="#">InDesign® Developer Documentation</a></li> </ul>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Specifico; non raccomandato se non in editoria digitale	
Racc. per la scrittura	Specifico; raccomandato (al posto di .indd) nel settore dell'editoria digitale <i>InDesign</i>	

16. Adobe® *InDesign*® è uno degli applicativi più diffusi per l'editing grafico, ma è un applicativo commerciale non aperto, come il formato nativo e binario per i suoi impaginati (estensione .indd). Tale formato è inoltre altamente instabile in quanto Adobe, che lo mantiene, lo cambia in continuazione da una variante all'altra del software. Per ridurre i rischi di interoperabilità dovuti all'estrema variabilità del formato nativo ".indd", Adobe ha introdotto una variante del formato basato su XML e chiamato *InDesign*® Markup Language (estensione .idml). Tale versione, oltre ad essere testuale ed estendibile, è anche parzialmente pubblicata sul sito Adobe, ed

<sup>11</sup> Ad esempio lo stesso *eBook* visualizzato su due dispositivi elettronici con display tecnicamente diversi (un *e-paper* monocromatico da 800×600 punti a 167dpi, rispetto a un LCD a colori da 1920×1080 — cfr. §2.6) potrebbe essere visualizzato con caratteri tipografici simili (magari di dimensioni diverse) e con una diversa distribuzione di caratteri su ogni linea allo scopo di rendere l'esperienza di lettura più agevole e la fruibilità più simile a quella di un libro su carta stampata.

è perciò consigliato come il formato d'elezione –al posto del formato nativo– per tutte le organizzazioni che archivino impaginati creati con *InDesign*<sup>®</sup>.

POSTSCRIPT™		FORMATO DI FILE
Nome completo	PostScript®	
Estensione/i	.ps	
Magic number	%!PS	
Tipo MIME	application/postscript	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario (libero), <i>de facto</i> , binario, deprecato	
Livello metadati	1	
Derivato da	Lisp	
Revisione	3 (1997)	
Riferimenti	<ul style="list-style-type: none"> <li>• Adobe, <i>PostScript® Language reference</i>, 3<sup>rd</sup> ed. (1999)</li> <li>• Adobe, <i>PostScript® Language reference supplement: Adobe® PostScript® 3™ version 3010 and 3011 Product Supplement</i>, 30 August 1999</li> </ul>	
Conservazione	No	
Racc. per la lettura	Raccomandato per l'editoria digitale	
Racc. per la scrittura	Sconsigliato	

17. Il formato PostScript™ deve il suo nome all'omonimo linguaggio di descrizione di pagine professionale. Come per i formati contenenti codici scritti in un linguaggio di programmazione, questo formato di file contiene un elenco ordinato di istruzioni in tale linguaggio PostScript™ (linguaggio di tipo pseudo-binario) che, eseguite una dopo l'altra da una stampante o altro dispositivo capace di interpretarle, hanno come effetto la stampa di un documento esattamente identico. Il PostScript™ è stato per anni uno dei linguaggi di riferimento per il trasporto e la conservazione di documenti finalizzati alla stampa digitale, sia di tipo testuale che grafico. La versatilità del formato è anche parte del motivo per cui lo standard PDF è basato su PostScript™. Ai formati per la produzione di documenti impaginati o altri tipi di stampa digitale, è tuttavia richiesto di supportare anche ipertesti e contenuti non strettamente stampabili (suono, video ,ecc.), per i quali tale formato, risultando dunque inadeguato, diviene obsoleto. Nonostante la grande varietà di documenti attualmente presenti salvati in questo formato (per il quale la capacità di lettura è ancora fortemente raccomandata alle organizzazioni di settore tecnico-editoriale), si sconsiglia di produrne degli altri, preferendovi formati più moderni. Gli applicativi dedicati alla formazione del documenti in tali formati al posto del PostScript™, così come gli applicativi di riversamento dal PostScript™ in questi formati devono tuttavia essere adeguatamente configurati affinché i documenti mantengano le caratteristiche di riproducibilità e qualità che il formato PostScript™ garantisce per

sua natura, permettendo al contempo di includere funzionalità moderne nel documento, quali contenuti ipertestuali e multimediali. Esempi di tali funzionalità sono la rappresentazione delle immagini in modalità vettoriale o, qualora le immagini siano di tipo raster, garantire qualità equivalente (ad esempio mediante algoritmi di compressione senza perdita); cfr. §2.6 e §2.7.

L <sup>A</sup> T <sub>E</sub> X		FORMATO DI FILE
Nome completo	LaTeX	
Estensione/i	.tex	
Specializzazione di	TeX	
Tipo MIME	application/x-tex	
Sviluppato da	comunità open source	
Tipologia di standard	aperto (licenza <a href="#">LPPL</a> ), estendibile, <i>de facto</i> , testuale	
Livello metadati	1	
Derivato da	T <sub>E</sub> X	
Revisione	2 <sub>ε</sub>	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.latex-project.org">www.latex-project.org</a></li> <li>• <a href="https://github.com/latex3">github.com/latex3</a></li> <li>• <a href="http://ctan.org">ctan.org</a> (Comprehensive T<sub>E</sub>X Archive Network)</li> </ul>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Specifico; raccomandato per testi tecnico-scientifici	
Racc. per la scrittura	Specifico; nessuna raccomandazione	

18. L<sup>A</sup>T<sub>E</sub>X è la specializzazione più comunemente più usata del linguaggio di impaginazione testi denominato T<sub>E</sub>X, inventato nel 1979 da Donald Knuth. La versione attualmente in uso è la 2<sub>ε</sub> (denominata L<sup>A</sup>T<sub>E</sub>X2<sub>ε</sub>). In realtà, l’albero “glottologico” del T<sub>E</sub>X comprende dialetti derivati direttamente dal linguaggio-madre T<sub>E</sub>X, così come dal L<sup>A</sup>T<sub>E</sub>X stesso, come ad esempio [AMS-L<sup>A</sup>T<sub>E</sub>X](#).

Come suggerisce il nome stesso, L<sup>A</sup>T<sub>E</sub>X è particolarmente efficace per la produzione di pubblicazioni tecnico-scientifiche pronte per la stampa e conformi a norme redazionali e tipografiche professionali. Ciò che ne ha determinato particolare diffusione nella comunità scientifica internazionale (nonostante la sua obsolescenza rispetto sia a linguaggi per ipertesti più evoluti come l’XML e a formati di documenti impaginati “WYSIWYG”,<sup>12</sup> che permettono una visualizzazione diretta dei contenuti) sta, in prima istanza, nella capacità –innata nel T<sub>E</sub>X e contemporaneamente potenziata e semplificata nel L<sup>A</sup>T<sub>E</sub>X– di descrivere complesse formule matematiche, la cui tipografia è rigorosamente rappresentata con leggibilità superiore ad applicativi di videoscrittura da “ufficio”. Il linguaggio, di per sé, si limita

<sup>12</sup> Acronimo dall’inglese «*what you see is what you get*» (parafrasabile in «esattamente così come lo vedi»).

a descrivere la distribuzione di testi e ipertesti (immagini, tabelle, formule/equazioni, bibliografia, note, così come i loro riferimenti) all'interno del documento, contornati da *tag* che si riferiscono a *template* esterni contenenti le regole stilistiche e tipografiche da rispettare (come ad esempio le fonti, cfr. §2.8). Il documento L<sup>A</sup>T<sub>E</sub>X è, in questo senso, analogo al codice sorgente di un linguaggio di programmazione o scripting (cfr. §2.15): ha bisogno di essere *compilato* per produrre un documento informatico consultabile e completamente impaginato, che si raccomanda sia prodotto sempre nel formato PDF o comunque –ove ciò non sia possibile– in uno dei formati raccomandati in questo paragrafo per la produzione di documenti impaginati.

È attualmente in sviluppo una revisione maggiore delle specifiche, denominata L<sup>A</sup>T<sub>E</sub>X3, che modifica diversi aspetti (sia dal punto di vista lessicale che grafico), allo scopo di aggiornare questo linguaggio e integrarlo con le tecnologie allo stato dell'arte nel campo della tipografia, dell'editoria e della multimedialità che, semplicemente, non esistevano negli anni '80 e la cui integrazione nel T<sub>E</sub>X e nei dialetti derivati è solo parzialmente avvenuta, non senza numerose difficoltà tecniche.

## 2.1.1 Raccomandazioni per la produzione di documenti

1. Il formato raccomandato per la produzione di documenti informatici in senso stretto (quindi, tra le altre cose, non più modificabili) il formato raccomandato è il PDF/A-1 per via della maggiore “superficie di interoperabilità”; il PDF in generale è comunque il formato più raccomandato per i documenti impaginati, inclusi quelli che devono rimanere parzialmente compilabili o commentabili (come i moduli delle procedure amministrative).
2. Le caratteristiche avanzate quali l'apposizione di firme e sigilli elettronici anche multipli (si veda il formato PAdES, §2.16), l'inclusione di documenti (anche in formati diversi) come *allegati* di un unico file PDF, l'inclusione di essenze multimediali e modelli bi- o tri-dimensionali manipolabili in tempo reale all'interno del documento, lo rendono particolarmente versatile in molteplici occasioni.
3. Per quanto riguarda i formati di documenti impaginati che possono essere revisionati e modificati, o dai quali si possono derivare altri documenti, si raccomanda siano prodotti in formato OpenDocument (.odt), interoperabilmente utilizzabile dai principali applicativi di videoscrittura e, laddove non sia possibile, nel formato OOXML (.docx), ma con profilo Strict. Nel caso di documenti semilavorati a carattere temporaneo e non definitivo è consigliabile anche l'utilizzo di formati

puramente “virtuali” quali quelli delle suite collaborative di fornitori di servizi in Cloud qualificati.

4. Per applicazioni specifiche, come l’editoria, la grafica o le pubblicazioni tecnico-scientifiche, possono essere raccomandabili anche altri formati definiti in questa sezione purché, in fase di conservazione, si valuti sempre l’interoperabilità del documento finito (a scopo di distribuzione attraverso vari mezzi di comunicazione) e della sua sorgente così (come generata da applicativi di videoscrittura o altro), in quanto tali requisiti potrebbero portare a differenti raccomandazioni di formato.

## 2.2 Iper testi

1. Rientrano in questa categoria tutti i documenti, prevalentemente testuali, che contengono iper testi, quali ad esempio riferimenti ad oggetti esterni (di tipo URI, URL o altro), ovvero codici di *markup* per rappresentare digitalmente insieme astratti di dati e loro ontologie.

XML		FORMATO DI FILE
Nome completo	Extensible Markup Language	
Estensione/i	.xml	
Magic number	<?xml 0x20	
Tipo MIME	application/xml, text/xml	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	SGML	
Revisione	1.0, 5 <sup>a</sup> edizione	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">XML 1.0 (5<sup>th</sup> Ed.)</a>, 2013</li> <li>• <a href="http://www.w3.org/standards/xml">www.w3.org/standards/xml</a></li> <li>• <a href="http://validator.w3.org">validator.w3.org</a></li> </ul>	
Conservazione	Sì, se conservato insieme a un <i>XML Schema</i>	
Racc. per la lettura	Generico; subordinato ad eventuali, ulteriori obblighi o raccomandazioni di conformità con schemi/dialetti.	
Racc. per la scrittura	Generico; subordinato ad eventuali, ulteriori obblighi o raccomandazioni di conformità con schemi/dialetti.	

2. Il principale tipo di sintassi è costituito dall’*Extensible Markup Language* (XML), la cui caratteristica aggiuntiva è di essere facilmente *human readable*. L’XML è estendibile in quanto:

- possono essere definite in continuazione nuove etichette;

- più dizionari di etichette possono essere usati con un approccio modulare all'interno del medesimo file XML mediante l'utilizzo dei *namespace* ("spazi di nomi") sui nomi delle etichette;
- è possibile definire, in XML stesso, sintassi specializzate mediante *schemi* (.xsd) o *dialetti* (.dtd);
- un medesimo documento XML (come file unico ovvero pacchetto costituito da più file XML) può essere logicamente composto da parti distinte, ciascuna delle quali utilizza etichette e regole sintattiche definite da diversi *namespace* o *schemi*, mentre le diverse parti possono riferirsi l'un l'altra sfruttando diversi meccanismi sintattici (p.es. *XQuery* e *XPath*).

3. Numerosi formati di file oggetto del presente Allegato che utilizzano il linguaggio XML impiegano un dialetto specializzato al loro contenuto; essi sono:

- OpenDocument e Microsoft® OOXML (cfr. § 2.1 e §2.5),
- XHTML, XSD, XSL, XSLT, MathML (§2.2),
- SVG (§2.7),
- tutti i formati descritti in §2.14 (FatturaPA, CDA2, asserzione SPID, ...),
- MusicXML (§2.9),
- IMSC1, TTML, e EBU-TT (§ 2.11)
- alcuni file obbligatori nei pacchetti IMF e DCP, nonché ACESclip (§2.12),
- KDM e firme elettroniche XADES (§2.16).

4. **Nota Bene:** Alcuni dei formati basati su XML sopraelencati mantengono l'estensione .xml del linguaggio madre, altri usano le proprie (e.g. .html/.htm, .svg, .ttml, .kdm). Si raccomanda che le Pubbliche Amministrazioni che producano documenti informatici in qualunque formato basato su XML non descritto dal presente Allegato ma che utilizzasse (in base alle proprie linee guida, specifiche tecniche, raccomandazioni o *best practices*) un'estensione "propria" diversa da .xml, laddove fosse consentito dall'uso applicativo delle applicazioni che elaborano file in tali formati, di "appendere" l'estensione .xml alla propria. Questo accorgimento manterrà ed esporrà l'estensione propria del formato a livello di UI, consentendo ai sistemi operativi privi di applicazioni specifiche per interpretare tali formati di aprire e visualizzare tali file come fossero normali file XML.

Esistono moltissime altre estensioni di XML che, pur non descritte qui, possono essere utilizzate e integrate in documenti XML per mezzo dell'estendibilità del *namespace*.

HTML	FORMATO DI FILE
Nome completo	Hypertext Markup Language
Estensione/i	.html, .htm
Magic number	<!DOCTYPE 0x20; <head>
Tipo MIME	text/html

Sviluppato da	World Wide Web Consortium
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale
Livello metadati	2
Derivato da	XML
Revisione	5.2
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">HTML 5.2</a>, 2017</li> <li>• <a href="#">validator.w3.org</a></li> <li>• W3C Recommendation <a href="#">XML 1.0 (5<sup>th</sup> Ed.)</a>, 2013</li> </ul>
Conservazione	Sì, se conservato insieme al/i CSS; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Specifico; raccomandato HTML5 per contenuti web

5. Un particolare dialetto di XML è HTML (ufficialmente codificato come XML puro a partire dalle sue versioni “XHTML” e “HTML5”), che serve a rappresentare il contenuto di pagine web. In questo caso HTML (.htm, .html) è affiancato dal CSS, linguaggio specifico per descrivere i fogli di stile che trasformano i componenti logici di una pagina in elementi grafici (la cosiddetta “presentazione” della pagina).

6. Il CSS può essere iniettato direttamente all’interno dell’HTML, oppure venire referenziato da esso in dei file esterni (estensione .css).

7. Sia XML, che HTML, che CSS sono tutti standard del W3C. Più in generale, una pagina web è un esempio di pacchetto di file (cfr. §1.1.2) costituito, come minimo, da un solo indice HTML, più eventualmente altri file in vari formati (anche non inclusi in questo Allegato), quali ad esempio HTML, CSS, WOFF, JavaScript, ecc.

XHTML	FORMATO DI FILE	
Nome completo	Extensible Hypertext Markup Language	
Estensione/i	.xhtml, .html	
Specializzazione di	XML	
Tipo MIME	application/xhtml+xml	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	HTML	
Revisione	1.1	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">XHTML™ Basic 1.1 (2<sup>nd</sup> Ed.)</a>, 2010</li> <li>• W3C Recommendation <a href="#">XHTML™ 1.0 (2<sup>nd</sup> Ed.)</a>, 2018</li> <li>• <a href="#">validator.w3.org</a></li> <li>• W3C Recommendation <a href="#">XML 1.0 (5<sup>th</sup> Ed.)</a>, 2013</li> </ul>	

Conservazione	Solo se conservato insieme al/i CSS
Racc. per la lettura	Generico con obbligo di riconoscimento
Racc. per la scrittura	Specifico; raccomandato HTML5 per contenuti web

8. L'HTML, originariamente (e fino a HTML 4.01), non era una specializzazione di XML; prima di introdurre la versione 5, è stato fatto dal W3C un tentativo di standardizzazione intermedio che ha portato ad un'altra versione di HTML, chiamato XHTML (a sua volta ramificato in due dialetti distinti –*Strict* e *Transitional*– sono i più diffusi, e in diverse versioni). Data la sua diffusione tale linguaggio (che condivide le estensioni di file con le versioni ufficiali di HTML) è stato incluso in questo elenco.

XSD	FORMATO DI FILE	
Nome completo	XML Schema Definition	
Estensione/i	.xsd	
Specializzazione di	XML	
Tipo MIME	application/xml	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	XML	
Revisione	2.0	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">W3C Recommendation XSL Schema Part 0: Primer, 2<sup>nd</sup> Ed., 2004</a></li> <li>• <a href="#">W3C Recommendation XSL Schema Part 1: Structures, 2<sup>nd</sup> Ed., 2004</a></li> <li>• <a href="#">W3C Recommendation XSL Schema Part 1: Datatypes, 2<sup>nd</sup> Ed., 2004</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Speciale; per la convalida di documenti in XML	
Racc. per la scrittura	Speciale; per la condivisione di sintassi e dialetti XML	

9. Questo formato è in grado di descrivere, sempre in linguaggio XML la sintassi e la grammatica associata ad un particolare [schema](#), che esso stesso definisce. Un documento XML può perciò essere convalidato in maniera automatica rispetto ad un dato schema, per verificare se ne rispetta tutti i criteri sintattici. Analogamente, un file XSD può essere usato per produrre in XML una struttura di dati o, più in generale, una procedura. In entrambe i casi (convalida o produzione di un documento XML rispetto ad uno schema), questa architettura consente di riutilizzare lo stesso algoritmo o applicativo, ma con la flessibilità aggiuntiva di poter

cambiare le regole sintattiche e grammaticali in automatico non appena viene cambiato lo schema di riferimento su file XSD.

XSL		FORMATO DI FILE
Nome completo	Extensible Stylesheet Language	
Estensione/i	.xsl	
Specializzazione di	XML ( <i>namespace xsl</i> )	
Tipo MIME	text/xsl	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	XML	
Revisione	2.0	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Working Draft <a href="#">XSL Requirements, v2.0</a>, 2008</li> <li>• W3C Recommendation <a href="#">XSL Requirements, v1.1</a>, 2006</li> <li>• <a href="http://www.w3.org/Style/XSL/">www.w3.org/Style/XSL/</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Generale; raccomandato per la visualizzazione di XML	
Racc. per la scrittura	Speciale; raccomandato per la costruzione di presentazioni grafiche di documenti in formato XML	

10. Un documento esistente in formato XML può essere trasformato in un altro documento, sia esso in XML o in qualunque altro formato, specificando le regole di traduzione mediante trasformazioni descritte –sempre in linguaggio XML– e raccolte in:

- File per la descrizione del linguaggio di stile (in caso si tratti di un linguaggio diverso da XML) o del dialetto (in caso si tratti di una specializzazione di XML) — in XSL (.xsl).

XSLT		FORMATO DI FILE
Nome completo	Extensible Stylesheet Language Transformations	
Estensione/i	.xslt	
Specializzazione di	XML ( <i>namespace xsl</i> )	
Tipo MIME	application/xslt+xml, text/xml	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	3	
Derivato da	DSSSL	
Revisione	2.0	

Riferimenti	• W3C Recommendation <a href="#">XSL Transformations (XSLT) v2.0, 2007</a>
Conservazione	Sì
Racc. per la lettura	Generale; raccomandato per la visualizzazione di XML
Racc. per la scrittura	Speciale; raccomandato per la costruzione di presentazioni grafiche di documenti in formato XML

- File per la descrizione delle trasformazioni del linguaggio di stile, che permette regole più complesse che, ad esempio, possono includere il traversamento della struttura XML del documento di partenza (tramite i sopracitati metodi *xQuery* e *xPath*) —XSLT (.xslt).

CSS	FORMATO DI FILE	
Nome completo	Cascaded Style Sheet	
Estensione/i	.css	
Magic number	–	
Tipo MIME	text/css	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	–	
Revisione	3	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">CSS 2.1 Specification</a>, 2011</li> <li>• W3C Recommendation <a href="#">CSS Basic User Interface module Level 3 (CSS3 UI)</a>, 2018</li> <li>• W3C Recommendation <a href="#">CSS Color module Level 3</a>, 2018</li> <li>• W3C Recommendation <a href="#">CSS Media Queries</a>, 2012</li> <li>• <a href="http://validator.w3.org">validator.w3.org</a></li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Generale; raccomandato per visualizzare pagine web	
Racc. per la scrittura	Generale; raccomandato per la presentazione di documenti sotto format di pagine web	

11. Il formato CSS effettua trasformazioni stilistiche di un documento HTML per permettere al suo contenuto di essere visualizzato graficamente, tramite un *web browser*, inclusi gli adattamenti “dinamici” del contenuto stesso. Una pagina web viene così rappresentata da vari file, tra i quali spiccano quelli delle seguenti due tipologie:

- il contenuto vero e proprio della pagina (testi, ipertesti e altri tipi di riferimenti ad altre pagine o contenuti), formato in HTML;

- la “presentazione” dei suddetti contenuti, formata in CSS.

12. Possono esistere più documenti CSS che adattano il medesimo contenuto a dispositivi di visualizzazione (p.es. stampa, monitor a bassa risoluzione, monitor ad alta risoluzione, dispositivi touch-screen, dispositivi per contenuti accessibili di vario tipo, ...), ovvero adattano più contenuti diversi uniformandone lo stile. La versione di linguaggio CSS da usare dipende dalla versione HTML del contenuto: si raccomanda CSS3 per HTML5, ovvero CSS2 per XHTML.

MARKDOWN	FORMATO DI FILE
Nome completo	Markdown
Estensione/i	.md
Magic number	–
Tipo MIME	text/markdown
Sviluppato da	John Gruber, Aaron Swartz
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale
Livello metadati	2
Derivato da	–
Revisione	0.28 (2017)
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-7763</a>, <a href="#">RFC-7764</a></li> <li>• <a href="http://spec.commonmark.org">spec.commonmark.org</a></li> </ul>
Conservazione	Sì, se conservato insieme agli oggetti da esso riferiti
Racc. per la lettura	Generale; raccomandato per produzione di testi e ipertesti pubblicati online
Racc. per la scrittura	Generale; raccomandato per produzione di testi e ipertesti pubblicati online

13. *Markdown* (“[md](#)”) è un linguaggio di markup pensato per scrivere contenuti testuali insieme ad una limitata quantità di ipertesti e di capacità “presentazionali”. La sintassi semplificata del markdown è pensata per rendere il contenuto di un ipertesto accessibile e traducibile, in automatico, in linguaggi e sintassi che ne permettono un’adeguata presentazione e trasmissione, come ad esempio HTML, EPUB, OOXML, PDF o altro. Nella previsione che sempre più servizi delle PPA.A. saranno prodotti e accessibili online, il markdown si configura dunque come il linguaggio d’elezione per l’archiviazione a breve e lungo termine di questi contenuti, che sono perciò resi indipendenti dalla pagina web o dal file ove possano temporaneamente essere rappresentati. Gli ipertesti in markdown si prestano ad essere conservati, nella loro sintassi originale, sia all’interno di basi di dati generiche (cfr. §2.3) che in documenti informatici indipendenti, sottoforma di file con estensione .md.

MATHML		FORMATO DI FILE
Nome completo	MathML	
Estensione/i	.mml, .xml	
Specializzazione di	XML	
Tipo MIME	text/mathml, text/mathml-renderer[*]	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	XML	
Revisione	3.0 (2014)	
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC 40314:2016, <i>MathML version 3.0, 2<sup>nd</sup> Ed.</i></li> <li>• W3C Recommendation <i>MathML version 3.0, 2<sup>nd</sup> Ed.</i>, 2014</li> <li>• W3C <i>Math Home</i></li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Speciale; obbligatorio per testi tecnico-scientifici basati su XML	
Racc. per la scrittura	Speciale; fortemente raccomandato per testi tecnico-scientifici; obbligatorio per quelli basati su XML	

14. MathML è un dialetto di XML adatto alla rappresentazione di formule matematiche generiche; tale estensione di XML viene dunque utilizzata per testi scientifici in qualsivoglia documento informatico basato su XML, suoi dialetti (e.g. XHTML) o linguaggi “imparentati” (e.g. HTML).

## 2.2.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda di usare per gli ipertesti i formati più aperti, interoperabili e indipendenti dall'applicativo utilizzato, come ad esempio l'XML (con i suoi dialetti) e il markdown. Nel caso specifico di documenti destinati ad uso tramite internet o intranet, la scelta ricadrebbe naturalmente sulle versioni più recenti di HTML (HTML5) e XHTML, anche se tali linguaggi da un lato mantengono una dipendenza dal formato del documento (“pagina web”), dall'altro sono largamente dipendenti –per la loro visualizzazione– da altri file che ne descrivono la rappresentazione grafica (e.g. stili XSLT/XSLT e fogli di stili CSS). Si invita dunque ad una scelta adeguata alle finalità del documento.

2. I documenti in formato XML sono adatti alla conservazione soltanto se accompagnati dal loro schema XML (XSD). Le pagine web possono essere mandate

in conservazione soltanto quando completamente statiche, combinando il “contenuto vero e proprio” in formato HTML (incluso XHTML), con la parte “presentazionale” in formato CSS. Le pagine web con contenuto dinamico (ad esempio codice JavaScript lato client) non sono adatte alla conservazione a meno di non conservare l'intero contenuto JavaScript (incluse le librerie eventualmente richiamate – cfr. §2.15) che, a sua volta, non deve riferirsi esternamente ad alcun altro documento.

## 2.3 Dati strutturati

1. In questa sezione si descrivono brevemente alcuni formati dedicati al trasporto di dati strutturati, intendendo con questa accezione riferirsi a formati ove la tipologia di contenuto non è predeterminata a priori. Esempi di applicazioni che fanno uso di dati strutturati sono le basi di dati (per le quali rappresentano qui i formati SQL e quelli relativi all'applicativo Microsoft® Access®). Si sottolinea che l'adeguatezza di una base di dati alla normativa vigente in materia di protezione dei dati personali (p.es. pseudonimia) e privacy può essere indipendente dal formato di file adottato, mentre è fortemente caratterizzata dai criteri architetturali adottati durante la fase progettuale.

SQL	FORMATO DI FILE
Nome completo	Structured Query Language
Estensione/i	.sql
Specializzazione di	Datalog query language
Tipo MIME	application/sql
Sviluppato da	International Organization for Standardization
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale
Livello metadati	4
Derivato da	Datalog
Revisione	SQL:2016
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-6922</a></li> <li>Famiglia di standard <b>9075</b> della ISO/IEC:</li> <li>• <a href="#">ISO/IEC 9075-1:2016</a>, <i>SQL Part 1 - framework</i></li> </ul>
Conservazione	Sì
Racc. per la lettura	Speciale; raccomandato per basi di dati relazionali
Racc. per la scrittura	Speciale; raccomandato per basi di dati relazionali

2. I file SQL servono a contenere configurazioni e tabelle per basi di dati relazionali, complete o parziali, sotto forma del loro linguaggio di programmazione comune. Ogni file SQL descrive la formazione della base di dati, “da zero” o a partire da una base supposta già esistente: fornendo un tale file ad un gestore di basi di dati vengono perciò costituite le sue tabelle. Vice versa, una o più tabelle possono essere archiviate effettuandone uno “scarico” (*dump* in inglese) in un file SQL che descrive come il contenuto dello scarico può essere formato, da zero, in un nuovo gestore di basi di dati che interpreti il medesimo linguaggio. A tale scopo bisogna dunque specificare che SQL è in realtà un ceppo linguistico, da cui sono derivati molteplici dialetti di SQL, differenziati a seconda dell’applicativo –commerciale o meno– che funge da gestore di basi di dati. Si raccomanda quindi, per l’archiviazione a lungo termine e l’interscambio, di utilizzare sempre il formato SQL standardizzato dalla ISO (e riportato in tabella).

3. Ove non possibile, va sempre indicata la versione esatta del linguaggio SQL adottato, incluso preferenzialmente il nome e la versione completa dell’applicativo di gestione (MySQL, Microsoft® SQL™, ecc.).

ACCESS® 2007		FORMATO DI FILE
Nome completo	Microsoft® Access® Connectivity Engine	
Estensione/i	.accdb	
Magic number	0x00010000 Standard ACE DB	
Tipo MIME	application/msaccess	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (chiuso), <i>de facto</i> , binario	
Livello metadati	3	
Derivato da	MS-MDB	
Revisione	2017	
Riferimenti	• Microsoft, <i>Which Access® file format should I use? - the .accdb file format</i> (2019)	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandato per piccole basi di dati	
Racc. per la scrittura	Speciale; sconsigliato	

4. Il formato proprietario usato da Microsoft per il suo gestore di basi di dati *Access*®, a partire dalla versione 2007, permette di archiviare non soltanto tabelle, ma anche righe di codice SQL e dati nonstrutturati. Tuttavia, essendo il formato proprietario e a sorgente chiusa, viene elencato qui in caso vi siano organizzazioni con basi di dati basati sugli applicativi Microsoft, affinché migrino i dati un un formato non proprietario ovvero, qualora non altrimenti possibile, dal vecchio formato .mdb (si legga più avanti) a quello attuale .accdb.

MS-MDB		FORMATO DI FILE
Nome completo	Microsoft® Access® Binary file format	
Estensione/i	.mdb	
Magic number	0x00010000 Standard Jet DB	
Tipo MIME	application/msaccess	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (chiuso), <i>de facto</i> , deprecato, binario	
Livello metadati	3	
Derivato da	–	
Revisione	2017	
Riferimenti	• Microsoft, <i>Which Access® file format should I use? - the .mdb file format</i> (2019)	
Conservazione	No	
Racc. per la lettura	Generico; valutare riversamento in formato aperto	
Racc. per la scrittura	Sconsigliato; valutare un riversamento in altro formato	

5. Il formato proprietario MDB è stato usato in precedenza da Microsoft per il suo gestore di basi di dati *Access*,<sup>®</sup> fino alla versione 2003. È ora un formato deprecato.

ODB		FORMATO CONTENITORE
Nome completo	Open Document Format for Database	
Estensione/i	.odf	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.oasis.opendocument.[data]base	
Sviluppato da	Organization for the Advancement of Structured Information Standards	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario, deprecato	
Livello metadati	3	
Derivato da	–	
Revisione	1.2 (2015)	
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC. • OASIS, <i>Open Document Format for Office Applications (OpenDocument)</i> , v1.2 (2015)	
Conservazione	No	
Racc. per la lettura	Generico; raccomandato solo a scopo di riversamento	
Racc. per la scrittura	Sconsigliato; valutare riversamento in altro formato	

6. Specializzazione del formato OpenDocument per la rappresentazione di basi di dati, ODP è un formato deprecato e va perciò evitata la produzione di nuovi file;

inoltre, si consiglia di valutare il riversamento di basi di dati preesistenti in questo formato.

JSON		FORMATO DI FILE
Nome completo	JavaScript Object Notation	
Estensione/i	.json	
Specializzazione di	JavaScript	
Tipo MIME	application/json	
Sviluppato da	dominio pubblico	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	JavaScript	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-8259</a></li> <li>• <a href="#">ECMA-404</a></li> <li>• <a href="#">json.org</a></li> <li>• ISO/IEC <a href="#">8825-8:2018</a>, <i>ASN.1 encoding rules, part 8: JSON</i></li> </ul>	
Conservazione	Sì, se adottato insieme a uno schema JSON	
Racc. per la lettura	Generico; obbligatorio; eventualmente subordinato a ulteriori obblighi di conformità con determinati schemi.	
Racc. per la scrittura	Fortemente raccomandato per documenti contenenti dati sia strutturati che non strutturati; eventualmente subordinato a ulteriori obblighi di conformità con determinati schemi.	

7. Il formato *JavaScript Object Notation* (JSON) è un altro formato estremamente versatile ed estendibile che, come XML, è usato in moltissimi ambiti informatici e viene dunque impiegato per svariate applicazioni. Come definito nello standard [RFC-8259](#) del 2018, in un file JSON le evidenze informatiche sono rappresentate gerarchicamente in più livelli:

- Ogni livello (compresa la “radice”) è delimitato da parentesi graffe ‘{’ e ‘}’.
- In ogni livello, ogni elemento (tranne l’ultimo) è separato dal successivo da una virgola ‘,’.
- Ogni elemento è costituito da una coppia **nome**–**valore**, separati fra loro da due punti ‘:’, ove il **nome** è sempre una stringa (delimitata da virgolette “”) e il **valore** può essere:
  - anch’esso una stringa (delimitata da virgolette “”);
  - un numero intero o in virgola mobile<sup>13</sup>;

<sup>13</sup> Sono ammessi segni ‘+’ e ‘-’, punto decimale ‘.’ e un numero arbitrario di cifre, ma non notazioni scientifiche (e.g. quella esponenziale).

- un booleano rappresentato dalle parole chiavi ‘true’ ovvero ‘false’;
  - un *array* di valori, delimitato da parentesi quadre ‘[’ e ‘]’, separati (tranne l’ultimo) da virgole ‘,’ e con ciascun valore essendo di un qualsiasi tipo in questo elenco,
  - un oggetto JSON (cioè sottolivello di questa medesima struttura);
  - un tipo di dato che non indica nulla, rappresentato dalla parola chiave ‘null’.
- Tra i caratteri di delimitazione<sup>14</sup> sopra elencati, possono essere aggiunti un qualsivoglia numero di caratteri di spaziatura e interruzione di linea (soprattutto nella rappresentazione di tale struttura dati in un file), ottenendo un’equivalenza del medesimo contenuto.
  - L’ordine degli elementi al medesimo livello di un *array* o di una struttura JSON è indifferente.

8. Un esempio di documento informatico rappresentato in formato JSON è dato dal seguente elenco di attributi di identificazione elettronica:

```

{
  "id": "cae8877c-e533-4d8a-9f38-d7f219392b1f",
  "firstName": "Mario",
  "lastName": "Rossi",
  "fiscalCode": "RSSMRA75L01H501A",
  "phoneNum": ["+393201234567", "+393398901234"],
  "children": [
    "id": "cae8877c-e533-4d8a-9f38-d7f219392b1f",
    "firstName": "Luigi",
    "lastName": "Bianchi",
    "fiscalCode": "RSSMRA75L01H501A",
    "phoneNum": ["+393332468013"],
    "children": [
      .....
    ],
    "alive?": true
  ],
  "alive?": no
}

```

9. Un vantaggio di JSON rispetto a XML è la semplicità della sintassi che, pur non offrendo capacità avanzate quali i *namespace* o la possibilità di “attraversare” la struttura ad albero (offerte da XML), dispone di una struttura più semplice da interpretare –soprattutto da parte di processi automatici– senza perdere la caratteristica fondamentale della leggibilità da parte dell’uomo. Un impiego particolare di JSON è in alcuni tipi di basi di dati che necessitano uno scambio di tabelle potenzialmente grandi e complesse ma non necessariamente relazionate fra

<sup>14</sup> Indicati, in questo elenco e come al solito nell’Allegato, mediante caratteri a spaziatura fissa.

loro: in tali casi viene solitamente considerata una rappresentazione di interscambio mediante JSON piuttosto che i formati nativi dei altri tipi di basi di dati (p.es. SQL). Un'ulteriore caratteristica del JSON nel rappresentare basi di dati è che ogni dato può avere una struttura completamente diversa dagli altri; per questo motivo tale formato è ideale per l'archiviazione l'elaborazione, in automatico, di dati cosiddetti "non strutturati".

JSON-LD		FORMATO DI FILE
Nome completo	JavaScript Object Notation for Linked Data	
Estensione/i	.jsonld	
Specializzazione di	JSON	
Tipo MIME	application/ld+json	
Sviluppato da	dominio pubblico	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	JavaScript	
Revisione	2014	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">JSON-LD 1.0</a>, 2014</li> <li>• W3C Recommendation <a href="#">JSON-LD 1.0 Processing Algorithms and API</a>, 2014</li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Generico; obbligatorio; eventualmente subordinato ad obblighi di conformità a schemi.	
Racc. per la scrittura	Fortemente raccomandato per documenti contenenti Open Data generati con procedure automatizzate	

10. Un particolare dialetto di JSON è costituito da JSON-LD, che segue una sintassi più rigida organizzata per poter gestire dati strutturati e collegati fra loro da relazioni astratte il più generiche possibili. Nell'ambito delle PPA.A., ad esempio, l'utilizzo di questo formato è –al pari di altri contenuti in questo Allegato– fortemente consigliato per la generazione di Open Data, particolarmente attraverso procedure automatizzate.

CSV		FORMATO DI FILE
Nome completo	Comma-Separated Value	
Estensione/i	.csv	
Magic number	–	
Tipo MIME	text/csv	
Sviluppato da	dominio pubblico	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	1	
Derivato da	tabelle preformattate in FORTRAN77	

Revisione	2005
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-4180</a></li> <li>• <a href="#">RFC-7111</a></li> <li>• <a href="#">W3C Recommendation <i>Model for tabular data and metadata on the Web</i>, 2015</a></li> <li>• <a href="#">dati.gov.it</a></li> </ul>
Conservazione	Sì
Racc. per la lettura	Generale; obbligatorio
Racc. per la scrittura	Raccomandato per documenti contenenti dati strutturati leggibili dall'uomo (inclusi gli Open Data)

11. Uno dei formati più semplici per la rappresentazione di dati *fortemente* strutturati è il CSV che è un file testuale ove i dati sono rappresentati in una tabella:

- Ogni riga della tabella è una linea del file, delimitata da un'opportuna evidenza di fine linea.
- Le colonne, all'interno di ogni linea, si distinguono perché delimitate da caratteri specifici (ad esempio la virgola ',' che da il nome al formato, ma sono possibili anche altre combinazioni di caratteri di interpunzione o di spaziatura).
- Opzionalmente, la prima linea del file (indicata con un carattere iniziale particolare e con la medesima distinzione in colonne del resto delle linee) costituisce una legenda circa il significato dei valori delle colonne.

12. Il formato CSV è uno dei formati d'elezione per la rappresentazione degli Open Data, il cui archivio nazionale per i dati aperti pubblici è [dati.gov.it](#).

JWT	CODEC
Nome completo	JSON Web Token
Estensione/i	–
Specializzazione di	JSON
Tipo MIME	application/jwt
Sviluppato da	pubblico dominio
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Derivato da	JSON
Revisione	2016
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-7797</a></li> <li>• <a href="#">jwt.io</a></li> <li>• <a href="#">ISO/IEC 29500-6:2017</a></li> <li>• <a href="#">RFC-7515</a></li> <li>• <a href="#">RFC-7516</a></li> </ul>
Conservazione	Sì, se da JSON-LD o conservato insieme a schema
Racc. per la lettura	Speciale; consigliato per flussi digitali in richieste POST

Racc. per la scrittura	Speciale; consigliato per flussi digitali in richieste POST
------------------------	---

13. Il *JSON Web Token (JWT)*, definito dall'[RFC-7797](#), è un codec<sup>15</sup> utilizzato per documenti informatici già organizzati in una struttura JSON; tale codifica ottimizza la dimensione dell'evidenza informatica e consente di trasferirla come un flusso digitale (cfr. §1.1.1) in tempo reale o attraverso un canale che permette un insieme limitato di caratteri — ad esempio inserendo l'evidenza in richieste HTTP di tipo POST. Il JWT (analogamente al JSON-LD) richiede che nella struttura JSON testuale possano essere presenti alcuni elementi, facoltativi ma dal significato predefinito, che semplificano il trasporto e la decodifica dell'evidenza JWT stessa.

Lo standard JWT include un sistema di controllo della propria integrità e può, facoltativamente, essere accompagnato da cifratura (per la confidenzialità), da apposizione di firma o sigillo elettronico nel pacchetto, o da entrambe. Le evidenze informatiche JWT firmate sono, impropriamente, chiamate *JSON Web Signature (JWS)* e definite nell'[RFC-7515](#); le evidenze informatiche JWT cifrate sono, impropriamente, chiamate *JSON Web Encryption (JWE)* e definite nell'[RFC-7516](#).

OOXML	FORMATO CONTENITORE
Nome completo	Office Open XML
Estensione/i	.docx, .xlsx, .pptx, ...
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Microsoft Corporation
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale
Livello metadati	4; cfr. §2.8
Derivato da	OpenXML; Microsoft® COM Structured Storage
Revisione	12.0 (2019)
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 29500-1:2016</a>, <i>fundamentals and markup language reference</i></li> <li>• <a href="#">ISO/IEC 29500-2:2012</a>, <i>open packaging conventions</i></li> <li>• <a href="#">ISO/IEC 29500-3:2015</a>, <i>markup compatibility and extensibility</i></li> <li>• <a href="#">ISO/IEC 29500-4:2016</a>, <i>transitional migration features</i></li> <li>• <a href="#">ECMA-376: Office Open XML File Formats</a>, 5<sup>th</sup> ed., 2016</li> <li>• <a href="http://officeopenxml.com">officeopenxml.com</a></li> </ul>
Conservazione	Sì, solo profilo <b>Strict</b> ; cfr. §2.8
Racc. per la lettura	–

<sup>15</sup> Per la precisione, la codifica binaria è ottenuta mediante algoritmo *Base64*, specificato in [RFC-4648](#).

14. Vengono elencati due formati contenitore utilizzati dalle principali suite di applicativi per ufficio: Microsoft® *Office*® e *LibreOffice*. Tali buste contengono in realtà un pacchetto di file che rappresenta, complessivamente, un documento informatico (testo impaginato, foglio di calcolo, presentazione, basi di dati, contenuto multimediale, o altro) mediante più file strutturati in un filesystem virtuale, con gerarchie di cartelle predeterminate. Il pacchetto, una volta formato in memoria, viene poi compresso in un unico file mediante algoritmi noti (tra quelli elencati in §2.13), o loro varianti. I file contenuti nel pacchetto descrivono sia i metadati interni del documento, che parte del documento informatico stesso: ad esempio testi, collegamenti ipertestuale e la loro rappresentazione grafica (impaginazione, colore, tipografia, ecc.) e sono tipicamente in formato XML. Eventuali contenuti ipertestuali (pagine web, immagini, suono, video, contenitori crittografici ecc.) sono rappresentati da file in altri formati –tipicamente aperti o proprietari ma liberi– (HTML, PNG, WAV, PEM, ecc.) a seconda della necessità. Il pacchetto di file viene di solito formato e archiviato nello storage soltanto previa compressione in un unico file, mentre al caricamento da parte di un applicativo viene scompattato in memoria. La strutturazione in un pacchetto di file consente una migliore gestione del documento particolarmente nei casi di dimensioni elevate del file: una lieve modifica parziale di un documento informatico molto grande comporta la modifica di un sottoinsieme di file costituenti il pacchetto, non di tutti, perciò lo sforzo computazionale si riduce, così come i rischi di corruzione dell'intero file in caso di problemi durante la scrittura di file così grandi.

15. *Office Open XML*<sup>16</sup> (*OOXML*) è il contenitore generico utilizzato prevalentemente dalle versioni più recenti (dalla 2007 in poi) della suite applicativa Microsoft® *Office*,® che si specializza a seconda della tipologia di documento da contenere (e di applicativo della suite). Un documento in formato OOXML è in realtà costituito da un pacchetto di file che sono poi compressi in un'unica busta ZIP (cfr. §2.13), rinominata con estensione differente a seconda della specializzazione.

16. In questo Allegato sono descritte tre specializzazioni di OOXML ai documenti impaginati (.docx, §2.1), ai fogli di calcolo e alle presentazioni multimediali (rispettivamente .xlsx e .pptx, §2.5)

---

<sup>16</sup> Da non confondersi con *OpenOffice.org XML* — formato simile utilizzato da versioni obsolete dell'omonima suite applicativa.

OPENDOCUMENT	FORMATO CONTENITORE
Nome completo	Open Document Format for Office Applications
Estensione/i	.odt, .ods, .odp, .odg, .odi, .odf
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Livello metadati	4
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC: <ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">26300-1:2015</a>, <i>ODF for Office Applications v1.2 - Part 1: OpenDocument Schema</i></li> <li>• ISO/IEC <a href="#">26300-3:2015</a>, <i>ODF for Office Applications v1.2 - Part 3: Packages</i></li> <li>• OASIS, <a href="#">Open Document Format for Office Applications (OpenDocument)</a>, v1.2 (2015)</li> </ul>
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	–
Racc. per la scrittura	–

17. OOXML è dotato di vari “profili”, che possono essere più o meno interoperabili. Per tutti i documenti della P.A., si consiglia perciò il profilo Strict, che è più restrittivo, ma consente di eliminare alcune estensioni “proprietarie” che possono ridurre l’interoperabilità dei formati.

18. Come per OOXML, anche OpenDocument è un contenitore generico di quelli sopraelencati, per archiviare documenti prodotti da suite applicative open source — prima fra tutte *LibreOffice*.

In questo allegato sono descritte alcune specializzazioni di OpenDocument ai documenti impaginati (.odt, §2.1), ai fogli di calcolo e alle presentazioni multimediali (rispettivamente .ods e .odp, §2.5), ai

CFB	FORMATO CONTENITORE
Nome completo	Compound File Binary file format
Estensione/i	.doc, .xls, .ppt, .pst; .aaf, ...
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	–
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario, estendibile, <i>de facto</i> , binario, deprecato

Livello metadati	–
Derivato da	Microsoft® COM Structured Storage
Revisione	9.0 (2018)
Riferimenti	• Microsoft, <a href="#">[MSD-CFB]: Compound File Binary file format v9.0 (2018)</a>
Conservazione	No; cfr. §2.8
Racc. per la lettura	–
Racc. per la scrittura	–

19. CFB è invece il contenitore di file su cui Microsoft® si è basata per le versioni obsolete della suite *Office*® (cfr. § 2.1 e §2.5). È anche il formato contenitore da cui deriva AAF (cfr. §2.12). Il formato CFB rappresenta all’interno un pacchetto di file organizzati in un filesystem virtuale vagamente ispirato al FAT<sup>17</sup> (anziché in un archivio compresso come fanno altri formati). Una delle principali problematiche del CFB, soprattutto nel caso di documenti informatici di grandi dimensioni, è ereditata proprio dal FAT, essendo caratterizzato dall’estrema facilità con file contenuti del pacchetto soffrono di **frammentazione** interna. Ad un livello più superficiale, ogni applicativo della suite Microsoft® *Office*® versione ‘2003’ o antecedenti utilizza una propria serie di tipi di file, dotati di estensioni differenti (p.es. .doc, .xls, .ppt, ..., cfr. §1.1.2), ma tutti basati su CFB;<sup>18</sup> a partire dalla versione ‘2007’ la suite ha abbandonato i formati basati su CFB in favore di quelli basati su OOXML (Office Open XML), producendo nuovi formati, stavolta strutturalmente differenti ma gemellati ai precedenti per via delle estensioni di file, ottenute quasi sempre aggiungendo una semplice ‘x’: .docx, .xlsx, .pptx, ....

## 2.3.1 Raccomandazioni per la produzione di documenti

1. La scelta dei formati di file per conservare dati strutturati quali grandi e piccole basi di dati è soggetta non soltanto alla tipologia dei dati “a riposo”, ma anche agli

<sup>17</sup> Acronimo di *File Allocation Table*, dal nome dell’evidenza informatica, contenuta (o replicata più volte) in dispositivo di storage a blocchi inizializzato con tale filesystem, per indicizzarne tutti i file contenuti e i loro metadati esterni (cfr. §1.1.2). Esistono diversi filesystem basati su FAT — alcuni aperti (FAT16, FAT32), altri coperti da licenze d’uso di proprietà di Microsoft Corporation (exFAT). Per ulteriori dettagli consultare [it.wikipedia.org/wiki/File\\_Allocation\\_Table](http://it.wikipedia.org/wiki/File_Allocation_Table) e i collegamenti ipertestuali ivi contenuti.

<sup>18</sup> A ciascuno di tali formati si affiancano delle varianti, strutturalmente identiche, per rappresentare specializzazioni dei medesimi documenti, quali ad esempio i “modelli di documento” (*template*, in inglese), per i quali cambia solo l’estensione del file (tipicamente una ‘t’ in sostituzione dell’ultimo carattere: p.es. .dot e .xlt).

aspetti “dinamici” legati alla loro generazione e riutilizzo. Sono perciò coinvolti aspetti fortemente quantitativi sui dati, quali:

- dimensione informatica delle evidenze “a riposo”,
- capacità dei flussi informatici “in transito” (banda richiesta e sue variazioni statistiche in base alla distribuzione geografica e cronologica, valutata su più scale di grandezza e indici statistici);
- previsioni sul ciclo di vita (generazione, modifiche, trasporto, archiviazione, distruzione);
- considerazioni in merito a conservazione e interoperabilità in generale (a livello europeo e nazionale);
- considerazioni in merito alla protezione dei dati, con particolare riferimento a:
  - dati personali e privacy: cfr. Regolamento (UE) N° 679/2016 (“GDPR”) del Parlamento europeo e del Consiglio e il D.Lgs. 101/2018;
  - trattamento da parte di infrastrutture critiche e fornitori di servizi essenziali: cfr. il D.Lgs. 65/2018 e la Direttiva (UE) N° 1148/2016 (“NIS”) da esso recepita.

2. Si raccomanda perciò alle PP.AA. di effettuare un’adeguata valutazione di interoperabilità, che tenga in considerazione anche dei sopracitati aspetti.

## 2.4 Posta elettronica

EML	FORMATO DI FILE	
Nome completo	Electronic Mail Format	
Estensione/i	.eml	
Magic number	–	
Tipo MIME	application/email	
Sviluppato da	comunità open source	
Tipologia di standard	aperto, estendibile, <i>de facto</i> , testuale	
Livello metadati	1	
Derivato da	<a href="#">RFC-822</a>	
Revisione	2008	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-5322</a></li> <li>• <a href="#">RFC-2822</a></li> <li>• US Library of Congress, <i>Email..(EMF)</i> (2014)</li> </ul>	
Conservazione	Sì; cfr. §2.8	

Racc. per la lettura	Generico; obbligatorio per singoli messaggi email
Racc. per la scrittura	Generico; obbligato per singoli messaggi email

1. Il formato EML rappresenta interamente l'evidenza informatica costituente un singolo messaggio di posta elettronica MIME, così come definito negli standard [RFC-5322](#) e [RFC-2822](#).

MBOX	FORMATO CONTENITORE
Nome completo	“default” <i>mbx</i> database format
Estensione/i	.mbx
Specializzazione di	EML
Tipo MIME	application/mbx
Sviluppato da	comunità open source
Tipologia di standard	aperto, estendibile, <i>de facto</i> , testuale
Livello metadati	3
Derivato da	sistema operativo UNIX
Revisione	2005
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-4155</a></li> <li>• <a href="#">RFC-2822</a></li> <li>• <a href="http://en.wikipedia.org/wiki/Mbox">en.wikipedia.org/wiki/Mbox</a></li> </ul>
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico; raccomandato per caselle di messaggi email
Racc. per la scrittura	Generico; raccomandato per caselle di messaggi email

2. Così come EML rappresenta, integralmente un singolo messaggio di posta elettronica, il formato MBOX può usarsi per contenerci diversi messaggi di posta elettronica, organizzati su più livelli.

MS-PST	FORMATO DI FILE
Nome completo	Microsoft® <i>Outlook</i> ® Personal Folder file
Estensione/i	.pst
Magic number	0xD0CF11E0A1B11AE1
Tipo MIME	application/vnd.ms-outlook
Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , binario
Livello metadati	3
Derivato da	Microsoft® Compound File binary format
Revisione	7.0 (2018)
Riferimenti	• Microsoft, <a href="#">[MS-PST]: Outlook Personal Folders (.pst) file format v7.0 (2018)</a>
Conservazione	No; cfr. §2.8

Racc. per la lettura	Generico; raccomandato per importare rubriche, ecc.
Racc. per la scrittura	Specifico; raccomandata migrazione dell'applicativo e, successivamente, dell'intero formato

3. Il formato proprietario usato in Microsoft® *Outlook*® (applicativo di rubrica messaggi e contatti) è un'alternativa al formato MBOX per memorizzare non soltanto intere caselle di posta (a loro volta strutturabili in sottocartelle), ma anche per memorizzare altre tipologie di dati utilizzabili in *Outlook*®, quali ad esempio schedari dei contatti, note personali, ecc. Il formato PST è anch'esso costituito da un pacchetto di file compressi in un unico file.

## 2.4.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda di utilizzare il formato EML per archiviare un singolo messaggio di posta elettronica, ovvero il formato MBOX per l'archiviazione di più messaggi ovvero di un'intera casella di posta elettronica.

## 2.5 Fogli di calcolo e presentazioni multimediali

1. Per formati di file maggiormente utilizzati per gli applicativi integrativi “da ufficio” si rimanda alle considerazioni già fatte in § 2.1 relativamente agli applicativi di videoscrittura ad essi affini, in particolare quelle al capoverso 10 del paragrafo in merito all'utilizzo delle fonti tipografiche.

EXCEL® 2007		FORMATO DI FILE
Nome completo	SpreadsheetML OOXML Extension	
Estensione/i	.xlsx, .xltx	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.openxmlformats-officedocument.spreadsheetml.sheet	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i>	
Livello metadati	3	
Derivato da	Office Open XML; Microsoft® Excel®	
Revisione	16.0 (2018)	

Riferimenti	<ul style="list-style-type: none"> <li>• Microsoft, <a href="#">Excel (.xlsx) extensions to SpreadsheetML file format v16.0</a> (2018)</li> <li>• <a href="#">officeopenxml.com</a>, <i>Anatomy of a SpreadsheetML file</i></li> </ul>
Conservazione	Sì, solo profilo <b>Strict</b> ; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Raccomandato nel profilo <b>Strict</b>

2. SpreadsheetML è il dialetto XML usato nei file di metadati all'interno di un pacchetto compresso in formato OOXML (§2.3), specializzato per la rappresentazione di fogli di calcolo (estensione .xlsx). È stato introdotto con la versione 2007 di Microsoft® *Office*®, ma è compatibile con moltissimi altri applicativi. L'unico profilo raccomandato di OOXML per SpreadsheetML è Strict.

3. Si segnala che Microsoft® *Excel*® presenta un *glitch* (i.e. un *bug* volutamente introdotto) considerando erroneamente l'anno 1900 d.C. come bisestile; il formato SpreadsheetML (profilo Transitional), di per sé, non corregge questo comportamento, permettendo il salvataggio, nelle celle di un foglio di calcolo, della data inesistente del 29 febbraio 1900. Tale inesattezza è però imputabile ad *Excel*® e non inficia la capacità di altri applicativi che fanno uso di codesto formato di file (p.es. [Google Documents](#)) di adeguarsi ad un corretto calcolo degli anni bisestili (correggendo automaticamente le date inesatte nei fogli di calcolo).

POWERPOINT® 2007		FORMATO DI FILE
Nome completo	PresentationML ooxml Extension	
Estensione/i	.pptx, .ppsx, .potx	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	application/vnd.openxmlformats-officedocument.presentationml.presentation	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i>	
Livello metadati	3	
Derivato da	Office Open XML; Microsoft® <i>PowerPoint</i> ®	
Revisione	15.0 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• Microsoft, <a href="#">PowerPoint (.pptx) extensions to ooxml file format v15.0</a> (2018)</li> <li>• <a href="#">officeopenxml.com</a>, <i>Anatomy of a PresentationML file</i></li> </ul>	
Conservazione	Sì, solo profilo <b>Strict</b> ; cfr. §2.8	
Racc. per la lettura	Generico con riconoscimento obbligatorio	
Racc. per la scrittura	Raccomandato nel profilo <b>Strict</b>	

3. PresentationML è il dialetto XML usato nei file di metadati all'interno di un pacchetto compresso in formato OOXML (§2.3), specializzato per la rappresentazione di presentazioni multimediali (estensione .pptx). È stato introdotto con la versione 2007 di Microsoft® Office®, ma è compatibile con moltissimi altri applicativi. L'unico profilo raccomandato di OOXML per PresentationML è **Strict**.

MS-XLS		FORMATO DI FILE
Nome completo	Microsoft® Excel® Binary file format	
Estensione/i	.xls	
Magic number	0xD0CF11E0A1B11AE1	
Tipo MIME	application/vnd.ms-excel	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , deprecato, binario	
Livello metadati	3	
Derivato da	Microsoft® Compound File binary format	
Revisione	8.0 (2018)	
Riferimenti	• Microsoft, <a href="#">[MS-XLS]: Excel Binary file format (.xls) structure v8.0 (2018)</a>	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Obbligatorio con riversamento raccomandato	
Racc. per la scrittura	Sconsigliato	

5. Il formato XLS è una specializzazione usata nei file di metadati all'interno di un pacchetto compresso in formato CFB (§2.3), specializzato per la rappresentazione di fogli di calcolo (estensione .xls). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® Office®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le P.P.AA. di accettare e aprire documenti in questo formato, si raccomanda di non formarne altri esemplari e di valutare il riversamento di fogli di calcolo preesistenti in altro formato della stessa tipologia: in quest'ordine, OpenDocument Spreadsheet (.ods) ovvero SpreadsheetML (.xlsx).

MS-PPT		FORMATO DI FILE
Nome completo	Microsoft® PowerPoint® Binary format	
Estensione/i	.ppt	
Magic number	0xD0CF11E0A1B11AE1	
Tipo MIME	application/vnd.ms-powerpoint	

Sviluppato da	Microsoft Corporation
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , deprecato, binario
Livello metadati	3
Derivato da	Microsoft® Compound File binary format
Revisione	6.0 (2018)
Riferimenti	• Microsoft, <a href="#">[MS-PPT]: PowerPoint (.ppt) Binary file format v6.0 (2018)</a>
Conservazione	No; cfr. §2.8
Racc. per la lettura	Obbligatorio con riversamento raccomandato
Racc. per la scrittura	Sconsigliato

6. Il formato PPT è una specializzazione usata nei file di metadati all'interno di un pacchetto compresso in formato CFB (§2.3), specializzato per la rappresentazione di presentazioni multimediali (estensione .ppt). È stato utilizzato, come formato principale per tali documenti fino alla versione 2003 di Microsoft® Office®, ma è compatibile con moltissimi altri applicativi. Nonostante l'obbligo per le PP.AA. di accettare e aprire documenti in questo formato, si raccomanda di non formarne altri esemplari e di valutare il riversamento di presentazioni preesistenti in altro formato della stessa tipologia: in quest'ordine, OpenDocument Presentation (.odp) ovvero PresentationML (.pptx).

ODS	FORMATO CONTENITORE
Nome completo	Open Document Format for Office Spreadsheets
Estensione/i	.ods
Specializzazione di	XML imbustato dentro ZIP
Tipo MIME	–
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC. • OASIS, <a href="#">Open Document Format for Office Applications (OpenDocument)</a> , v1.2 (2015)
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Fortemente raccomandato

7. Il formato OpenDocument Spreadsheet è una specializzazione dell'omonimo formato (§2.3) per rappresentare fogli di calcolo (estensione .ods). È attualmente

utilizzato dalla suite open source di applicativi da ufficio *LibreOffice*, anche se è pienamente utilizzabile in Microsoft® *Office*®, in OpenOffice.org e in altri applicativi che elaborano documenti di questo tipo.

ODP		FORMATO CONTENITORE
Nome completo	Open Document Format for Presentations	
Estensione/i	.odp	
Specializzazione di	XML imbustato dentro ZIP	
Tipo MIME	–	
Sviluppato da	Organization for the Advancement of Structured Information Standards	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	–	
Revisione	1.2 (2015)	
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC. • OASIS, <i>Open Document Format for Office Applications (OpenDocument)</i> , v1.2 (2015)	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Generico con riconoscimento obbligatorio	
Racc. per la scrittura	Fortemente raccomandato	

8. Il formato OpenDocument Presentation è una specializzazione dell’omonimo formato (§2.3) per rappresentare fogli di calcolo (estensione .odp). È attualmente utilizzato dalla suite open source di applicativi da ufficio *LibreOffice*, anche se è pienamente utilizzabile in Microsoft® *Office*®, in OpenOffice.org e in altri applicativi che elaborano documenti di questo tipo.

## 2.5.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda alle PPA.A. la produzione di fogli di calcolo e presentazioni multimediali in formati aperti e consistenti con gli applicativi “da ufficio” più diffusi sul territorio nazionale e comunitario: in particolare, si individua nei formati derivati da OOXML (profilo Strict) e da OpenDocument le alternative più valide.
2. Nel caso di documenti semilavorati a carattere temporaneo e non definitivo è consigliabile anche l’utilizzo di formati puramente “virtuali” quali quelli delle suite collaborative di fornitori di servizi in Cloud qualificati,<sup>19</sup> purché tali formati siano

<sup>19</sup> Si veda a tale proposito le Circolari AGID N°2/2018 e N°3/2018.

interoperabili e disponibili su sistemi informativi senza vincoli o particolari requisiti tecnologici (ad esempio, totalmente fruibili attraverso browser web).

## 2.6 Immagini raster

1. Si dicono *raster* tutte le immagini che sono descritte come un insieme finito di punti (*pixel*) virtuali disposti regolarmente su una griglia rettangolare. Il numero di punti lungo i due lati del rettangolo (lunghezza e larghezza) costituiscono le dimensioni dell'immagine, mentre il numero di bit necessari a rappresentare le caratteristiche di ciascun pixel (espresso in bit/pixel) è chiamata profondità o (*bit-depth*) dell'immagine. Tali caratteristiche sono tipicamente le coordinate-colore (*code-values*) di ciascun pixel secondo un tipo di codifica matematica ove ogni possibile colore rappresentabile dalle immagini (*gamut*) è definito dalle coordinate di uno spazio-colore astratto, all'interno del quale la gamut dell'immagine rappresenta una varietà discreta.

2. A seconda delle esigenze di conservazione possono essere utili o necessari riferimenti che permettono di correlare la distribuzione spaziale dei pixel di un'immagine raster con dimensioni fisiche. Alcuni formati di file descrivono tali informazioni mediante metadati interni, che possono essere facoltativi o meno. La scelta del formato di file per usi professionali dipende spesso dalla possibilità di creare e, successivamente, fruire di tali metadati, rilevanti sia per raster che provengono da oggetti reali (come nel caso di fotografie, scansioni digitali e diagnostica medica), che per immagini di sintesi usate per la produzione oggetti reali (p.es. stampe o modelli di altro tipo).

3. In alcuni casi sono indicati le dimensioni equivalenti dell'immagine in unità di misura fisiche (lunghezza, larghezza, profondità; ovvero aree, volumi); in altri casi è indicata la risoluzione espressa come densità di punti per unità di misura lineare, quali punti/pollice ("dpi", cioè *dots per inch*) ovvero pixel/cm (nel caso dei raster i termini "punto" e "pixel" sono spesso intercambiabili).

4. Il numero di bit usati per rappresentare il colore dei pixel è chiamata profondità di colore (*colour-depth*) e coincide con l'intera profondità dell'immagine raster qualora la sola caratteristica rappresentata sia il colore dei pixel.

5. Altre volte sono rappresentate una o più di altre caratteristiche del pixel (in alternativa o in aggiunta al colore), quali:

- trasparenza (chiamata anche "alfa", *alpha* in inglese),
- densità ottica,
- riflettanza,
- intensità radiante,

- velocità angolare o lineare,

ciascuna di queste caratteristiche del pixel (inclusa ciascuna coordinata dello spazio-colore) sono chiamate, individualmente, “canali” dell’immagine; il numero di bit usati per rappresentare ciascun canale (qualora sia uguale per tutti i canali) permette di specificare la profondità dell’immagine, alternativamente, in bit/canale.

6. Ad esempio, un’immagine raster a colori che usa il tipico modello colorimetrico rosso-verde-blu e un canale alfa, tutti a 16 bit/canale (4 canali in tutto: RGB $\alpha$ ) ha dunque una profondità complessiva di 64bit/pixel e una profondità-colore di 48 bit/pixel.

7. Molti formati di immagini raster possono –opzionalmente o obbligatoriamente– implementare algoritmi di compressione dati per ottenere una minore occupazione di spazio. Tali algoritmi sono *lossless* ovvero *lossy*, a seconda che la compressione sia reversibile (cioè sia possibile, decomprimendo, ritornare punto per punto all’immagine originale) o meno.

8. Un’altra possibilità per le immagini raster è una rappresentazione mediante sotto-campionamento, cioè utilizzando una codifica con un modello di spazio-colore a 3 componenti (anziché un modello RGB), ove il primo canale ([luminanza](#)) ha una risoluzione spaziale piena (cioè è codificato per ogni punto dell’immagine), mentre gli altri due canali, detti complessivamente di [crominanza](#),<sup>20</sup> sono codificati con una minore risoluzione.

9. I formati di immagini raster maggiormente diffusi per usi non professionali, quali ad esempio web e fotografia amatoriale, sono: PNG, JPEG (.jpg, .jpeg), TIFF (.tif, .tiff), GIF.

10. I formati di immagini raster diffusi per vari usi professionali quali grafica, stampa industriale, fotografia e cinematografia, si differenziano dai precedenti per un ampio supporto –ed effettivo utilizzo– di metadati interni, prevalentemente di tipo colorimetrico. Tra questi formati si annoverano: OpenEXR (.exr), Adobe® DNG (.dng), JPEG2000 (.jp2k, .jp2c), DPX, Adobe® *Photoshop*® (.psd), ARRIRAW (.ari).

PNG		FORMATO DI FILE
Nome completo	Portable Network Graphics	
Estensione/i	.png	
Magic number	0x89 PNG 0x0D0A1A0A	
Tipo MIME	image/png	
Sviluppato da	ACME	
Tipologia di standard	aperto, <i>de iure</i> , binario, muto	
Livello metadati	3	

<sup>20</sup> Tali canali codificano le differenze cromatiche da un colore neutro –di solito qualche tipo di verde– la cui intensità è rappresentata dalla sola luminanza. Gli spazi-colore di questo tipo (p.es.  $Y'_{iBcR}$  e  $Y'm$ ) sono nati per permettere la retrocompatibilità del segnale televisivo analogico a colori con quello in bianco e nero, affiancati da altre tecnologie indipendenti, quali il sotto-campionamento.

Derivato da	–
Revisione	1.2, 2ª edizione
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 15948:2004</a></li> <li>• W3C Recommendation <a href="#">PNG Specification (2<sup>nd</sup> Ed.)</a>, 2003</li> <li>• <a href="#">RFC-2083</a></li> <li>• <a href="#">www.libpng.org</a></li> </ul>
Conservazione	Sì
Racc. per la lettura	Generico; con riconoscimento obbligatorio della v1.0
Racc. per la scrittura	Generico; fortemente raccomandato per immagini a 16 ovvero 48 bit/pixel (più eventuale trasparenza) senza particolari obblighi relativi ad altri metadati

11. Il formato PNG è particolarmente raccomandato per la rappresentazione di immagini raster che non hanno bisogno di essere accompagnate da metadati particolarmente complessi (come quelli colorimetrici, geometrico-fisico o ottici). La versione 1.0 di questo formato (cfr. [RFC-2083](#)) –ancora largamente utilizzata e, per questo motivo, ammessa parimenti per la produzione di nuovi documenti raster– supporta un insieme ristrettissimo di metadati, per la cui mancanza il formato di questa versione è poco usato in ambiti professionali. Sono invece supportate nativamente le profondità di 24 e 48 bit/pixel in tricromia, la trasparenza sotto forma di un ulteriore canale “alfa”, nonché uno dei pochi formati non professionali ad ammettere la compressione dell’immagine mediante algoritmo *lossless*. La versione 1.2 del formato introduce alcuni metadati più professionali che permettono, ad esempio, di specificare autori e brevi descrizioni, orari di modifica, così come metadati colorimetrici (quali le coordinate di cromaticità delle primarie RGB e del punto di bianco, profili ICC integrati, dimensioni fisiche dell’immagine, ecc.).

JPEG	FORMATO DI FILE	
Nome completo	JPEG File Interchange Format (JFIF)	
Estensione/i	.jpg, .jpeg	
Magic number	0xFFD8, 0xFFD8FFE00010 JFIF 0x0001	
Tipo MIME	image/jpg, image/jpeg	
Sviluppato da	Joint Photographic Experts Group	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	4	
Derivato da	–	
Revisione	2012	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ITU-T Recommendation T.81</a>, 1992</li> <li>• <a href="#">ITU-T Recommendation T.871</a>, 2011</li> <li>• <a href="#">www.jpeg.org/jpeg</a></li> <li>• <a href="#">www.exif.org/Exif2-2.PDF</a></li> </ul>	

Conservazione	Sì, solo per immagini formate nativamente in JPEG
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Generico; fortemente raccomandato per immagini fotografiche senza particolari vincoli qualitativi

12. Il formato JPEG è un altro “pilastro” storico per le immagini raster, permettendo una loro rappresentazione generica e, soprattutto, estremamente compatta per via dell’uso di un algoritmo di compressione *lossy*, in cui alcuni parametri algoritmici sono selezionabili in fase di formazione del file, permettendo così un bilanciamento tra “qualità” dell’immagine<sup>21</sup> e dimensione del file. Le immagini sono inoltre codificate sempre in uno spazio-colore del tipo  $Y^w$  e sotto-campionate; non sono supportate le trasparenze. Nonostante queste carenze lo standard *EXIF* estende il formato per la sola rappresentazione di metadati interni, tra i quali possono essere presenti:

- informazioni sull’hardware o software usato per creare o modificare l’immagine (p.es. modello di fotocamera, ottiche, flash e altra apparecchiatura, con i loro parametri di scatto);
- data, ora ed eventuale posizione geografica della creazione;
- nome o altre caratteristiche dell’autore;
- eventuali licenze d’uso dell’immagine (Copyright©, Creative Commons, ecc.);
- informazioni colorimetriche (spazio-colore, punto di bianco, profilo ICC, ecc.);
- eventuale proiezione piana di uno spazio curvo (p.es. equi-rettangolare, altrimenti detta ‘latitudine/longitudine’ o, più impropriamente, “360°”).

13. Qualora si disponga delle medesime immagini in un formato di maggiore qualità (in termini di risoluzione, di assenza di compressione *lossy*, o altro), si consiglia di non riversare mai in JPEG il medesimo contenuto (a meno che non si tratti di una seconda copia per altri scopi).

TIFF	FORMATO DI FILE
Nome completo	Tagged Image File Format
Estensione/i	.tiff, .tif
Magic number	II 0x2A00; MM 0x002A
Tipo MIME	image/tiff
Sviluppato da	Adobe Systems
Tipologia di standard	proprietario (libero), estendibile, <i>de iure</i> , binario

<sup>21</sup> Da intendersi qui come fedeltà dell’immagine compressa (con perdite dovute alla compressione) rispetto all’immagine originale non compressa. Tale quantità è misurata con opportune metriche, tra cui quelle basate sul rapporto segnale-rumore percepito, o *pSNR*.

Livello metadati	4
Derivato da	–
Revisione	2004
Riferimenti	<ul style="list-style-type: none"> <li>• Adobe, <a href="#">TIFF™ Revision 6.0</a>, 1992</li> <li>• <a href="http://www.adobe.io/open/standards/TIFF">www.adobe.io/open/standards/TIFF</a></li> </ul> Famiglia di standard <b>12234</b> della ISO: <ul style="list-style-type: none"> <li>• ISO <a href="#">12234-2:2001</a>, TIFF/EP</li> <li>• ISO <a href="#">12234-3:2016</a>, XMP</li> <li>• ISO <a href="#">12639:2004</a>, TIFF/IT</li> <li>• <a href="#">RFC-2306</a>, TIFF-F</li> <li>• <a href="#">RFC-3949</a>, TIFF-FX</li> <li>• <a href="http://www.exif.org/Exif2-2.PDF">www.exif.org/Exif2-2.PDF</a></li> </ul>
Compressione	Sì, senza compressione
Racc. per la lettura	Generico con riconoscimento obbligatorio
Racc. per la scrittura	Specifico per l'editoria; raccomandato per la produzione di immagini raster finali

13. Il formato TIFF è il capostipite dei formati raster professionali, pur essendo ancora considerato appartenente alla categoria dei formati generali per le immagini raster. Nato con poche varianti e metadati prevalentemente per rappresentare immagini pronte sia per l'invio telematico (tramite fax) che per la stampa professionale –monocromatica o “offset”– è stato successivamente esteso dalla Adobe, fino a diventare uno standard aperto e *de iure*, con moltissime caratteristiche aggiuntive:

- segmentazione dell'immagine nel file per linee ovvero per riquadri;<sup>22</sup>
- segmentazione a più livelli sovrapposti;<sup>23</sup>
- spazi-colore con un qualsivoglia numero di canali (inclusa la trasparenza, o canale *alfa*);
- metadati aggiuntivi circa la rappresentazione spaziale (unità di misura, ecc.);
- metadati aggiuntivi circa le condizioni ideali per la visualizzazione (caratteristiche del monitor) o per la stampa professionale (intento di rappresentazione, codici di particolari colori “spot”, ecc.);
- compressione secondo vari algoritmi, generalmente *lossless*.

Infine, anche nelle immagini TIFF –come per le JPEG– possono essere inseriti metadati EXIF.

GIF	FORMATO DI FILE
Nome completo	Graphic Image file Format

<sup>22</sup> Utili per ottimizzarne l'archiviazione su alcuni storage, la trasmissione attraverso specifici canali, la robustezza in caso di corruzione.

<sup>23</sup> Utile per immagini in fase di post-produzione, cioè quando sono semilavorati le cui modifiche devono essere reversibili.

Estensione/i	.gif	
Magic number	GIF89a; GIF87a	
Tipo MIME	image/gif	
Sviluppato da	CompuServe	
Tipologia di standard	deprecato, proprietario (libero), <i>de iure</i> , binario, muto	
Livello metadati	1	
Derivato da	–	
Revisione	89a (1989)	
Riferimenti	• W3C, <a href="#">Graphics Interchange Format™</a> , ©1990 CompuServe	
Conservazione	No	
Racc. per la lettura	Generico con riconoscimento obbligatorio	
Racc. per la scrittura	Sconsigliato, tranne che in due casi legati al web	

14. Il formato GIF venne introdotto nella fine degli anni '80 per rappresentare immagini fotorealistiche quando le capacità dei computer di visualizzare simultaneamente molti colori erano limitate. Alcune delle novità tecniche di questo formato sono sopravvissute sino ad oggi, tanto che vi sono ancora molti casi d'uso soprattutto nelle pagine web. Anche se esistono oggi formati molto più adeguati per le immagini fotorealistiche, il formato, implementando fra le altre cose un'ana compressione *lossless*, è ancora tecnicamente valido per immagini con le seguenti caratteristiche:

- numero colori fino a un massimo di 256, scelti da una tavolozza con 32 bit di profondità;<sup>24</sup>
- supporto per una trasparenza assente ovvero totale,<sup>25</sup> senza diversi gradi di opacità;
- supporto per più immagini che si alternano in sequenza (con cadenza preselezionata) per rappresentare uno sprite dotato di caratteristiche di animazione basilari (si parla, in questo caso di “GIF animate”);<sup>26</sup>

Le immagini con bassissimi requisiti di animazione, trasparenza e numero di colori (tipicamente loghi o porzioni di elementi grafici minimalisti), come quelle che si trovano in diversi siti web, spesso salvate in questo formato.

<sup>24</sup> La tavolozza è quella di un generico modello RGB con 8 bit/canale, per un totale di  $2^{8+8+8} = 2^{32} \approx 16.8$  milioni di colori.

<sup>25</sup> Nel GIF la trasparenza è rappresentata da uno dei 256 colori della tavolozza, che può essere indicato come tale nei metadati interni.

<sup>26</sup> Le GIF animate sono ancora vincolate ad avere un massimo di 256 colori per fotogramma (inclusa la trasparenza), anche se i colori scelti possono cambiare da fotogramma a fotogramma.

16. A causa della sua obsolescenza, se ne sconsiglia l'uso per nuove immagini, salvo in cui l'immagine da archiviare sia destinata all'uso in pagine web e rientri, nella sua forma originaria (o formato di partenza) all'interno dei vincoli sopraelencati.

EXR		FORMATO DI FILE
Nome completo	OpenEXR™	
Estensione/i	.exr	
Magic number	v/1 0x01	
Tipo MIME	image/x-exr	
Sviluppato da	Industrial Light and Magic	
Tipologia di standard	aperto, estendibile, <i>de facto</i> , binario	
Livello metadati	4	
Derivato da	–	
Revisione	2013	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.openexr.com/documentation">www.openexr.com/documentation</a></li> <li>• WetaDigital, <i>The Theory of OpenEXR Deep Samples</i>, 2013</li> </ul>	
Conservazione	Sì, senza compressione	
Racc. per la lettura	Speciale; raccomandato in ambito cinetelevisivo	
Racc. per la scrittura	Speciale; raccomandato in ambito cinetelevisivo	

17. Il formato OpenEXR è stato recentemente inventato ed è oggi mantenuto, dalla comunità dei creativi dell'animazione cinematografica ma, a causa della sua versatilità e del supporto per un numero qualsiasi e facilmente estendibile di metadati, è oggi fortemente consigliato per la produzione di immagini raster –sia finali che, soprattutto, semilavorati– per la grafica e la produzione cinetelevisiva. A causa del formato specifico, non è richiesto il suo riconoscimento al di fuori delle organizzazioni dei sopracitati settori.

18. OpenEXR supporta immagini raster con le seguenti caratteristiche:

- segmentazione dell'immagine in vari modi diversi (per linee, a tasselli, per strati);
- supporto di più spazi-colore, inclusi astratti con un numero qualsivoglia elevato di canali (ciascuno associato ai propri metadati);
- supporto per un numero qualsivoglia elevato di livelli, ciascuno dotato dei propri metadati;
- data, ora ed eventuale posizione geografica della creazione;
- nome o altre caratteristiche dell'applicazione creatrice, ovvero dell'autore (se umano);
- eventuale supporto di vari algoritmi di compressione (sia *lossy* che *lossless*);
- supporto di metadati interni la cui tassonomia rientra in *namespace* estendibili.

19. Inoltre, grazie alla versatilità nel numero di livelli e di canali di colore (e la possibilità di identificarli ciascuno con un nome), è possibile memorizzare nei punti di un'immagine raster salvata in OpenEXR non soltanto il colore, quanto piuttosto informazioni relative ad altre caratteristiche tecniche, fisiche o cinetiche dell'immagine, rappresentabili punto per punto. Esempi sono:

- il cosiddetto “**deep EXR**”, ove più livelli sovrapposti mantengono una dei medesimi oggetti a diversi gradi di “profondità” rispetto ad immagini piane;
- le *texture*, che sono comuni raster, le cui coordinate cartesiane sono chiamate  $(u,v)$ , che rappresentano una “pelle” da avvolgere intorno ad una superficie artificiale tridimensionale (come quelle rappresentate in formati descritti in §2.7) mediante una trasformazione conforme che prende il nome, appunto, di *mappa uv*.

20. In alcuni casi, l'immagine tradizionalmente costituita da un raster ove i punti rappresentano dei colori è contenuta in un primo livello, mentre in altri livelli sono rappresentate altre quantità relative alla medesima immagine. Due esempi, estremamente riduttivi, di tali quantità, utili particolarmente nella produzione di effetti speciali digitali (VFX) e nell'animazione in CG (dall'inglese, “computer-grafica”), sono:

- *velocity map*, ove i 2 o 3 canali  $(u,v,w)$  associati ad ogni punto rappresentano le componenti cartesiane della velocità istantanea del punto della superficie;
- *optical map*, ove i canali (uno o più) associati ad ogni punto rappresentano caratteristiche ottiche del materiale in quel punto, quali ad esempio opacità/trasparenza, riflettanza, assorbanza, emittanza, ecc.

21. Per quanto riguarda i metadati interni, purtroppo, la mancanza di un registro unificato è causa del proliferare incontrollato degli stessi: unica pecca per un formato altrimenti validissimo e fortemente consigliato per la produzione di *qualsiasi* tipo di immagine raster.

JPEG2000		FORMATO DI FILE
Nome completo	JPEG 2000	
Estensione/i	.png	
Magic number	0x89 PNG 0x0D0A1A0A	
Tipo MIME	image/jp2	
Sviluppato da	Joint Photographic Experts Group	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	–	
Revisione	2020/1	

Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-3745</a></li> </ul> Famiglia di standard <b>15444</b> della ISO: <ul style="list-style-type: none"> <li>• <a href="#">ISO 15444-1:2016</a></li> <li>• <a href="#">ISO 15444-2:2004</a></li> <li>• <a href="#">ISO 15444-6:2013</a></li> <li>• <a href="#">ISO 15444-6:2011</a></li> <li>• <a href="#">ISO 15444-12:2015</a></li> </ul>
Conservazione	No
Racc. per la lettura	Speciale; raccomandato nell'elaborazione professionale di immagini in vari ambiti
Racc. per la scrittura	Speciale; raccomandato nell'elaborazione professionale di immagini in vari ambiti

22. Il formato JPEG2000 utilizza una compressione basata su trasformata *wavelet*, cosiddetta multi-risoluzione, poiché l'evidenza informatica ivi rappresentata codifica prima i dettagli "grossolani" (cd. a bassa frequenza) dell'immagine, poi i dettagli via via più "fini" (cd. ad alte frequenze). A fronte di una maggiore complessità nella produzione (i.e. nella compressione) dell'immagine, il vantaggio tecnologico offerto da questo formato risiede nel fatto che la decodifica successiva dell'immagine (i.e. la sua decompressione) può avvenire anche non integralmente e interrompersi a un certo livello. In tal caso viene riprodotta una versione "a banda ristretta", cioè a risoluzione inferiore dell'immagine originale, in quanto sono state usate componenti a bassa frequenza. L'uso del formato è dunque preferibile laddove l'utilizzo professionale sia vincolato da uno o più dei seguenti fattori:

- immagini di dimensioni molto grandi, comparate a
- basse capacità computazionali del dispositivo di visualizzazione;
- canale di comunicazione tra lo storage ove è archiviata l'immagine e il dispositivo di visualizzazione.

DICOM	FORMATO DI PACCHETTO
Nome completo	Digital Imaging and Communications in Medicine
Estensione/i	
Magic number	128 byte qualsiasi, seguiti da <b>DICM</b>
Tipo MIME	image/dicom
Sviluppato da	National Electrical Manufacturers Association
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Livello metadati	2
Derivato da	–
Revisione	2018
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://dicom.nema.org/medical/dicom">dicom.nema.org/medical/dicom</a>, ps3.10</li> <li>• <a href="http://dicom.nema.org/medical/dicom">dicom.nema.org/medical/dicom</a>, capitolo 7</li> </ul>
Conservazione	Sì, se lo sono tutti i file del pacchetto

Racc. per la lettura	Speciale; raccomandato in ambito diagnostica sanitaria
Racc. per la scrittura	Speciale; raccomandato in ambito diagnostica sanitaria

23. Il formato DICOM consente di aggiungere alle immagini raster diversi metadati relativi all'aspetto sanitario del loro contenuto, quali ad esempio un elenco di metadati facoltativi e non esaustivi comprende:

- il nome degli specialisti che hanno eseguito l'acquisizione, l'elaborazione o la refertazione,
- il nome e modello delle apparecchiature di acquisizione e parametri elettronici, fisico-chimici, meccanici impiegati per un dato esame diagnostico,
- la data, l'ora e il nome della struttura ove sia stato effettuato l'esame diagnostico,
- eventuali commenti sul pacchetto di immagini nella sua interezza (ad esempio il testo del referto), sulla specifica immagine, o su una porzione della stessa.

DNG		FORMATO DI FILE
Nome completo	Adobe® Digital Negative	
Estensione/i	.dng	
Specializzazione di	TIFF/EP	
Tipo MIME	image/x-adobe-dng	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario ( <u>brevettato</u> ), estendibile, <i>de iure</i> , binario	
Livello metadati	4	
Derivato da	TIFF™	
Revisione	10.1.0.0 (2017)	
Riferimenti	• Adobe, <u><i>Digital Negative (DNG) Specification v1.4.0.0, 2012</i></u>	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandato in ambito fotografico e cinetelevisivo	
Racc. per la scrittura	Speciale; raccomandato in ambito fotografico e cinetelevisivo	

24. Il formato DNG (“negativo digitale”) di Adobe consiste in una specializzazione del formato TIFF, dotato di diverse estensioni relative alla quantità di metadati di accompagnamento (che include, tra l'altro, l'intera gamma di metadati EXIF e XMP) ma soprattutto consente di memorizzare immagini grezze (“raw”) provenienti da sensori digitali con diverse caratteristiche elettroniche e geometriche. La procedura di conversione effettuata a monte permette di transcodificare un'immagine raster altrimenti memorizzata in formati di file per lo più proprietari del costruttore della fotocamera o cinepresa, mediante un applicativo che, al momento della

transcodifica, comprende il formato nativo e le informazioni sullo specifico modello dell'apparato di acquisizione. Il risultato è un'immagine visivamente fedele, identica all'originale, ma archiviata in un formato aperto e interoperabile, non più soggetto all'obsolescenza tecnologica né dell'apparato di acquisizione originario, né del formato di file proprietario di origine.

PSD		FORMATO DI FILE
Nome completo	Adobe® <i>Photoshop</i> ® Standard Baseline file	
Estensione/i	.psd	
Magic number	8BPS	
Tipo MIME	image/x-psd	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , binario	
Livello metadati	4	
Derivato da	–	
Revisione	2016	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.adobe.com">www.adobe.com</a></li> <li>• <a href="http://FSDeveloper.com">FSDeveloper.com</a>, <a href="#">Adobe Photoshop File Formats Specification 2006</a></li> <li>• <a href="https://github.com/layervault/psd.rb">github.com/layervault/psd.rb</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Specifico; obbligatorio in ambito beni culturali e comunicazione	
Racc. per la scrittura	Specifico; obbligatorio in ambito beni culturali e comunicazione	

25. Il formato nativo di Adobe *Photoshop*® si è evoluto notevolmente nel tempo e comprende attualmente la possibilità non solo di archiviare immagini a più livelli e con elevatissima variabilità tecnica,<sup>27</sup> ma anche informazioni vettoriali e tridimensionali di complemento alle immagini raster, che coadiuvano il loro utilizzo in molteplici contesti industriali, quali il design, la computer grafica (CG), l'architettura e la postproduzione cinetelvisiva. Si raccomanda l'utilizzo di questo formato per la creazione di semilavorati, particolarmente quando vadano elaborati dal particolare software applicativo in oggetto. Per l'archiviazione a lungo termine e la conservazione invece, si consiglia di riversare il contenuto in altri formati più aperti e interoperabili (quali OpenEXR, DNG o TIFF).

ARRIRAW		FORMATO DI FILE
Nome completo	ARRIRAW	
Estensione/i	.ari	
Magic number	ARRI 0x12345678; ARRI 0x78563412	

<sup>27</sup> Si segnala la presenza un dialetto del formato PSD specificatamente per archiviazione e riutilizzo di immagini di grandissime dimensioni: il *Photoshop Large Format* (formato molto simile all'originario, che adotta l'estensione di file .psb).

Tipo MIME	image/arriraw
Sviluppato da	Arnold & Richter Cine Technik GmbH
Tipologia di standard	proprietario (libero), estendibile, <i>de iure</i> , binario
Livello metadati	4
Derivato da	–
Revisione	2018
Riferimenti	<ul style="list-style-type: none"> <li>documentazione registrata SMPTE <a href="#">RDD30:2014</a></li> <li>documentazione registrata SMPTE <a href="#">RDD31:2014</a></li> </ul>
Conservazione	No
Racc. per la lettura	Speciale; riprese cinematografiche
Racc. per la scrittura	Speciale; sconsigliata la produzione al di fuori dell'ambito cinematografico

26. Il formato ARRIRAW è un formato proprietario della ARRI GmbH, ma aperto, utilizzato attualmente come formato nativo “*raw*” per le sue cineprese digitali, che è stato candidato per diventare standard SMPTE. Nonostante si tratti di un formato proprietario, ne è un esempio virtuoso, in quanto esso supporta più tipologie di codifiche di immagine, nonché di metadati avanzati a contorno dell'immagine stessa, quali le informazioni colorimetriche (codifica dello spazio-colore, parametri di correzioni impostati direttamente sulla cinepresa, importati *una tantum* da file, ovvero comunicati in tempo reale da un'applicazione con connessione di rete diretta sulla cinepresa), quelle relative all'area attiva del fotogramma, alla velocità di ripresa mediante TimeCode (il formato ne supporta fino a 7 tipi differenti e indipendenti fra loro), ai metadati di produzione, ecc. In teoria, il formato ARRIRAW potrebbe essere utilizzato per produrre nuove immagini raster in una miriade di codifiche e di formati.

DPX	FORMATO DI FILE	
Nome completo	Digital Picture Exchange	
Estensione/i	.dpx	
Magic number	SDPX, XPDS	
Tipo MIME	image/x-dpx	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	4	
Derivato da	Kodak® Cineon™	
Revisione	2.0 (2014)	
Riferimenti	<ul style="list-style-type: none"> <li>standard SMPTE <a href="#">ST268:2014</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Specifico; obbligatorio in ambito cinetelevisivo	

27. Il formato DPX (originariamente sviluppato da Kodak come evoluzione del formato Cineon<sup>®</sup> usato nell'omonimo scanner digitale per le pellicole cinematografiche 35mm e successivamente divenuto uno standard SMPTE) permette la rappresentazione di immagini raster con differenti caratteristiche tecniche, oltre a un considerevole numero di metadati. L'attuale versione 2.0 suddivide i metadati in quattro categorie: generici, cinematografici, televisivi e "utente". Tra i metadati delle categorie cinetelevisive vi è la possibilità di rappresentare indicazioni per collocare con precisione l'immagine come fotogramma di una particolare sequenza video, quali:

- numerazione del fotogramma relativa all'inizio della sequenza,
- TimeCode (con relativi *framerate* e modalità di scansione del fotogramma, cfr. §2.10),
- KeyKode<sup>™</sup> del fotogramma rispetto al rullo di pellicola fotochimica da cui è stato scansionato digitalmente (con relativa *film-speed*).

28. Il formato si presta dunque ad una rappresentazione di documenti video mediante pacchetti di file, ove ciascun fotogramma è archiviato in un file separato (cfr. pacchetto DI basato su DPX, cfr. §2.12). In linea di principio il formato DPX ammette tra i metadati anche quelli che associano colorimetria digitale rappresentata nel raster dalla densitometria dell'emulsione di partenza (da cui il fotogramma è stato scansionato) o di destinazione (sulla quale s'intende possa essere stampato digitalmente), anche se pochissimi applicativi per la postproduzione cinematografica ne fanno realmente uso. Nonostante il DPX sia stato l'indiscusso formato di riferimento per la produzione, postproduzione e archiviazione digitale di contenuti cinematografici sin dall'avvento del Digital Intermediate (DI, cfr. §2.12), tre fattori ne hanno rapidamente ridotto l'importanza:

- il declino della produzione cinematografica su pellicola e la consistente riduzione di processi di scansione digitale di tali pellicole (ora quasi esclusivamente effettuati a scopo di restauro e conservazione);
- il mancato utilizzo di moltissimi metadati rappresentabili nel formato DPX da parte di gran parte dei software applicativi, che avrebbe invece incrementato l'efficacia di tale formato;
- la comparsa di nuovi standard tecnologici per la rappresentazione dell'immagine digitale, quali ad esempio l'elevata latitudine di posa (HDR). A tale scopo l'SMPTE sta sviluppando una nuova versione più moderna del formato DPX.

29. Mentre si obbliga agli enti tecnici operanti nel settore della postproduzione, archiviazione e conservazione cinematografica di leggere immagini nel formato DPX, allo scopo di preservare l'accessibilità a contenuti provenienti da archivi in pellicola già digitalizzati o archivi digitali di DI basati su DPX, si raccomanda fortemente di considerare formati alternativi, quali ad esempio OpenEXR, ovvero i pacchetti di master interoperabile (IMF, cfr. §2.12).

ACES	
Nome completo	Academy Color Encoding System
Estensione/i	.exr, .mxf, .amf, .clf
Tipologie MIME	image/exr, application/mxf
Sviluppato da	Academy of Motion Picture Arts and Sciences
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i>
Derivato da	–
Revisione	1.1.0 (2018)
Riferimenti	Standard e bollettini tecnici dell'AMPAS: <ul style="list-style-type: none"> <li>• <a href="#">TB-2014-012</a>, <i>ACES version 1.0 component names</i></li> </ul> Famiglia di standard <b>ST2065</b> della SMPTE: <ul style="list-style-type: none"> <li>• <a href="#">ST2065-1:2012</a>, <i>Academy Color Encoding Specification</i></li> <li>• <a href="#">ST2065-4:2013</a>, <i>ACES image container file layout</i></li> <li>• <a href="#">ST2065-5:2016</a>, <i>mapping ACES into MXF container</i></li> <li>• <a href="#">ST2067-50:2018</a>, <i>IMF - Application #5: ACES</i></li> <li>• <a href="http://www.oscars.org/aces">www.oscars.org/aces</a></li> <li>• <a href="http://www.acescentral.com">www.acescentral.com</a></li> <li>• W. Arrighetti, 'The ACES: a professional color-management framework for production, post-production and archival of still and motion pictures', <i>Journal of Imaging</i>, Vol.3, N°4, pp.189-225, MDPI, 2017</li> </ul>
Conservazione	Sì
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; consigliato in post-produzione, archiviazione e conservazione di contenuti cinetelevisivi in ACES

30. Il sistema *Academy Color Encoding System (ACES)*, standard SMPTE introdotto dall'AMPAS, permette di descrivere in maniera unificata gli spazi-colore e i processi produttivi di elaborazione e trasporto del colore digitale nelle applicazioni professionali in campo cinetelevisivo. ACES si prefigge come una possibile soluzione alla rappresentazione di immagini raster (e video) catturate da dispositivi

e camere con molteplici colorimetrie (spesso proprietarie), al trasporto di metadati colorimetrici tra processi dominati da svariati *vendor*, e visualizzabili con una moltitudine di tecnologie di visualizzazione (p.es. LED, OLED, plasma, ecc., così come HDR+, Dolby Vision,<sup>®</sup> HLG, ecc.). Il trasporto di file codificati con la colorimetria ACES può avvenire sia con il formato OpenEXR con l'aggiunta di specifici vincoli e metadati<sup>28</sup> (standard [ST2065-4](#)), sia imbustando una sequenza di fotogrammi, già nel formato EXR, all'interno di un contenitore MXF (cfr. standard [ST2065-5](#) e §2.12) anch'esso con determinati vincoli e metadati. Ulteriori informazioni colorimetriche in ACES possono essere rappresentate accompagnando, il contenuto audiovisivo in un pacchetto di file contenente uno o più *sidecar file* nel formato AMF (cfr. §2.12).

## 2.6.1 Raccomandazioni per la produzione di documenti

1. Come già discusso sopra all'inizio della sezione, i formati di immagini raster vanno distinti innanzi tutto tra le finalità generiche e specializzate — queste ultime differenti a seconda dell'ambito: sanità, architettura e urbanistica, grafica e pubblicità (inclusa la produzione online), intrattenimento (inclusi l'animazione o CG, così come produzione, postproduzione ed effetti speciali cinetelevisivi).

2. Per i formati generici (PNG, JPEG, TIFF, GIF) sussiste in generale l'obbligo di riconoscimento. Nonostante tale obbligo in merito ai formati generali, le singole P.P.A.A., qualora accettino documenti informatici in formati di immagini raster generici tra quelli sopra elencati per un loro procedimento amministrativo o a scopo di conservazione, possono decidere di limitare ulteriormente l'accettazione di tali formati ad un loro sottoinsieme, specificatamente allo scopo di ridurre o uniformare i formati dei documenti.

3. Per la produzione di immagini raster, invece, la scelta dell'uno piuttosto che dell'altro formato generico, ovvero di uno di tali formati invece di uno specializzato, deve essere motivata da motivazioni tecniche ovvero da una valutazione di interoperabilità. In particolare si raccomanda:

- Il formato TIFF per immagini raster —generate o riversate in tale formato— dove la rappresentazione fedele del documento sia un vincolo tecnico o giuridico e dove la capacità di complementare l'immagine con trasparenze,

---

<sup>28</sup> Il vincolo principale è nell'assenza di compressione e nella codifica nello spazio-colore ACES2065-1 (standard [ST2065-1](#)); devono inoltre essere presenti alcuni metadati colorimetrici facoltativi del formato OpenEXR, più un metadata booleano specifico di ACES.

livelli aggiuntivi e un certo livello di “metadati tecnici” (e.g. spazio-colore, impostazioni di stampa o scansione, raccordo con dimensioni fisiche di rappresentazione, etc.) costituisca un valore aggiunto.

- Il formato JPEG per la produzione di immagini originali e rettangolari il cui scopo sia meramente rappresentativo e non probatorio; il livello di compressione per la produzione di tali immagini sarà dunque scelto in maniera adeguata a non compromettere lo scopo rappresentativo del documento.
- Il formato JPEG per il riversamento di immagini raster rettangolari ove la conservazione della qualità originale dell'immagine non costituisca un impedimento giuridico o non sia un vincolo esatto; in particolar modo si preferisca tale formato per immagini di provenienza fotografica, scegliendo anche in questo caso un adeguato livello di compressione.
- Il formato PNG per immagini raster –generate o riversate in tale formato– ove sia importante il mantenimento della qualità –rispettivamente massima o originale– solo relativamente ad una rappresentazione su schermi digitali non professionali. Sono un esempio di tale esigenza la produzione di immagini o fotografie digitali per l'utilizzo su pagine web o sulle GUI di software applicativi, così come loghi e altri simboli grafici, spesso coadiuvati da effetti di trasparenza.
- Il formato GIF per immagini raster che soddisfano i requisiti del formato precedente (PNG) salvo l'appartenenza all'ambito fotografico, ma abbiano in più almeno una delle seguenti caratteristiche tecniche:
  - utilizzo di un numero complessivo di valori colorimetrici non superiore a 256;
  - assenza di trasparenze, ovvero
  - impiego di soli due livelli di trasparenza: ‘trasparenza totale’ e ‘opacità totale’;
  - piccola animazione costituita da pochi fotogrammi, riprodotti ciclicamente o una sola volta, ove ogni fotogramma soddisfi le precedenti caratteristiche.

4. Per quanto riguarda settori specifici, si raccomanda invece l'utilizzo di formati specializzati nei settori produttivi di riferimento, quali editoria, grafica, pubblicità, sanità, edilizia, architettura, intrattenimento, produzione cinetelvisiva. Si raccomandano perciò le seguenti adozioni:

- Il formato OpenEXR (anche detto, colloquialmente, “EXR”) per immagini raster relative a produzione, postproduzione, archiviazione e soprattutto conservazione di contenuti cinetelvisivi, pubblicitari, videoludici, animazione e beni culturali — che si tratti di semilavorati, master o

documenti definitivi. Il formato sia inoltre corredato adeguatamente dal più ampio spettro possibile di metadati a scopo archivistico.

- Formato DICOM per tutte le immagini diagnostiche di provenienza sanitaria, adeguatamente corredato dai metadati di produzione e refertazione,
- Formato JPEG2000 per le immagini raster di grandi dimensioni di competenza territoriale (e.g. immagini satellitari, demaniali, catastali), urbanistico e militare.
- Formato DNG per scatti provenienti da fotocamere o cineprese digitali — siano essi generati o riversati dai formati nativi in tale formato.
- Formato DPX per fotogrammi provenienti direttamente da scansioni digitali di pellicole cinematografiche non ulteriormente elaborate (per le quali si preferisce un riversamento nel formato OpenEXR durante le fasi della postproduzione).
- Formato ARRIRAW per le immagini provenienti dal girato originale di cinecamere ARRI (quali quelle della famiglia ALEXA ovvero AMIRA) — salvo quando esigenze di produzione cinetelevisiva richiedano che le camere *formino* il loro girato direttamente in formati video che adottano compressione *lossy*.<sup>29</sup>
- Formato PSD per immagini definitive provenienti da, ovvero semilavorati destinati all'elaborazione da parte di software di fotoritocco specializzati che supportino tale formato — nativamente o per compatibilità.

5. Tra i formati sopra individuati, il PNG e le varianti di TIFF e OpenEXR (EXR) senza ausilio di compressione, ovvero con algoritmi di compressione privi di perdita (*lossless*), sono i formati più adatti alla conservazione. Possono essere adatti alla conservazione anche il formato JPEG ovvero le varianti di TIFF e EXR che adottino algoritmi di compressione, ma solo qualora le immagini siano state nativamente generate in codesti formati (p.es. provenienti da fotocamere ovvero scanner digitali). Sono dunque esclusi dalla conservazione i riversamenti di immagini in formati che aggiungono (o cambiano) algoritmi di compressione adottati. Gli eventuali algoritmi di compressione adottati in conservazione devono tuttavia essere algoritmi aperti, previsti e pienamente descritti nelle specifiche tecniche dei formati stesso (ovvero nelle cui specifiche tecniche sono riportati i nomi degli standard relativi a codesti algoritmi di compressione).

---

<sup>29</sup> Ad esempio, contenitori QuickTime o MXF (§2.12) che imbustano video Apple® ProRes® ovvero Avid® DNxHD™, cfr. §2.10.

## 2.7 Immagini vettoriali e modellazione digitale

1. Si chiamano vettoriali le immagini rappresentate nel file mediante una descrizione algoritmica della geometria e del colore che le compone, utilizzando tecniche descrittive più o meno complesse. I modelli multidimensionali sono una generalizzazione delle immagini vettoriali utilizzando tre o più dimensioni (a prescindere dal problema della visualizzazione, che è spesso demandato alle applicazioni più o meno specializzate).

2. La descrizione delle immagini vettoriali è fatta in uno spazio geometrico virtuale, mediante coordinate tipicamente adimensionali, sebbene nei metadati interni di alcuni tipi di file impiegati, e/o nelle informazioni metriche usate dalle primitive, possono essere presenti riferimenti a dimensioni reali. Anche la rappresentazione di caratteristiche quali colore, trasparenze o riflettanze può avvenire mediante una o più delle seguenti tecniche:

- coordinate di spazi-colore riferiti ad ambienti a luce emessa o riflessa (in inglese, rispettivamente, *output-referred* o *scene-referred*), ovvero ad altri tipi di colorimetrie.
- etichette di colore che rimandano a specifici cataloghi di vernici o altri coloranti (p.es. “blu cobalto”, “Pantone®33M”, “smalto dorato”, ecc.),
- etichette che rimandano a cataloghi di materiali, tipicamente specifici per applicazione o riferiti altrove mediante file o etichette che rimandano a basi di dati esterne (p.es. “mogano laminato”, “calcestruzzo”, “cristallo smerigliato”, “ebano lucido”, “lino”, “tartan”, ecc.).

3. La potenziale multidimensionalità rappresentata in questi file, e la loro caratteristica intrinseca di descrivere immagini scomposti in oggetti distinti (tipicamente primitive geometriche con caratteristiche aggiuntive quali nomi/etichette, colori, trasparenze, collegamenti logici ad altri oggetti, ecc.) consente di salvare anche informazioni circa l'animazione –automatica o programmabile– di alcuni oggetti rispetto ad altri.

4. I formati di file più usati e specifici per immagini vettoriali sono: SVG, Adobe® *Illustrator*® (.ai), Encapsulated PostScript™ (.eps).

5. I modelli digitali sono un'estensione delle immagini vettoriali (cfr. §2.7) ma a spazi con tre o più dimensioni. Anche in questo caso gli oggetti virtuali sono descritti in maniera geometrica e corredati da metadati. Le applicazioni principali per questi file sono la progettazione edile e industriale, l'architettura, l'intrattenimento e le scienze in genere.

6. I formati di file più usati per modelli bi- e tridimensionali sono ben distinti tra categorie aperte e categorie chiuse (sia rispetto alle specifiche che rispetto alla proprietà intellettuale — cfr. §2.7):

Tra i primi ci sono Autodesk® DXF, Autodesk® FBX, Blender (.blend), Wavefront OBJ, Google SketchUp (.skp), Stereolitography (.stl); tra i secondi, invece, figurano Autodesk® AutoCAD® (.dwg), Autodesk® Maya® (.ma, .mb), Autodesk® 3ds Max® (.3ds), Maxon® Cinema4D (.c4d).

SVG		FORMATO DI FILE
Nome completo	Scalable Vector Graphics	
Estensione/i	.svg, .svgz	
Specializzazione di	XML ( <i>namespace</i> <a href="#">svg</a> )	
Tipo MIME	image/svg+xml, image/svg+xml+zip	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, <i>de jure</i> , testuale	
Livello metadati	4	
Derivato da	–	
Revisione	1.1 (second edition)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">W3C Recommendation SVG 1.1 (2<sup>nd</sup> Ed.)</a>, 16 agosto 2011</li> <li>• <a href="https://github.com/W3C/svgwg">github.com/W3C/svgwg</a></li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Generico; fortemente raccomandato	

7. Il formato SVG, basato su XML, descrive un'immagine vettoriale componente per componente, utilizzando l'estendibilità del linguaggio per "etichettare" opzionalmente alcune parti di queste componenti affinché possano essere referenziate da altri documenti o applicativi (ad es., una pagina web in HTML e il suo foglio di stile CSS allo scopo di migliorare l'interattività con le immagini vettoriali). Data la sua versatilità e l'apertura dello standard è il formato fortemente raccomandato per l'uso, la trasmissione e la conservazione di tutte le immagini vettoriali.

C'è una nuova versione proposta per essere la futura [SVG 2.0](#); essa supporta alcune caratteristiche quali l'animazione dei componenti. Tale versione, tuttavia, non è allo stato attuale raccomandata.

ILLUSTRATOR		FORMATO DI FILE
Nome completo	Adobe® <i>Illustrator</i> ® artwork	
Estensione/i	.ai	
Specializzazione di	PDF, Encapsulated PostScript™	
Tipo MIME	application/illustrator	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario (libero), <i>de facto</i> , binario	
Livello metadati	3	

Derivato da	Adobe® Encapsulated PostScript™, Adobe® PDF
Revisione	2019
Riferimenti	• Adobe Developer Support, <i>Adobe Illustrator File Format Specification</i> , 1998
Conservazione	No; cfr. §2.8
Racc. per la lettura	Specifico; nessuna raccomandazione
Racc. per la scrittura	Specifico; non raccomandato salvo che per scambio di semilavorati (a breve termine) tra reparti di design

8. Il formato proprietario dell'applicativo di disegno vettoriale Adobe® *Illustrator*® è in realtà un contenitore di un tipo specializzato di documento PDF ovvero di Encapsulated PostScript™, contenente estensioni particolari interpretabili dall'applicativo. Il formato è evoluto parecchio con le versioni successive di *Illustrator*®, che però ha sempre mantenuto la retrocompatibilità totale. Essendo l'applicativo molto diffuso tale formato è qui indicato perché è uno standard di riferimento per documenti in particolari ambiti (editoria e grafica pubblicitaria). Mentre è un formato consigliato per dei semilavorati (qualora vadano elaborati tramite *Illustrator*®), si sconsiglia di utilizzarlo per la produzione di documenti destinati alla conservazione, valutando piuttosto un riversamento dei documenti esistenti in altro formato più interoperabile (e.g. SVG).

ENCAPSULATED POSTSCRIPT	FORMATO DI FILE	
Nome completo	Encapsulated PostScript®	
Estensione/i	.eps	
Specializzazione di	PostScript®	
Tipo MIME	image/eps, application/eps	
Sviluppato da	Adobe Systems	
Tipologia di standard	proprietario (libero), <i>de facto</i> , binario, deprecato	
Livello metadati	1	
Derivato da	PostScript®	
Revisione	3.0 (1992)	
Riferimenti	• Adobe, <u><i>Encapsulated PostScript File Format Specifications, v3.0</i></u> (1992)	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Specifico; raccomandato nei reparti di design	
Racc. per la scrittura	Specifico; non raccomandato	

9. Il formato EPS (Encapsulated PostScript™) è un dialetto del linguaggio PostScript™ (cfr. §2.1) con alcune distinzioni, come ad esempio la rappresentazione di un oggetto all'intero di una regione rettangolare confinata in una singola pagina

e la possibilità di memorizzare una “pre-visualizzazione” raster (cd. *previen*) dell'intero contenuto. Di fatto, il formato è utilizzato il più delle volte per rappresentare singoli disegni o immagini da allegare successivamente a documenti PostScript™ impaginati ovvero, per via dell'apertura del formato, importarlo in altri applicativi di elaborazione vettoriale. Dato che il contenuto del documento è descritto nel linguaggio omonimo, orientato alle primitive di stampa, i file EPS non descrivono le immagini vettoriali come “oggetti” nell'accezione moderna, non supportando scenari di utilizzo più modulari o estendibili, come invece permette la scelta di formati più evoluti, quali ad esempio l'SVG. Il formato Encapsulated PostScript™ è dunque raccomandato in lettura per aprire documenti già esistenti, ma si sconsiglia la produzione di altri documenti in tale formato, invitando inoltre le P.P.AA. a valutare il riversamento dei file esistenti in altri formati interoperabili (e.g. SVG).

ODG	FORMATO DI FILE
Nome completo	Open Document Graphics
Estensione/i	.odg
Magic number	XML imbustato dentro ZIP
Tipo MIME	application/vnd.oasis.opendocument.graphics
Sviluppato da	Organization for the Advancement of Structured Information Standards
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario
Livello metadati	3
Derivato da	–
Revisione	1.2 (2015)
Riferimenti	Famiglia di standard <b>26300</b> della ISO/IEC: <ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">26300-1:2015</a>, <i>ODF for Office Applications v1.2 - Part 1: OpenDocument Schema</i></li> <li>• ISO/IEC <a href="#">26300-3:2015</a>, <i>ODF for Office Applications v1.2 - Part 3: Packages</i></li> <li>• OASIS, <a href="#">Open Document Format for Office Applications (OpenDocument)</a>, v1.2 (2015)</li> </ul>
Conservazione	No; cfr. §2.8
Racc. per la lettura	Generico; raccomandato solo a scopo di riversamento
Racc. per la scrittura	Sconsigliato

10. Il formato ODG è il dialetto del formato OpenDocument (cfr. §2.3) per le immagini vettoriali; è incluso in questo elenco prevalentemente perché è completamente aperto ed è un necessario complemento agli altri dialetti, anche se il suo principale impiego è come allegato presente all'interno di testi impaginati (.odt), fogli di calcolo (.ods) e presentazioni multimediali (.odp).

DXF		FORMATO DI FILE
Nome completo	AutoCAD® Drawing Interchange Format	
Estensione/i	.dxf	
Magic number	– / AutoCAD Binary DXF 0x0D0A1A00	
Tipo MIME	image/vnd.dxf	
Sviluppato da	Autodesk	
Tipologia di standard	proprietario, libero, <i>de facto</i> , testuale e binario	
Livello metadati	2	
Derivato da	–	
Revisione	2020/1	
Riferimenti	• Autodesk, <a href="#">DXF Reference</a> , 2011	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Specifico; nessuna raccomandazione	
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione	

11. Pur trattandosi di un formato testuale (che descrive gli oggetti che compongono il modello o l'immagine mediante *primitive grafiche*) DXF permette una compressione facoltativa allo scopo di ridurre l'occupazione digitale del file. Tuttavia il numero di primitive grafiche utilizzate in questo formato non permette una rappresentazione con il medesimo livello semantico o di dettaglio tecnico di altri formati (p.es. i colori o i materiali); di conseguenza il formato non è completamente interoperabile con essi o con i loro applicativi.

DWF		FORMATO DI FILE
Nome completo	AutoCAD® Design Web Format	
Estensione/i	.dwfx, .dwf	
Magic number	–	
Tipo MIME	model/vnd.dwf, drawing/dwf, image/dwf	
Sviluppato da	Autodesk	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	3	
Derivato da	Open Packaging Convention	
Revisione	6.0	
Riferimenti	• Autodesk Knowledge Network, <a href="#">About DWF and DWFX Files</a> • ISO/IEC 29500-2:2012	
Conservazione	No; cfr. §2.8	
Racc. per la lettura	Specifico; raccomandato in applicazioni CAD	

Racc. per la scrittura	Specifico; raccomandato per scambio e archiviazione di disegni e modelli tecnici in ambito CAD
------------------------	--

12. Il formato DWF è stato specificatamente pensato per l'interoperabilità; è infatti basato, dalla versione 6.0, sullo standard ISO/IEC [29500-2](#) dell'*open packaging* (lo stesso usato da OOXML, §2.3), e dunque costituito da un file ZIP contenente più file differenti (XML per la descrizione del modello; PNG per le *preview* e le *texture*). Pur trattandosi di un formato testuale (che descrive gli oggetti che compongono il modello o l'immagine mediante *primitive grafiche*) il medesimo formato permette anche la compressione allo scopo di ridurre l'occupazione digitale del file. È spesso utilizzato come formato di interscambio e, tra tutti i formati imparentati, è quello con le specifiche più aperte, perciò è utilizzabile anche per archiviazione e conservazione.

DWG	FORMATO DI FILE	
Nome completo	Autodesk® AutoCAD® Drawing	
Estensione/i	.dwg, .dwt	
Magic number	AC1032 (le ultime cifre variano con versione)	
Tipo MIME	application/acad, image/vnd.dwg	
Sviluppato da	Autodesk	
Tipologia di standard	proprietario, libero, <i>de facto</i> , binario	
Livello metadati	2	
Derivato da	–	
Revisione	DWG 2018	
Riferimenti	<ul style="list-style-type: none"> <li>Autodesk, <a href="#">AutoCAD .dwg file format</a></li> <li>Open Design, <a href="#">Specification for .dwg</a>, v5.4.1 (2018)</li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Specifico; nessuna raccomandazione	
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione	

13. Il formato DWG è anch'esso proprietario ma ampiamente utilizzato per lo scambio di immagini vettoriali (prevalentemente bidimensionali) nel campo del disegno tecnico e dell'architettura.

FBX	FORMATO DI FILE	
Nome completo	Autodesk® FBX®	
Estensione/i	.fbx	
Magic number	AC1032	
Tipo MIME	model/vnd.fbx	
Sviluppato da	Autodesk	

Tipologia di standard	proprietario (libero), chiuso, estendibile, <i>de facto</i>
Livello metadati	3
Derivato da	–
Revisione	2019 Extension 2
Riferimenti	<ul style="list-style-type: none"> <li>• Autodesk Knowledge Network, <a href="#">Autodesk FBX Files</a></li> <li>• Blender Foundation, <a href="#">FBX Binary file format specification</a></li> </ul>
Conservazione	Sì; cfr. §2.8
Racc. per la lettura	Specifico; raccomandato per modelli di progettazione
Racc. per la scrittura	Specifico; sconsigliato in archiviazione/conservazione

14. Il formato FBX, proprietario e chiuso ma completamente libero nel suo utilizzo, è utilizzato da vari applicativi di modellazione tridimensionale (ambito CAD e altro) prevalentemente come formato di interscambio. La sua estrema versatilità e il supporto del formato da parte di diversi applicativi professionali lo renderebbero adatto anche per archiviazione e conservazione, se non fosse per l'assenza di specifiche tecniche condivise.

STL	FORMATO DI FILE	
Nome completo	Stereolithography file format	
Estensione/i	.stl	
Magic number	solid; –	
Tipo MIME	model/stl, model/x.stl-ascii binary	
Sviluppato da	3D Systems (Albert-Battaglin Consulting Group)	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i>	
Livello metadati	1	
Derivato da	–	
Revisione	2.0 (2009)	
Riferimenti	<ul style="list-style-type: none"> <li>• J.D. Hiller, H. Lipson, <a href="#">STL 2.0: a proposal for a universal multi-material additive manufacturing file format</a>, 2009</li> <li>• <a href="#">all3dp.com/what-is-stl-file-format-extension-3d-printing</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Specifico; obbligatorio nel campo della stampa 3D	
Racc. per la scrittura	Specifico; raccomandato nel campo della stampa 3D	

15. Il formato STL (da non confondersi con l'omonimo formato per sottotitoli, cfr. § 2.11) è uno dei tanti standard *de facto* ed interoperabili per la modellazione

tridimensionale industriale; recentemente si è affermato come formato d'elezione per la trasmissione di modelli per produzione tramite le tecniche di “stampa 3D” o stereolitografia. In quanto formato completamente aperto si consiglia il suo utilizzo per la produzione di prototipi con tale destinazione d'uso o loro archiviazione, anche se la mancanza di caratteristiche più avanzate (adatte alla prototipazione professionale (e.g. in ambito ingegneristico) non lo rendono un candidato ideale per qualunque modello tridimensionale.

### 2.7.1 Raccomandazioni per la produzione di documenti

1. Si raccomanda la creazione di immagini vettoriali e modelli tridimensionali in formati aperti ed interoperabili: per le immagini vettoriali sullo standard SVG del W3C viene adottato in un numero sempre crescente di contesti ed è oltretutto in continuo aggiornamento con nuove funzionalità.

## 2.8 Caratteri tipografici

1. Un esempio specializzato di immagine vettoriale –in questo caso bidimensionale e monocromatica– è costituita dal singolo “glifo” (i.e. carattere tipografico), per il quale possono essere rappresentate forme distinte nello stesso file. All'interno di un file di fonti tipografiche (*font* in inglese) esiste una tabella ove, per un sottoinsieme di tutti i possibili caratteri tipografici rappresentabili da un sistema operativo (e codificati mediante codici numerici negli standard ASCII, UNICODE, ovvero UTF-8 e UTF-16), è contenuta la rappresentazione vettoriale del glifo corrispondente al carattere. In un file di font ai caratteri può corrispondere più di un glifo, che rappresenta varianti di quel carattere a seconda del tipo (e.g. tondo o corsivo), del peso (e.g. sottile, regolare, grassetto, nero), di altri fattori stilistici (e.g. numerali vecchio stile o meno) e, in alcuni casi, della dimensione/grandezza del carattere per tener conto del cosiddetto “aggiustamento ottico”. In alcuni casi tali variazioni stilistiche dei glifi sono mantenute in file separati (ad esempio un file per ciascuna combinazione di tipi e pesi), che vanno a costituire dunque un “pacchetto di font” (cfr. definizioni date in §1.1.2).

2. Le seguenti famiglie di caratteri tipografici –organizzati in macro-tipologie– sono considerati “standard” da diversi organi di settore (come il [W3C](#)) — si leggano le raccomandazioni più sotto:

- “**bastoni**”: sans-serif, Arial, Helvetica, Trebuchet, Verdana, Lucida Sans, Comic Sans;
- **con grazie**: serif, Times, Times New Roman, Palatino, Georgia;
- **larghezza fissa**: monospace, Courier, Courier new, Lucida Console;
- **simboli**: Symbol, Zapf Dingbats, Webdings, Wingdings.

3. I caratteri tipografici di cui al punto precedente sono chiamati, all’interno delle Linee guida di cui questo Allegato fa parte, “font interoperabili”. Le P.P.A.A. che producono documenti informatici il cui contenuto dipende anche dai caratteri tipografici impiegati, si impegnano a prendere le misure tecnico-organizzative del caso (inclusa l’effettuazione di una valutazione di interoperabilità, cfr. §3.1), affinché la produzione di tali documenti includa i caratteri tipografici utilizzati nel file stesso ovvero sia costituito da un pacchetto di file contenente anche i caratteri tipografico. Qualora ciò non sia tecnicamente possibile, le P.P.A.A. si adoperano per utilizzare solamente caratteri tipografici interoperabili.

4. I formati più diffusi e interoperabili di font tipografici sono

- d) TrueType (.ttf) e la sua evoluzione, OpenType (.otf), utilizzati negli applicativi dei principali SO tradizionali e mobile;
- e) Web Open Font Format (.woff, .woff2), usati per le pagine web.

OPENTYPE		FORMATO DI FILE
Nome completo	OpenType®	
Estensione/i	.otf	
Magic number	OTTO 0x00	
Tipo MIME	font/otf, application/x-font-otf	
Sviluppato da	Microsoft, Adobe, Apple, Google	
Tipologia di standard	proprietario (libero), <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	TrueType®	
Revisione	1.8.3	
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC 14496-22:2015</li> <li>• Microsoft <a href="#">OpenType® specifications 1.8.3 (2018)</a></li> <li>• <a href="#">RFC-2361</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Specifico; obbligatorio	

TRUE TYPE		FORMATO DI FILE
Nome completo	TrueType®	
Estensione/i	.ttf	

Magic number	true 0x00	
Tipo MIME	font/ttf, application/x-font-ttf	
Sviluppato da	Apple, Microsoft	
Tipologia di standard	proprietario (libero), <i>de facto</i> , binario	
Livello metadati	1	
Derivato da	Adobe Type-1	
Revisione	1994	
Riferimenti	<ul style="list-style-type: none"> <li>• Apple Developer, <a href="#">TrueType™ Reference Manual</a></li> <li>• Microsoft <a href="#">Typography webpage</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Specifico; valutare utilizzo del formato OpenType	

WOFF	FORMATO CONTENITORE	
Nome completo	Web Open Font Format	
Estensione/i	.woff2; .woff	
Magic number	wOF2; wOFF	
Tipo MIME	font/woff2, application/font-woff	
Sviluppato da	Mozilla Foundation, Opera Software, Microsoft	
Tipologia di standard	proprietario (libero), <i>de iure</i> , binario	
Livello metadati	1	
Derivato da	OpenType®	
Revisione	2.0	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation, <a href="#">WOFF 2.0</a>, 2018</li> <li>• W3C Recommendation, <a href="#">WOFF 1.0</a>, 2012</li> <li>• <a href="https://github.com/W3C/woff">github.com/W3C/woff</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; raccomandato per tipografia di contenuti web	
Racc. per la scrittura	Specifico; raccomandato per caratteri nonstandard in pagine web	

## 2.8.1 Raccomandazioni per la produzione di documenti

1. Sia per l'utilizzo applicativo che per quello web si fanno le seguenti due raccomandazioni:

- a) Qualora di adoperino caratteri tipografici standard (come indicati all’inizio della sezione) i punti seguenti non costituiscono più raccomandazioni.
- b) Si includano sempre i file dei caratteri tipografici utilizzati nel documento (quando tali caratteri possono essere imbustati nel formato del documento),<sup>30</sup> ovvero si formi un pacchetto di file (cfr. §1.1.1) che comprenda anche tali caratteri tipografici.
- c) Qualora i caratteri tipografici siano utilizzati per rappresentare testi scritti (come semplice collezione di simboli), scegliere solo caratteri tipografici che contengano un numero sufficiente di glifi a rappresentare *almeno* i caratteri alfanumerici, di interpunzione e diacritici del linguaggio utilizzato, della lingua italiana e di quella inglese.
- d) Ottemperare, se possibile, alla raccomandazione 1. per i caratteri alfanumerici, di interpunzione e diacritici di tutte le lingue dell’Unione Europea;<sup>31</sup>
- e) Qualora dei caratteri tipografici non standard siano utilizzati per rappresentare testi scritti, mettere in atto tutte le metodiche tecniche e operative previste dai formati di file e di pacchetti utilizzati affinché, nel caso in cui i file dei caratteri tipografici non siano disponibili, l’applicativo usato per visualizzare, stampare o riprodurre il documento possa effettuare sostituzioni dei caratteri tipografici<sup>32</sup> con altri caratteri standard, senza che ciò risulti in una variazione sostanziale del contenuto informativo del documento.

2. Per ogni altra considerazione riguardo l’uso dei caratteri tipografici nei documenti informatici si rimanda alle *Linee guida sull’accessibilità* e alle *Linee guida di design*, anch’esse emanate dall’Agenzia per l’Italia Digitale.

## 2.9 Audio e musica

1. La rappresentazione digitale dei segnali audio è divisa in due categorie: quella per “forme d’onda” e quella, più indiretta, per metadati. Nel primo caso il segnale sonoro è rappresentato mediante un’approssimazione digitale dell’onda sonora, registrata o riprodotta. In fase di registrazione del sonoro la forma d’onda si ottiene mediante campionamento (misurato in numero di campioni per secondo, o *sample rate*) e quantizzazione (misurato in bit per campione); il prodotto di tali misure

<sup>30</sup> Come accade, ad esempio per alcuni tipi di file PDF (§2.1) di pacchetti IMF ovvero DCP (§2.12).

<sup>31</sup> Le raccomandazioni 1. e 2. servono a confermare, a priori, che il carattere tipografico può potenzialmente rappresentare altri caratteri tipografici e alfabetici qualora il testo andasse modificato ovvero tradotto in altra lingua.

<sup>32</sup> Tali sostituzioni possono avvenire anche a catena, purché terminino sempre con un carattere tipografico standard (denominato, in inglese, *fallback font*). Si consideri, come esempio, la seguente catena di sostituzioni tipografiche: Minion Pro > Minion Std > Noto Serif > Albertina > Times New Roman > Times > serif.

costituisce il **data-rate** audio (anche detto *bit-rate* perché misurato in bit per secondo). Un file o un flusso audio può rappresentare le forma d'onda di più sorgenti sonore contemporaneamente — dette “canali”.

2. I campioni audio di una forma d'onda possono subire una compressione digitale allo scopo di ridurre le dimensioni occupate. I formati più noti per la memorizzazione di tali segnali audio sono il Waveform RIFF (.wav), MP3, FLAC, OGG e Broadcast Wave (.bwf).


3. Nel secondo caso, invece, il file contiene una rappresentazione temporale di suoni pre-campionati (che possono essere contenuti nel medesimo file, o riferendosi a file esterni contenenti le loro forme d'onda) e degli eventuali effetti associati a tali campioni ovvero alla loro riproduzione. L'applicazione principale per tali file è la rappresentazione di brani musicali, ove il timbro di ciascuno strumento è associato a banche dati generiche di suoni (che obbediscono a standard quali General MIDI) ovvero salvato come forma d'onda esterna, mentre il file audio contiene la partitura completa, nota per nota. Appartengono a questa tipologia i file musicali registranti uno standard quale il MIDI (.mid).

WAV	FORMATO CONTENITORE	
Nome completo	[Broadcast] Waveform File	
Estensione/i	.wav, .bwf, .rf64	
Magic number	WAVE, RIFF	
Tipo MIME	audio/wave	
Sviluppato da	IBM; Microsoft	
Tipologia di standard	proprietario, libero, <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	Resource Interchange File Format (RIFF)	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">Microsoft, <i>Multimedia Data Standards Update</i> (1994)</a></li> <li>• <a href="#">RFC-2361</a></li> <li>• <a href="#">EBU Recommendation R111 (2007)</a></li> <li>• <a href="#">EBU - Tech 3285-1, <i>Broadcast Wave (BWF)</i> (2011)</a></li> <li>• <a href="#">EBU - Tech 3306, <i>RF64</i> (2018)</a></li> <li>• <a href="http://soundfile.sapp.org/doc/WaveFormat">soundfile.sapp.org/doc/WaveFormat</a></li> </ul>	
Conservazione	Sì, senza compressione	
Racc. per la lettura	Generico; obbligatorio per audio qualunque	
Racc. per la scrittura	Generico; fortemente raccomandato per audio qualunque	

MP3		FORMATO DI FILE / CODEC
Nome completo	MPEG-1, Layer 3	
Estensione/i	.mp3	
Magic number/FourCC	0xFFFB30; ID3 / mp3	
Tipo MIME	audio/mpeg	
Sviluppato da	Moving Pictures Expert Group	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	4	
Derivato da	MPEG-ES	
Revisione	1998	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 11172-3:1993</a></li> <li>• <a href="#">ISO/IEC 13818-3:1998</a></li> <li>• <a href="http://mpgedit.org/mpgedit/mpeg_format/MP3Format.html">mpgedit.org/mpgedit/mpeg_format/MP3Format.html</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Generico; raccomandato per contenuti musicali	

AIFF		FORMATO DI FILE
Nome completo	Audio Interchange File Format	
Estensione/i	.aiff, .aifc, .aif	
Magic number	AIFF; AIFC	
Tipo MIME	audio/aiff	
Sviluppato da	Moving Pictures Expert Group	
Tipologia di standard	proprietario (libero), estendibile, <i>de facto</i> , binario	
Livello metadati	3	
Derivato da	Electronic Arts® Interchange File Format (IFF)	
Revisione	1.3 (1991)	
Riferimenti	<ul style="list-style-type: none"> <li>• Apple Developer, <a href="#">Audio Interchange File Format: "AIFF"</a></li> <li>• <a href="http://www.mmsp.ece.mcgill.ca/Documents/AudioFormats/AIFF">www.mmsp.ece.mcgill.ca/Documents/AudioFormats/AIFF</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Nessuna raccomandazione	
Racc. per la scrittura	Nessuna raccomandazione	

FLAC		FORMATO DI FILE / CODEC
Nome completo	Free Lossless Audio Codec	
Estensione/i	.flac	

Magic number/FourCC	fLaC / FLAC	
Tipo MIME	audio/flac	
Sviluppato da	comunità open source	
Tipologia di standard	aperto (licenze <a href="#">GNU GPL</a> e BSD), <i>de facto</i> , binario	
Livello metadati	3	
Derivato da	–	
Revisione	1.3.2 (2017)	
Riferimenti	• <a href="http://xiph.org/flac">xiph.org/flac</a>	
Conservazione	Sì	
Racc. per la lettura	Specifico; raccomandato	
Racc. per la scrittura	Specifico; raccomandato	

RAW	FORMATO DI FILE	
Nome completo	Audio “Raw”	
Estensione/i	.pcm, .raw, .sam, ...	
Magic number	–	
Tipo MIME	audio/basic	
Sviluppato da	comunità open source e altri <i>vendor</i>	
Tipologia di standard	aperto, <i>de facto</i> , muto, binario	
Livello metadati	1	
Derivato da	–	
Revisione	–	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.fmtz.com/misc/raw-audio-file-formats">www.fmtz.com/misc/raw-audio-file-formats</a></li> <li>• <a href="http://en.wikipedia.org/wiki/Au_file_format">en.wikipedia.org/wiki/Au_file_format</a></li> <li>• <a href="http://www-mmmsp.ece.mcgill.ca/Documents/AudioFormats/AU">www-mmmsp.ece.mcgill.ca/Documents/AudioFormats/AU</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; raccomandato per le registrazioni ambientali	
Racc. per la scrittura	Specifico; raccomandato per le registrazioni ambientali	

VORBIS	CODEC	
Nome completo	Vorbis	
Profili	–	
Codice FourCC	vorb	
Sviluppato da	comunità open source	
Tipologia di standard	aperto, <i>de facto</i>	

Derivato da	–
Revisione	2015
Riferimenti	• <a href="http://Xiph.Org">Xiph.Org</a> , <a href="#">Vorbis I specification</a> , 2015 • <a href="http://xiph.org/vorbis">xiph.org/vorbis</a>
Conservazione	No
Racc. per la lettura	Specifico; raccomandato
Racc. per la scrittura	Nessuna raccomandazione

MusicXML		FORMATO DI FILE
Nome completo	MusicXML™	
Estensione/i	.musicxml	
Specializzazione di	XML	
Tipo MIME	application/vnd.recordare.musicxml	
Sviluppato da	W3C Music Notation Community Group	
Tipologia di standard	aperto, estendibile, <i>de facto</i> , testuale	
Livello metadati	4; cfr. §2.8	
Derivato da	MakeMusic® MusicXML, MuseData™, Humdrum™	
Revisione	3.1 (2017)	
Riferimenti	• <a href="#">W3C Community Group Final Report, MusicXML 3.1</a> , 2017 • <a href="http://www.musicxml.com">www.musicxml.com</a>	
Conservazione	Sì	
Racc. per la lettura	Specifico; raccomandato per le partiture musicali	
Racc. per la scrittura	Specifico; fortemente consigliato per partiture musicali	

MIDI		FORMATO DI FILE
Nome completo	Musical Instrument Digital Interface	
Estensione/i	.mid, .midi	
Magic number	MThd	
Tipo MIME	audio/midi, application/x-midi	
Sviluppato da	MIDI Manufacturers Association (MMA)	
Tipologia di standard	aperto, estendibile, <i>de facto</i> , binario	
Livello metadati	1	
Derivato da	–	
Revisione	1.1	

Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.midi.org/specifications">www.midi.org/specifications</a></li> <li>• McGill, <i>Standard MIDI-File Format Spec. 1.1.</i></li> <li>• McGill, <i>Standard MIDI Files (“SMF”).</i></li> <li>• RFC-6295</li> <li>• <i>General MIDI (“GM”) Specifications: GM1, Roland® GS, Yamaha® XG, GM2.</i></li> </ul>
Conservazione	Sì, purché adottando solo strumenti General MIDI
Racc. per la lettura	Specifico; obbligatorio per la riproduzione di musica strumentale; raccomandato per partiture musicali
Racc. per la scrittura	Specifico; raccomandato per partiture musicali con orchestrazione rappresentabile da questo standard

## 2.9.1 Raccomandazioni per la produzione di documenti

1. Per quanto riguarda la creazione di documenti audio (di entrambe le categorie elencate all’inizio della sezione) si raccomanda la scelta di formati interoperabili ed aperti: di conseguenza tutti i formati elencati –ad eccezione di AIFF– soddisfano tale caratteristica. Il wave, essendo in realtà un contenitore, è poi soggetto alla scelta del codec per rappresentare il contenuto audio. In questo caso si raccomandano codec aperti (come il “*raw*” non compresso, ovvero il PCM o il  $\mu$ -law). La scelta di formati “*raw*,” sebbene dettata spesso da esigenze contingenti, andrebbe evitata in quanto tali formati sono notoriamente muti (cfr. §1.2.2) e quindi può essere difficile ricostruire le caratteristiche, sia ambientali che tecniche, di registrazione e di campionamento.

2. Resta appannaggio delle singole organizzazioni valutare i parametri qualitativi in merito ai codec audio impiegati (ove sussistano come parametri variabili), tenendo conto ancora una volta di eventuali vincoli normativi, amministrativi e tecnologici. La scelta a priori dei parametri qualitativi può aiutare a standardizzare un processo e verificare che tutti gli organi coinvolti possano leggere o scrivere file con tali parametri.

3. Tra i formati sopra individuati, il WAV (con codifica PCM non compressa) e tutti i formati “*raw*” senza ausilio di compressione sono i formati più adatti alla conservazione. Nei casi in cui non si può evitare la compressione della forma d’onda, può essere adottato anche il formato FLAC.

## 2.10 Video

1. Un file (ovvero un flusso) video *strictu sensu* rappresenta una sequenza ordinata di immagini raster (dette fotogrammi — *frame* in inglese) riprodotte ad una velocità temporale fissa, espressa in numero di fotogrammi al secondo (alle volte si usa la sigla “fps” o, più impropriamente, l’unità di misura Hertz, “Hz”). Per il resto si applicano al video le stesse descrizioni relative alle immagini raster: risoluzione, profondità di colore, colorimetria, ecc.
2. Anche nel video, come per le immagini statiche e l’audio, è possibile implementare diversi algoritmi di compressione allo scopo di ridurre le dimensioni del file ovvero del flusso digitale. Quando la compressione riguarda individualmente e separatamente ogni singolo fotogramma si parla di compressione *intra-frame* (che è concettualmente identica a quella applicata alle immagini raster); quando la compressione utilizza le informazioni residue di un fotogramma (calcolate rispetto ai fotogrammi precedenti o antecedenti) si parla invece di compressione *inter-frame*.
3. Quest’ultima tipologia di compressione utilizza modelli matematici e statistici tipicamente più sofisticati di quelli usati nella prima tipologia, il che rende spesso l’operazione di codifica più lunga e laboriosa di quella di decodifica. Per il motivo di cui al punto precedente, la compressione *inter-frame* è raccomandata per applicazioni ove la tecnologia, le tempistiche e i costi si distribuiscano in modo da avere una generazione del video più lunga, laboriosa e in generale dispendiosa, a fronte di una minore complessità di decompressione a carico dei dispositivi riproduttori<sup>33</sup>.
4. Al contrario, la compressione *intra-frame*, isolando ogni fotogramma in un’evidenza compressa a se stante, pur non fornendo in generale gli stessi rapporti di compressione di quella *inter-frame*, la rendono spesso —ma non sempre— preferibile in due particolari casi d’uso:
  - quando sia frequente la riproduzione casuale del documento video, che consiste nel saltare da un punto all’altro della *timeline*<sup>34</sup> (discontinuità temporale) piuttosto che riprodurla sequenzialmente;
  - quando il documento debba potersi modificare (cioè aggiungendo, inserendo, sostituendo o eliminandone sue parti dalla *timeline*) senza alterarne la qualità.
5. Algoritmi di compressione *intra-frame* molto diffusi —non necessariamente associati a specifici formati di file— includono l’MJPEG, l’AVC-Intra (di proprietà di

---

<sup>33</sup> La compressione *inter-frame* favorisce dunque gli scenari d’uso ove la codifica (compressione) è effettuata una tantum da dispositivi centralizzati e computazionalmente potenti, a fronte di una riproduzione (decompressione) in serie, effettuata da una moltitudine di dispositivi riproduttori “*consumer*” con caratteristiche tecnologiche inferiori (inclusa la necessità di risparmio energetico). Un esempio tipico è la riproduzione cine-televisiva o in streaming on-demand, ove i riproduttori spaziano dai televisori ai *tablet*, agli *smartphone*.

<sup>34</sup> La *timeline* verrà definita in §2.12.

Panasonic®), la famiglia di codec proprietari ProRes® della Apple®, i vari video-codec (“VC”) della SMPTE e il derivato proprietario dal codec VC-3: la famiglia DNxHD® della Avid®.

6. Algoritmi di compressione inter-frame largamente diffusi sono invece MPEG-2, MPEG-4, H.264 (e una sua variante proprietaria: AVCHD), XAVC (detto anche impropriamente “H.265”) e la famiglia XDCAM™, anch’essa proprietaria e da non confondere con i formati del pacchetto di file usato nella medesima famiglia di prodotti (e in questo Allegato indicato in maniera tipograficamente diversa come “XDCAM”, cfr. §2.12).

HEVC / H.265		CODEC
Nome completo	High Efficiency Video Coding	
Profili	Main, High; 13 livelli	
Codice FourCC	hevc, h265, x265	
Sviluppato da	Joint Collaborative Team on Video Coding (JCT-vc)	
Tipologia di standard	proprietario (royalty per varie tipologie d’uso), de iure	
Derivato da	MPEG-H Part 2	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC 23008-2:2017</li> <li>• ISO/IEC 23008-2/Amd-1:2018</li> <li>• ITU-T Recommendation H.265 (2018)</li> <li>• ETSI TS-126-114 v15.7.0 (2019)</li> <li>• x265.org/hevc-h265</li> </ul>	
Conservazione	No	
Racc. per la lettura	Generale; raccomandato	
Racc. per la scrittura	Generale; sconsigliato per archiviazione	

H.264 / AVC		CODEC
Nome completo	Advanced Video Coding	
Profili	21 profili e 20 livelli	
Codice FourCC	h264, x264, avc1, davc, vssh, v264	
Sviluppato da	Joint Collaboration Team on Video Codec (JCT-vc)	
Tipologia di standard	proprietario (royalty per uso commerciale), de iure	
Derivato da	MPEG-4 Part 2 (Visual), H.263	
Revisione	2014	
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC 14496-10:2014</li> <li>• ITU-T Recommendation H.264 (2019)</li> <li>• ETSI TS-126-114 v15.7.0 (2019)</li> <li>• x265.org/hevc-h265</li> </ul>	
Conservazione	Sì, purché con profili e livelli almeno “High”	

Racc. per la lettura	Generale; obbligatoria la lettura
Racc. per la scrittura	Generale; raccomandato per archiviazione o conservazione di contenuti non cinetelevisivi ovvero master cinetelevisivi già sottoposti a elaborazione finale

MP4V		CODEC
Nome completo	MPEG-4 Part 2 MPEG-4 Visual	
Profili	21 profili (tra cui SP, ASP, SSTP)	
Codice FourCC	mp4v, mp42, avc1, v264	
Sviluppato da	Video Coding Experts Group (VCEG), Moving Picture Experts Group (MPEG)	
Tipologia di standard	proprietario ( <i>royalty</i> per uso commerciale), <i>de iure</i>	
Derivato da	H.263, MPEG-2 Part 2	
Revisione	2014	
Riferimenti	• ISO/IEC 14496-2:2004	
Conservazione	No	
Racc. per la lettura	Generale; obbligatoria la lettura	
Racc. per la scrittura	Generale; raccomandato per archiviazione non a lungo termine; sconsigliato in conservazione ovvero quando sono necessari ulteriori metadati	

H.263		CODEC
Nome completo	H.263 (XviD)	
Profili	vari profili	
Codice FourCC	h263, s263	
Sviluppato da	Video Coding Experts Group	
Tipologia di standard	proprietario ( <i>royalty</i> per uso commerciale), <i>de iure</i>	
Derivato da	MPEG-2 Part 2	
Revisione	2006	
Riferimenti	• ITU-T Recommendation <a href="#">Y.4414/H.263</a> (2005) • ETSI <a href="#">TS-126-141</a> v15.0.0 (2018)	
Conservazione	No	
Racc. per la lettura	Generale; obbligatoria la lettura	
Racc. per la scrittura	Generale; sconsigliata la produzione	

MPEG2		CODEC
Nome completo	MPEG-2 Part 2	
Profili	7 profili e 4 livelli	
Codice FourCC	mp2v	
Sviluppato da	Video Coding Experts Group, Moving Picture Experts Group	
Tipologia di standard	aperto, <i>de iure</i>	
Derivato da	MPEG-1	
Revisione	2018	
Riferimenti	• ISO/IEC 13818-2:2013	
Conservazione	Sì	
Racc. per la lettura	Generale; obbligatoria la lettura	
Racc. per la scrittura	Generale; sconsigliato per archiviazione e conservazione di contenuto cinetelevisivo professionale	

DNxHD		CODEC
Nome completo	DNxHD <sup>®</sup> / DNxHR <sup>™</sup> <sup>35</sup>	
Profili	vari <i>bit-rate</i> in Mb/s / LB, SQ, HQ, 444, HQX	
Codice FourCC	AVdn	
Sviluppato da	Avid	
Tipologia di standard	proprietario ( <u>licenza commerciale</u> ), <i>de facto</i>	
Derivato da	SMPTE VC-3	
Revisione	Codecs LE 2.7.3 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.avid.com">www.avid.com</a></li> <li>• <a href="http://avid.force.com">avid.force.com</a></li> </ul> Famiglia <b>st2019</b> di standard/raccomandazioni SMPTE: <ul style="list-style-type: none"> <li>• <a href="http://st2019-1:2014">st2019-1:2014</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione	

7. Il codec audio/video proprietario, indicato semplicemente come DNxHD<sup>®</sup>, dotato di compressione *lossy* e intra-frame, consiste in una specializzazione di alcuni profili del codec aperto VC-3 standardizzato dalla SMPTE (descritto altrove in questa sezione), adattato per l'utilizzo nella post-produzione non-lineare di documenti audiovisivi professionali. In particolar modo le essenze audio video sono vincolate a un insieme discreto di risoluzioni spaziali, profondità di colore, *framerate* e bit-rate costanti o variabili, ottimizzati per contenuti in risoluzione HD (1920×1080 punti,

<sup>35</sup> I nomi commerciali dei codec sono acronimi di 'Digital Nonlinear Extensible High Definition' e 'High Dynamic Range' rispettivamente.

si parla in questo caso di codec DNxHD<sup>®</sup>) e l’UltraHD 4K (3840×2160, si parla in questo caso di codec DNxHR<sup>™</sup>) che andranno successivamente montati e post-processati (ad esempio tramite operazioni di *color-grading* –in HDR o meno– *compositing*), possibilmente mediante operazioni “non-distruttive”, cioè riducendo il più possibile l’impatto che tali procedimenti di post-produzione avranno sulla qualità del documento masterizzato. La produzione del formato è chiusa e proprietaria, sebbene sia uno standard de facto del settore cinetelevisivo che diversi applicativi hardware e software sono in grado sia di produrre che di riprodurre. Nella loro declinazione nativa, le essenze audio/video con codec DNxHD<sup>®</sup> sono imbustate in un contenitore MXF (descritti nel §2.12) anch’esso dotato di particolari metadati. Tali metadati coadiuvano e semplificano il collegamento logico delle essenze audiovisive che, contenute in file separati, vengono associate insieme temporalmente da parte degli applicativi di montaggio non-lineare. È tuttavia possibile imbustare essenze DNxHD<sup>®</sup> n altri formati *wrapper*, come ad esempio il QuickTime.

PRORES	CODEC	
Nome completo	ProRes <sup>®</sup>	
Profili	Proxy, LT, 422, HQ, 4444, XQ, RAW	
Codice FourCC	apco, apcs, apcn, apch, ap4h, ap4x, aprh/aprn	
Sviluppato da	Apple Incorporated	
Tipologia di standard	proprietario ( <i>royalty</i> per la produzione), <i>de facto</i>	
Derivato da	Apple Intermediate Codec	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• Apple, <a href="#">ProRes White Paper</a> (2018)</li> <li>• Apple, <a href="#">ProRes RAW White Paper</a> (2018)</li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandato nel montaggio cinetelevisivo	
Racc. per la scrittura	Sconsigliato per l’archiviazione o conservazione.	

8. L’Apple ProRes<sup>®</sup> è un codec audio/video proprietario dotato di compressione *lossy* e intra-frame, specializzato anch’esso per il montaggio non-lineare di documenti audiovisivi professionali. È dotato di diversi profili cui sono associate profondità di colore e bit-rate predeterminati (mentre non vi sono vincoli alla risoluzione o al *framerate* come accade per altri codec)

AV1	CODEC	
Nome completo	AOMedia Video 1	
Profili	3 profili e 10 livelli	
Codice FourCC	av01	
Sviluppato da	Alliance for Open Media	

Tipologia di standard	aperto, <i>de facto</i>
Derivato da	VP9, VP10
Revisione	2018
Riferimenti	<a href="https://aomediacodec.github.io/av1-spec">aomediacodec.github.io/av1-spec</a>
Conservazione	No
Racc. per la lettura	Speciale; raccomandato per contenuti in <i>streaming web</i>
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

DASH / VP9		CODEC
Nome completo	Video Partition structured video codec #9	
Profili	–	
Codice FourCC	VP90	
Sviluppato da	Google	
Tipologia di standard	proprietario (libero), <i>de facto</i>	
Derivato da	VP8	
Revisione	2014	
Riferimenti	<ul style="list-style-type: none"> <li>• Google, <a href="#">VP9 bitstream &amp; decoding process specification v0.6</a> (2016)</li> <li>• ISO/IEC <a href="#">14496-12:2015</a></li> <li>• ISO/IEC <a href="#">14496-12:2015 /Amd 2:2018</a></li> <li>• Standard SMPTE <a href="#">ST2086:2014</a></li> <li>• <a href="http://www.webmproject.org/vp9">www.webmproject.org/vp9</a></li> <li>• <a href="https://github.com/webmproject/vp9-dash">github.com/webmproject/vp9-dash</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Speciale; raccomandato per contenuti in <i>streaming web</i>	
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione	

CINEFORM		CODEC
Nome completo	SMPTE Video Codec #5	
Profili	3 profili e 10 livelli	
Codice FourCC	CFHD	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, <i>de iure</i>	
Derivato da	GoPro® CineForm™	
Revisione	2016	
Riferimenti	Famiglia <a href="#">st2073</a> di standard SMPTE: <ul style="list-style-type: none"> <li>• <a href="#">ST2073-1:2014</a>, <a href="#">RP2073-2:2017</a>, <a href="#">ST2073-3:2015</a>, <a href="#">ST2073-4:2015</a>, <a href="#">ST2073-5:2015</a>, <a href="#">ST2073-6:2015</a></li> <li>• <a href="https://gopro.github.io/cineform-sdk">gopro.github.io/cineform-sdk</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	

Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione
------------------------	--

VC-3		CODEC
Nome completo	SMPTE Video Codec #3	
Profili	-, <b>HQ</b>	
Codice FourCC	AVdn	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, <i>de iure</i>	
Derivato da	SMPTE VC-2 (“Dirac Pro”)	
Revisione	2002	
Riferimenti	Famiglia <b>st2019</b> di standard/prassi SMPTE: <ul style="list-style-type: none"> <li>• ST2019-1:2014, RP2019-2:2016, ST2019-4:2014</li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; consigliato in post-produzione cinetelevisiva	

HDCAM		CODEC
Nome completo	HDCAM	
Profili	-, <b>SR [Lite]</b> , <b>SQ</b> , <b>HQ</b> ; diversi <i>bitrate</i>	
Codice FourCC	–	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	proprietario (libero), <i>de iure</i>	
Derivato da	Sony HDCAM™	
Revisione	2005	
Riferimenti	<ul style="list-style-type: none"> <li>• Standard SMPTE <a href="#">ST367M:2001</a> <i>Type D-11 HDCAM picture compression and data stream format</i></li> <li>• Standard SMPTE <a href="#">ST368:2002</a>, <i>for digital television tape recording - 12.65mm Type D-11 format</i></li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato per riprodurre e riversare repertori in nastri digitali HDCAM™ (formato D-11)	
Racc. per la scrittura	Speciale; sconsigliato per la produzione di nastri	

DIRAC Pro		CODEC
Nome completo	SMPTE Video Codec #2 “Dirac Pro”	
Profili	-, <b>SR [Lite]</b> , <b>SQ</b> , <b>HQ</b>	

Codice FourCC	Bbcd	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, <i>de iure</i>	
Derivato da	BBC "Dirac"	
Revisione	2016	
Riferimenti	Famiglie st2042 e st2047 di standard SMPTE: <ul style="list-style-type: none"> <li>• ST2042-1:2090, RP2042-2:2009, RP2042-3:2010,</li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione	

XAVC		CODEC
Nome completo	XAVC™	
Profili	H.264 livello 5.2	
Codice FourCC	Xavc	
Sviluppato da	Sony	
Tipologia di standard	proprietario ( <i>royalty</i> per uso commerciale), <i>de facto</i>	
Derivato da	MPEG-2, H.263, MPEG-4 Part 2	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.xavc-info.org">www.xavc-info.org</a>, <i>XAVC profiles and Operating Points v1.20</i> (2016)</li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Da <i>non</i> utilizzare per la produzione di documenti.	

XDCAM		CODEC
Nome completo	XDCAM™	
Profili	DVCAM, IMX, SD, EX, HD422, HD, SD422	
Codice FourCC	xdv1, xdv2, ..., xdv9, xdva	
Sviluppato da	Sony	
Tipologia di standard	proprietario ( <i>royalty</i> per uso commerciale), <i>de facto</i>	
Derivato da	MPEG-4 Part 2, MPEG-2 Part 2, DV	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://sonybiz.net">sonybiz.net</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione	

BRAW		FORMATO DI FILE
Nome completo	Blackmagic RAW	
Profili	XXXXX	
Codice FourCC	Braw	
Sviluppato da	Blackmagic Design	
Tipologia di standard	proprietario	
Derivato da	CinemaDNG™	
Revisione	2018	
Riferimenti	• <a href="http://www.blackmagicdesign.com">www.blackmagicdesign.com</a>	
Conservazione	No	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; sconsigliata la produzione	

AVC - INTRA		CODEC
Nome completo	AVC-Intra™	
Profili	2 <i>bit-rate</i> e 6 risoluzioni	
Codice FourCC	ai[5 1][p q 2 3 5 6]	
Sviluppato da	Sony	
Tipologia di standard	proprietario ( <i>royalty</i> per uso commerciale), <i>de iure</i>	
Derivato da	MPEG-4 Part 10	
Revisione	2014	
Riferimenti	• prassi raccomandata SMPTE <a href="#">RP2027:2012</a> • ISO/IEC <a href="#">14496-10:2014</a>	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandata la lettura	
Racc. per la scrittura	Da <i>non</i> utilizzare per la produzione di documenti.	

9. AVC-Intra deriva dal profilo High 10 Intra di H.264.

MJPEG		FORMATO DI FILE / CODEC
Nome completo	Motion JPEG	
Profili	A, B	
Codice FourCC	mjpg, mjpa, mjpg	
Sviluppato da	comunità open source	
Tipologia di standard	aperto, <i>de facto</i>	
Derivato da	JPEG	
Revisione	1998	
Riferimenti	• <a href="#">RFC-2435</a>	
Conservazione	Sì	
Racc. per la lettura	Generico con obbligo in lettura	

Racc. per la scrittura	Generico; consigliato per contenuti non cinetelevisivi che non necessitano di ulteriori metadati
------------------------	--

10. Il formato MJPEG, come recita il suo stesso acronimo, «Motion JPEG», è un formato video ove l'essenza video è codificata come una sequenza di immagini raster nel formato JPEG, adottando dunque una compressione *lossy* e intra-frame. Nonostante il formato sia datato, la sua semplicità di codifica lo rende ancora raccomandato in tutti gli utilizzi non professionali ove il documento informatico non abbia particolari requisiti di qualità (o comunque requisiti di qualità non superiore a quella della compressione JPEG scelta per l'essenza MJPEG).

## 2.10.1 Raccomandazioni per la produzione di documenti

1. I file e i flussi multimediali —e in particolar modo quelli video— contengono evidenze con caratteristica peculiare rispetto a tutte le altre tipologie di file: i flussi video (compressi o meno che siano) hanno una dimensione digitale elevata e, tipicamente, richiedono anche una banda passante minima in caso vadano formati, riprodotti o addirittura elaborati in tempo reale. Per questo motivo le scelte dei formati avranno un'elevata variabilità in base alla finalità d'uso e ai vincoli tecnologici ad esse collegati.<sup>36</sup>

2. Lo strumento della valutazione di interoperabilità (cfr. §3.1) può venire in contro alla risoluzione *ex ante* delle problematiche di cui al punto precedente, allo scopo di individuare prima i codec da usare per far fronte a tutte le esigenze e vincoli (normativi, amministrativi e tecnologici) in merito al documento video, durante il corso di tutto il suo ciclo vita.

3. Ciò detto, i codec da preferire per creare nuove evidenze video di uso generico —cioè avulse da casi d'uso peculiari di specifici settori quali la produzione, postproduzione e conservazione dei contenuti audiovisivi— sono quelli aperti e standard de iure, quali:

---

<sup>36</sup> Ad esempio, un'evidenza video potrebbe essere usata da un certo numero di utenze poco dopo la sua formazione, che richiedono tecnologie di elaborazione in tempo reale, a fronte delle quali è necessaria la produzione o la transcodifica in un codec ad elevato rapporto di compressione. Potrebbe anche esserci un vincolo di conservazione dell'evidenza originale piuttosto che di quella elaborata, che potrebbe avere o meno diversi requisiti di qualità. A fronte di questa seconda finalità, potrebbe essere pensato un procedimento per cui l'evidenza originale viene formata impiegando un codec senza compressione e la massima risoluzione possibile, mentre il file elaborato segue un ciclo vita diverso, al termine del quale possa o debba essere distrutto. Qualora anche il file elaborato vada conservato, potrebbe essere necessario prevedere un solo flusso, a fronte del quale andrebbe effettuata una scelta diversa riguardo alla transcodifica intermedia, allo scopo di assolvere ai vincoli qualitativi iniziali.

- **MPEG4 Part-10** (colloquialmente indicato con il nome di “H.264”) in quanto largamente diffuso soprattutto negli apparati di riproduzione software e hardware. Tale codec è da preferirsi per contenuti già montati e ricondotti ad una risoluzione e una qualità accettabile per tutto il ciclo vita del documento.
  - **MPEG2 Part-2** qualora il ciclo vita del documento video e le sue finalità d’uso impongano privilegiare la semplicità computazionale dell’algoritmo di decompressione rispetto a fattori quali la qualità o la dimensione binaria dell’evidenza.
  - Qualunque codec senza compressione, ovvero con una compressione priva di perdite. In tali casi sono valutabili tutte le rappresentazioni del documento video mediante **sequenze di file** (cfr. §2.12), ove i singoli file adottano formati con i medesimi requisiti di interoperabilità (cfr. §2.6) inclusa l’assenza di compressione ovvero la compressione *lossless*.
4. Nel caso di esigenze specifiche, si possono valutare anche altri codec, quali ad esempio:
- VP9 (anche detto “DASH”) qualora il contenuto sia stato generato per applicazioni multiplatforma (prevalentemente online) e non sia soggetto ad ulteriori modifiche.
  - VC-3 (in particolar modo la sua variante “commerciale”: l’Avid® DNxHD®) qualora il contenuto sia destinato al montaggio video (incluse successive archiviazioni del girato originale) e in assenza di ulteriori vincoli tecnologici.
5. Resta appannaggio delle singole organizzazioni valutare i parametri qualitativi in merito ai codec audio impiegati (ove sussistano come parametri variabili), tenendo conto ancora una volta di eventuali vincoli normativi, amministrativi e tecnologici. La scelta a priori dei parametri qualitativi può aiutare a standardizzare un processo e verificare che tutti gli organi coinvolti possano leggere o scrivere file con tali parametri.
6. I codec video più adatti alla conservazione –comunque tutti dotati di compressione con perdita– sono l’MPEG-4 Part-10

## 2.11 Sottotitoli, didascalie e dialoghi

1. Astrattamente, esiste una terza rappresentazione del suono legata ai *dialoghi* (rispetto a quelle descritte in §2.9) che consiste nella trascrizione più o meno letterale di ciò che una o più voci esprimono in una linea temporale, più eventualmente altre informazioni di contesto e ambiente.

2. La necessità di rappresentare il parlato in una forma leggibile è prevalentemente legata a quattro casi d'uso, in alcuni casi concorrenti fra loro:

- a) conservare dialoghi in forma scritta, eliminando la complessità tecnica o giuridica di conservare una registrazione multimediale degli stessi;
- b) arricchire un dialogo con ulteriori informazioni quali, ad esempio, il nome (o la qualifica) dei partecipanti, il momento esatto e la *consecutio* temporale con cui le frasi sono pronunciate;
- c) complementare il dialogo con informazioni relative all'ambiente o al contesto, a beneficio di spettatori ipoudenti o non-udenti, come nel caso di riproduzioni audiovisive;
- d) fornire la traduzione di testi e dialoghi in lingue diverse da quella o quelle determinate preventivamente per i destinatari individuati per un particolare contenuto audiovisivo.

3. Le trascrizioni giuridiche ottemperano complessivamente ai casi d'uso 1 e 2 (e 4 in caso di testimoni stranieri, ove siano effettuate da traduttori giurati). Invece le trascrizioni di dialoghi in ambito cinetelevisivo –chiamate in inglese, nella loro accezione più generale, *timed-text*– si dividono tradizionalmente in tre categorie:

- **sottotitoli** (in inglese *subtitles*, abbreviati in “*subs*”) — ottemperano al solo caso d'uso 4;
- **sottotitoli per non-udenti** (in inglese *deaf or hard-of-hearing*, ovvero *DHH*) — ottemperano al solo caso d'uso 3;
- **didascalie** (in inglese *closed captions*, ovvero *CC*) — ottemperano al caso d'uso 2 sebbene, sovente combinati con tipologie di sottotitoli di cui sopra, ottemperino anche ai casi 3 o 4.

4. Il settore dell'intrattenimento sta venendo rivoluzionato dalla comparsa di innovativi servizi di fruizione tramite internet dei contenuti audiovisivi sotto forma di flussi multimediali (i cosiddetti servizi **SVOD**, cioè *streaming video on-demand*); tali servizi consentono, tra le altre cose, una *localizzazione*<sup>37</sup> molto più puntuale, precisa e multilingua, che li rende ancora più pervasivi e globali.

5. La normativa di riferimento per sottotitoli e didascalie dal punto di vista di accessibilità e qualità (soprattutto quando sono mostrate in sincronia e sovrainpressione, rispettivamente, con essenze audio e video) è regolamentata in particolare dalla norma ISO/IEC [20071-23](#) del 2018.

**TTML**

FORMATO DI FILE

Nome completo Timed Text Markup Language

<sup>37</sup> La *localizzazione* è un processo riadattamento incrociato (in inglese *versioning*) di un contenuto rispetto a molteplici *territori*. Quando ciò riguarda il solo adattamento linguistico (anziché comprendere anche aspetti culturali, religiosi, giuridici) di audiovisivi, si parla più semplicemente di *riedizione*, che comprende il video, il *doppiaggio* per l'audio e la sottotitolazione (trascrizione di dialoghi e didascalie).

Estensione/i	.ttml, .dfxp	
Specializzazione di	XML ( <i>namespace</i> <code>tt</code> , <code>tt[p s m]</code> e altri)	
Tipo MIME	application/ttml+xml	
Sviluppato da	World Wide Web Consortium Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	Distribution Format Exchange Profile (DFXP)	
Revisione	1.0 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation <a href="#">TTML 2</a>, 2018</li> <li>• W3C Recommendation <a href="#">TTML 1 (3<sup>rd</sup> Ed.)</a>, 2018</li> <li>• ETSI <a href="#">EN-303-560</a> v1.1.1 (2018)</li> </ul> Famiglia <b>2052</b> di standard/raccomandazioni SMPTE: <ul style="list-style-type: none"> <li>• <a href="#">ov2052-0</a>:2013</li> <li>• <a href="#">st2052-1</a>:2013</li> <li>• ISO/IEC <a href="#">14496-30</a>:2018</li> <li>• EBU - <a href="#">Tech 3380</a>, <i>EBU-TT-D subtitling distribution format</i> v1.0.1 (2018)</li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Speciale; obbligatorio in campo cinetelevisivo	
Racc. per la scrittura	Speciale; raccomandato in campo cinetelevisivo	

6. Il formato [TTML](#) (precedentemente chiamato DFXP) è, ad oggi, la declinazione più generica e completa relativamente alle possibilità tecniche e operative di aggiungere ad un documento audiovisivo una o più trascrizioni differenti. Il formato, adottato sempre di più come standard a livello europeo (*de iure*: cfr. norma [EN-303-560](#) della ETSI) e internazionale<sup>38</sup> supporta qualunque tipo di lingua scritta e sue eventuali caratteristiche diacritiche (, integrando informazioni sulla presentazione dei sottotitoli all'interno del riquadro del video (posizione,<sup>39</sup> colore, dimensione, parametri tipografici completi), relativamente all'asse temporale (apparizione, scomparsa e altri effetti di animazione).

IMSC1	FORMATO DI FILE	
Nome completo	Internet Media Subtitles and Captions	
Estensione/i	.ttml	

<sup>38</sup> Esistono diversi standard *de facto*, quali ad esempio le [Linee guida di NETFLIX sulla sottotitolazione](#) (in inglese).

<sup>39</sup> È anche possibile specificare la profondità ("*Z-depth*") rispetto alla parallasse nel caso di sottotitoli su contenuti stereoscopici (S3D).

Specializzazione di	TTML	
Tipo MIME	application/ttml+xml	
Sviluppato da	World Wide Web Consortium	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	W3C Timed Text Markup Language, versione 2	
Revisione	1.1 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• W3C Recommendation, <a href="#">TTML profiles for IMSC 1.1</a>, 2018</li> <li>• Netflix, <a href="#">What does a properly formatted TTML file look like?</a></li> <li>• Netflix, <a href="#">Italian Timed Text Style Guide</a>, 2018</li> </ul>	
Conservazione	Sì; cfr. §2.8	
Racc. per la lettura	Speciale; raccomandato in campo cinetelevisivo	
Racc. per la scrittura	Speciale; raccomandato in campo cinetelevisivo	

7. Il W3C ha deciso di standardizzare ulteriormente il generico formato TTML, derivando perciò le specifiche [IMSC1](#) adottate, tra le altre cose dal formato di master interoperabile (IMF, cfr. §2.12). IMSC1 ha due profili: uno ove i sottotitoli sono rappresentati mediante solo testo, l'altro ove il sottotitolo è rappresentato da un'immagine (tipicamente nel formato PNG con supporto completo del canale alfa, cfr. §2.6). L'esigenza di introduzione di questo profilo è stata necessaria per il diffondersi di notevoli dialetti di TTML da parte di diversi organi di standardizzazione, che hanno portato il formato originale –originariamente disegnato per essere il più interoperabile possibile– a creare notevoli problemi di compatibilità.<sup>40</sup> Il profilo IMSC1, oltretutto, è stato concepito anche per ottemperare ad esigenze proprie della distribuzione dei contenuti, quali l'adattamento dei dialoghi a diverse revisioni del contenuto audiovisivo, alla riedizione dei dialoghi in altre lingue o secondo esigenze diverse (cfr. distinzioni fra le varie tipologie di dialoghi sincronizzati all'inizio della sezione), alla transcodifica dei sottotitoli in altro formato.

EBU-TT	FORMATO DI FILE	
Nome completo	EBU Timed Text (EBU-TT)	
Estensione/i	.xml	
Specializzazione di	XML ( <i>namespace ebutt[m s dt]</i> )	

<sup>40</sup> Tale problema si è aggravato per il fatto che –come accade anche per molti altri formati di file per sottotitoli e didascalie– vi è un elevato riutilizzo della medesima estensione di file per formati anche molto diversi fra loro, cfr. §1.1.3.

Tipo MIME	application/ttml+xml
Sviluppato da	European Broadcasting Union
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i> , testuale
Livello metadati	2
Derivato da	W3C Timed Text Markup Language, versione 1
Revisione	1998
Riferimenti	Famiglia 33x0 di standard tecnici EBU (2017): <ul style="list-style-type: none"> <li>• <a href="#">Tech 3350</a>, <i>part 1: subtitling format v1.2</i></li> <li>• <a href="#">Tech 3360</a>, <i>part 2: mapping EBU STL to EBU-TT v1.0</i></li> <li>• <a href="#">Tech 3370</a>, <i>part 3: mapping EBU STL to EBU-TT v1.0</i></li> <li>• <a href="#">Tech 3380</a>, <i>subtitling distribution format v1.0.1 (2018)</i></li> <li>• <a href="#">Tech 3390</a>, <i>part M: metadata definitions v1.0</i></li> </ul>
Conservazione	No; cfr. §2.8
Racc. per la lettura	Speciale; obbligatorio in campo cinetelevisivo
Racc. per la scrittura	Speciale; raccomandato il campo cinetelevisivo ove richiesto da applicativi o capitolati

8. La [EBU](#) ha adattato il formato TTML agli specifici vincoli del mondo dell'audiovisivo, definendo così una specifica del medesimo formato, chiamato **EBU-TT**.

Analogamente, anche la [SMPTE](#), ha definito una specifica TTML per i medesimi scopi, chiamata **SMPTE-TT**, che però è stata adottata prevalentemente dalla versione dei pacchetti per il cinema digitale (DCP) e quindi raccomandata in altra sezione di questo Allegato ad essi dedicata, cfr. §2.12.

STL	FORMATO DI FILE	
Nome completo	EBU Subtitling Data Exchange Format	
Estensione/i	.STL	
Magic number	0x3?3?3? STL	
Tipo MIME	-	
Sviluppato da	European Broadcasting Union	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	1	
Derivato da	-	
Revisione	1.0 (1991)	
Riferimenti	• EBU - <a href="#">Tech 3264</a> (1991)	

Conservazione	No
Racc. per la lettura	Speciale; raccomandato in campo cinetelevisivo
Racc. per la scrittura	Speciale; sconsigliato per la produzione e archiviazione

9. Il formato STL (da non confondersi con l'omonimo formato per modelli 3D per applicazioni stereolitografiche, cfr. §2.7) è stato per anni lo standard di riferimento in campo cinetelevisivo, perciò un grandissimo numero di contenuti risultano dotati di sottotitoli e didascalie in questo formato, in svariate lingue. Il formato tuttavia contiene solo indicazioni relative ai TimeCode ove i sottotitoli appaiono e scompaiono, al testo della lingua e a pochissime indicazioni visive su come presentare i sottotitoli, peraltro ampiamente non sempre utilizzate o rispettate dagli applicativi rispettivamente di creazione e riproduzione video.

### 2.11.1 Raccomandazioni per la produzione di documenti

1. Per la produzione di sottotitoli e didascalie in ambito cinetelevisivo, così come per finalità di conservazione, si raccomanda l'utilizzo del formato TTML del W3C, conforme al profilo IMSC1 e senza la specifica di caratteri tipografici esterni.

## 2.12 Contenitori e pacchetti di file multimediali

1. La registrazione e riproduzione di immagini e suoni contemporaneamente necessita innanzi tutto del sincronismo tra gli elementi costituenti un flusso multimediale. Per questo motivo tali flussi o file (a seconda del livello di astrazione adattato) sono disposti in una "linea temporale virtuale" (*timeline*, in inglese) che adotta un riferimento temporale autonomo<sup>41</sup> chiamato **TimeCode**.

2. Un esempio di sintassi per un TimeCode sincronizzato con un flusso video digitale (la cui unità indivisibile è il fotogramma) è, ad esempio, "04:23:56:07"<sup>42</sup>. Un esempio di sintassi per un TimeCode sincronizzato con un flusso audio digitale

<sup>41</sup> Per analogia, mentre la datazione di un'evidenza informatica mediante marcatura temporale è un riferimento temporale "assoluto", la temporizzazione di uno specifico punto della timeline è un riferimento temporale "relativo", che diviene assoluto solo nel momento in cui la riproduzione della timeline inizia ad un determinato istante temporale.

<sup>42</sup> Leggasi «4 ore, 23 minuti, 56 secondi e 7 fotogrammi» (i fotogrammi si azzerano al secondo in base al numero di fps, cfr. §2.10).

(la cui unità indivisibile è il campione sonoro) è, ad esempio, “00:06:32.01436”<sup>43</sup>. Più in generale i TimeCode sono normati da standard di riferimento, quali la raccomandazione [BT.1366](#) della ITU, la famiglia di standard [ST12](#) della SMPTE, la EBU [Tech 3097](#).

3. Nel caso multimediale un flusso o file contiene spesso evidenze informatiche diverse per audio, video, e altri tipi di metadati (quali ad esempio sottotitoli, informazioni per i non udenti, uno o più TimeCode di riferimento, ecc.), che sono complessivamente chiamate **essenze**. Esse –ciascuna potenzialmente codificata con parametri e algoritmi diversi– sono racchiuse in un unico file contenitore, il quale ne facilita il sincronismo (eventualmente grazie alla presenza di una o più essenze TimeCode) e le descrive allo scopo di migliorarne la riproduzione o l’utilizzo.

4. Le essenze possono a loro volta contenere più *canali*. Nel caso dell’audio essi sono associati ad un particolare dispositivo di riproduzione ovvero alla direzione spaziale della sorgente sonora, p.es. canale dei totali sinistra ( $L_t$ ), canale centrale (C), canale degli effetti a bassa frequenza (LFE), canale per il surround di destra ( $R_s$ ). Nel caso di immagini statiche o video, i canali possono codificare un singolo canale cromatico dello spazio-colore riprodotto (cfr. §2.6), ad es. rosso (R), verde (G), blu (B) ovvero uno di due stereogrammi (occhio destro e occhio sinistro):

5. Così come una partitura musicale descrive per prima cosa tutti gli strumenti coinvolti e contiene le informazioni –sia comuni che specifiche per ogni parte– affinché un’orchestra possa rieseguire il brano, allo stesso modo un contenitore multimediale può contenere uno o più dei seguenti fattori (la cui presenza possibile e/o obbligatoria dipende dallo specifico formato della busta, cfr. §1.1.1):

- informazioni globali circa il documento multimediale (e.g. titolo del film/brano, nome dell’autore/regista, anno di produzione, durata nominale, livello di censura, data/ora di masterizzazione del file, ecc.);
- numero e tipologia delle essenze presenti e loro suddivisione in “tracce” per la riproduzione; per ciascuna essenza possono essere presenti altri metadati come, ad esempio:
  - nome o altro tipo di descrizione dell’essenza;
  - codec dell’essenza (ad esempio tramite codice FourCC);
  - velocità dell’essenza video (fotogrammi/secondo) o audio (campioni/secondo);
  - nome e numero di canali dell’essenza video (e.g. RGB, RGB $\alpha$ , CMYK, ...; occhio destro/sinistro) o audio (e.g. monoaurale, stereo, quadrifonico, ‘5.1’, ‘7.1’, Dolby-E<sup>®</sup>, ‘22.1’, Dolby<sup>®</sup> Atmos<sup>™</sup>, ...);
  - in caso di essenza multi-canale, eventuale nome dei singoli canali;

---

<sup>43</sup> Leggasi «6 minuti, 32 secondi e 1436 campioni» (i campioni si azzerano al secondo in base al sample rate: p.es. 44100Hz, cfr. §2.9).

- profondità digitale dell'essenza immagine/video (bit/pixel) o audio (bit/campione);
- *data-rate* minimo, medio e/o massimo di ciascun essenza.
- lingua utilizzata per il parlato nell'audio (se presente) ovvero nei sottotitoli;
- 1 essenza video (nel caso di video stereoscopico potrebbe essere presente un'unica essenza con due canali, ovvero due essenze video distinte — una per ciascuno stereogramma, associati rispettivamente all'occhio destro e sinistro);
- 3 essenze audio (e.g. 'suoni ed effetti', 'colonna sonora italiana', 'colonna sonora inglese');
- 5 essenze sottotitoli (e.g. 'sottotitoli in italiano', 'sottotitoli in italiano per non-udenti', 'didascalie in inglese', 'sottotitoli in francese', 'didascalie in tedesco per non-udenti');
- 1 essenza TimeCode<sup>44</sup>.

6. Come primo vantaggio, l'utilizzo di un formato contenitore consente ad applicazioni di conservazione e archiviazione di estrapolare molte informazioni da un file complesso e di grandi dimensioni (quale spesso è il file multimediale) senza dover implementare tutti i possibili codec necessari per decodificarne le essenze audio\video (cosa necessaria, invece, per poter riprodurre il file). Inoltre, il formato contenitore separa molto nettamente, al suo interno, le evidenze informatiche delle singole essenze, permettendone un'estrapolazione segmentata, molto più efficace e spesso anche con economia di spazio di archiviazione e tempi di elaborazione.

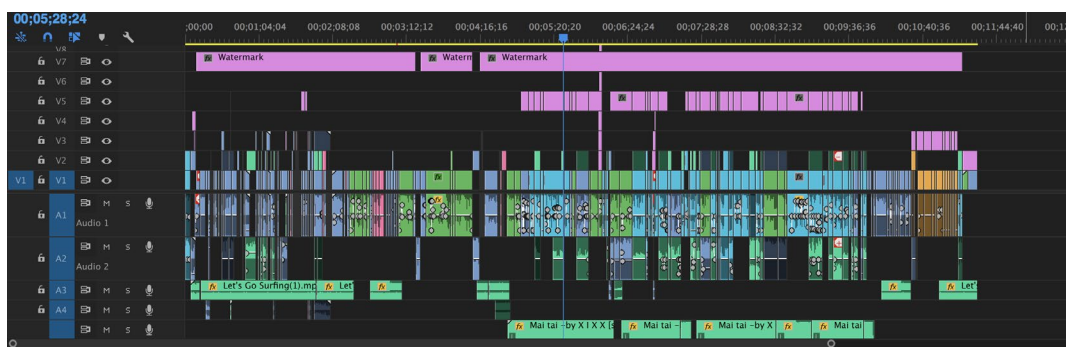
7. In alcuni casi di pertinenza multimediale, ad esempio, una o più essenze vengono ricodificate allo scopo di alternarne il *data-rate* o semplicemente per cambiare il codec utilizzato: si parla in tal caso, di *transcoding* delle essenze. Quando si cambia una o più essenze per un file multimediale (ad esempio per togliere una colonna sonora non più necessaria, aggiungere una traccia sottotitoli, ovvero sostituire una traccia video monoscopica con una stereoscopica) si parla di *re-wrapping*. Quando infine si cambia il formato di busta contenente l'intero file multimediale, ma mantenendo invariate le essenze, si parla di *trans-wrapping* — che è tipicamente un'operazione molto meno computazionalmente onerosa.

---

<sup>44</sup> Un esempio in cui sono presenti più tracce TimeCode è quando sono necessari più riferimenti temporali diversi (allo scopo di sincronizzare il flusso con altri sistemi informativi o altri flussi): ad esempio potrebbe essere presente un TimeCode "assoluto" espresso in orario diurno sulle 24 ore e uno "relativo" a un inizio temporale arbitrario rappresentato da "00:00:00:00".



**Figura 1** Esempio di una timeline semplice di un file multimediale con una traccia video (monoscopica) e una traccia audio binaurale (2 canali stereo).



**Figura 2** Esempio di una timeline di un file multimediale più complesso, con 9 tracce video (di cui una stereoscopica), 18 tracce audio mono o binaurali (cioè a 1 o 2 canali), 1 traccia TimeCode e diverse tracce sottotitoli nascoste.

8. Un'alternativa all'impiego di buste multimediali (cfr. §1.1.1) come sopra descritta è costituita dall'organizzazione delle singole essenze in file separati, poi riorganizzati in un pacchetto di file, ove le essenze siano logicamente associate fra loro in vari modi, come definito nel §1.1.2. Esempi di pacchetti multimediali sono ad esempio il pacchetto di master interoperabile (IMP), il pacchetto per il cinema digitale (DCP) e il pacchetto XDCAM, cfr. §2.12.

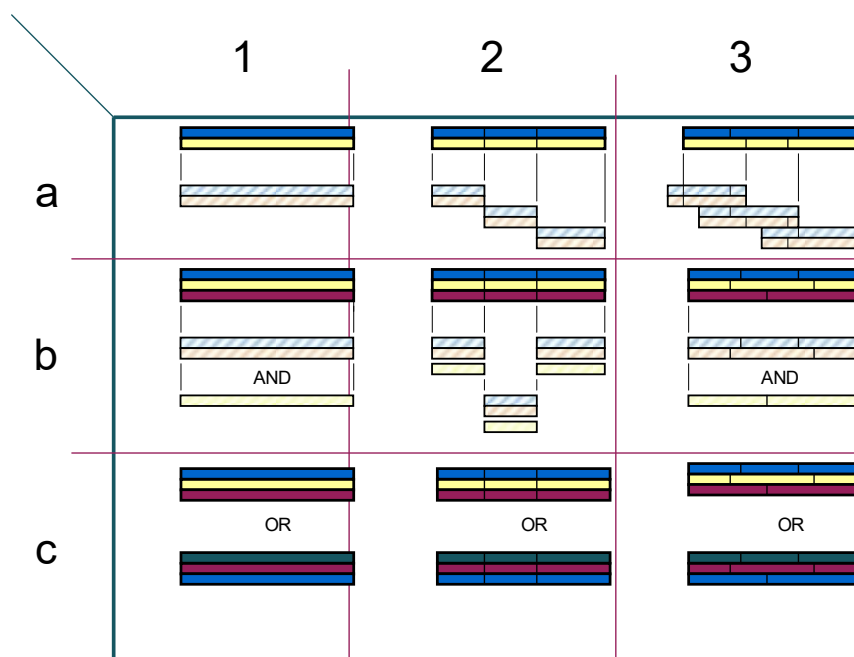
9. Per quanto riguarda le essenze video –nel caso di semilavorati o master di elevata qualità– è spesso preferito l'impiego della sola *naming convention*, ove ogni fotogramma del video è contenuto in un file separato, mentre i file sono numerati in sequenza cronologica (rispetto alla loro timeline relativa), costituendo dunque un pacchetto chiamato “sequenza di fotogrammi” (*frame sequence*, ovvero *frame-per-file* in inglese). Formati di immagini raster spesso adottati per tali sequenze di fotogrammi sono l'OpenEXR, il DPX (§2.6), così come il TIFF (soprattutto nei pacchetti DCDM), e il CinemaDNG (§2.12).

MXF		FORMATO CONTENITORE
Nome completo	Material Exchange Format	
Estensione/i	.mxf	
Magic number	–	
Tipo MIME	application/mxf	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	4	
Derivato da	–	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-4539</a> (2006)</li> <li>Documenti SMPTE, prevalentemente standard ('ST'):               <ul style="list-style-type: none"> <li>• base: ST377; EG41, EG42</li> <li>• schemi operativi: ST378, ST390–393, ST407, ST408</li> <li>• contenitori: ST379, ST381–389, ST394, ST405</li> <li>• registri e dizionari di metadati: ST380, ST436; RP210, RP224</li> </ul> </li> <li>• <a href="http://www.smpte.org">www.smpte.org</a></li> </ul>	
Conservazione	Sì, solo usando codec adatti alla conservazione	
Racc. per la lettura	Speciale; obbligo in lettura in tutti i settori audiovisivi	
Racc. per la scrittura	Speciale; raccomandato per la produzione, lo scambio e l'archiviazione di contenuti cinetelevisivi	

10. Il formato contenitore MXF è stato introdotto dalla SMPTE in un tentativo di standardizzare un formato per contenuti e flussi (cfr. §1.1.1) audiovisivi professionali che fosse utilizzabile lungo l'intera filiera cinetelevisiva, supportando il maggior numero di procedimenti: dalla produzione dei contenuti (camere digitali e animazione), attraverso tutte le fasi della post-produzione, sino alla distribuzione su diverse piattaforme (cinema digitale, televisione digitale terrestre e satellitare, streaming via internet, ecc.) e successiva archiviazione. Il formato MXF è regolamentato da diversi standard dell'SMPTE (fare riferimento alla tabella qui sopra), ma il principale fra loro è l'[ST377](#). Il contenitore è professionale in quanto estremamente flessibile nell'imbustare più essenze di tipologie differenti, e supportare un'ampia gamma di metadati interni, associabili a diversi livelli semantici del contenuto, incluse specifiche posizioni della timeline)<sup>45</sup>. I metadati supportati sono estendibili: oltre ad una serie di metadati minimi supportati, la SMPTE mantiene

<sup>45</sup> Metadati associabili a particolari posizioni della *timeline* sono, ad esempio, commenti e annotazioni di montatori, coloristi, tecnici digitali o assistenti alla regia; l'elenco delle persone reali (e.g. ospiti, attori) ovvero fittizi (personaggi) inquadrati in quel momento.

un registro ove ad ogni semantica è associato un codice binario (*UL*, ovvero *unified label* in inglese). Il registro è consultabile applicativamente o interattivamente sul sito [smpte-ra.org](http://smpte-ra.org), ovvero direttamente sotto forma di [XML](#) (§2.2). Per supportare molteplici casi di utilizzo, procedure di elaborazione e di tecnologie di stoccaggio e trasporto dei contenuti e dei flussi multimediali, le essenze stesse possono essere disposte in una molteplicità di strutture differenti all'interno dell'evidenza informatica complessiva. Ad esempio, la registrazione simultanea e in tempo reale, nel medesimo file MXF, di due flussi video provenienti da una cinepresa stereoscopica e di flussi audio provenienti da più microfoni disposti in scena, prevede che le essenze audio e video siano disposte in maniera “interlacciata”: il contenitore MXF avvolge perciò, sequenzialmente, ciascun fotogramma, seguito dalle essenze audio relative alla durata del medesimo fotogramma, seguito dal fotogramma successivo e così via.



**Figura 3** Tassonomia degli schemi operativi del formato MXF: sulle ascisse è rappresentata la complessità della timeline (indicata con un numero ordinale); sulle ordinate quella dei pacchetti (indicata con una lettera minuscola).

11. Per completare la descrizione di insieme del formato MXF, la SMPTE fornisce degli **schemi operativi** (*operational patterns* in inglese, abbreviati in **OP**), per i quali si invita a far riferimento ai relativi standard in tabella (oltre che allo standard principale [ST377](#)). In questi schemi operativi una timeline è astratta ulteriormente separando la suddivisione (e la “complessità”) delle sue tracce e canali, dall’insieme di file (“pacchetti materiali”) da cui è logicamente composta. In una tale tassonomia un contenuto multimediale (un’unica timeline) è rappresentato da un *pacchetto di contenitori MXF*, ciascuno contenente una o più essenze. La costruzione della

timeline logica del contenuto a partire dai file MXF costituenti può avvenire in modi diversi, la cui complessità dipende da una duplice organizzazione virtuale. Da una parte vi è quella delle essenze lungo la timeline (cfr. l'elenco alfabetico per righe, di complessità crescente, in **Figura 2**):

- a. ogni istante della timeline è riferito a una o più essenze contenute in un unico file;
- b. ogni istante della timeline è riferito a più essenze contenute in uno o più file;<sup>46</sup>
- c. vi sono due o più timeline alternative<sup>47</sup>, ciascuna delle quali è riferita a una o più essenze contenute in uno o più file;

Dall'altra vi è l'organizzazione di come le varie essenze della timeline siano distribuite in un pacchetto di uno o più file (cfr. l'elenco numerico per colonne, di complessità crescente, nella medesima **Figura 2**):

1. il pacchetto contiene essenze usate interamente e della medesima durata della timeline;<sup>48</sup>
2. il pacchetto contiene più sequenze di essenze, usate interamente, adiacenti fra loro lungo la timeline;<sup>49</sup>
3. il pacchetto contiene più sequenze di essenze, ciascuna delle quali (contenuta in file differenti) può essere usata parzialmente o interamente.<sup>50</sup>

12. Ad esempio, lo schema operativo **OP1a** corrisponde a quello della singola clip audio/video con le cui essenze sono tutte di pari durata<sup>51</sup>, dove cioè un singolo file contiene all'interno l'audio, il video e gli eventuali sottotitoli e può quindi essere riprodotto autonomamente dall'inizio alla fine. Lo schema operativo **OP3c**, invece, prevede un montaggio asincrono tra le varie tracce, con i contenuti potenzialmente estratti da essenze di durata più lunga e contenuta in diversi file del pacchetto e, in più, la possibilità che vi siano più montaggi alternativi tra cui scegliere. Gli schemi operativi permettono di indicare queste differenti tipologie mediante metadati nei file MXF costituenti il pacchetto, ma anche di vincolarli logicamente fra di loro, cosa particolarmente utile sia nel caso in cui i file perdano l'affinità per referenza

---

<sup>46</sup> Nel gergo del montaggio audiovisivo, si dice che tali essenze sincronizzate sono 'in *gang*' (letteralmente, "raggruppate") fra loro.

<sup>47</sup> La selezione di una delle timeline alternative, o il passaggio dall'una all'altra, non fanno parte dello schema operativo, anche se ciò è solitamente computo in automatico dall'applicazione che riproduce il contenuto, ovvero da una scelta manuale dello "spettatore".

<sup>48</sup> In questo caso la timeline è fatta da una sola sequenza (o "taglio"), la cui riproduzione coinvolge per intero le essenze di uno o più file.

<sup>49</sup> In questo caso la timeline è fatta da più sequenze (o "tagli"), fra loro contigue nel tempo, come avviene nel caso d'uso della *playlist*.

<sup>50</sup> Questo è lo scenario tipico usato nel montaggio audiovisivo, ove porzioni di clip "sorgenti" sono montate in una timeline, tipicamente separate da tagli netti.

<sup>51</sup> Un altro schema operativo non descritto in Figura è l'**OP-Atom**: una variante dell'**OP1a** ove le essenze sono inoltre tutte auto-contenute in un singolo file.

(venendo archiviati in percorsi differenti o non stabili nel tempo), sia nel caso di successive modificazioni del contenuto. In quest'ultimo caso, modifiche parziali del contenuto multimediale vengono effettuate sui soli file MXF che contengono le essenze interessate, senza ricostruire o modificare il contenuto nella sua interezza. Più avanti sono descritti alcuni pacchetti di file che implementano proprio questa flessibilità degli schemi operativi del contenitore MXF: il formato di master interoperabile (IMF) e il pacchetto di cinema digitale (DCP).

13. Per tutti i motivi sopra esposti il contenitore MXF è fortemente raccomandato come formato contenitore d'elezione per la produzione e il riversamento di qualunque contenuto multimediale (audio, video, dialoghi), accompagnato ovviamente da una scelta adeguata dei codec da impiegare.

MP4		FORMATO CONTENITORE
Nome completo	MPEG-4, Part 14	
Estensione/i	.mp4, .m4a, .m4v	
Magic number	0x00000000 ftyp	
Tipo MIME	video/mp4, audio/mp4	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	Apple® QuickTime™, MPEG-4 Part 12	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ISO/IEC 14496-14:2018</a></li> <li>• <a href="#">ISO/IEC 14496-12:2015</a></li> <li>• <a href="#">RFC-4337</a> (2006)</li> <li>• <a href="#">mp4ra.org</a></li> </ul>	
Conservazione	Si	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Generico; altamente consigliato per la produzione audiovisiva generica di contenuti auto-consistenti	

14. La parte 14 del gigantesco standard MPEG-4 della ISO, ma anche contenuta nella [RFC-4337](#) (più colloquialmente chiamata *MP4*) descrive uno standard *de iure* derivato moltissime sue caratteristiche dal formato Apple QuickTime (si legga sotto). Per questo motivo, e anche a causa della sua elevata versatilità sia nel numero e tipologie di essenze supportate al suo interno, che per la capacità di includere molteplici metadati interni nel file, è obbligatoria la capacità di leggere tale contenitore da parte di qualunque organizzazione, mentre è fortemente consigliato di adottarlo per la produzione di documenti solo video o audiovisivi — laddove non sia preferibile un formato con gradi di interoperabilità ancora maggiori — quale IMF ad esempio (sotto descritto).

IMF		FORMATO DI PACCHETTO
Nome completo	Interoperable Master Format	
Estensione/i	[.pkl cpl], .xml, .mxf, ...	
Tipologie MIME	application/xml, /mxf, ...	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i>	
Livello metadati	4	
Derivato da	SMPTE Digital Cinema Package	
Revisione	2019	
Riferimenti	Famiglia di standard <b>ST2067</b> della SMPTE: <ul style="list-style-type: none"> <li>• <b>base:</b> ST2067-1, ST2067-2:2013, ST2067-3:2016, ST2067-5:2012, ST2067-101:2017, ST2067-102:2014, ST2067-200:2018;</li> <li>• <b>audio:</b> ST2067-6:2012, ST2067-8:2013;</li> <li>• <b>applicazioni:</b> ST2067-10, ST2067-20:2013, ST2067-21:2016, ST2067-30:2013, ST2067-40:2017, ST2067-50:2018</li> <li>• SMPTE RDD47:2019, <i>Isosynchronous Stream of XML Documents (ISXD) plugin</i></li> <li>• SMPTE Report, <i>TTML features for IMF Data essence</i>, 2012</li> <li>• <a href="http://www.smpte.org">www.smpte.org</a></li> <li>• <a href="http://www.imfug.com">www.imfug.com</a></li> </ul>	
Conservazione	Sì, con Applicazioni IMF che usano codec conservabili	
Racc. per la lettura	Speciale; obbligatorio per il trattamento e l'interscambio di master e semilavorati cinetelevisivi	
Racc. per la scrittura	Speciale; obbligatorio per interscambio, archiviazione e conservazione di contenuti cinetelevisivi.	

15. Il **formato master interoperabile (IMF)** è descritto dalla famiglia di standard **ST2067** della SMPTE ed è nato dall'esigenza condivisa dai maggiori studi cinetelevisivi del mondo di gestire e conservare contenuti audiovisivi in maniera organizzata e attenta all'impatto che tale tipo di documenti, –per effetto delle loro grandi dimensioni informatiche– hanno nei processi di produzione, trasferimento, archiviazione, localizzazione e distribuzione internazionale. Una metodologia che è stata seguita nell'individuazione di tale formato è quella di massimizzare il riutilizzo di porzioni di contenuti audiovisivi che sono identici fra l'oro, archiviate nello stesso formato di pacchetto. Ciò avviene immancabilmente nelle riedizioni del medesimo contenuto (in caso di doppiaggio e altri adattamenti), nonché quando lo stesso master viene trasferito tra più enti durante le fasi di post-produzione, distribuzione e archiviazione.

16. Un documento informatico in tale formato è chiamato ‘pacchetto master interoperabile’ (*IMP*) e comprende sempre dei contenuti multimediali rappresentati nel tempo lungo una timeline (cfr. §2.10 articolo 1), chiamata *composizione*.

17. IMF utilizza ampiamente le caratteristiche di estendibilità offerte dal formato XML (usato per file *sidecar* di un IMP, che ne contengono i metadati globali), così come l’interoperabilità della busta MXF e dei suoi schemi operativi, per contenere le essenze audio, video, oltre ai dialoghi e ad altri metadati “temporali” (cioè localizzati cronologicamente in punti specifici della timeline).

18. Un IMP contiene sempre almeno i seguenti file XML:

- un ‘elenco di impacchettamento’ (*PKL*, *packing list* in inglese), che contiene il nome completo di un dato pacchetto, l’*UID* ad esso associato e altri suoi metadati, oltre nome, dimensione, impronta crittografica (cfr. §2.16) e UID associati a ciascuno dei file facenti parte dell’IMP;
- una ‘scaletta della composizione’ (*CPL*, *composition playlist* in inglese) che descrive come la timeline del contenuto sia composta a partire dalle risorse (file) indicizzate nella PKL del medesimo pacchetto e, opzionalmente, anche da PKL di altri pacchetti.

19. Un pacchetto master interoperabile è un pacchetto di file in base alla definizione data in §1.1.1, ma la sua CPL, potendo riferirsi anche ad altre PKL oltre alla propria, può descrivere il contenuto di una composizione utilizzando anche contenitori multimediali appartenenti ad altri IMP. Un pacchetto IMF che faccia uso di altre PKL oltre la propria viene chiamato ‘pacchetto complementare’ (*supplemental package*, in inglese),<sup>52</sup> in quanto dipende da uno o più IMP differenti dal proprio. Il caso d’uso degli IMP complementari è quello di riedizioni o adattamenti successivi del medesimo contenuto, quali:

- doppiaggio (i.e. cambio della lingua parlata);
- aggiunta, o cambio, di *timed text* (i.e. sottotitoli di vario tipo, cfr. § 2.11);
- sostituzione di cartelli e altre parti di video ove vada inserito un testo in una lingua differente (*texted*), o ne vada aggiunto ove non era presente (*textless*);
- riedizione di parti del contenuto audiovisivo per altre finalità di adattamento;
- aggiunta o sostituzione di marche, loghi, o interi titoli di testa o di coda;
- sostituzione dell’intero contenuto con altre codifiche con diverse specifiche tecniche (ad esempio video stereoscopico, HDR/WCG, HFR;<sup>53</sup> audio con diverso numero di canali, ecc.).

20. IMF ammette anche altri tipi di file *sidecar* opzionali, sempre in XML, quali:

---

<sup>52</sup> In tal caso la CPL di un pacchetto complementare si dice essere un *versioning file* (*VF*) — mentre invece un pacchetto IMF che si riferisce soltanto alla propria PKL (e quindi ai suoi file MXF), si dice essere —almeno tecnicamente— nella ‘versione originale’ (*OV*).

<sup>53</sup> Acronimi commerciali che stanno rispettivamente per *high dynamic range*, *wide colour gamut* e *high frame rate*.

- un ‘elenco dei profili d’uscita’ (*OPL*, *output profile list* in inglese), che contiene informazioni tecniche su come generare file multimediali auto-consistenti in altri formati di file, incluse informazioni sul formato video (risoluzione, rapporto d’aspetto, ritagli e ingrandimenti) e audio (numero di canali e lingue impiegate) da utilizzare;<sup>54</sup>
- una ‘mappa di composizione accessoria’ (*SCM*, *sidecar composition map*), che può racchiudere commenti, annotazioni, ovvero metadati “globali” associabili all’IMP nella sua interezza — particolarmente utile ai fini dell’archiviazione a lungo termine di qualunque tipi di informazione accessoria riguardo al contenuto audiovisivo stesso.

21. Gli eventuali sottotitoli, così come i metadati associabili a particolari punti della timeline (cosiddetti “locali”) sono entrambi rappresentati come tracce in un IMP, venendo codificati in XML imbustati ciascuno in file MXF facenti parte del pacchetto. Il dialetto XML dei sottotitoli è sempre TTML o sue ulteriori specializzazioni (cfr. §2.11).

22. Gli altri tipi di metadati locali sono codificabili in file XML senza ulteriori vincoli di specializzazione, associati a particolari istanti della timeline e raggruppati in uno o più buste. Ciascun siffatto contenitore di metadati costituisce un *flusso isocrono di documenti XML* (*ISXD*). Si raccomanda di avere un file MXF separato per ogni tipologia macroscopica di metadati.<sup>55</sup>

23. Allo scopo di incrementare l’interoperabilità, accanto agli standard che descrivono i componenti generici di IMF, ve ne sono altri che descrivono i suoi schemi operativi, chiamati “Applicazioni”. In questi documenti vengono descritti ulteriori vincoli tecnici che armonizzano gli IMP formati per determinate finalità, come ad esempio i codec da usare per le essenze, la loro risoluzione, le specifiche sugli spazi-colore e altre informazioni colorimetriche, la suddivisione delle tracce audio multicanale in “campi sonori”, la compressione audio-video, il formato dei sottotitoli, e così via. Molte di queste Applicazioni sono diventate standard di consegna per diversi attori del mercato cinetelevisivo, soprattutto nel campo SVOD (distribuzione a consumo via etere/satellite/internet).

24. Sebbene IMF resti un formato specifico per i settori cinetelevisivi, all’interno di questi è fortemente raccomandata la produzione di documenti in questo formato: sia nei casi di documenti “semilavorati”, per i quali siano cioè previsti ulteriori

---

<sup>54</sup> Bisogna ricordare che, sebbene IMF sia un formato adatto per la post-produzione e l’archiviazione, il suo uso principale è come master cinetelevisivo, da intendersi successivamente convertito in formati specifici agli scopi di post-produzione, distribuzione e conservazione.

<sup>55</sup> Ad esempio 4 file MXF per contenere 4 differenti ISXD: uno con l’elenco dei nomi di attori e/o personalità presenti in ad ogni cambio di scena; uno con informazioni di produzione ad ogni cambio scena (illuminazione, ottiche, parametri delle configurazioni della cinepresa); uno con parametri relativi al restauro fotogramma per fotogramma (difetti fisici della pellicola sia riparati che solo individuati, finestra del fotogramma completo da cui è estratto il fotogramma cinetelevisivo, ecc.); uno con informazioni di postproduzione e visualizzazione in tempo reale (correzione del colore in HDR, parametri degli effetti speciali, coordinate giroscopiche della camera, ecc.).

adattamenti quali montaggio, doppiaggio o altro; sia qualora il contenuto sia destinato ad archiviazione a lungo termine e conservazione. Le PPA.A. di settore sia adoperano per adottare il formato IMF per tali scopi nel minor tempo possibile.

25. Per le organizzazioni che manipolano un elevato numero di IMP, si raccomanda l'uso di un applicativo di gestione dei contenuti che –sfruttando i file sidecar di cui all'articolo 18– consenta una migliore razionalizzazione degli storage contenenti tali contenuti, tramite il tracciamento completo dei file costituenti ogni pacchetto IMP.

MATROSKA		FORMATO CONTENITORE
Nome completo	Matroska	
Estensione/i	.mkv, .mka, .mks, .mk3d	
Magic number	0x1A45DFA3	
Tipo MIME	video/x-matroska, audio/x-matroska	
Sviluppato da	comunità open source	
Tipologia di standard	aperto (licenza <a href="#">CC BY 4.0</a> ), <i>de facto</i> , binario	
Livello metadati	3	
Derivato da	Multimedia Container Format (MCF), Extensible Binary Meta Language (EBML)	
Revisione	1.4.9 (20 aprile 2017)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.matroska.org">www.matroska.org</a></li> <li>• <a href="https://github.com/Matroska-Org">github.com/Matroska-Org</a></li> <li>• <a href="https://matroska-org.github.io">matroska-org.github.io</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Generale con obbligo in lettura	
Racc. per la scrittura	Generale; raccomandato per la produzione non cinetelevisiva di contenuti cronologicamente continui	

26. Il contenitore [Matroska](#) è un altro formato estremamente versatile capace di contenere molteplici essenze di vario tipo. Se ne raccomanda inoltre l'uso in tutti i campi della produzione audiovisiva, salvo nei casi d'uso specifici della post-produzione o sua archiviazione, dove sono preferibili formati contenitori più professionali, quali MXF ovvero MP4.

WEBM		FORMATO CONTENITORE
Nome completo	WebM	
Estensione/i	.webm, .weba	
Magic number	0x1A45DFA3	
Tipo MIME	video/webm, audio/webm	
Sviluppato da	Google; On2 Technologies	
Tipologia di standard	proprietario (licenza <a href="#">tipo BSD</a> ), <i>de facto</i> , binario	
Livello metadati	1	
Derivato da	Matroska, VP9 (video), Vorbis (audio)	

Revisione	2018
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.webmproject.org">www.webmproject.org</a></li> <li>• <a href="http://www.matroska.org">www.matroska.org</a></li> <li>• <a href="http://www.vorbis.com">www.vorbis.com</a></li> </ul>
Conservazione	No
Racc. per la lettura	Generico; raccomandata la lettura
Racc. per la scrittura	Generico; raccomandata la produzione per brevi clip finalizzate alla distribuzione via internet

27. Il contenitore WebM è ad oggi uno degli standard de facto per la condivisione di contenuti audiovisivi sottoforma di flussi in *streaming* via internet. È in pratica costituito dalla combinazione di una busta Matroska, del codec VP9 per le essenze video e di quello Vorbis per le essenze audio.

MPEG2-TS	FORMATO CONTENITORE	
Nome completo	MPEG-2 Transport Stream	
Estensione/i	.ts, .m2ts	
Magic number	G	
Tipo MIME	video/MP2T	
Sviluppato da	Moving Picture Experts Group	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , robusto, binario	
Livello metadati	1	
Derivato da	MPEG-2	
Revisione	2018	
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">13818-1:2018</a></li> <li>• ITU-T Recommendation <a href="#">H.222.0</a> (2018)</li> <li>• ETSI <a href="#">TS-101-154 v2.6.1</a> (2019)</li> </ul>	
Conservazione	No	
Racc. per la lettura	Generale raccomandato	
Racc. per la scrittura	Speciale; raccomandato per la produzione finale di contenuti cronologicamente continui	

MPEG2-PS	FORMATO CONTENITORE	
Nome completo	MPEG-2 Program Stream	
Estensione/i	.mpg, .mpeg, .vob, .m2p	
Magic number	0x0001BA	
Tipo MIME	video/MP2P	
Sviluppato da	Moving Picture Experts Group	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , binario	
Livello metadati	1	
Derivato da	MPEG-2	
Revisione	2018	

Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">11172-3:1993</a></li> <li>• ISO/IEC <a href="#">13818-1:2018</a></li> <li>• ITU-T Recommendation <a href="#">H.222.0</a> (2018)</li> </ul>
Conservazione	No
Racc. per la lettura	Generale; raccomandato
Racc. per la scrittura	Speciale; sconsigliato per archiviazione/conservazione

28. L'MPEG-2 *Transport Stream (TS)* e *Program Stream (PS)* sono due formati busta utilizzati per contenere essenze audiovisive, in due scenari di utilizzo diversi:

- MPEG2-TS, introdotto originariamente per una riproduzione sequenziale sotto forma di flusso digitale (cfr. §1.1.1) trasmesso attraverso un canale di comunicazione non affidabile, quale ad esempio il “digitale terrestre”;<sup>56</sup> per questo motivo l'MPEG2-TS è dotato di messaggi di verifica dell'integrità legati a meccanismi di protezione del flusso digitale. Adotta inoltre una disposizione interlacciata delle essenze per migliorare le prestazioni dovute allo scenario d'uso della riproduzione sequenziale.
- MPEG2-PS, introdotto originariamente per la distribuzione televisiva aerea o via cavo, è disegnato per contenere flussi audiovisivi digitali (cfr. §1.1.1, con estensioni preferite .mpg e .mpeg), insieme ai metadati necessari al mantenimento della sincronia, al controllo di qualità della banda impiegata e all'organizzazione del canale di comunicazione di tipo televisivo (e.g. supporta il numero e il nome del programma/canale, ecc.). L'MPEG2-PS è disegnato per la riproduzione casuale ed è adottato come contenitore per le evidenze informatiche nei dischi di formato DVD e simili (adottando, in questo caso, l'estensione .vob).

29. Inizialmente questi formati di busta supportavano codec della famiglia MPEG-2, anche se è possibile utilizzare altri tipi di codec.

AVI	FORMATO DI FILE	
Nome completo	Advanced Video Interleave	
Estensione/i	.avi	
Magic number	RIFF	
Tipo MIME	video/avi, video/msvideo	
Sviluppato da	Microsoft Corporation	
Tipologia di standard	proprietario (libero), <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	Resource Interchange File Format (RIFF)	
Revisione	2008	

<sup>56</sup> Cioè i canali di comunicazione che seguono gli standard di comunicazione denominati **DVB** della ITU e della EBU.

Riferimenti	<ul style="list-style-type: none"> <li>• Microsoft, <a href="#">AVI RIFF File Reference</a>, vs.85 (2008)</li> <li>• <a href="#">RFC-2361</a></li> <li>• Hackaday, <a href="#">AVI File Format</a></li> </ul>
Conservazione	No
Racc. per la lettura	Generale con obbligo in lettura
Racc. per la scrittura	Generale; sconsigliata la produzione

30. Il formato di busta AVI è una declinazione del più generico formato contenitore RIFF (da cui derivano anche WAVE e AIFF nel campo audio, cfr. §2.9). È stato, storicamente, uno dei primi formati di contenitore destinato a documenti audiovisivi e dunque a supportare l'uso di codec molteplici per le sue essenze. La mancanza di particolari metadati professionali, tuttavia, oltre ad una poca descrizione dei codec impiegati, lo rendono poco adatto ad usi professionali, perciò se ne sconsiglia l'uso per la creazione di nuovi file laddove vi sia un'alternativa possibile.

Ogg	FORMATO CONTENITORE	
Nome completo	Ogg encapsulated format	
Estensione/i	.ogg, .oga, .ogv	
Magic number	OggS	
Tipo MIME	audio/ogg, video/ogg, application/ogg	
Sviluppato da	comunità open source	
Tipologia di standard	aperto (licenza tipo BSD), <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	–	
Revisione	0 (2003)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-3533</a></li> <li>• <a href="#">RFC-5334</a></li> <li>• <a href="#">xiph.org/vorbis</a></li> </ul>	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandata lettura	
Racc. per la scrittura	Speciale; sconsigliata post-produzione cinetelevisiva	

31. Il formato OGG è un contenitore completamente aperto ed estremamente versatile, raccomandato per l'archiviazione di essenze audio, ma al di fuori del caso d'uso cinetelevisivo, dove si raccomandano altri formati di file.

QUICKTIME	FORMATO CONTENITORE	
Nome completo	QuickTime™ File Format	
Estensione/i	.mov, .qt	
Magic number	0x00000000 moov	

Tipo MIME	video/quicktime
Sviluppato da	Apple
Tipologia di standard	proprietario, estendibile, <i>de facto</i> , deprecato
Livello metadati	4
Derivato da	–
Revisione	2016
Riferimenti	• Apple, <a href="#">QuickTime File Format Specifications</a> (2016)
Conservazione	No
Racc. per la lettura	Generale; raccomandata la lettura
Racc. per la scrittura	Generale; sconsigliata la produzione

32. Il contenitore QuickTime, di proprietà della Apple, è stato a lungo uno dei contenitori più usati per le essenze multimediali, grazie soprattutto alla sua estendibilità. Nonostante si tratti di un formato aperto (la Apple pubblica e revisiona continuamente le sue specifiche tecniche), ne detiene la proprietà intellettuale e ne ha solo parzialmente liberalizzato la produzione al di fuori di applicativi o dispositivi hardware di proprietà della Apple o vincolati da accordi di licenza. Per questo motivo, nonostante ne sia fortemente consigliata la capacità di riproduzione da parte di tutte le organizzazioni che utilizzano, elaborano, o producono contenuti audiovisivi, la produzione di nuovi contenuti in questo formato è fortemente sconsigliata (a meno che non sia l'unico formato supportato da specifici applicativi). Inoltre la smpte e la iso hanno derivato dal QuickTime il formato MP4, completamente aperto.

DCP	FORMATO DI PACCHETTO	
Nome completo	SMPTE Digital Cinema Package	
Estensione/i	[.pkl cpl].xml, .mxf, ...	
Tipologie MIME	application/xml, /mxf, ...	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	proprietario (libero), estendibile, <i>de iure</i>	
Livello metadati	3	
Derivato da	DCP della DCI (Digital Cinema Initiative) e “InterOp”	
Revisione	1.3 (2018)	

Riferimenti	Famiglie di standard ('ST'), prassi raccomandate ('RP'), regole tecniche ('EG') <b>429-433</b> della SMPTE: <ul style="list-style-type: none"> <li>• <b>pacchetto:</b> ST429-2:2009, ST429-3:2007, ST429-6:2006, ST429-7:2006, ST429-8:2007, ST429-9:2007</li> <li>• <b>video:</b> ST429-4:2006, ST428-11:2009, ST428-21:2011, ST428-2:2006, EG432-1:2010;</li> <li>• <b>audio:</b> ST428-1:2006, ST428-2:2006, ST428-3:2006</li> <li>• <b>sottotitoli:</b> ST429-5:2009, ST429-12:2008, ST428-21:2011;</li> <li>• <a href="http://www.smpte.org">www.smpte.org</a></li> <li>• <a href="http://www.dcinovies.com">www.dcinovies.com</a></li> </ul>
Conservazione	No (cfr. §2.8 per i sottotitoli)
Racc. per la lettura	Speciale; raccomandato per la distribuzione e post-produzione cinematografica
Racc. per la scrittura	Speciale; raccomandato per distribuzione e (non criptato) per archiviazione di contenuti cinematografici

33. Il formato di **pacchetto per il cinema digitale** (DCP, *digital cinema package* in inglese) è un pacchetto di file il cui scopo è contenere una copia di contenuto cinematografico da distribuire nelle sale di proiezione. Esistono due tipi di standard DCP: quello della *Digital Cinema Initiatives* (DCI), ora obsoleto, e quello della SMPTE, più recente, che attualmente supporta tutte le novità tecniche.

34. Un DCP è costituito da file multimediali MXF, con schema operativo **OP2b**, contenenti separatamente almeno una traccia audio (in formato PCM non compresso) e una video (con compressione inter-frame di tipo *wavelet*),<sup>57</sup> più alcuni **sidecar** file in XML. Da questo punto di vista, l'architettura del pacchetto è simile a quella del formato di master interoperabile (IMF, sopra descritto). Ciò che rende le DCP peculiari sono i vincoli ai formati audiovisivi delle sale teatrali; la possibilità, mediante messaggi inseriti in specifici istanti della timeline della composizione, di comandare operazioni in sala quali il controllo del proiettore, del sistema di tende, sipari e luci, o di altri dispositivi di intrattenimento proprietari; la possibilità di cifrare l'intero contenuto sbloccandolo soltanto con una chiave crittografica (cfr. §2.16) generata in maniera sicura, tipicamente dallo stesso applicativo che ha masterizzato la DCP.

35. Le DCP cifrate hanno infatti tutti i loro file MXF cifrati, ciascuno mediante crittografia simmetrica (algoritmo AES) con *chiave-contenuto* a 256 bit. La chiave-contenuto di ciascun MXF è sempre archiviata e distribuita cifrata da una chiave pubblica (RSA), la cui corrispondente chiave privata è confidenzialmente mantenuta

<sup>57</sup> La compressione impiegata, visivamente priva di perdite (*visually lossless* in inglese), è la medesima utilizzata dall'algoritmo JPEG2000, cfr. §2.7.

da dispositivi certificati dalla DCI — tipicamente dispositivi di masterizzazione o riproduzione del contenuto (attaccati ai proiettori delle sale cinematografiche), ai quali viene distribuita l'evidenza informatica contenente la chiave-contenuto da sbloccare per riprodurre il DCP. Tale evidenza è formata in un particolare file chiamato KDM (cfr. §2.16).

36. L'uso della crittografia per proteggere i DCP pone tuttavia diverse problematiche in merito all'archiviazione a lungo termine e alla conservazione dei documenti cinetelevisivi in tale formato: in seguito a smarrimento o a scadenza naturale dei certificati a chiave pubblica, infatti, non sarebbe più possibile generare altre KDM che potrebbero sbloccare la DCP.

37. Mentre da una parte si raccomanda che le organizzazioni dedicate alla produzione e riproduzione di opere cinematografiche compiute siano in grado di riprodurre almeno le DCP *non* cifrate, si sconsiglia alle medesime organizzazioni di produrre DCP, salvo per le seguenti finalità:

- DCP *non* criptate per finalità di archiviazione a lungo termine e conservazione del master dedicato alla proiezione cinematografica;
- DCP *criptate* per la sola finalità di distribuzione nelle sale cinematografiche.

85. Si sconsiglia di produrre DCP secondo lo standard DCI (ovvero secondo lo standard *de facto* e intermedio fra i due qui elencati, denominato “InterOp”), favorendo invece lo standard *de iure* SMPTE in quanto è l'unico a supportare, mediante aggiornamenti lenti ma costanti delle specifiche, le migliorie tecnologiche delle sale cinematografiche, sia in campo audio, che video, che intrattenimento di sala in generale.

39. Si raccomanda alle organizzazioni che archiviano un contenuto in formato DCP di archivarne anche una versione in un formato indipendente dalle caratteristiche tecniche di una sala cinematografica digitale, quali quelli individuati in questo stesso capitolo.

DCDM		FORMATO DI PACCHETTO
Nome completo	Digital Cinema Distribution Master	
Estensione/i	.tif/.tiff, .wav	
Tipologie MIME	image/tiff, sound/wav	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, estendibile, retrocompatibile, <i>de iure</i>	
Livello metadati	2	
Derivato da	Tagged Information File Format	
Revisione	1.3 (27 giugno 2018)	

Riferimenti	Famiglia <b>st428</b> di standard/prassi SMPTE: <ul style="list-style-type: none"> <li>• <b>video</b>: ST428-1:2006, ST428-5:2010, ST428-9:2008, RP428-6:2009; Adobe® <b>TIFF™</b> <a href="#">Revision 6.0</a> (1992)</li> <li>• <b>audio</b>: ST428-2:2006, ST428-3:2006, ST428-4:2010, ST428-3:2006; EBU - <a href="#">Tech 3285-1 2.0</a> (2001)</li> <li>• <b>sottotitoli</b>: ST428-7:2010, ST428-10:2008, ST429-5: 2009; ST428-5:2010</li> <li>• <a href="http://www.smpte.org">www.smpte.org</a></li> </ul>
Conservazione	Sì (cfr. §2.8 per i sottotitoli)
Racc. per la lettura	Speciale; obbligatorio per la post-produzione e distribuzione cinematografica
Racc. per la scrittura	Speciale; raccomandato per l'archiviazione di contenuti per la distribuzione cinematografica, previa riversamento in pacchetto IMF Application #4

40. Il master per la distribuzione del cinema digitale (DCDM) è un altro formato basato su sequenze di fotogrammi, ove l'essenza audio è costituita da file WAVE monaurali (uno per ciascun canale stereo, 5.1 ovvero 7.1) mentre l'essenza video è costituita da file TIFF adeguatamente formati (cfr. §2.6), che codificano l'immagine nello spazio-colore DCI  $X'Y'Z'$ , basato su *code-value* a numeri interi e sulla colorimetria riferita alla luce proiettata su uno schermo bianco, che però, da un punto di vista teorico, comprende ogni colore visibile da un "osservatore standard". Il pacchetto DCDM, così come il DCP sopra descritto, esistono in due versioni: uno primo standard *de facto* della DCI e il più recente standard *de iure* della SMPTE, cui ci si raccomanda di attenersi.

41. Sebbene la lettura del DCDM sia obbligatoria per le organizzazioni che si occupano della post-produzione e della masterizzazione per il cinema digitale, nonché fortemente consigliata per l'archiviazione a lungo termine dei contenuti cinematografici, si consiglia altresì la produzione dei futuri master cinematografici nel formato IMF, che presenta caratteristiche di maggior interoperabilità con le filiere contemporanee di distribuzione cinematografica, oltre a supportare un maggior numero di metadati e di resilienza alle riedizioni.

42. Si consiglia il riversamento di tutti i pacchetti DCDM in pacchetti IMF Application #4 (cosiddetta "Cinema mezzanine").

CINEMADNG		FORMATO DI FILE
Nome completo	Adobe® CinemaDNG™	
Estensione/i	.dng; .wav	
Specializzazione di	TIFF/EP	
Tipo MIME	video/x-adobe-dng	
Sviluppato da	Adobe Systems	

Tipologia di standard	proprietario ( <u>brevettato</u> ), estendibile, <i>de iure</i> , binario
Livello metadati	2
Derivato da	Adobe® DNG
Revisione	1.1.0.0 (2011)
Riferimenti	<ul style="list-style-type: none"> <li>• Adobe, <u>CinemaDNG image data format specification</u> v1.1.0.0, 2011</li> <li>• Adobe, <u>Digital Negative (DNG) Specification</u> v1.4.0.0, 2012</li> </ul>
Conservazione	No
Racc. per la lettura	Speciale; fortemente raccomandato per archiviazione, conservazione e post-produzione fotocinematografica
Racc. per la scrittura	Speciale; fortemente consigliato per archiviazione/ conservazione fotografica; consigliato riversamento su IMF in caso cinematografico

43. Il formato CinemaDNG™ è una specifica aperta della Adobe per rappresentare il video professionale sotto forma di sequenze di fotogrammi, ove ciascun file è rappresentato come DNG.

D.I. BASATO SU EXR		FORMATO DI PACCHETTO
Nome completo	Digital Intermediate	
Estensione/i	.exr; .wav	
Tipologie MIME	image/exr, sound/wav	
Sviluppato da	major film studio	
Tipologia di standard	aperto, retrocompatibile, <i>de facto</i>	
Livello metadati	2	
Derivato da	–	
Revisione	–	
Riferimenti	• <a href="http://www.smpte.org">www.smpte.org</a>	
Conservazione	Si	
Racc. per la lettura	Speciale; obbligatorio in post-produzione cinetelevisiva	
Racc. per la scrittura	Speciale; fortemente raccomandato per l'archiviazione cinetelevisiva; consigliato riversamento in IMF	

D.I. BASATO SU DPX		FORMATO DI PACCHETTO
Nome completo	Digital Intermediate	
Estensione/i	.dpx; .wav	
Tipologie MIME	image/x-dpx, sound/wav	
Sviluppato da	Technicolor; Kodak	
Tipologia di standard	aperto, retrocompatibile, <i>de facto</i> , deprecato	
Livello metadati	2	

Derivato da	—
Revisione	—
Riferimenti	—
Conservazione	No
Racc. per la lettura	Speciale; obbligatorio in post-produzione cinetelevisiva
Racc. per la scrittura	Speciale; consigliato per archiviazione di scansioni da pellicola cinematografica; consigliato riversamento in IMF, ovvero in DI basato su EXR

44. Il nome *Digital Intermediate (DI)* indica il processo di post-produzione cinematografica digitale che ha soppiantato l’analogo processo fotochimico su pellicola da 16mm, 35mm o 65mm. Agli albori della post-produzione digitale, quando la fotografia era prevalentemente su pellicola negativa e la proiezione nelle sale basata su pellicole positive, il processo DI cominciava con la scansione digitale del negativo già sviluppato –fotogramma per fotogramma– e terminava con la stampa digitale (*film-out*, in inglese) su pellicola internegativa o interpositiva di pari calibro, da cui venivano poi stampate le copie positive in 35mm o 70mm per la distribuzione. Con l’avvento predominante delle cineprese digitali da un lato del processo e i proiettori per il cinema digitale dall’altro, il termine di è oggi diventato semplice sinonimo di post-produzione interamente digitale. È rimasta comunque l’esigenza di memorizzare i contenuti video in pacchetti di file a “sequenza di fotogrammi” (cfr. §2.12) in quanto ciò rende più semplice la modifica di singole scene, parti di scene e persino fotogrammi individuali — sia dal punto di vista dello storage ove il contenuto è memorizzato, che delle prestazioni degli applicativi impiegati. Per gli stessi motivi, le sequenze di fotogrammi non utilizzano compressione, o al più utilizzano algoritmi *lossless* (dunque, considerando la sequenza di fotogrammi come un unico flusso video, si tratta sempre di compressione intra-frame, cfr. §2.10). La suddivisione in “rulli” (cioè clip audiovisive della durata di 15–25 minuti circa<sup>58</sup>) è di solito rispettata dividendo le sequenze di fotogrammi in sottocartelle del medesimo pacchetto

45. L’audio viene invece codificato in uno o più file WAVE (cfr. §2.9), tipicamente monoaurali, uno per canale. Non esistono veri e propri documenti che descrivono tali specifiche, così come la loro archiviazione a lungo termine (storicamente in nastri digitali LTO mediante il formato di archiviazione TAR, cfr. §2.13): si tratta, dunque, di uno vero e proprio standard *de facto*.

46. Per quanto riguarda il formato di file usato per i singoli fotogrammi, il DI tradizionale ha da molto tempo adottato il formato DPX (creato dalla Kodak® come evoluzione del Cineon™ e standardizzato poi dalla SMPTE, cfr. §2.6), in quanto tale formato permette nativamente la rappresentazione digitale della densitometria di

<sup>58</sup> Considerando un framerate di 24fps tipico del cinema, questo equivale dai 20'000 ai 30'000 fotogrammi.

una pellicola negativa scansionata, ovvero di una positiva stampata, oltre a supportare metadati tipici della postproduzione cinematografica.<sup>59</sup> Il formato DPX tuttavia, nonostante sia attualmente sotto revisione da parte di SMPTE, non è più adeguato agli standard di archiviazione multimediale moderni, a causa della poca efficacia nel mantenere metadati inerenti alle annotazioni o alla codifica colorimetrica. Per questo e altri motivi, come ad esempio le esigenze tecniche della computer-grafica (CG) e degli effetti speciali digitali (VFX), i pacchetti DI contemporanei hanno abbandonato il formato DPX in favore di OpenEXR (anch'esso introdotto in §2.6).

47. Si raccomanda a tutti gli enti operanti nel settore della post-produzione cinematografica di poter leggere pacchetti di file di entrambe i tipo, anche se si sconsiglia fortemente la produzione di nuove sequenze di fotogrammi in formato DPX (in favore del formato OpenEXR). Per la produzione di nuovi pacchetti destinati all'archiviazione o conservazione, si raccomanda inoltre l'impiego dell'IMF (sopra descritto), per la sua maggiore capacità di interoperabilità e riusabilità.

AMF	FORMATO DI PACCHETTO	
Nome completo	ACES Metadata File	
Estensione/i	.amf	
Tipologie MIME	application/amf+xml	
Sviluppato da	Academy of Motion Picture Arts and Sciences	
Tipologia di standard	aperto, estendibile, retrocompatibile, testuale	
Livello metadati	3	
Derivato da	ACESclip	
Revisione	1.2 (2019)	
Riferimenti	Standard e bollettini tecnici dell'AMPAS: <ul style="list-style-type: none"> <li>• <a href="#">TB-2014-009</a>, <i>ACES clip-level metadata file format</i></li> <li>• <a href="#">S-2014-006</a>, <i>A common file format for Look-Up Tables</i></li> <li>• <a href="#">TB-2014-012</a>, <i>ACES version 1.0 component names</i></li> <li>• <a href="#">TB-2014-010</a>, <i>design, integration and use of ACES LMT</i></li> <li>• <a href="http://www.oscars.org/aces">www.oscars.org/aces</a></li> <li>• <a href="http://www.acescentral.com">www.acescentral.com</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Speciale; consigliato in post-produzione cinetelevisiva	

<sup>59</sup> Quali il TimeCode (cfr. §2.12) e il KeyCode™: quest'ultimo, in pratica, un UID che si associa al singolo fotogramma –addirittura della singola perforazione– al numero di serie di ogni rullo, insieme alla sua marca ed emulsione fotochimica.

Racc. per la scrittura	Speciale; consigliato in post-produzione, archiviazione e conservazione di contenuti cinetelevisivi in ACES
------------------------	---

48 Il formato ACESclip è un dialetto XML riservato ad un file *sidecar* che possa accompagnare diversi tipi di file video, all'interno di un processo di trasporto, elaborazione o archiviazione di contenuti che rispetti, colorimetricamente, il sistema ACES introdotto in §2.6. In particolare si consiglia di affiancare un file ACESclip (estensione .ACESclip.xml) sia a file con contenuti compatibili alle specifiche colorimetriche ACES (in pratica, il solo spazio-colore ACES2065-1 descritto nello standard [ST2065-1](#)).

XDCAM	FORMATO DI PACCHETTO	
Nome completo	XDCAM™ package	
Estensione/i	.mxf, .xml, ...	
Tipologie MIME	application/mxf, /xml, ...	
Sviluppato da	Sony Corporation	
Tipologia di standard	proprietario (chiuso), <i>de facto</i>	
Livello metadati	4	
Derivato da	–	
Revisione	–	
Riferimenti	–	
Conservazione	No	
Racc. per la lettura	Speciale; raccomandato in post-produzione e distribuzione di contenuti cinetelevisivi	
Racc. per la scrittura	Speciale; sconsigliata la produzione	

49. Il formato di pacchetto proprietario XDCAM è utilizzato da alcune cinecamere della Sony Corporation, anche se il nome XDCAM™ si riferisce a una gamma ben più ampia di prodotti per il video professionale, inclusi dispositivi di archiviazione (*Professional Disc*, ovvero dischi P2) e di riproduzione. Come formato di pacchetto, XDCAM prevede una ramificazione in sottocartelle predefinite, l'uso di vari codec video (e.g. DV, MPEG-2 parte 2, MPEG-4 ovvero M4V), più alcuni file XML di contorno, che ne descrivono i metadati e il pacchetto d'insieme. A causa delle licenze d'uso legate al formato, se ne sconsiglia fortemente l'uso per la produzione di nuovi contenuti (salvo laddove il capitolato tecnico di consegna lo preveda come unica opzione per una data qualità oggettiva). Tuttavia, la sua ampia diffusione come standard *de facto* impone di considerarlo come formato da poter aprire da parte delle organizzazioni che si occupano di post-produzione o masterizzazione dei contenuti.

## 2.12.1 Raccomandazioni per la produzione di documenti

1. Per quanto riguarda la produzione di documenti audiovisivi in generale, come verrà anche ribadito nel capitolo sul riversamento (§3.3), si raccomanda una valutazione di interoperabilità su tutti i formati di tutte impiegati in un documento informatico multimediale. In particolar modo, qualora il contenuto audiovisivo sia rappresentato da un pacchetto di file (ove, tipicamente, ciascun file descrive metadati, singole essenze o loro porzioni) andrà valutata l'interoperabilità del formato del pacchetto, seguito dall'interoperabilità di ogni file potenzialmente contenuto in esso. Per ciascun file andrà valutata l'interoperabilità del formato contenitore ([wrapper](#), cfr. §1.1.1), se del caso, la tipologia di essenze in esso rappresentate e dunque l'interoperabilità dei codec usati da ciascuna essenza nel contenitore.

2. Relativamente ai soli formati di contenitori e pacchetti multimediali oggetto di questa sezione, si fanno le seguenti raccomandazioni:

- Per contenuti audiovisivi, prevalentemente di natura cinetelevisiva o comunque con destinazioni d'uso professionali –siano essi master per la distribuzione tramite i canali della televisione tradizionale o OTT– da sottoporre o meno a procedimenti di archiviazione o conservazione, si raccomanda particolarmente il [formato master interoperabile \(IMF\)](#). Tale formato di pacchetto di file consente, tecnicamente, una separazione delle essenze (anche relativamente a edizioni multiple e localizzazione); operativamente, può trasportare anche la separazione del contenuto in sue parti funzionali (e.g. marche e loghi iniziali, prologo, titoli di testa, “capitoli”, titoli di coda, ecc.). In entrambe i casi, tali separazioni possono essere sfruttate in caso di riedizione, trasporto e archiviazione, allo scopo di minimizzare tempi, risorse computazionali e occupazione di storage, riducendo i costi infrastrutturali e migliorando al contempo le caratteristiche archivistiche del contenuto. Si raccomanda, tuttavia, di formare i pacchetti IMF secondo una specifica “Applicazione” (anch'esse standardizzate dalla SMPTE) relativa al dato contenuto, in modo da estendere l'interoperabilità con le aziende di settore che le adottano. Il formato IMF può invece non essere ideale quando si verificano una o più delle seguenti condizioni:
  - sia necessario conservare le essenze audiovisive senza perdita di qualità della compressione,
  - non sia un'Applicazione IMF adeguata al processo, o
  - sia necessaria una modifica del contenuto per cui è preferibile l'utilizzo di sequenze di fotogrammi (cfr. qui sotto).

- Per contenuti sempre con destinazioni d'uso professionale (prevalentemente cinetelevisivi) ove sia necessario preservare la massima qualità video (tramite assenza di compressione o l'uso di compressione *lossless*) e, al contempo, è preferibile un approccio basato su sequenze di fotogrammi, si raccomanda l'uso di [DI basato su EXR](#).
- Per particolari casi d'uso cinetelevisivi, vincolati a specifiche regole tecniche, è possibile adottare altri formati, come ad esempio:
  - il pacchetto di cinema digitale (DCP) per la distribuzione finale dei film nelle sale cinematografiche;<sup>60</sup>
  - il [DI basato su sequenze di DPX](#) per contenuti scansionati da pellicole cinematografiche e non ulteriormente elaborati;
  - l'[MPEG2](#) per la sola trasmissione dei contenuti come flussi in tempo-reale (e.g. televisione via cavo, satellitare, ovvero OTT).
- Per tutti gli altri tipi di contenuto, si raccomanda l'utilizzo di un solo file contenitore che racchiuda tutte le essenze e i metadati necessari comunque alla riproduzione del documento audiovisivo. In particolar modo, si raccomanda l'utilizzo del *wrapper* [MXF](#), in quanto potenzialmente integrabile con funzionalità avanzate che rendono facilmente riutilizzabile un contenuto generico anche in ambiti professionali.
- Per contenuti audiovisivi generici, ove sia prioritario facilitarne la riproduzione da parte di applicativi di larga diffusione (anziché dotarlo di un contenitore professionale che supporti metadati interoperabili e una migliore facilità di riversamento), si raccomanda in particolar modo il *wrapper* [MP4](#).

## 2.13 Archivi compressi

1. **Nota Bene:** Alcuni dei pacchetti di file oggetto del presente Allegato sono di fatto creati, come ultimo passaggio, impacchettando una porzione di filesystem (cfr. §1.1.2) in un unico file compresso, utilizzando formati descritti nel presente capitolo o meno. Tali documenti sono dunque rappresentati, grazie a questo stratagemma tecnico, da un unico file anziché da un pacchetto — con indubbi vantaggi sia operativi che normativi.

2. Alcuni di questi formati mantengono l'estensione file del formato di archiviazione sopra descritto (e.g. .zip, .tar, .7z, ...); altri utilizzano estensioni proprie (e.g. .docx/.xlsx/.pptx, .od?, .woff/.woff2, .jar, .apk, .ipa).

---

<sup>60</sup> Si sconsiglia di utilizzare il DCP come formato per archiviazione e conservazione per via della compressione jpeg2000 delle essenze video e, soprattutto, a causa della crittografia a chiave mista pubblica/privata con cui vengono formate le copie per le sale e che rischia, senza una corretta gestione delle chiavi crittografiche (cfr. §2.16), di rendere inutilizzabile il documento archiviato in DCP.

3. Un tipico esempio ove sono impiegate entrambe le convenzioni è rappresentato quando il documento, originariamente costituito da più file, è riversato in un unico file mediante due passaggi distinti e consecutivi: prima viene “pacchettizzato” in un unico file; successivamente tale file viene compresso usando un formato a scelta tra una pluralità di formati (e i corrispondenti algoritmi di compressione). Molto diffuso è l’uso della pacchettizzazione in formato TAR seguita da compressione, ove si adottano due *naming convention* alternative: quella con ‘doppia estensione’ (all’estensione .tar viene concatenata quella dello specifico algoritmo di compressione) e quella ove un’unica estensione di file indica la concatenazione dei due formati. Tale dualismo si trova, ad esempio, per le compressioni GZIP (.tar.gz ovvero .tgz), BZIP2 (.tar.bz2 / .tbz), 7-Zip (.tar.7z / .t7z), LZMA (.tar.lzma / .tlz), XZ (.tar.xz e .txz), ecc.

TAR	FORMATO CONTENITORE	
Nome completo	UNIX Standard Tape Archive (TAR)	
Estensione/i	.tar	
Magic number	ustar	
Tipo MIME	application/x-tar	
Sviluppato da	comunità open source	
Tipologia di standard	aperto, retrocompatibile, <i>de iure</i> , binario	
Livello metadati	1	
Derivato da	PKZIP	
Revisione	7 (2017)	
Riferimenti	<ul style="list-style-type: none"> <li>• IEEE 1003.1:2017, <i>POSIX base specifications, issue 7</i></li> <li>• GNU, <i>Basic Tar Format</i>, (2017)</li> </ul>	
Conservazione	Sì, ma dipende dal contenuto della busta TAR	
Racc. per la lettura	Generico; obbligatoria la lettura	
Racc. per la scrittura	Generico; raccomandata la produzione per archivi su nastri digitali generici o file applicativi Linux/UNIX	

ZIP	FORMATO CONTENITORE	
Nome completo	Zip	
Estensione/i	.zip, .zipx	
Magic number	PK 0x[0304 0506 0708]	
Tipo MIME	application/zip	
Sviluppato da	PKWARE®	
Tipologia di standard	proprietario (libero), retrocompatibile, <i>de iure</i> , binario	
Livello metadati	3	
Derivato da	PKZIP	

Revisione	6.3.5 (2018)
Riferimenti	<ul style="list-style-type: none"> <li>• ISO/IEC <a href="#">21320-1:2015</a></li> <li>• PKWARE, <a href="#">.ZIP File Format Specification</a>, v6.3.5 (2018)</li> </ul>
Conservazione	Sì, ma dipende dal contenuto della busta ZIP
Racc. per la lettura	Generico; obbligatoria dalla versione 6.3.1 (2007)
Racc. per la scrittura	Generico; raccomandata la versione 6.3.1 o precedenti

GZIP		FORMATO CONTENITORE
Nome completo	GNU Zip	
Estensione/i	.gzip	
Magic number	0x01F8B	
Tipo MIME	application/gzip	
Sviluppato da	comunità open source	
Tipologia di standard	aperto ( <a href="#">GNU LGPL</a> ), retrocompatibile, <i>de iure</i> , binario	
Livello metadati	1	
Derivato da	PKZIP	
Revisione	6.3.5 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">RFC-1952</a></li> <li>• <a href="#">RFC-6713</a></li> <li>• <a href="http://www.zlib.org/rfc-gzip.html">www.zlib.org/rfc-gzip.html</a></li> </ul>	
Conservazione	Sì, ma dipende dal contenuto della busta GZIP	
Racc. per la lettura	Generico; obbligatorio	
Racc. per la scrittura	Generico; raccomandato per archivi contenenti applicativi Linux/UNIX	

7-ZIP		FORMATO CONTENITORE
Nome completo	7-Zip compressed archive format	
Estensione/i	.7z	
Magic number	7z 0xBCAF271C	
Tipo MIME	application/x-7z-compressed	
Sviluppato da	Igor Pavlov	
Tipologia di standard	aperto ( <a href="#">GNU LGPL</a> ), retrocompatibile, <i>de facto</i> , binario	
Livello metadati	3	
Derivato da	compressione Lempel-Ziv-Markov (LZMA)	
Revisione	18.06 (2018)	
Riferimenti	• Pavlov I., <a href="#">LZMA SDK</a> (2018)	
Conservazione	Sì, ma dipende dal contenuto della busta 7-Zip	

Racc. per la lettura	Generico; consigliato
Racc. per la scrittura	Generico; consigliato

RAR	FORMATO CONTENITORE
Nome completo	Roshal Archive file format
Estensione/i	.rar; .r[00-99]
Magic number	Rar! 0x1A0700, Rar! 0x1A070100
Tipo MIME	application/java-archive
Sviluppato da	Eugene (algoritmo) e Alexander (applicativi) Roshal
Tipologia di standard	aperto (lettura), proprietario (scrittura), retrocompatibile, <i>de facto</i>
Livello metadati	3
Derivato da	compressione Lempel-Ziv-Storer-Szymański (LZSS)
Revisione	5.61 (2018)
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.rarlab.com">www.rarlab.com</a></li> <li>• <a href="http://theunarchiver.com">theunarchiver.com</a></li> </ul>
Conservazione	No
Racc. per la lettura	Generico; altamente sconsigliato; valutare opportunità di riversamento in altro formati di archiviazione
Racc. per la scrittura	Generico; Sconsigliato.

JAR	FORMATO CONTENITORE
Nome completo	Java Archive file format
Estensione/i	.jar
Magic number	0x5F27A889
Tipo MIME	application/jar-archive
Sviluppato da	Verizon Media; Oracle Corporation
Tipologia di standard	proprietario (libero), retrocompatibile, <i>de facto</i> , binario
Livello metadati	3
Derivato da	ZIP
Revisione	2018
Riferimenti	<ul style="list-style-type: none"> <li>• Oracle, <a href="#">JAR File Overview</a>, 2018</li> <li>• Oracle, <a href="#">JAR File Specification</a>, 2018</li> </ul>
Conservazione	Sì, ma dipende dal contenuto della busta JAR
Racc. per la lettura	Specifico; raccomandato in ambito ICT e sviluppo codice
Racc. per la scrittura	Specifico; raccomandato in ambito ICT e sviluppo codice in linguaggio Java

ISO	FORMATO CONTENITORE	
Nome completo	Immagine di volume ISO9660	
Estensione/i	.iso	
Magic number	CD001 (dal 32768, <sup>mo</sup> 34817, <sup>mo</sup> o 36865 <sup>mo</sup> byte)	
Tipo MIME	application/x-iso9660-image	
Sviluppato da	International Organization for Standardization	
Tipologia di standard	proprietario (libero), retrocompatibile, <i>de iure</i> , binario	
Livello metadati	1	
Derivato da		
Revisione	6.3.5 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ECMA-119</a>, 3<sup>rd</sup> Ed. (2017)</li> <li>• ISO/IEC <a href="#">13490-1</a>:1995, [...]: <i>General</i></li> <li>• ISO/IEC <a href="#">13490-2</a>:1995, [...]: <i>Volume &amp; file structure</i></li> <li>• <a href="#">ECMA-168</a>, 2<sup>nd</sup> ed., 1994</li> <li>• Famiglia di standard <b>13346</b> della ISO/IEC</li> <li>• <a href="#">ECMA-167</a>, <i>Universal Disk Format (UDF)</i>, 3<sup>rd</sup> ed., 1997</li> </ul>	
Conservazione	Sì, ma dipende dal contenuto della busta ISO9660	
Racc. per la lettura	Specifico; fortemente raccomandato in ambito ICT	
Racc. per la scrittura	Specifico; raccomandato in ambito ICT per immagini normali e forensi di dispositivi di <i>storage</i> a blocchi	

4. Questo standard descrive prevalentemente due oggetti che possono a livello logico contenersi l'una nell'altra:

1. un contenitore generico per la memorizzazione “byte per byte” di un'evidenza informatica costituente il volume di un dispositivo di *storage* a blocchi (tipicamente ad accesso casuale);
2. un filesystem (cfr. §1.1.2), la cui specifica è codificata nello standard deprecato [ISO 9660](#);

4. Lo standard ISO 9660, obsoleto, è stato sostituito, sia come storage che come filesystem virtuale, da altri due standard: l'ISO 13490, che è prevalentemente un suo aggiornamento; l'ISO 13346, denominato *Universal Disk Format* (UDF), che introduce invece contenitore e filesystem nuovi. In passato, diverse estensioni furono introdotte –come standard *de facto* però– da alcune organizzazioni: le Apple [ISO9660 Extensions](#) (per il filesystem proprietario HFS+), l'IEEE P1282 (“Rock Ridge”), il Microsoft® “[Joilet](#)”, l'IBM “El Torito”. Come filesystem invece, l'ISO9660 (che continua a dare il nome al formato di file) e le sue estensioni furono originariamente impiegati per i dischi ottici di tipo CD, DVD e BluRay (BD) — nelle versioni “ROM”

a sola-lettura o meno. Il formato, rappresentato in un unico file è stato utilizzato per distribuire immagini trasportabili di tali dischi, allo scopo di masterizzarli in un secondo momento. In una terza fase temporale, si è consolidato come standard *de facto* per conservare immagini “pseudoforensi” di versioni installabili o preinstallate di alcuni software, simulandone la distribuzione nell’obsoleto supporto informatico basato su disco.

VMDK		FORMATO CONTENITORE E DI PACCHETTO
Nome completo	Virtual Machine Disk Format	
Estensione/i	.vmdk	
Magic number	KDMV 0x[01 02]000000	
Tipo MIME	application/x-vmdk	
Sviluppato da	VMware (Dell Incorporated)	
Tipologia di standard	aperto, retrocompatibile, <i>de facto</i> , binario o testuale	
Livello metadati	3	
Derivato da	ISO 660	
Revisione	VMFS-5 (2011)	
Riferimenti	<ul style="list-style-type: none"> <li>• VMware, <a href="#">Virtual Disk Format</a> (2011)</li> <li>• VMware, <a href="#">Virtual Disk Development Kit (VDDK)</a> v6.7.1</li> </ul>	
Conservazione	Sì, ma dipende dal contenuto della busta VMDK	
Racc. per la lettura	Usare sos o applicativi commerciali nei reparti IT.	
Racc. per la scrittura	Usare sos o applicativi commerciali nei reparti IT.	

5. Il formato VMDK, proprietario VMware ma standard *de facto*, permette di rappresentare uno storage a blocchi in formato “sparso” (cioè rappresentando solo i blocchi effettivamente inizializzati dal dispositivo), in uso da parte di macchine virtuali e container. È un formato sia di contenitore che di pacchetto perché è disponibile in due varianti: nella prima è un singolo file che contiene sia l’header con i metadati interni, sia il contenuto a blocchi vero e proprio dello storage virtualizzato. Nella seconda variante, invece, è costituito da un file di testo contenente i soli metadati più uno o più file binari contenenti solo la rappresentazione blocco per blocco di parti del dispositivo.

DMG		FORMATO CONTENITORE
Nome completo	Apple® Disk Image	
Estensione/i	.dmg	
Specializzazione di	Immagine di volume iso9660	
Tipo MIME	application/x-apple-diskimage	
Sviluppato da	Apple Incorporated	

Tipologia di standard	proprietario (libero), retrocompatibile, <i>de facto</i> , binario
Livello metadati	3
Derivato da	Apple New Disk Image Format (NDIF, .img)
Revisione	–
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://newosxbook.com/DMG.html">newosxbook.com/DMG.html</a></li> <li>• Apple, <a href="#">File System Programming Guide</a> (2018)</li> </ul>
Conservazione	No
Racc. per la lettura	Nessuna raccomandazione
Racc. per la scrittura	Valutare riversamento in altri formati per dati semplici. Conservare/archiviare i file .dmg in caso di backup di applicativi nativi Apple (macOS®, iOS®, ecc.).

### 2.13.1 Raccomandazioni per la produzione di documenti

1. La raccomandazione circa i formati da utilizzare per la produzione di archivi compressi non può che essere dettata dalle finalità d'uso dell'archivio. Per il resto – con l'eccezione del formato RAR e del DMG di Apple– tutti i formati descritti in questa sezione sono sufficientemente aperti. Mentre la scelta su ZIP, GZIP (e loro varianti) piuttosto che 7-Zip è dettata spesso da esigenze tecniche specifiche degli algoritmi di compressione.

## 2.14 Documenti amministrativi

1. Sono qui elencati alcuni formati di file utilizzati per documenti amministrativi di utilizzo generale, da parte delle P.P.AA. e di altri enti, su tutto il territorio nazionale, quali:

- fascicolo sanitario elettronico,
- fatturazione elettronica,
- protocollo informatico,
- asserzioni elettroniche legate a schemi di identificazione elettronica e a loro utilizzi in capo ad autenticazione, autorizzazione, sottoscrizione o altro.

2. Si precisa che, per lo svolgimento di procedimenti amministrativi non contemplati in questa sezione, le PPA.A. posso utilizzare anche altri formati di file descritti sia nel resto di questo Allegato, sia non compresi da esso qualora, in quest'ultimo caso, i formati non siano sostituibili con formati previsti nell'Allegato e sia comunque stata fatta una valutazione di interoperabilità.<sup>61</sup>

FATTURAPA		FORMATO DI FILE
Nome completo	fattura elettronica FatturaPA	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	application/xml	
Sviluppato da	Agenzia delle Entrate	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	-	
Revisione	1.2.1 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.fatturapa.gov.it">www.fatturapa.gov.it</a></li> <li>• <a href="#">Specifiche tecniche operative del formato della fattura del sistema di interscambio v1.2.1 (2018)</a></li> <li>• <a href="#">Schema del file XML Fattura PA v1.2.1 (2018)</a></li> <li>• <a href="#">Foglio di stile per visualizzare la fattura v1.2.1 (2018)</a></li> <li>• Agenzia delle Entrate, <i>Allegato A</i> del D.M. 55/2013</li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; consultare la normativa in materia	
Racc. per la scrittura	Specifico; consultare la normativa in materia	

3. La fattura elettronica è creata, trasmessa, elaborata e conservata centralmente dal [Sistema di Interscambio \(SdI\)](#) dell'Agenzia delle Entrate, ovvero da altri applicativi ad esso interconnessi. Il formato della fattura elettronica è costituito da un file XML nel dialetto FatturaPA, che comprende tutte le varianti di processo della fatturazione convenzionale, suddivisi in tre macro-aree:

- dati anagrafico-fiscali delle parti (prestatore/cedente e committente/cessionario),
- metadati relativi alla fattura elettronica stessa, alle valute e al suo trasporto nel SdI,

<sup>61</sup> Si veda in tal senso, per quanto riguarda il protocollo informatico le Linee guida cui questo Allegato afferisce, per quanto riguarda gli schemi di identificazione elettronica e i servizi fiduciari elettronici il §2.16 del presente Allegato, che rimanda alla normativa attualmente in vigore.

- descrizione dei beni o servizi oggetto della fatturazione da un punto di vista fiscale,
- metadati inerenti all'eventuale trasporto fisico dei beni oggetto della fatturazione.

4. È anche prevista la possibilità di allegare alla fattura uno o più allegati che vengono codificati <sup>62</sup> e “immersi” all'interno del file (che diviene così un contenitore).

CDA2		FORMATO DI FILE
Nome completo	Clinical Document Architecture	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	application/xml	
Sviluppato da	HL7 International	
Tipologia di standard	proprietario (libero), estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	HL7 CDA Rel. 1.0	
Revisione	2.0 (2018)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">ISO/HL7 27932:2005</a>, <i>HL7 Clinical Document Architecture</i></li> <li>• <a href="http://www.fascicolosanitario.gov.it/Standard-documentali">www.fascicolosanitario.gov.it/Standard-documentali</a></li> <li>• <a href="#">Foglio di stile</a> per la consultazione interoperabile</li> <li>• <a href="#">Circolare AGID N°4/2017</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; consultare la normativa in materia	
Racc. per la scrittura	Specifico; consultare la normativa in materia	

5. Il CDA è uno standard di markup basato su XML pensato per lo scambio informatico di documenti clinici ed è, inoltre, uno degli standard di riferimento per il Fascicolo Sanitario Elettronico (FSE), la cui normativa si può trovare sul sito ufficiale del FSE: [www.fascicolosanitario.gov.it](http://www.fascicolosanitario.gov.it). Il CDA è uno standard definito originariamente da ANSI e successivamente sviluppato dall'organizzazione senza scopi di lucro Health Level 7. Il CDA specifica la sintassi e fornisce una struttura di base (data set di riferimento) per realizzare l'intera semantica di un documento clinico (guida implementativa). Un documento CDA è in grado di contenere qualunque tipo di informazione clinica; supporta inoltre testo non strutturato e può incorporare documenti nei formati PDF, DocumentML e RichText Format, così

<sup>62</sup> Per la precisione, la codifica binaria è ottenuta mediante algoritmo *Base64*, specificato in [RFC-4648](#).

come immagini di tipo JPEG e PNG. La versione 2 del CDA è stata adottata dallo standard ISO/HL7 27932 del 2005.

SEGNATURA DI PROTOCOLLO		FORMATO DI FILE
Nome completo	Segnatura di protocollo	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	application/xml	
Sviluppato da	Agenzia per l'Italia Digitale	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	-	
Revisione	2013	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="#">Allegato 6 alle Linee guida per la formazione, gestione e conservazione del documento informatico</a></li> <li>• <a href="#">Foglio di stile per visualizzare la segnatura (2018)</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; si veda la normativa nelle presenti Linee guida	
Racc. per la scrittura	Specifico; si veda la normativa nelle presenti Linee guida	

6. La segnatura di protocollo è descritta nell'Allegato 6 delle presenti Linee guida.

ASSERZIONE SPID		FORMATO DI FILE
Nome completo	Asserzione SPID	
Estensione/i	.xml	
Specializzazione di	XML	
Tipo MIME	text/xml	
Sviluppato da	Agenzia per l'Italia Digitale	
Tipologia di standard	aperto, estendibile, <i>de iure</i> , testuale	
Livello metadati	2	
Derivato da	Security Assertion Markup Language, sso profile; OpenID Connect	
Revisione	1.0 (2014)	
Riferimenti	<ul style="list-style-type: none"> <li>• <a href="http://www.spid.gov.it">www.spid.gov.it</a></li> <li>• <a href="#">AGID, Regolamento recante Le Regole Tecniche v1.0 (2014)</a></li> <li>• <a href="#">D.P.C.M. 24 ottobre 2014</a></li> </ul>	
Conservazione	Sì	
Racc. per la lettura	Specifico; consultare normativa in materia	

Racc. per la scrittura	Riservato alla federazione SPID, costituita da gestori di identità digitale, fornitori di servizi e <i>attribute authority</i> .
------------------------	--

7. Le asserzioni legate al [Sistema Pubblico di Identità Digitale \(SPID\)](#), siano esse in linguaggio SAML (basato su XML), ovvero in formato JWT (basato su JSON), cfr. §2.3, sono da considerarsi un formato a se stante in quanto possono trasportate e, se adeguatamente gestite, conservare a lungo termine dati personali o sensibili di persone fisiche o giuridiche. Per tali motivi tali asserzioni sono normate da altre Regole Tecniche emanate dall’Agenzia per l’Italia Digitale.

## 2.15 Applicazioni e codice sorgente

1. Esistono una miriade di formati per codificare le applicazioni (altrimenti dette, impropriamente anche se a causa di una forzatura storica, *binari*). Tipicamente, tali formati dipendono dall’architettura dell’hardware e dal SO impiegato. Per tale motivo figurano tanto gli eseguibili Microsoft® (.exe, .com, .msi), quanto quelli macOS® (.pkg), quanto le *app* per dispositivi mobili, sia Android (.apk), che iOS® (.ipa). Oltre agli eseguibili, le porzioni di codice statico (.a, .lib) e dinamico (.so, .dll, .dylib) sono anch’esse dotate di formati specifici, largamente dipendenti dal SO.

2. La distinzione si semplifica nel caso dei codici sorgente scritti nei vari linguaggi di programmazione –interpretati o compilati– per i quali la tipologia di file è in realtà unica: un semplice file di testo (con codifica dei caratteri ASCII ovvero in qualche variante di UNICODE o UTF), la cui estensione (e, di conseguenza, anche il tipo MIME) da un’indicazione logica circa il linguaggio di programmazione o di *scripting* in cui sono codificate le proposizioni al suo interno.

3. Né il formato dei file contenenti le applicazioni, né i linguaggi di programmazione sono oggetto delle Linee guida di cui il presente Allegato è parte integrante. Si rimandano le P.P.A.A. alle *Linee guida sul riuso del software* per gli obblighi e le raccomandazioni in materia di sviluppo applicativo.

## 2.16 Applicazioni crittografiche

1. Per meglio chiarire il contesto, si premette che i servizi fiduciari elettronici sono normati da fonti di livello pari o superiore a quello delle presenti Linee guida, le quali contengono obblighi e raccomandazioni anche in merito ai formati di file utilizzati per tali servizi. Tali fonti, includenti le loro successive modificazioni, sono:

- Regolamento (UE) N°910/2014 del Parlamento europeo e del Consiglio ([regolamento “eIDAS”](#));
- Decisioni di Esecuzione (UE) collegate con il regolamento eIDAS;
- articoli 20, 21, 24, 28, 35 e 36 del CAD;
- *Linee Guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*, emanate con Determinazione AgID N°121/2019;
- D.P.C.M. del 21 maggio 2013 (*Nuove Regole Tecniche Firma Elettronica Avanzata*).

2. I documenti informatici normati dalle suddette fonti, utilizzati per servizi fiduciari elettronici e altri servizi che impiegano la crittografia, al fine di aumentare le caratteristiche di confidenzialità, integrità, autenticità e non ripudio di evidenze informatiche, si classificano, generalmente, in:

- a) buste crittografiche contenenti firme, sigilli o validazioni temporali elettroniche ed, eventualmente, i documenti informatici stessi a cui tali servizi fiduciari afferiscono;
- b) certificati elettronici di creazione di firma, sigillo o validazione temporale elettronica;
- c) certificati elettronici di autenticazione di siti web ([WAC](#));
- d) certificati elettronici di attribuzione o autenticazione;
- e) certificati elettronici di certificazione;
- f) richieste di sottoscrizione di certificato elettronico;
- g) liste di revoca o di fiducia (di certificati elettronici);
- h) buste contenenti chiavi crittografiche;
- i) buste contenenti documenti cifrati elettronicamente;
- j) buste contenenti impronte crittografiche;

3. Nel caso in cui la busta crittografica contenga solo la firma elettronica (o le firme elettroniche), senza il documento stesso a cui essa o esse si riferiscano logicamente, si parla di [firma detached](#); quando invece la busta crittografica contiene sia il documento che la sua firma elettronica si parla di firma [enveloping](#); quando, infine, il documento informatico costituisca esso stesso busta crittografica per la firma apposta, si parla di firma [enveloped](#). La stessa distinzione nominativa si applica, *mutatis mutandis*, al [sigillo](#) elettronico ovvero alla [validazione temporale](#) elettronica.

4. Viene aggiunta una specifica relativa allo standard *de facto* dei file contenenti una o più impronte crittografiche in un formato puramente testuale (ASCII) e alcuni formati relativamente al trasporto di informazioni crittografiche in ambiti specifici.

CHECKSUM		FORMATO DI FILE
Nome completo	impronta crittografica	
Estensione/i	.sha2, .sha1, .md5, .ripemd160, ...	

Magic Number	—
Sviluppato da	—
Tipologia di standard	aperto, <i>de facto</i> , testuale
Livello metadati	1
Derivato da	XAdES
Revisione	—
Riferimenti	• SANS, <a href="#">An introduction to file integrity checking on UNIX systems</a> , GIAC paper, 2003
Conservazione	No
Racc. per la lettura	Generale; obbligo di lettura come normale file di testo
Racc. per la scrittura	Generale; raccomandato la produzione di un'impronta <i>detached</i> così costituita in assenza di altri meccanismi di verifica dell'integrità impliciti nei formati o non collegati con essi da vincoli logici più forti e robusti.

5. Per quanto concerne le **impronte crittografiche** (anche dette *digest* o *thumbprint* in inglese) e le chiavi crittografiche, ove esse non siano utilizzate per finalità, ovvero non siano contenute in file il cui formato non è altrimenti definito da altre fonti normative, si raccomanda di adottare la seguente metodica per creare e archiviare un digest *detached* di file (il cui nome generico sia *nomefile.ext*):

- a) scegliere una funzione di *hash* crittografico adeguatamente robusta (si raccomanda SHA-256 o superiore, come definito in [RFC-6234](#) ovvero da Avvisi pubblicati da AgID) e rappresentare il nome dell'algoritmo mediante una stringa di caratteri alfanumerici minuscoli *hash*: senza interruzioni, caratteri di spaziatura o altri simboli (ad esempio, sha256 per SHA-256, ripemd160 per RIPEMD a 160 bit, md5 per MD5 e così via);
- b) calcolare l'impronta crittografica dell'intero file con la funzione di *hash* di cui al punto 1;
- c) creare un file chiamato *nomefile.ext.hash* (che avrà dunque estensione *.hash*), possibilmente nella medesima cartella ove si trova il file stesso;
- d) salvare in questo file, mediante codifica ASCII a 7-bit (cfr. [RFC-2045](#)) la sola rappresentazione esadecimale (con cifre minuscole) dell'impronta di cui al punto 2; non andranno aggiunti altri caratteri (incluse spaziature e a-capo — *newline* in inglese), né prima né dopo l'impronta;
- e) per quanto possibile, mantenere la località di referenza tra il file originale e quello contenente la sua impronta crittografica mediante i metodi esposti nel §1.1.2, cioè mantenendo sempre file e impronta nella medesima cartella, con la medesima *naming convention* definita ai punti 1 e 2 di questo elenco numerato.

KDM		FORMATO DI FILE
Nome completo	Key Delivery Message	
Estensione/i	.kdm.xml	
Specializzazione di	XML	
Tipo MIME	application/kdm+xml	
Sviluppato da	Society of Motion Picture and Television Engineers	
Tipologia di standard	aperto, retrocompatibile, <i>de iure</i> , testuale	
Livello metadati	4	
Derivato da	XML Digital Signature	
Revisione	–	
Riferimenti	Famiglia di standard <b>ST430</b> della SMPTE: <ul style="list-style-type: none"> <li>• <a href="#">ST430-1:2006</a>, <i>D-Cinema operations - KDM</i></li> <li>• <a href="#">ST430-2:2006</a>, <i>D-Cinema operations - Digital Certificate</i></li> <li>• W3C Recommendation <a href="#">XML Signature Syntax and Processing, 2002</a> (deprecato)</li> </ul>	
Conservazione	No	
Racc. per la lettura	Specifico; raccomandato per le sale cinematografiche	
Racc. per la scrittura	Specifico; raccomandato nella produzione dei master cinematografici per la distribuzione nelle sale	

6. Il formato DCP è un formato di busta contenente le cosiddette “chiavi di contenuto” nel contesto del cinema digitale (per i cui formati audiovisivi vedasi §2.12), cioè chiavi simmetriche AES a 256 bit di lunghezza), fino ad uno specifico server Digital Cinema, cui è concessa la facoltà di riprodurre il contenuto di un determinato pacchetto di cinema digitale (DCP) entro un intervallo di tempo finito e predeterminato. Per ogni DCP cifrato, infatti, le essenze di ciascun file MXF sono cifrate ciascuna con una chiave di contenuto. La sicurezza del DCP si ottiene cifrando ulteriormente tutte le chiavi di contenuto di un dato DCP mediante crittografia asimmetrica (RSA a 2048 bit di lunghezza), ove ciascun server è dotato di un HSM contenente sia la chiave privata della coppia (e il relativo certificato di creazione di sigillo elettronico avanzato) che un orologio indipendente anti-manomissione per la validazione temporale elettronica. Su tutti i KDM si appone un sigillo *enveloping* che protegge da contraffazione la specifica DCP da riprodurre (mediante sia l’UID del pacchetto stesso che le impronte crittografiche dei singoli file che lo costituiscono, cfr. §1.1.1), l’intervallo temporale durante il quale ne è concessa la riproduzione e, soprattutto, la copia cifrata delle sue chiavi di contenuto.

### 3 Raccomandazioni sui formati di file

1. I formati da utilizzare nell'ambito delle presenti Linee guida sono quelli previsti nel §2 del presente Allegato. Nello scegliere tali formati di file, da utilizzare per i propri documenti informatici, le organizzazioni possono effettuare la valutazione di interoperabilità (§3.1) che prediliga formati aperti, non proprietari, standard *de iure*, estendibili, parlanti, completamente robusti, indipendenti dal dispositivo –secondo la classificazione fatta in §1.2.2– al fine di:

- prevenire il rischio della loro obsolescenza tecnologica (rischio che incrementa con il divergere delle caratteristiche del formato da quelle sopraelencate);
- mitigare il rischio del *vendor lock-in*,<sup>63</sup> che sussiste soprattutto per i formati proprietari, non codificati in standard *de iure*, o per quelli dipendenti dal dispositivo;
- facilitare il più possibile un loro futuro **riversamento** in altro formato, prediligendo caratteristiche quali l'estendibilità, la codifica testuale, la compatibilità in avanti e, in misura minore, la robustezza.

2. I formati di file, di contenitori, di pacchetti di file e di codec elencati nel §2 rappresentano, in generale, una famiglia allargata, con candidati più o meno adatti ad un particolare scopo. Nel caso dei codec video, allo scopo di indicare esempi di formati non interoperabili da utilizzare il meno possibile per conservazione o archiviazione, sono elencati anche alcuni codec chiusi o con particolari limitazioni d'uso dovute a licenze, brevetti o royalties, allo scopo di indicare esplicitamente le organizzazioni che avessero documenti multimediali con tali codec verso un riversamento o altra procedura di gestione documentale mirata.

3. Così come accade per i sistemi di archiviazione digitale (**storage**) –e per tutta la tecnologia in generale– non si può pensare che un formato di file, seppur revisionato nel tempo, possa essere perennemente attuale né di uso corrente. L'obsolescenza dei formati di file e dei dispositivi di archiviazione può essere mitigata soltanto mediante *riversamenti periodici* da una tecnologia verso un'altra; questo vale tanto per le tecnologie di storage che per i formati dei file.

4. Per questo motivo, si consiglia che le PPA.A. e le imprese che hanno necessità di archiviazione e riuso a lungo e lunghissimo termine dei documenti informatici, pianifichino in anticipo una strategia di selezione degli *storage* e dei formati di file che sia il più possibile congiunta, in modo da minimizzare il numero di riversamenti relativi a ciascuno di questi due fattori (ottimizzando la continuità operativa e, nel complesso, riducendo i costi derivanti da tali operazioni).

---

<sup>63</sup> Consiste, in questo caso, nell'impossibilità tecnologica e/o giuridica di elaborare file (inclusa la conversione in altri formati) senza l'ausilio del proprietario del formato: avvalendosi di sue consulenze, beni, tecnologie, proprietà intellettuale, licenze software o altro.

### 3.1 Valutazione di interoperabilità

1. La valutazione di interoperabilità in merito ai formati dei file, prevista dalle Linee guida di cui il presente Allegato è parte integrante, può essere redatta da qualunque ente pubblico o privato tratti documenti informatici. La valutazione di interoperabilità è redatta con cadenza annuale dalle PP.AA. che trattino documenti informatici in formati diversi da quelli di cui al presente Allegato, ovvero conformi a questi formati ma utilizzati disapplicando gli obblighi e raccomandazioni ivi contenuti.

2. Allo scopo di effettuare la valutazione di interoperabilità, le organizzazioni effettuano una ricognizione di tutte le loro procedure amministrative e/o processi di business, allo scopo di individuare ogni tipologia di documenti informatici trattati (o trattabili). Il valore di questa ricognizione può andare ben al di là degli scopi di cui alle presenti Linee guida.

3. La valutazione di interoperabilità consiste in un dettagliato rapporto circa le seguenti azioni (obbligatorie se indicate in **grassetto**):

- a) Includere nell'attività di classificazione (cfr. §1.2.2) un **censimento dei formati** di file e delle tipologie di storage attualmente utilizzati, con particolare riferimento a quelli non elencati nel §2 del presente Allegato.
- b) Per ciascun formato di file adottato, elencare tutti i **dettagli tecnici** dei medesimi, quali ad esempio:
  - ◆ nome dei formati e, laddove applicabile, dei dialetti, profili, codec, schemi operativi;
  - ◆ suddivisione tra formati generici e specifici (cfr. §1.2.3);
  - ◆ versioni utilizzate nei documenti già esistenti, ovvero producibili dagli attuali applicativi;
  - ◆ altre caratteristiche tecniche non vincolate dalle specifiche di cui ai punti precedenti (e.g. lingue adottate nei testi, numero di canali audio, spazi-colore, risoluzione per immagini e video, *bitrate* massimo, algoritmi di cifratura, presenza di password, ecc.).
- c) Elencare i **processi di riversamento** di formato attualmente in corso nell'organizzazione, con particolare riferimento ai software applicativi impiegati e alle procedure tecniche (automatiche, semiautomatiche o completamente manuali) adottate per configurare tali riversamenti, con lo scopo prioritario di rendere tali riversamenti riproducibili.
- d) Elencare le motivazioni attuali che hanno portato alla scelta di ciascun formato di file per il trattamento dei documenti informatici. In particolar modo, se del caso, distinguere i formati di file tra quelli adottati per i documenti:

- ◆ accettati “in entrata” dal pubblico ovvero da altre organizzazioni,
  - ◆ utilizzati ad uso esclusivamente interno,
  - ◆ pubblicati, ovvero prodotti “in uscita” verso altre organizzazioni,
  - ◆ archiviati ovvero mandati in conservazione.
- e) Valutare l’esistenza di standard o di iniziative di standardizzazione a livello internazionale, europeo e nazionale, relativamente alle tipologie di documenti informatici trattati.
- f) Quantificare l’eventuale **necessità** di operare sui medesimi documenti informatici nell’arco di una finestra temporale futura.
- g) Valutare gli scenari ove successive modificazioni o revisioni dei documenti vengano prodotte in formati diversi da quello originale.
- h) Valutare la sussistenza di leggi o altri tipi di obblighi in merito alla **conservazione delle evidenze informatiche nel formato originale** di acquisizione o formazione.
- i) Valutare i formati di file di **categorie specifiche**, nonché l’opportunità di riutilizzo dei documenti informatici di ciascuna classe (come da punto 1) da parte di PP.AA. e organizzazioni che operano al di fuori dello specifico settore per il quale il formato e i suoi scenari d’utilizzo sono stati prefigurati.
- j) Dipendenza dei formati di file da:
- ◆ licenze d’uso, marche e brevetti o altra **proprietà intellettuale**,
  - ◆ sistemi e architetture **proprietarie**, o comunque,
  - ◆ sistemi e architetture che, pur senza i suddetti vincoli, sono comunque associati a costi di manutenzione ordinaria o straordinaria, senza la quale diviene a rischio o è fortemente ridotta la capacità di elaborare i suddetti documenti.
- k) Inserimento dell’obsolescenza dei formati di file e delle tecnologie di archiviazione all’interno di una più ampia strategia di trasformazione digitale dell’organizzazione.

Si faccia riferimento al Glossario delle presenti linee guida per la definizione dei termini non ulteriormente introdotti in questo Allegato (e che sono qui indicati in colore azzurro Italia).

4. La valutazione di interoperabilità, in quanto parte della gestione documentale, andrebbe effettuata periodicamente allo scopo di individuare tempestivamente cambiamenti delle condizioni espresse dai punti sopra elencati e permettere quindi di valutare eventuali azioni. È proprio nella ripetizione della valutazione di interoperabilità ad intervalli regolari che divengono manifesti i formati in via di obsolescenza (quando non già conservati in un formato obsoleto).

## 3.2 Indice di interoperabilità

1. Allo scopo di coadiuvare la valutazione dei formati di file relativamente all'interoperabilità, l'Agenzia propone innanzi tutto un modello semplificato e quantitativo ove, ad ogni formato di file (anche quelli non elencati nel §2 di questo Allegato), viene associato un valore numerico. Tale valore assegnato al formato è dato dalla somma dei valori associati a tutte le caratteristiche di cui ai punti a)–g) del capitolo §1.2.2.

2. Nel caso di formati di pacchetti o contenitori, andrà fatta una valutazione per ogni componente e considerato come addendo il valore più basso (cioè peggiore) per ciascuna delle sue componenti.

Per un formato contenitore andrà valutato sia il formato della busta che il formato del suo contenuto, ad esempio per i contenitori multimediali (cfr. §2.12), il formato dei codec di ciascuna essenza ivi contenuta; per un formato di pacchetto andranno valutati i formati di tutti i file compresi nel pacchetto e, qualora il pacchetto comprenda dei file contenitori, valutarli con il medesimo criterio sopra esposto.

3. Sia per i formati contenitori che per quelli di pacchetto verrà usato come addendo, per caratteristica, il valore numerico peggiore tra quelli dei suoi file (o dei codec di ciascun file). Si prenda, a titolo di esempio, l'indice di interoperabilità di uno specifico pacchetto di file ove tutti i file utilizzino formati indipendenti dal dispositivo tranne un file multimediale, la cui busta e tutte le sue essenze sono anch'esse indipendenti dal dispositivo tranne una sola essenza audio (che ad esempio potrebbe richiedere la presenza di un dispositivo hardware proprietario per la sua decodifica). Il pacchetto andrà considerato comunque come “dipendente dal dispositivo” e quindi gli verrà applicato un modificatore pari a 0 (anziché a +3), proprio a causa della presenza dell'unico file il cui formato è dipendente dal dispositivo.

4. Considerando una scala che va dal file più interoperabile (con indice pari a 20) a quello meno interoperabile (indice pari a 0), un valore pari a 12 o superiore può essere considerato sufficiente dal punto di vista dell'impatto di tale formato relativamente ad interoperabilità e obsolescenza; valori inferiori indicano problematiche oggettive che vanno affrontate il prima possibile in ottica di riversamento o altre metodologie.

5. Si precisa che l'indice di interoperabilità è meramente indicativo, in quanto non tiene conto di alcuna peculiarità che un'organizzazione possa avere in merito a specifici formati di file. Ad esempio, l'utilizzo di formati chiusi, proprietari o dipendenti dal dispositivo dovrebbe essere sempre un fattore di esclusione almeno nella scelta di formati da usarsi per la formazione di nuovi documenti informatici.

### 3.3 Riversamento

1. Il riversamento di formato, precedentemente introdotto, comporta il trasferimento di un documento informatico in un formato di file diverso: contestualmente, ciò può comportare anche una duplicazione da un sistema di storage ad un altro (volume, disco, nastro, filesystem, storage ad oggetti o altri). Quando si parla di riversamento di file, s'intende un riversamento di almeno il suo formato. Per quanto già detto nell'introduzione al §3, le strategie relative alla gestione dei formati e dei sistemi di storage vanno spesso di pari passo; perciò, può essere in alcuni casi operativamente ed economicamente vantaggioso effettuare i riversamenti di formato contestualmente a quelli di storage. I riversamenti vengono pianificati a seguito di una nuova valutazione di interoperabilità, considerando i costi e i benefici di una tale operazione.

2. Quando si effettua un riversamento finalizzato alla conservazione del file si può e, in certi casi previsti dalla legge, si deve, conservare anche la copia del file nel formato originario. In entrambe questi casi il file originario è conservato indipendentemente dal suo formato di file originario, purché sia conservata anche –in una forma logicamente e univocamente legata ad esso– copia conforme del medesimo in un formato adatto alla conservazione (tra quelli individuati al §2 del presente Allegato). Le considerazioni in questo e nei successivi paragrafi si applicano non solo ai formati di file, ma anche, *mutatis mutandis*, ai formati di buste, pacchetti di file, flussi binari e codec. Lo scopo del riversamento congiunto alla conservazione del documento nel formato originario è consentire la convalida di firme, sigilli o validazioni temporali elettroniche che, eventualmente già presenti nel documento originario, non potrebbero essere riportate –senza invalidarle– nel documento riversato.

3. Quando si effettua un riversamento finalizzato alla conservazione, il file riversato è una copia digitale di un documento digitale e, come tale, la conformità della copia è attestata in base alla normativa vigente, inclusa la certificazione di processo come riportata nell'Allegato 3 delle presenti Linee guida.

4. È importante che nella scelta dei nuovi formati di file (e, *mutatis mutandis*, di contenitori, pacchetti di file, flussi digitali e codec), così come nella scelta metodologica circa l'esecuzione del riversamento, si considerino le peculiarità tecniche del formato sorgente e di quello riversato, con particolare riferimento sia alla perdita di dati e metadati, sia alla diversa qualità o rappresentazione tecnica dei medesimi.

5. Quando si effettua un riversamento massivo finalizzato alla conservazione di più documenti informatici –a prescindere se sia conservato o meno il documento nel suo formato originario– il processo di riversamento include i passaggi indicati nel successivo elenco numerato. Tali passaggi –particolarmente 1 e 2– possono essere

inquadri come parte di un processo certificato di conformità della copia riversata (cfr. Allegato 3 delle presenti linee guida).

1. Il riversamento di un formato viene effettuato mediante un processo certificato che ne garantisce l'integrità (effettiva o per lo meno sostanziale, come intesa nel punto 2) e la riproducibilità. Ogni procedura di riversamento è descritta nel manuale di gestione e, se del caso (cfr. §3.1), nella valutazione di interoperabilità, in tutti i suoi dettagli tecnici, inclusi quelli sui formati di destinazione e quelli riversati.
2. Per le PP.AA., il riversamento avviene sempre in formati che ne migliorano l'interoperabilità, o comunque non la peggiorano (come, stabilito, ad esempio, mediante il calcolo dell'indice di interoperabilità), tenendo conto degli obblighi sulla specificità di formato introdotti in §2.2. In particolar modo *non* sono opportuni, relativamente alla classificazione di formati di cui al §1.2.2, i seguenti riversamenti, da un formato:
  - aperto verso formati chiusi,
  - non proprietario, ovvero proprietario a libero utilizzo, verso formati proprietari,
  - non dipendente dal dispositivo verso formati dipendenti da dispositivo,
  - formato parlante verso formati muti.
3. Per ogni file riversato di un processo massivo automatico ovvero semiautomatico il processo produce un'attestazione del riversamento specifico di quel file, ove le attestazioni circa documenti riversati come parte della medesima procedura vengono collezionati in un [registro di riversamento](#), che contiene (globalmente rispetto alla particolare procedura e individualmente per ogni file elaborato) almeno:
  - a. un riferimento temporale opponibile a terzi ai sensi dell'art. 41 del DPCM 22 febbraio 2013 relativo all'inizio o alla fine del riversamento (indicando chiaramente a quale dei due tempi ciascun riferimento temporale si riferisca);
  - b. indicazioni sul sistema informativo impiegato (per esempio: nome, numero di revisione sia del sistema operativo che del software; nome della macchina e suoi indirizzi di rete o altri numeri identificativi unici delle componenti hardware; identificativi unici del software quali i numeri di licenza; nome o identificativo unico e orario di accesso al sistema operativo dell'utenza sotto cui l'applicativo ha agito);
  - c. nome del file sorgente, posizione nel filesystem e metadati esterni (cfr. §1.1.2);

- d. formato sorgente del file, sua versione del formato e metadati interni (cfr. §1.1.3);
  - e. impronta crittografica del file sorgente;
  - f. nome del file riversato, posizione nel filesystem e metadati esterni;
  - g. formato di riversamento, sua versione e metadati interni convertiti dal punto d);
  - h. impronta crittografica del file destinazione;
  - i. in caso di file contenitori (come sorgente o destinazione), i metadati ai punti d, g<sup>64</sup> si intendono riferiti alla busta, cui si aggiunge elenco completo del contenuto della medesima (p.es. essenze e i codec impiegati per ciascuna di esse, con i loro eventuali metadati e profili); deve inoltre essere previsto –nei casi ove sia tecnicamente possibile– file con imbustamento nidificato (cfr. §1.1.1);
  - j. in caso di pacchetti di file (come sorgente o destinazione), i controlli c–h<sup>65</sup> si intendono riferiti a ciascun file componente il pacchetto, cui si aggiunge l’indicazione dei metadati deducibili dall’intero pacchetto nella sua interezza, laddove non esplicitamente descritti negli eventuali file-manifesto (cfr. §1.1.1);
  - k. eventuali errori tecnici, anomalie o ambiguità riscontrate durante il riversamento.
4. Nel rispetto delle leggi sulla privacy in vigore (D.Lgs. N°101 del 10 agosto 2018, del GDPR e loro successive modificazioni), il riversamento in altro formato di file costituisce un’ulteriore occasione per ottemperare agli obblighi in materia di adeguatezza, pertinenza, minimizzazione ed esattezza dei dati personali ivi contenuti, così come della liceità del loro trattamento e della loro eventuale pseudonimia.
  5. Qualora sussistano obblighi di legge (come nel caso della protezione dei dati personali o della conservazione sostitutiva) o altri tipi di vincoli nel preservare l’evidenza informatica costituita dal documento nella sua interezza, il documento nel formato originale viene conservato *insieme* a un suo riversamento in formato più interoperabile. Tale associazione logica deve anch’essa essere scritta nel registro di riversamento (ad esempio associando le impronte crittografiche dei due come indicate ai punti e,h<sup>66</sup> del punto 2).
  6. Salvo in casi in cui siano applicabili le considerazioni di cui ai punti 3 o 4, un riversamento di formato altera l’evidenza informatica, intaccandone dunque l’integrità da un punto di vista strettamente tecnico; esistono tuttavia riversamenti di formato che mantengono il contenuto documentale *sostanzialmente* invariato (inclusi quelli discussi nei punti 3 o 4), costituendo

<sup>64</sup> Leggasi «al punto d più al punto g».

<sup>65</sup> Leggasi «i controlli dal c all’h».

<sup>66</sup> Leggasi «al punto e più al punto h».

una valida possibilità per il riversamento. Tali possibilità di riversamento, qualora siano individuate, sono comprese nel manuale di gestione documentale. In esso viene descritto come il contenuto documentale viene sostanzialmente preservato, incluse le considerazioni sulla similitudine tra le due evidenze informatiche. Sono incluse anche una o più delle seguenti trasformazioni che, se applicabili, sono effettuate durante il riversamento:

- In caso il documento nel formato originale venga mantenuto per assolvere ad obblighi di legge o altro, specificare come i due file (l'originale e il riversato) vengano logicamente associati fra loro (come descritto al punto 4).
- Laddove le evidenze vengano modificate da algoritmi non reversibili (p.es. compressione con perdita) un'analisi puntuale o statistica dell'ammontare di informazione persa durante il riversamento (p.es. misurata in SNR minimi e massimi tra l'essenza sorgente e quella destinazione), con riferimento a standard di misura riconosciuti a livello internazionale, europeo o nazionale.
- In caso di perdita di metadati interni, indicare quali metadati si perdono e come essi vengano comunque riportati nel registro di riversamento.
- In caso metadati convertiti biunivocamente da un formato all'altro (incluso il caso in cui più metadati nel formato sorgente siano oggetto di accorpamenti o separazioni in altri metadati nel formato di destinazione), descrivere gli algoritmi che sono implementati per ciascun metadato.<sup>67</sup>
- In caso di metadati interni convertiti in maniera *non* invertibile, descrivere gli algoritmi impiegati (come al punto precedente), aggiungendo esplicitamente quali informazioni si perdono e come esse siano trasformate irreversibilmente.<sup>68</sup>
- In caso il formato destinazione ammetta dei metadati obbligatori che non hanno un analogo nel formato sorgente (ovvero ammetta metadati facoltativi che si ritiene comunque opportuno inserire nel

---

<sup>67</sup> A titolo di esempio, sia dato un campo 'Scadenza' nel formato sorgente e un campo 'NotAfter' nel formato destinazione, le cui sintassi sono, rispettivamente, il numero intero di giorni passati da un'epoca pari al 1 gennaio 2019 (fuso orario italiano: CEST) e una stringa di testo formattata come da [RFC-3339](#) (in fuso orario UTC). Viene dunque specificato l'algoritmo, perfettamente invertibile, che mappa un valore di "42" in "2019-02-14T01:00:00Z".

<sup>68</sup> A titolo di esempio, sia dato un campo 'dimensione1' nel formato sorgente e un campo 'Width' nel formato destinazione. Nel manuale di riversamento, andrà giustificata la motivazione per cui un valore di "-42.58cm" nel formato sorgente, dotato di segno e unità di misura, viene mappato in "426" indicato implicitamente in millimetri e arrotondato al numero intero più vicino. È anche opportuno che sia indicato il motivo per cui un metadato relativo ad una dimensione (spaziale?) non meglio identificata sia (sempre?) mappato in un campo riservato alla 'larghezza' di qualcosa.

formato riversato, anche se non hanno un analogo nel formato originario), specificare come gli vengono assegnati valori.

7. In alcuni casi,<sup>69</sup> imbustando un documento informatico in un contenitore aggiuntivo potrebbe mantenere integro il contenuto all'interno, perciò un riversamento in tal senso –cioè un semplice imbustamento del documento senza alterarlo– può essere reversibile. L'integrità del file nella sua interezza è tuttavia compromessa. Analogamente reversibile è invece includere un documento rappresentato da un file all'interno di un pacchetto di file. Entrambi le metodologie non risolvono i problemi di interoperabilità e obsolescenza originali per cui il riversamento è stato concepito, ma possono mitigarli, soprattutto se vengono scelti contenitori o pacchetti parlanti che compensano la mancanza di metadati nel formato originale.
  8. Analogamente al punto 3, in alcuni casi, un documento che viene re-imbustato (cfr. §1.1.1), nel senso che il riversamento consiste nel sostituire la busta che lo conteneva con un'altra, potrebbe mantenere, in alcuni casi, l'integrità del contenuto della busta. Verrebbe persa comunque l'integrità della busta e, come per il punto 3, l'integrità del file nella sua interezza. Tuttavia questa metodologia potrebbe risolvere un problema di obsolescenza e interoperabilità legato al solo formato della busta usata in precedenza.
6. Quando si effettui un riversamento *non* finalizzato alla conservazione è comunque opportuno considerare i passaggi elencati al precedente punto 5, ad eccezione dei punti 1 e 2 del medesimo elenco, che si riferiscono al riversamento qualora inquadrato in processi di conservazione o certificazione di processo.

---

<sup>69</sup> Alcuni formati contenitori, imbustando un documento, si limitano ad aggiungervi una busta costituita da una o più evidenze informatiche in punti predeterminati del documento o essenza originale (tipicamente in testa e in coda, ma anche inseriti in parti centrali). Quando avviene tecnicamente un procedimento di questo tipo l'evidenza informatica imbustata è alterata *reversibilmente*, potendo quindi essere ricostruita bit a bit. Alcuni formati di contenitore di file, tuttavia, effettuano alterazioni irreversibili del contenuto, che dunque non rimane integro a seguito di un'operazione di "sbustamento" (in inglese, *unwrapping*).

## Certificazione di processo

*Allegato 3 al documento “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.*

## Indice

---

Indice	2
CAPITOLO 1	4
Premessa	4
1.1.    Scopo e campo di applicazione del documento	4
1.2.    Certificazione di processo: principi generali	4
CAPITOLO 2	6
Regole di utilizzo della certificazione di processo	6
2.1.    Conformità allo standard ISO	6
2.2.    Efficacia probatoria della certificazione di processo	7
2.3.    Ciclo di dematerializzazione: requisiti, fasi e controlli	8
2.4.    Validazione della certificazione di processo	12

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

---

## CAPITOLO 1

---

### Premessa

---

#### 1.1. Scopo e campo di applicazione del documento

Lo scopo del presente allegato è quello di descrivere le modalità di adozione della certificazione di processo, considerata una modalità prevista dagli articoli [22 comma 1bis Copie informatiche di documenti analogici](#) e [23-ter comma 1bis Documenti amministrativi informatici](#) del CAD. L'adozione del processo descritto nel presente documento riguarda tutti i soggetti indicati nell'art. 2 commi 2 e 3 del CAD che eseguono la dematerializzazione massiva dei documenti analogici e che vogliono garantire la corrispondenza del contenuto e forma della copia informatica all'originale analogico, non volendo ricorrere allo strumento del *raffronto* dei documenti in quanto oneroso e, in alcuni casi, impraticabile. La finalità dello strumento certificazione di processo è quella di incentivare e facilitare la digitalizzazione dei flussi informativi, nel caso di un elevato numero di documenti da scansionare.

#### 1.2. Certificazione di processo: principi generali

Per assicurare l'efficacia probatoria dei documenti informatici e delle copie, la *certificazione di processo*, è stata introdotta<sup>1</sup> dal legislatore con la finalità di favorire la dematerializzazione di grosse quantità di documenti analogici. Si tratta di una delle due modalità previste per assicurare che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, insieme a quella tradizionalmente nota come *raffronto dei documenti*. Il legislatore ha previsto l'adozione di tecniche in grado di garantire la corrispondenza della

---

<sup>1</sup> Il Decreto Legislativo 13 dicembre 2017, n. 217 (in G.U. 12/01/2018, n.9) ha disposto l'introduzione del comma 1-bis all'art. 22 ovvero la *certificazione di processo*.

forma e del contenuto dell'originale e della copia, come si legge all'art. 22 comma 1bis del CAD:

*«la copia per immagine su supporto informatico di un documento analogico è prodotta mediante processi e strumenti che assicurano che il documento informatico abbia contenuto e forma identici a quelli del documento analogico da cui è tratto, previo raffronto dei documenti o attraverso certificazione di processo nei casi in cui siano adottate tecniche in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia»*

Nel modello di certificazione di processo devono concorrere due elementi fondamentali:

- la presenza di una procedura tecnologica in grado di garantire la corrispondenza della forma e del contenuto dell'originale e della copia;
- la previa descrizione e certificazione di questo processo, al fine di conferire ai documenti risultanti dal processo di scansione l'efficacia probatoria prevista:

*«Le copie per immagine su supporto informatico di documenti originali formati in origine su supporto analogico hanno la stessa efficacia probatoria degli originali da cui sono estratte, se la loro conformità è attestata da un notaio o da altro pubblico ufficiale a ciò autorizzato, secondo le regole tecniche stabilite ai sensi dell'articolo 71».* (art. 22 comma 2 del CAD)

La procedura tecnologica in grado di garantire tali certezze è stata tradotta in termini di efficienza gestionale dell'organizzazione preposta alla scansione massiva dei documenti e in termini di diligenza di comportamento dei soggetti preposti alla certificazione di processo.

## CAPITOLO 2

---

### Regole di utilizzo della certificazione di processo

---

#### 2.1. Conformità allo standard ISO

La locuzione “certificazione di processo” richiama le certificazioni in materia di qualità, sicurezza, ambiente (ecc.), nel cui ambito si assiste alla presenza di due tipologie possibili di certificazione: la certificazione di prodotto e la certificazione di processo (detta anche “di sistema”), con le seguenti accezioni:

- “certificazione di prodotto/servizio” intesa come una forma di “assicurazione diretta”, con cui una terza parte indipendente accerta la rispondenza di un determinato prodotto o servizio ai requisiti di legge applicabili o a procedure regolamentari autonomamente individuate;
- “certificazione di sistema o di processo” intesa come una forma di “assicurazione indiretta”, in quanto assicura la capacità di un’organizzazione di strutturarsi e gestire le proprie risorse ed i propri processi produttivi in modo tale da identificare e soddisfare i requisiti stabiliti dalle parti interessate<sup>2</sup>.

La certificazione in generale attesta che una determinata attività, o uno specifico prodotto, rispetta i requisiti che l’organizzazione si è data oppure i requisiti di una norma specifica. La certificazione è sempre ed in ogni caso una procedura con cui con cui una terza parte indipendente dà assicurazione scritta che un prodotto, un servizio, un processo è conforme ai requisiti specificati.

Pertanto, partendo dalla sopradetta assunzione, la “certificazione di processo” prevista dal comma 1-bis dagli artt. 22 e 23-ter del CAD, di fatto, è più propriamente una *certificazione di un risultato* ottenuto attraverso un determinato

---

<sup>2</sup> Fonte: [http://www.uni.com/index.php?option=com\\_content&view=article&id=157&Itemid=2428](http://www.uni.com/index.php?option=com_content&view=article&id=157&Itemid=2428)

processo. Il risultato, infatti, ovvero il prodotto, consiste in una copia informatica di documento analogico, e la certificazione di processo produce sostanzialmente una *certificazione di conformità di una copia ad un originale*; purché essa risulti corredata da una completa descrizione del processo attraverso il quale una simile copia è stata ottenuta.

La certificazione di processo mira a conseguire il medesimo risultato della “certificazione tradizionale”, rappresentato dal tradizionale metodo di raffronto fra originale e copia. Pertanto, detto “processo” dovrà caratterizzarsi non solo dal punto di vista *oggettivo* (strumenti tecnologici, procedure, organizzazione,...) ma anche da quello *soggettivo* per attestare l’efficacia probatoria della certificazione di processo. Quindi, nella certificazione di processo non ci si potrà limitare a descrivere il processo con il quale è stata creata la copia digitale, ma occorrerà anche, necessariamente, certificare la copia *risultato*. Di conseguenza, due sono gli effetti che si determinano:

- per l’ambito *oggettivo*: il ciclo di dematerializzazione massiva dovrà essere certificato da organismo terzo in accordo agli standard ISO 9001 e ISO 27001<sup>3</sup>, con campo di applicazione specifico per i servizi di progettazione e dematerializzazione massiva di documenti;
- per l’ambito *soggettivo*: il ciclo di dematerializzazione dovrà concludersi con il metodo del raffronto a campione dei documenti, generando una certificazione ovvero un risultato probatorio differente a seconda che il rapporto di verifica sia firmato da un pubblico ufficiale o da un soggetto privato.

## 2.2. Efficacia probatoria della certificazione di processo

L’efficacia probatoria di un documento-copia, in tutta la normativa vigente, varia se rimessa all’intervento di un pubblico ufficiale o a quello di un soggetto privato. Il CAD, infatti, ai commi 2 e 3 dell’art. 22 e comma 3 dell’art. 23-ter distingue il valore probatorio “privilegiato” che fa piena prova fino a querela di falso (ex art. 2700 del c.c.) se la conformità all’originale è assicurata da un notaio o Pubblico Ufficiale a ciò autorizzato, dal valore probatorio “semplice” che fa piena prova

---

<sup>3</sup> Qualora si presentassero casi in cui non fossero disponibili tali certificazioni (es. nelle sedi della PA situate fuori dai confini nazionali che dovessero affidare il servizio all’esterno), i fornitori dovranno dimostrare il possesso di sistemi organizzativi e di sicurezza o di altre certificazioni rispondenti agli stessi requisiti previsti dai suddetti standard.

fino a disconoscimento se la conformità all'originale è data da un soggetto privato. Si veda, al riguardo, la seguente tabella:

Soggetto firmatario	Valore probatorio ex artt. 22 e 23-ter del CAD
Notaio o PU a ciò autorizzato →	L'atto pubblico ovvero l' <i>attestazione di conformità</i> fa piena prova fino a querela di falso (ex art. 2700 del c.c.).
Privato →	Una copia fatta da chiunque fa piena prova fino a disconoscimento.

Ne consegue che si parla propriamente di certificazione di processo solo qualora l'attestazione di conformità venga rilasciata da notaio o Pubblico Ufficiale a ciò autorizzato e sottoscritta per mezzo della firma digitale o di altra firma elettronica qualificata (ex artt. 22 comma 2 e 23-ter comma 3 del CAD). Nel caso di soggetto privato, non si produrrà una certificazione di processo ma unicamente un rapporto di verifica sottoscritto dallo stesso che fa piena prova fino a disconoscimento.

### 2.3. Ciclo di dematerializzazione: requisiti, fasi e controlli

La descrizione del processo di dematerializzazione va eseguita non solo per dare sostanza all'intero impianto della certificazione di processo ma, anche, per estendere in maniera massiva il processo di conversione dall'analogico al digitale a tutto il lotto di documenti sottoposti a scansione. Specificare quali debbano essere i requisiti tecnici cui attenersi, le fasi ed i controlli da seguire permetterà di avere una sorta di "presunzione" di efficacia probatoria delle copie realizzate anche in periodi di scansione diversi purché afferenti allo stesso progetto o lotto di copie digitalizzate. Il notaio/PU o privato descrivono l'intero processo e ne certificano il funzionamento verbalizzando, prima ancora che l'attività di scansione massiva venga avviata sull'intero lotto di documenti, la conformità di alcune copie campione agli originali analogici ricorrendo al tradizionale raffronto dell'originale con la copia, in modo da "congelare" i criteri di qualità e sicurezza da adottare alle successive copie informatiche.

Allo scopo di assicurare la riconducibilità della copia realizzata a quello specifico procedimento di scansione, la "certificazione iniziale" dovrà generare un codice univoco da inserire tra i metadati di ciascun documento copia o, in alternativa, riportare l'elenco dei valori di hash relativi a ciascuna copia informatica frutto della scansione effettuata. In questo modo si eviterà che copie realizzate con altri procedimenti possano essere "inserite" fraudolentemente tra quelle prodotte dal

processo certificato, acquisendo la relativa efficacia probatoria. Laddove richiesta dalla natura dell'attività, il singolo documento estratto dal procedimento di scansione o l'intero lotto potrà successivamente essere "certificato" da notaio o PU a ciò autorizzato attraverso la verifica di corrispondenza del codice oppure della variabile di hash calcolata su ciascun documento a valle della scansione massiva fatta.

In particolare, la descrizione del procedimento di dematerializzazione presente nell'attestazione di conformità<sup>4</sup> o rapporto di verifica contiene le seguenti minime informazioni:

- Anagrafica Committente;
- Nominativo e ruolo del verbalizzante (privato, notaio o PU a ciò autorizzato);
- Codice identificativo univoco presente tra i metadati del documento copia (in alternativa al listato dei valori di hash calcolati sulle copie informatiche);
- Identificativo (tipologia e numero) del campione di documenti copia utilizzati per la certificazione iniziale;
- Numero, tipologia e quantità del lotto di documenti analogici sottoposti a scansione;
- Tipologia e quantità del lotto di documenti cui il campione appartiene;
- Requisiti tecnici e/o vincoli di progetto di scansione massiva;
- Finalità della scansione (es.: statistico, storico, probatorio,...);
- Riferimento contratto tra fornitore e committente (in caso di *outsourcing*);
- Luogo, data e orario inizio e fine della scansione a cui si è assistito;
- Nomi referenti presenti al processo di scansione (opzionale);
- Riferimento documentazione di analisi, di progetto o di sistema utilizzata a supporto del processo di dematerializzazione;
- Nome e versione del sw di elaborazione digitale delle immagini utilizzato;
- Segnalazione di eventuali criticità, anomalie riscontrate;
- Indicazione delle fasi e dei controlli o della procedura ISO 9001 di riferimento, che a titolo esemplificativo possono essere rappresentate da:

---

<sup>4</sup> Cfr. § 2.5 Linee Guida sul documento informatico “[...] L’attestazione di conformità della copia informatica di un documento amministrativo analogico, formato dalla Pubblica Amministrazione, ovvero da essa detenuto, può essere inserita nel documento informatico contenente la copia informatica o essere prodotta come documento informatico separato contenente un riferimento temporale e l'impronta di ogni copia per immagine. Il documento informatico contenente l'attestazione è sottoscritto con firma digitale o con firma elettronica qualificata o avanzata del funzionario delegato.

- Sanificazione, fascicolazione e normalizzazione (despillatura) dei documenti analogici,
- Settaggio (selezione dei parametri di acquisizione) del sw di image processing;
- Scansione batch dei documenti,
- Indicizzazione (metadatazione),
- Verifica qualità immagini digitalizzate,
- Segnalazione incongruenze.

Per l'acquisizione massiva dei documenti si ricorre a scanner professionali che devono essere dotati di sistemi di lettura ottica ovvero di algoritmi di elaborazione digitale delle immagini in grado di migliorare la qualità delle immagini medesime e correggere automaticamente i più comuni errori. Di seguito, le funzionalità minime da assicurare per un software di elaborazione digitale delle immagini:

- Auto orientamento,
- Bilanciamento della luce e del colore,
- Correzione della deformazione,
- Correzione della curvatura,
- Rotazione e ribaltamento,
- Controllo qualità (proprietà delle immagini, come luminosità, contrasto, varianza, colore dominante, dimensioni, colori, inclinazione,...).

I suddetti requisiti tecnologici sono accompagnati dai vincoli di progetto rappresentati – ad esempio - dall'utilizzo o finalità che si vuole fare dell'immagine (memorizzazione storica a lungo termine, probatorio, distribuzione via web,...), dalla tipologia di documento sottoposto a scansione, dalla numerosità del lotto di documenti da scansionare, dalla percentuale di errore ritenuta tollerabile nel controllo visivo di qualità o ancora dagli obblighi di visualizzazione e ricerca imposti dalla normativa vigente<sup>5</sup>, che impongono di settare i software di *image processing* a valle dell'analisi dell'archivio analogico fatta. Le certificazioni di sistema ISO 9001 e 27001 rappresentano pertanto - lato organizzazione – una ragionevole garanzia di qualità e sicurezza a fronte delle variabili tecnologiche individuate.

Le Pubbliche Amministrazioni che vogliono svolgere in autonomia la dematerializzazione massiva di documenti analogici possono non ricorrere alle certificazioni ISO assumendo in toto la responsabilità della qualità del processo.

---

<sup>5</sup> A titolo esemplificativo, qualora si intenda conservare in formato digitale scritture contabili già stampate a suo tempo su supporto cartaceo, il processo di acquisizione dell'immagine, dovrà svolgersi come previsto dalla risoluzione dell'[Ag. Entrate del 15 giugno 2009, n. 158/E](#), che presuppone che “l'immagine acquisita rispecchi in maniera fedele, corretta e veritiera il contenuto rappresentativo del documento”.



## 2.4. Validazione della certificazione di processo

Come detto, la certificazione di processo si caratterizza, sia dal punto di vista oggettivo sia da quello soggettivo, per attestare l'efficacia probatoria della certificazione di processo (§1.2). Pertanto, è indispensabile validare la conformità di un documento-copia rispetto ad un documento-originale di partenza.

A valle del processo di scansione massiva, la riconducibilità del documento copia alla certificazione iniziale è validata dal notaio/PU o soggetto privato che rilascia un verbale di “certificazione di chiusura” attraverso la verifica di corrispondenza del codice univoco presente tra i metadati o del valore di hash su un campione di documenti individuato<sup>6</sup>.

Trattandosi di attività ovviamente non “delegabile”, essa sarà rimessa all'apprezzamento esclusivo e diretto del pubblico ufficiale o soggetto privato autorizzato.

Il controllo visivo si sostanzia nell'attestare i requisiti tecnici essenziali di leggibilità<sup>7</sup> del documento immagine risultato della scansione, di garanzia dell'integrità<sup>8</sup> del contenuto e di completezza<sup>9</sup> del processo di scansione.

Evidentemente, l'attestazione di conformità o rapporto di verifica è sottoscritto con firma digitale o altra firma elettronica qualificata, come stabilito ai sensi dagli artt. 22 comma 2 e 23-ter comma 3 del CAD.

---

<sup>6</sup> Per il piano di campionamento, si segnala la norma UNI ISO 2859 “Procedimenti di campionamento nell'ispezione per attributi - Parte 1: Schemi di campionamento indicizzati secondo il limite di qualità accettabile (AQL) nelle ispezioni lotto per lotto”.

<sup>7</sup> Leggibilità: il documento deve poter essere accessibile senza un eccessivo sforzo e deve essere garantita la leggibilità a occhio umano.

<sup>8</sup> Integrità: il documento informatico è considerato inalterato ovvero immutato rispetto all'originale.

<sup>9</sup> Completezza: corrispondenza tra le pagine del documento scansionato ottenute rispetto all'originale.

# Attestazione di conformità nei processi di scansione massiva ex artt. 22 e 23-ter CAD

A

## Ciclo di dematerializzazione

*Certificato ISO 9001 e 27001*

1. Analisi e progettazione
  - Analisi delle esigenze
  - Analisi dell'archivio analogico
2. Normalizzazione
  - Presa in carico della documentazione
  - Riorganizzazione fascicoli
3. Scannerizzazione
  - Digitalizzazione immagini
  - Verifica qualità
4. Indicizzazione
  - Acquisizione dati
  - Segnalazione incongruenze

B

## Raffronto dei documenti



Tramite un piano di campionamento, il pubblico ufficiale o il soggetto privato procede ad un confronto visivo tra l'originale analogico e la copia informatica per verificare la corrispondenza del contenuto e della forma, se necessario<sup>1</sup>.  
 A conclusione del raffronto, il pubblico ufficiale o il soggetto privato sottoscrive elettronicamente rispettivamente l'attestazione di conformità o il rapporto di verifica. La sottoscrizione in entrambi i casi chiarisce che il processo di scansione ha prodotto un risultato conforme all'originale e che tale risultato si estende a tutto il lotto dei documenti scansionati.

C

## Valore probatorio



Attestazione di conformità certificata dal notaio o PU, *valore probatorio «privilegiato»*

Rapporto di verifica del soggetto privato, *valore probatorio «semplice»*

<sup>1</sup> ricorrendo al pubblico ufficiale che attesta la conformità di tutti quei dati ed informazioni che con il passaggio dal supporto analogico a quello informatico inevitabilmente si perdono, la corrispondenza da verificare si limita al contenuto e non anche alla forma.

## **Standard e Specifiche tecniche**

***Allegato 4 al documento “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.***

## Indice

---

Indice	2
CAPITOLO 1	4
Premessa	4
1. Scopo e campo di applicazione del documento	4
2. Standard e Specifiche tecniche	4
2.1 <i>per la gestione documentale</i>	4
2.1 <i>per la conservazione digitale</i>	5
3.1 <i>per Sicurezza informatica</i>	6

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

# CAPITOLO 1

---

## Premessa

---

### 1. Scopo e campo di applicazione del documento

Il presente documento fornisce indicazioni sugli standard e le specifiche tecniche da ritenersi coerenti con le linee guida sulla formazione, gestione e conservazione dei documenti informatici. Per la natura stessa dell'argomento trattato, il presente documento viene periodicamente aggiornato e pubblicato online sul sito dell'Agenzia per l'Italia digitale.

### 2. Standard e Specifiche tecniche

Di seguito sono riportati i principali standard e specifiche tecniche di riferimento nell'ambito della formazione, gestione e conservazione di documenti informatici e documenti amministrativi informatici. In particolare:

#### 2.1. per la gestione documentale

**UNI ISO 15489-1** - Informazione e documentazione - Gestione dei documenti di archivio - Principi generali sul record management.

**UNI ISO 15489-2** - Informazione e documentazione - Gestione dei documenti di archivio – Linee Guida sul record management.

**ISO/TS 23081-1** - Information and documentation - Records management processes – Metadata for records – Part 1 – Principles, Quadro di riferimento per lo sviluppo di un sistema di metadati per la gestione documentale.

**ISO/TS 23081-2** - Information and documentation - Records management processes – Metadata for records – Part 2 – Conceptual and implementation issues, Guida pratica per l'implementazione.

**ISO 16175-1** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 1: Overview and statement of principles.

**ISO 16175-2** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 2: Guidelines and functional requirements for digital records management systems.

**ISO 16175-3** - (ICA) Information and documentation -- Principles and functional requirements for records in electronic office environments -- Part 3: Guidelines and functional requirements for records in business system.

**ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core.

**ISO 9001** – Sistemi di gestione per la qualità – Requisiti.

**ISO 30300:2011** Information and documentation - Management systems for records - Fundamentals and vocabulary;

**ISO 30301:2011** Information and documentation - Management systems for records – Requirements.

**ISO 30302:2015** Information and documentation - Management systems for records - Guidelines for implementation.

**ISO/TR 23081-3** - Information and documentation — Managing metadata for records — Part 3: Self-assessment method

**MoReq 2001** Model requirements for the management of electronic records.

**MoReq 2** Specification 2008 Model requirements for the management of electronic records – che individua i requisiti funzionali della gestione documentale.

**MoReq2010** Modular requirements for records systems.

## **2.2. per la conservazione digitale**

**UNI 11386** - Standard SInCRO - Supporto all'Interoperabilità nella Conservazione e nel Recupero degli Oggetti digitali.

**ISO 14721** - OAIS (Open Archival Information System), Sistema informativo aperto per l'archiviazione.

**ISO 15836** - Information and documentation - The Dublin Core metadata element set, Sistema di metadata del Dublin Core

**ISO/TR 18492** - Long-term preservation of electronic document-based information.

**ISO 20652** - Space data and information transfer systems - Producer-Archive interface - Methodology abstract standard.

**ISO 20104** - Space data and information transfer systems — Producer-Archive Interface Specification (PAIS).

**ISO/CD TR 26102** - Requirements for long-term preservation of electronic records.

**SIARD** Software Independent Archiving of Relational Databases 2.0

**Ministère de la culture et de la communication**, Service interministériel des Archives de France, Standard d'échange de données pour l'archivage. Transfert – Communication – Élimination – Restitution - Modification, ver. 2.1, 2018

**METS** - Metadata Encoding and Transmission Standard

**PREMIS** – PREservation Metadata: Implementation Strategies.

**EAD (3)/ISAD (G)**

**EAC (CPF)/ISAAR (CPF)/NIERA (CPF)**

**SCONS2/EAG/ISDIAH**

### **2.3. Per affidabilità (certificazione/valutazione- autovalutazione)**

**ISO 16363** - Space data and information transfer systems -- Audit and certification of trustworthy digital repositories

**ISO 16919** - Space data and information transfer systems -- Requirements for bodies providing audit and certification of candidate trustworthy digital repositories

**ISO 17068** - Information and documentation -- Trusted third party repository for digital records

## **2.1 per Sicurezza informatica**

**ISO/IEC 27001** - Information technology - Security techniques - Information security management systems – Requirements, Requisiti di un ISMS (Information Security Management System);

**ISO/IEC 27017** - Information technology -- Security techniques -- Code of practice for information security controls based on ISO/IEC 27002 for cloud services;

**ISO/IEC 27018** - Information technology -- Security techniques -- Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors;

**ETSI TS 101 533-1 V1.2.1** - Technical Specification, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 1: Requirements for Implementation and Management, Requisiti per realizzare e gestire sistemi sicuri e affidabili per la conservazione elettronica delle informazioni;

**ETSI TR 101 533-2 V1.2.1** - Technical Report, Electronic Signatures and Infrastructures (ESI); Information Preservation Systems Security; Part 2: Guidelines for Assessors, Linee guida per valutare sistemi sicuri e affidabili per la conservazione elettronica delle informazioni.

## I metadati

***Allegato 5 al documento “Linee Guida sulla formazione, gestione e conservazione dei documenti informatici”.***

Indice	<b>Errore. Il segnalibro non è definito.</b>
1. INTRODUZIONE	<b>Errore. Il segnalibro non è definito.</b>
2. METADATI DEL DOCUMENTO INFORMATICO	5
2.1 XSD METADATI DEL DOCUMENTO INFORMATICO	19
3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO	26
3.1 XSD METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO	41
4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE	50
4.1 XSD METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE	61

---

Questo allegato è parte integrante al testo delle linee guida sulla *Formazione, gestione e conservazione dei documenti informatici*.

---

# 1. Introduzione

Il presente allegato illustra i metadati relativi al documento informatico, al documento amministrativo informatico e all'aggregazione documentale informatica, intendendo, con quest'ultima, sia il fascicolo informatico, che la serie documentale.

Le implementazioni effettuate rispetto all'allegato alla precedente versione delle Linee guida si sono rese necessarie per ottemperare sempre più ai principi di interoperabilità, trasparenza e conoscenza approfondita del contesto documentale.

Il lessico utilizzato permette di astrarsi dal particolare dominio di appartenenza al fine di permettere una piena circolarità degli oggetti digitali e una semplificazione del loro recupero nel tempo.

L'elaborazione degli schemi è stata effettuata tenendo conto anche delle informazioni necessarie in vista della conservazione a lungo termine.

Gli schemi sotto riportati sono organizzati in modo da indicare per ogni metadato:

- **Informazione:** il nome;
- **Sottocampi:** l'eventuale sottostruttura del metadato complesso;
- **Valori ammessi:** valori accettati all'interno del campo;
- **Tipo dato:** numerici o alfanumerici;
- **Obbligatorietà:** l'indicazione di obbligatorietà, eventualmente condizionata;
- **Nuova definizione:** metadati nuovi o ridefiniti rispetto all'allegato alla normativa precedente;
- **Definizione:** indicazione sulla modalità di utilizzo del metadato.

Gli schemi di metadati relativi al documento informatico e al documento amministrativo informatico - se si esclude, per quest'ultimo caso, l'identificativo legato alla segnatura del protocollo - presentano sostanziali analogie strutturali, alle quali, però, corrispondono particolari e determinati controlli di obbligatorietà e codifica.

Sono stati definiti metadati complessi volti a garantire la massima flessibilità in termini di utilizzo.

Esemplificativo di tale intervento, il metadato "*Soggetti*", che consente di tipizzare gli attori che a vario titolo - "*Ruolo*" - concorrono alla definizione del documento informatico, del documento amministrativo informatico o della stessa aggregazione documentale, garantendo la possibilità di indicare molteplici tipologie di soggetti, dalle persone fisiche alle AOO delle Amministrazioni Pubbliche.

L'attività di **indicizzazione, individuazione e ricerca** è significativamente agevolata dalla definizione di metadati legati:

- alla tipologia - "*Tipologia documentale*" o "*Tipologia fascicolo*";
- alla registrazione - "*Dati registrazione*";
- all'Oggetto - "*Chiave descrittiva*";
- alla Classificazione - "*Classificazione*";

Particolarmente rilevante è il metadato complesso "*Assegnazione*" dell'aggregazione documentale informatica. Tale metadato, strutturato in vari sottocampi opportunamente valorizzati, consente di tracciare ogni passaggio dell'aggregazione per competenza o per conoscenza, al fine di garantire la massima trasparenza nell'ambito di qualsiasi procedimento amministrativo della PA.

## 2. METADATI DEL DOCUMENTO INFORMATICO

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>IdDoc</b>					NO, ma ridefinito
	Impronta	Rappresenta l'hash del documento	Binary	SI	
	Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	
	Identificativo	Come da sistema di identificazione formalmente definito	Alfanumerico	SI	
<b>Definizione</b>					
<p><i>Identificativo univoco e persistente associato in modo univoco e permanente al documento informatico in modo da consentirne l'identificazione.</i></p> <p><i>Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento.</i></p> <p><i>L'impronta è generata impiegando la funzione di hash, come da definizione nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento".</i></p> <p><i>Il metadato è costituito dai sottocampi:</i></p> <ul style="list-style-type: none"> <li><i>Impronta: sottocampo in cui viene memorizzato l'hash del documento</i></li> <li><i>Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato riportati nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"</i></li> <li><i>Identificativo: come da sistema di identificazione formalmente definito</i></li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Modalità di formazione		Indicare: <ul style="list-style-type: none"> <li>• <i>creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;</i></li> <li>• <i>acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;</i></li> <li>• <i>memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;</i></li> </ul>	Alfanumerico	SI	SI

		<ul style="list-style-type: none"> <li>• generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica.</li> </ul>			
--	--	--	--	--	--

#### **Definizione**

*Indica la modalità di generazione del documento informatico.*

*Sono previste le seguenti modalità secondo quanto riportato nelle Linee guida:*

- a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;*
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;*
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;*
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Tipologia documentale		<ul style="list-style-type: none"> <li>Fatture</li> <li>Determine</li> <li>Delibere</li> </ul>	Alfanumerico	SI	SI
<b>Definizione</b>					
<i>Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Dati di registrazione					
	Tipologia di flusso	<ul style="list-style-type: none"> <li>In uscita</li> <li>In entrata</li> <li>Interno</li> </ul>	Alfanumerico	SI	SI
	Tipo registro	<ul style="list-style-type: none"> <li>Nessuno,</li> <li>Protocollo Ordinario/ Protocollo Emergenza</li> <li>Repertorio/Registro</li> </ul>	Alfanumerico	SI	SI
	Data registrazione	nel caso di documento non protocollato: <ul style="list-style-type: none"> <li>Data di registrazione del documento</li> </ul> nel caso di documento protocollato: <ul style="list-style-type: none"> <li>Data di registrazione di protocollo</li> </ul>	Datetime	SI	NO, ma ridefinito

	Numero Documento	<p>nel caso di documento non protocollato:</p> <ul style="list-style-type: none"> <li>Numero di registrazione del documento</li> </ul> <p>nel caso di documento protocollato:</p> <ul style="list-style-type: none"> <li>Numero di protocollo</li> </ul>	Alfanumerico	SI	SI
	IdRegistro	Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI, nel caso di documento registrato	SI

#### Definizione

*Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato. Si intende per registrazione l'operazione che, in senso lato, associa ad un documento una data e un numero. In tale ottica quindi potrebbe non essere identificabile uno specifico registro, ma sono sempre identificabili una data di registrazione e un numero di registrazione del documento.*

*Sono previsti i seguenti sottocampi:*

- *Tipologia di flusso:* indica se si tratta di un documento in uscita, in entrata o interno.
- *Tipo registro:* indica il sistema di registrazione adottato: protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.
- *Data:* è la data associata al documento all'atto della registrazione
- *Numero documento:* Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- *IdRegistro:* Identificativo del registro in cui il documento viene registrato.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Chiave descrittiva</b>					
	Oggetto	Testo libero	Alfanumerico	SI	SI

	Parole chiave	Testo libero	Alfanumerico	NO	SI
<b>Definizione</b>					
<p><i>Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti sottocampi:</i></p> <ul style="list-style-type: none"> <li>• <i>Oggetto: testo libero;</i></li> <li>• <i>Parole Chiave: da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.</i></li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Soggetti</b>					
	Ruolo	<ul style="list-style-type: none"> <li>• Autore</li> <li>• Mittente</li> <li>• Destinatario</li> <li>• Assegnatario</li> <li>• Operatore</li> <li>• Altro</li> </ul>	Alfanumerico	SI, e nel caso di documento protocollato è obbligatorio indicare almeno il Mittente e il Destinatario	NO, ma ridefinita
	Tipo soggetto	<ul style="list-style-type: none"> <li>• PF per Persona Fisica</li> <li>• PG per Organizzazione</li> <li>• PA per le Amministrazioni Pubbliche</li> </ul>	Alfanumerico	SI	SI

	Nominativo	<p>Nominativo:</p> <p>se Tipo soggetto = PF:  ✓ cognome e nome;</p> <p>se Tipo soggetto = PG:  ✓ denominazione</p> <p>se Tipo soggetto = PA:  ✓ denominazione Amministrazione \  denominazione AOO;</p>	Alfanumerico	SI	SI
	Codice	<p>Codice identificativo:</p> <p>se Tipo soggetto = PF  ✓ codice fiscale</p> <p>se Tipo soggetto = PG:  ✓ codice fiscale;</p> <p>se Tipo soggetto = PA:  ✓ Codice IPA dell'Amministrazione  \ Codice AOO</p>	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	NO	SI
<b>Definizione</b>					

Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo. Sono definiti quindi i seguenti attributi:

- **Ruolo:** consente di indicare, a seconda delle necessità, l'autore del documento, il mittente, il destinatario, l'assegnatario. Obbligatorio indicare almeno l'autore o il mittente. In particolare, per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Verifica modifica documento"
- **Tipo soggetto:** consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche
- **Nominativo:** valorizzato a seconda del tipo soggetto.
- **Codice:** valorizzato a seconda del tipo soggetto.
- **UOR:** Unità Organizzativa di riferimento. Non obbligatorio Il metadato ha una struttura ricorsiva.

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Allegati</b>						
	Numero allegati		0:n	Number	SI	SI
	Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
		IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
		Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI

#### Definizione

Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:

- **IdDoc:** Identificativo del documento relativo all'allegato
- **Descrizione:** Titolo dell'Allegato

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Classificazione</b>		<i>sia nel caso di documento protocollato che nel caso di documento non protocollato</i>			
	Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	NO	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	NO	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	NO	SI
<b>Definizione</b>					
<p><i>Classificazione del documento secondo il Piano di classificazione utilizzato:</i></p> <ul style="list-style-type: none"> <li>• <i>Indice di classificazione:</i> Codifica del documento secondo il Piano di classificazione utilizzato</li> <li>• <i>Descrizione:</i> Descrizione per esteso dell'Indice di classificazione indicato.</li> <li>• <i>Piano di classificazione:</i> se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione</li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Riservato</b>		<ul style="list-style-type: none"> <li>• Vero: se il documento è considerato riservato</li> <li>• Falso: se il documento non è considerato riservato</li> </ul>	Boolean	SI	SI
<b>Definizione</b>					
<p><i>Rappresenta il livello di sicurezza di accesso al documento:</i></p> <ul style="list-style-type: none"> <li>• <i>Vero:</i> se il documento è considerato riservato</li> <li>• <i>Falso:</i> se il documento non è considerato riservato.</li> </ul> <p><i>Consente di gestire gli accessi al documento al solo personale autorizzato.</i></p>					

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Identificativo del formato</b>						
	Formato		Previsti dall'Allegato 2 delle Linee Guida	Alfanumerico	SI	SI
	Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione	Alfanumerico	SI, quando rilevabile	SI
		Nome prodotto		Alfanumerico		SI
		Versione prodotto		Alfanumerico		SI
		Produttore		Alfanumerico		SI
<b>Definizione</b>						
<p>Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. È costituito dai seguenti sottocampi:</p> <ul style="list-style-type: none"> <li>• <i>Formato:</i> secondo quanto previsto dall'Allegato 2 delle Linee Guida.</li> <li>• <i>Prodotto software:</i> Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi: <ul style="list-style-type: none"> <li>○ <i>Nome prodotto</i></li> <li>○ <i>Versione prodotto</i></li> <li>○ <i>Produttore</i></li> </ul> </li> </ul>						

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
--------------	------------	----------------	-----------	----------------	-------------------

<b>Verifica</b>					
	Firmato Digitalmente	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Sigillato Elettronicamente	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Marcatura Temporale	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Conformità copie immagine su supporto informatico	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = b	SI
<b>Definizione</b>					
<i>Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>IdAgg</b>		Identificativo del fascicolo o della serie <i>come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.</i>	Alfanumerico	NO	SI

**Definizione**

*Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE. Metadato ricorsivo.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>IdIdentificativoDocumentoPrincipale</b>		IdDoc del documento principale		SI, nel caso in cui sia presente un documento principale	SI

**Definizione**

*Identificativo univoco e persistente del Documento principale*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Versione del documento</b>		1,2,3....	Alfanumerico	SI	SI

**Definizione**

*Versione del documento.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tracciate modifiche documento</b>					
	Tipo modifica	<ul style="list-style-type: none"> <li>• Annullamento</li> <li>• Rettifica</li> <li>• Integrazione</li> <li>• Annotazione</li> </ul>	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Codice fiscale dell'autore della modifica	Codice fiscale del soggetto definito con ruolo Operatore nel metadato "Soggetti"	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Data Modifica		Datetime	Si, nel caso di versione > 1 o in caso di annullamento	SI
	IdDoc versione precedente	Identificativo documento versione precedente		Si, nel caso di versione > 1 o in caso di annullamento	SI

#### Definizione

*Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore"*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tempo di conservazione</b>		<ul style="list-style-type: none"> <li>• 9999</li> <li>• 5 anni</li> <li>• 10 anni</li> <li>• .....</li> </ul>	Numerico	NO	SI

---

**Definizione**

*Tempo di conservazione del documento desunto dal Piano di conservazione integrato con il Piano di classificazione (ove presenti) o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Note</b>		Testo Libero	Alfanumerico	NO	SI
<b>Definizione</b>					
<i>Eventuali indicazioni aggiuntive</i>					

## 2.1 XSD METADATI DEL DOCUMENTO INFORMATICO

### Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="DocumentoInformatico">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="IdDoc">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="Impronta" Type="xs:base64Binary" />
              <xs:element name="Algoritmo" Type="xs:string" default="SHA-256"/>
              <xs:element name="Identificativo" Type="xs:string" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="ModalitaDiFormazione">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="creazione tramite utilizzo di strumenti software che assicurino la
produzione di documenti nei formati previsti in allegato 2"/>
              <xs:enumeration value="acquisizione di un documento informatico per via telematica o su
supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico"/>
              <xs:enumeration value="memorizzazione su supporto informatico in formato digitale delle
informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili ad utente"/>
              <xs:enumeration value="generazione o raggruppamento anche in via automatica di un insieme di
dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma
statica"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
        <xs:element name="TipologiaDocumentale" Type="xs:string" />
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

Emergenza"/>

```
<xs:element name="DatiDiRegistrazione">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="TipologiaDiFlusso">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="In entrata"/>
            <xs:enumeration value="In uscita"/>
            <xs:enumeration value="Interno"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="TipoRegistro">
        <xs:simpleType>
          <xs:restriction base="xs:string">
            <xs:enumeration value="Nessuno"/>
            <xs:enumeration value="Protocollo Ordinario/Protocollo
              Emergenza"/>
            <xs:enumeration value="Repertorio/Registro"/>
          </xs:restriction>
        </xs:simpleType>
      </xs:element>
      <xs:element name="DataRegistrazione" Type="xs:date" />
      <xs:element name="NumeroDocumento" Type="xs:string" />
      <xs:element name="IdRegistro" Type="xs:string" minOccurs="0" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="ChiaveDescrittiva">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Oggetto" Type="xs:string" />
      <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0" maxOccurs="5" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded" >
  <xs:complexType>
    <xs:sequence>
```

```

        <xs:element name="Ruolo">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="Autore"/>
                    <xs:enumeration value="Mittente"/>
                    <xs:enumeration value="Destinatario"/>
                    <xs:enumeration value="Assegnatario"/>
                    <xs:enumeration value="Operatore"/>
                    <xs:enumeration value="Altro"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="TipoSoggetto">
            <xs:simpleType>
                <xs:restriction base="xs:string">
                    <xs:enumeration value="PF"/>
                    <xs:enumeration value="PG"/>
                    <xs:enumeration value="PA"/>
                </xs:restriction>
            </xs:simpleType>
        </xs:element>
        <xs:element name="Nominativo" Type="xs:string" />
        <xs:element name="Codice" Type="xs:string" />
        <xs:element name="UOR" Type="xs:string" minOccurs="0" />
    </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Allegati">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="NumeroAllegati" >
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:minInclusive value="0"/>
                        <xs:maxInclusive value="999"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="IndiceAllegati" minOccurs="0" maxOccurs="unbounded">

```

```

name="Impronta" Type="xs:base64Binary" />
name="Algoritmo" Type="xs:string" default="SHA-256"/>
name="Identificativo" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Descrizione" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Classificazione" minOccurs="0">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="IndiceDiClassificazione" Type="xs:string" />
      <xs:element name="Descrizione" Type="xs:string" />
      <xs:element name="PianoDiClassificazione" Type="xs:string" minOccurs="0" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Riservato" Type="xs:boolean" />
<xs:element name="IdentificativoDelFormato">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Formato" Type="xs:string" />
      <xs:element name="ProdottoSoftware" minOccurs="0">
        <xs:complexType>
          <xs:sequence>

```

```

minOccurs="0" />
minOccurs="0" />
minOccurs="0" />
<xs:element name="NomeProdotto" Type="xs:string"
<xs:element name="VersioneProdotto" Type="xs:string"
<xs:element name="Produttore" Type="xs:string"
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Verifica" minOccurs="0">
<xs:complexType>
<xs:sequence>
<xs:element name="FirmatoDigitalmente" Type="xs:boolean" />
<xs:element name="SigillatoElettronicamente" Type="xs:boolean" />
<xs:element name="MarcaturaTemporale" Type="xs:boolean" />
<xs:element name="ConformitaCopieImmagineSuSupportoInformatico" Type="xs:boolean" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="IdAgg" minOccurs="0" maxOccurs="unbounded">
<xs:complexType>
<xs:sequence>
<xs:element name="TipoAggregazione">
<xs:simpleType>
<xs:restriction base="xs:string">
<xs:enumeration value="Fascicolo"/>
<xs:enumeration value="Serie Documentale"/>
<xs:enumeration value="Serie Di Fascicoli"/>
</xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="IdAggregazione" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="IdIdentificativoDocumentoPrincipale" minOccurs="0">

```

```

        <xs:complexType>
            <xs:sequence>
                <xs:element name="Impronta" Type="xs:base64Binary" />
                <xs:element name="Algoritmo" Type="xs:string" default="SHA-256"/>
                <xs:element name="Identificativo" Type="xs:string" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="VersioneDelDocumento" Type="xs:string" />
    <xs:element name="TracciatoreModificheDocumento" minOccurs="0" >
        <xs:complexType>
            <xs:sequence>
                <xs:element name="TipoModifica">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="Annullamento"/>
                            <xs:enumeration value="Rettifica"/>
                            <xs:enumeration value="Integrazione"/>
                            <xs:enumeration value="Annotazione"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="CodiceFiscaleAutoreDellaModifica">
                    <xs:simpleType>
                        <xs:restriction base="xs:string" >
                            <xs:pattern value="[A-Z]{6}[0-9LMNPQRSTUV]{2}[ABCDEHLMRST][0-9LMNPQRSTUV]{2}[A-Z][0-9LMNPQRSTUV]{3}[A-Z]" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="DataModifica" Type="xs:dateTime" />
                <xs:element name="IdDocVersionePrecedente">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Impronta" Type="xs:base64Binary" />
                            <xs:element name="Algoritmo" Type="xs:string"
                                default="SHA-256"/>
                            <xs:element name="Identificativo" Type="xs:string" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

```

```

</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="TempoDiConservazione" minOccurs="0">
  <xs:simpleType>
    <xs:restriction base="xs:integer">
      <xs:minInclusive value="1"/>
      <xs:maxInclusive value="9999"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="Note" type="xs:string" minOccurs="0" />
</xs:sequence>
</xs:complexType>
</xs:element>
</xs:schema>
```

### 3. METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>IdDoc</b>						
	Impronta crittografica del documento					
		Impronta	Rappresenta l'hash del documento	Binary	SI	NO, ridefinito.
		Algoritmo	Rappresenta l'algoritmo applicato Default = SHA-256	Alfanumerico	SI	SI
	Segnatura		Segnatura del protocollo	Alfanumerico	SI, nel caso di documento protocollato	
	Identificativo		Come da sistema di identificazione formalmente definito	Alfanumerico	SI	
<b>Definizione</b>						

*Identificativo univoco e persistente associato in modo univoco e permanente al documento amministrativo informatico in modo da consentirne l'identificazione.*

*Inoltre, rappresenta le informazioni necessarie per verificare l'integrità del documento. Il metadato è costituito dai sottocampi:*

- *Impronta crittografica del documento: a sua volta suddiviso in:*
  - *Impronta: sottocampo in cui viene memorizzato l'hash del documento*
  - *Algoritmo: sottocampo nel quale deve essere indicata la tipologia dell'algoritmo applicato secondo quanto riportato nell'Allegato 6 delle Linee Guida nella tabella 1 del paragrafo 2.2 "Regole di processamento"*
- *Segnatura: segnatura di protocollo, da indicare obbligatoriamente nel caso di documento amministrativo protocollato, a sua volta strutturato come da Allegato 6 delle Linee Guida*
- *Identificativo: come da sistema di identificazione formalmente definito*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Modalità di formazione		Indicare <ul style="list-style-type: none"> <li>• <i>creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee;</i></li> <li>• <i>acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione</i></li> </ul>	Alfanumerico	SI	SI

		<p>della copia informatica di un documento analogico;</p> <ul style="list-style-type: none"> <li>• memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;</li> <li>• generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica</li> </ul>			
<b>Definizione</b>					

Indica la modalità di generazione del documento informatico.

Sono previste le seguenti modalità, secondo quanto riportato nelle Linee guida:

- a) creazione tramite l'utilizzo di strumenti software che assicurino la produzione di documenti nei formati previsti nell'Allegato 2 delle Linee Guida;
- b) acquisizione di un documento informatico per via telematica o su supporto informatico, acquisizione della copia per immagine su supporto informatico di un documento analogico, acquisizione della copia informatica di un documento analogico;
- c) memorizzazione su supporto informatico in formato digitale delle informazioni risultanti da transazioni o processi informatici o dalla presentazione telematica di dati attraverso moduli o formulari resi disponibili all'utente;
- d) generazione o raggruppamento anche in via automatica di un insieme di dati o registrazioni, provenienti da una o più banche dati, anche appartenenti a più soggetti interoperanti, secondo una struttura logica predeterminata e memorizzata in forma statica

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tipologia documentale</b>		<ul style="list-style-type: none"> <li>• Fatture</li> <li>• Determine</li> <li>• Delibere</li> <li>...</li> </ul>	Alfanumerico	SI	SI
<b>Definizione</b>					
<i>Metadato funzionale che indica la tipologia del documento tra quelle trattate per lo svolgimento delle attività.</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Dati di registrazione</b>					

	Tipologia di flusso	<ul style="list-style-type: none"> <li>• In uscita</li> <li>• In entrata</li> <li>• Interno</li> </ul> <p>Per documenti interni si intende i documenti scambiati all'interno della medesima AOO</p>	Alfanumerico	SI	SI
	Tipo registro	<ul style="list-style-type: none"> <li>• Protocollo Ordinario/ Protocollo Emergenza,</li> <li>• Repertorio/Registro</li> </ul>	Alfanumerico	SI	SI
	Data registrazione	<p>nel caso di documento non protocollato:</p> <ul style="list-style-type: none"> <li>• Data di registrazione del documento</li> </ul> <p>nel caso di documento protocollato:</p> <ul style="list-style-type: none"> <li>• Data di registrazione di protocollo.</li> </ul>	Datetime	SI	NO, ma ridefinito

	Numero Documento		<p>nel caso di documento non protocollato:</p> <ul style="list-style-type: none"> <li>• Numero di registrazione del documento</li> </ul> <p>nel caso di documento protocollato:</p> <ul style="list-style-type: none"> <li>• Numero di protocollo</li> </ul>	Alfanumerico	SI	NO, ma ridefinito
	IdRegistro		Codice identificativo del registro in cui il documento viene registrato.	Alfanumerico	SI	SI
	Amministrazione che effettua la registrazione					
		Codice IPA Amministrazione		Alfanumerico	SI	NO, ma ridefinito
		Codice IPA AOO		Alfanumerico	SI	NO, ma ridefinito
<b>Definizione</b>						

Metadato che comprende i dati di registrazione del documento sia nel caso di documento protocollato che non protocollato.

Sono previsti i seguenti sottocampi:

- **Tipologia di flusso:** indica se si tratta di un documento in uscita, in entrata o interno. Per documento interno si intende un documento scambiato tra le diverse UOR afferenti alla stessa AOO
- **Tipo registro:** indica il sistema di registrazione adottato: protocollo ordinario/ protocollo emergenza, o Repertorio/Registro.
- **Data:** è la data associata al documento all'atto della registrazione
- **Numero documento:** Numero identificativo del documento nel caso di documento non protocollato (ad esempio, numero fattura), numero di protocollo nel caso di documento protocollato.
- **IdRegistro:** Identificativo del registro in cui il documento viene registrato.
- **Amministrazione che effettua la registrazione:** codice IPA dell'Amministrazione e dell'AOO che sta effettuando la registrazione

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Chiave descrittiva</b>					
	Oggetto	Testo libero	Alfanumerico	SI	SI
	Parole chiave	Testo libero	Alfanumerico	NO	SI

#### Definizione

Metadato funzionale volto a riassumere il contenuto del documento o comunque a chiarirne la natura. È costituito da seguenti sottocampi:

- **Oggetto:** testo libero;
- **Parole Chiave:** da compilare facoltativamente attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca del documento. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
--------------	------------	----------------	-----------	----------------	-------------------

Soggetti					
	Ruolo	<ul style="list-style-type: none"> <li>• Autore</li> <li>• Mittente</li> <li>• Destinatario</li> <li>• Assegnatario</li> <li>• Operatore</li> <li>• RUP</li> </ul>	Alfanumerico	SI, e nel caso di documento protocollato è obbligatorio indicare almeno il Mittente e il Destinatario	SI
	Tipo soggetto	<ul style="list-style-type: none"> <li>• PF per Persona Fisica</li> <li>• PG per Organizzazione</li> <li>• PA per le Amministrazioni Pubbliche</li> </ul>	Alfanumerico	SI	SI
	Nominativo	<p>Nominativo:</p> <p>se Tipo soggetto = PF:            ✓ cognome e nome;</p> <p>se Tipo soggetto = PG:            ✓ denominazione</p> <p>se Tipo soggetto = PA:            ✓ denominazione Amministrazione \              denominazioneAOO;</p>	Alfanumerico	SI	SI

	Codice	<p>Codice identificativo:  se Tipo soggetto = PF:  ✓ codice fiscale</p> <p>se Tipo soggetto = PG:  ✓ codice fiscale</p> <p>se Tipo soggetto = PA:  ✓ Codice IPA dell'Amministrazione \  Codice AOO</p>	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	Obbligatorio nel caso si stia indicando Ruolo = RUP	SI
	Indirizzi digitali di riferimento	Posta elettronica certificata – domicilio digitale	Alfanumerico	SI	SI
<b>Definizione</b>					

Indica il metadato che consente di individuare le informazioni relative a tutti i soggetti coinvolti e competenti sul documento a vario titolo e definiti dal campo Ruolo.

Sono definiti quindi i seguenti attributi:

- **Ruolo:** consente di indicare, a seconda delle necessità, il l'autore del documento, il mittente, il destinatario e assegnatario. In particolare, per "Operatore" si intende il soggetto autorizzato ad apportare modifiche/integrazioni al documento, la cui definizione si renderà obbligatoria nel caso in cui venga compilato il metadato "Verifica modifica documento"
- **Tipo soggetto:** consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche o responsabile unico del procedimento.
- **Nominativo:** valorizzato a seconda del tipo soggetto
- **Codice:** valorizzato a seconda del tipo soggetto.
- **UOR:** Unità Organizzativa di riferimento. Obbligatorio nel caso si stia indicando il RUP
- **Indirizzi digitali di riferimento:** valorizzato con il recapito associato al soggetto. Il metadato ha una struttura ricorsiva.

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Allegati</b>						
	Numero allegati		0:n	Numerico	SI	SI
	Indice allegati		Da indicare per ogni allegato se Numero allegati > 0			
		IdDoc	Identificativo del documento relativo all'allegato		SI, se numero allegati > 0	SI
		Descrizione	Testo libero	Alfanumerico	SI, se numero allegati > 0	SI
<b>Definizione</b>						
Indica il numero di allegati al documento e, nell'eventualità che il numero di allegati indicati sia maggiore di zero, devono essere compilati, in modalità ricorsiva, i dati:						
<ul style="list-style-type: none"> <li>• <b>IdDoc:</b> Identificativo del documento relativo all'allegato</li> <li>• <b>Descrizione:</b> Titolo dell'allegato</li> </ul>						

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Classificazione</b>		<i>sia nel caso di documento protocollato che nel caso di documento non protocollato</i>			
	Indice di classificazione	Codifica del documento secondo il Piano di classificazione utilizzato	Alfanumerico	SI	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	SI	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	SI	SI
<b>Definizione</b>					
<p><i>Classificazione del documento secondo il Titolare utilizzato:</i></p> <ul style="list-style-type: none"> <li>• <i>Indice di classificazione: Codifica del documento secondo il Piano di classificazione utilizzato</i></li> <li>• <i>Descrizione: Descrizione per esteso dell'Indice di classificazione indicato.</i></li> <li>• <i>Piano di classificazione: riportare l'URI di pubblicazione del Piano di classificazione</i></li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Riservato</b>		<ul style="list-style-type: none"> <li>• Vero: se il documento è considerato riservato</li> <li>• Falso: se il documento non è considerato riservato</li> </ul>	Boolean	SI	SI
<b>Definizione</b>					
<p><i>Rappresenta il livello di sicurezza di accesso al documento:</i></p> <ul style="list-style-type: none"> <li>• <i>Vero: se il documento è considerato riservato</i></li> <li>• <i>Falso: se il documento non è considerato riservato</i></li> </ul> <p><i>Consente di gestire gli accessi al documento al solo personale autorizzato.</i></p>					

Informazione	Sottocampi		Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Identificativo del formato</b>						
	Formato		Previsti dall'Allegato 2 delle Linee guida	Alfanumerico	SI	SI
	Prodotto software		Prodotto software utilizzato per la creazione del documento e relativa versione	Alfanumerico	SI, quando rilevabile	SI
		Nome prodotto		Alfanumerico		SI
		Versione prodotto		Alfanumerico		SI
		Produttore		Alfanumerico		SI
<b>Definizione</b>						
<p>Indica il formato del documento e la versione del software utilizzato per la creazione del documento stesso. È costituito dai seguenti sottocampi:</p> <ul style="list-style-type: none"> <li>• <i>Formato:</i> secondo quanto previsto dall'Allegato 2 delle Linee Guida.</li> <li>• <i>Prodotto software:</i> Prodotto software utilizzato per la creazione del documento e relativa versione, suddiviso a sua volta in tre sottocampi: <ul style="list-style-type: none"> <li>○ <i>Nome prodotto</i></li> <li>○ <i>Versione prodotto</i></li> <li>○ <i>Produttore</i></li> </ul> </li> </ul>						

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Verifica</b>					

	Firmato Digitalmente	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Sigillato Elettronicamente	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Marcatura Temporale	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = a/b	SI
	Conformità copie immagine su supporto informatico	<ul style="list-style-type: none"> <li>• Vero</li> <li>• Falso</li> </ul>	Boolean	SI, obbligatorio nel caso di modalità di formazione doc = b	SI

#### Definizione

*Check di controllo presenza Firma elettronica, Sigillo, Marcatura temporale e Conformità copie immagine nelle modalità di formazione del documento informatico previste nelle Linee Guida.*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
--------------	------------	----------------	-----------	----------------	-------------------

<b>IdAgg</b>		Identificativo del fascicolo o della serie <i>come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE.</i>	Alfanumerico	SI	SI
<b>Definizione</b>					
<i>Identificativo univoco dell'Aggregazione come definito nel successivo paragrafo dei METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE. Metadato ricorsivo.</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>IdIdentificativoDocumentoPrincipale</b>		IdDoc del documento principale		SI, nel caso in cui sia presente un documento principale	SI
<b>Definizione</b>					
<i>Identificativo univoco e persistente del Documento principale</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Versione del documento</b>		1,2,3....	Alfanumerico	SI	SI
<b>Definizione</b>					
<i>Versione del documento</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tracciature modifiche documento</b>					
	Tipo modifica	<ul style="list-style-type: none"> <li>• Annullamento</li> <li>• Rettifica</li> <li>• Integrazione</li> <li>• Annotazione</li> </ul>	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Codice fiscale dell'autore della modifica	Codice fiscale del soggetto definito con ruolo Operatore nel metadato "Soggetti"	Alfanumerico	Si, nel caso di versione > 1 o in caso di annullamento	SI
	Data modifica		Datetime	Si, nel caso di versione > 1 o in caso di annullamento	SI
	IdDoc versione precedente	Identificativo documento versione precedente		Si, nel caso di versione > 1 o in caso di annullamento	SI

#### Definizione

*Metadato volto a tracciare la presenza di operazioni di modifica effettuate sul documento e la data in cui esse sono state effettuate. L'autore delle modifiche è tracciato nel metadato "Soggetti" con il ruolo "Operatore"*

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tempo di conservazione</b>		<ul style="list-style-type: none"> <li>• 9999</li> <li>• 5 anni</li> <li>• 10 anni</li> <li>• .....</li> </ul>	Numerico	NO	SI

### Definizione

Tempo di conservazione del documento desunto dal Piano di conservazione formalmente integrato al Piano di classificazione o prescritto dalla normativa salvo contenzioso. In generale il tempo di conservazione a livello di singolo documento deve essere indicato solo qualora esso presenti un tempo di conservazione distinto da quello assegnato all'aggregazione documentale informatica a cui il documento stesso appartiene. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
Note		Testo Libero	Alfanumerico	NO	SI
<b>Definizione</b>					
Eventuali indicazioni aggiuntive utili ad indicare situazioni particolari.					

## 3.1 XSD METADATI DEL DOCUMENTO AMMINISTRATIVO INFORMATICO

### Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">
  <xs:element name="DocumentoAmministrativoInformativo">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="IdDoc">
          <xs:complexType>
            <xs:sequence>
              <xs:element name="ImprontaCrittograficaDelDocumento">
                <xs:complexType>
```



```

</xs:element>
<xs:element name="TipoRegistro">
  <xs:simpleType>
    <xs:restriction base="xs:string">
      <xs:enumeration value="Protocollo Ordinario/Protocollo
Emergenza"/>
      <xs:enumeration value="Repertorio/Registro"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="DataRegistrazione" Type="xs:date" />
<xs:element name="NumeroDocumento" Type="xs:string" />
<xs:element name="IdRegistro" Type="xs:string" />
<xs:element name="AmministrazioneCheEffettuaRegistrazione">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="CodiceIPAAmmministrazione"
Type="xs:string" />
      <xs:element name="CodiceIPAAOO" Type="xs:string" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="ChiaveDescrittiva">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Oggetto" Type="xs:string" />
      <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0" maxOccurs="5" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded" >
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Ruolo">
        <xs:simpleType>
          <xs:restriction base="xs:string">

```

```

        <xs:enumeration value="Autore"/>
        <xs:enumeration value="Mittente"/>
        <xs:enumeration value="Destinatario"/>
        <xs:enumeration value="Assegnatario"/>
        <xs:enumeration value="Operatore"/>
        <xs:enumeration value="RUP"/>
    </xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="TipoSoggetto">
    <xs:simpleType>
        <xs:restriction base="xs:string">
            <xs:enumeration value="PF"/>
            <xs:enumeration value="PG"/>
            <xs:enumeration value="PA"/>
        </xs:restriction>
    </xs:simpleType>
</xs:element>
<xs:element name="Nominativo" Type="xs:string" />
<xs:element name="Codice" Type="xs:string" />
<xs:element name="UOR" Type="xs:string" minOccurs="0" />
<xs:element name="IndirizziDigitaliDiRiferimento" Type="xs:string" minOccurs="1"
maxOccurs="unbounded"/>
    </xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="Allegati">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="NumeroAllegati">
                <xs:simpleType>
                    <xs:restriction base="xs:integer">
                        <xs:minInclusive value="0"/>
                        <xs:maxInclusive value="999"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
            <xs:element name="IndiceAllegati" minOccurs="0" maxOccurs="unbounded">
                <xs:complexType>

```



```

        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Riservato" Type="xs:boolean" />
<xs:element name="IdentificativoDelFormato">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Formato" Type="xs:string" />
            <xs:element name="ProdottoSoftware" minOccurs="0">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="NomeProdotto" Type="xs:string"
minOccurs="0" />
                        <xs:element name="VersioneProdotto" Type="xs:string"
minOccurs="0" />
                        <xs:element name="Produttore" Type="xs:string"
minOccurs="0" />
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="Verifica" minOccurs="0">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="FirmatoDigitalmente" Type="xs:boolean" />
            <xs:element name="SigillatoElettronicamente" Type="xs:boolean" />
            <xs:element name="MarcaturaTemporale" Type="xs:boolean" />
            <xs:element name="ConformitaCopieImmagineSuSupportoInformatico" Type="xs:boolean" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="IdAgg" minOccurs="1" maxOccurs="unbounded">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="TipoAggregazione">
                <xs:simpleType>
                    <xs:restriction base="xs:string">

```

```

        <xs:enumeration value="Fascicolo"/>
        <xs:enumeration value="Serie Documentale"/>
        <xs:enumeration value="Serie Di Fascicoli"/>
    </xs:restriction>
</xs:simpleType>
</xs:element>
<xs:element name="IdAggregazione" Type="xs:string" />
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="IdIdentificativoDocumentoPrincipale" minOccurs="0">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="ImprontaCrittograficaDelDocumento">
                <xs:complexType>
                    <xs:sequence>
                        <xs:element name="Impronta" Type="xs:base64Binary" />
                        <xs:element name="Algoritmo" Type="xs:string"
                            default="SHA-256"/>
                    </xs:sequence>
                </xs:complexType>
            </xs:element>
            <xs:element name="Segnatura" Type="xs:string" minOccurs="0" />
            <xs:element name="Identificativo" Type="xs:string" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="VersioneDelDocumento" Type="xs:string"/>
<xs:element name="TracciatureModificheDocumento" minOccurs="0" >
    <xs:complexType>
        <xs:sequence>
            <xs:element name="TipoModifica">
                <xs:simpleType>
                    <xs:restriction base="xs:string">
                        <xs:enumeration value="Annullamento"/>
                        <xs:enumeration value="Rettifica"/>
                        <xs:enumeration value="Integrazione"/>
                        <xs:enumeration value="Annotazione"/>
                    </xs:restriction>
                </xs:simpleType>
            </xs:element>
        </xs:sequence>
    </xs:complexType>
</xs:element>

```



---

```
                </xs:simpleType>
            </xs:element>
            <xs:element name="Note" Type="xs:string" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
</xs:schema>
```

## 4. METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
IdAgg					
	TipoAggregazione	Indicare: <ul style="list-style-type: none"> <li>• Fascicolo</li> <li>• Serie Documentale</li> <li>• Serie di fascicoli</li> </ul>	Alfanumerico	SI	SI
	IdAggregazione	Come da sistema di identificazione formalmente definito.	Alfanumerico	SI	NO, ma ridefinito
<b>Definizione</b>					
<p><i>L'idAgg è una sequenza di caratteri alfanumerici associata in modo univoco all'aggregazione documentale informatica in modo da consentirne l'identificazione, indica se si tratta di un Fascicolo o di una Serie Documentale o di una serie fascicoli.</i></p> <p><i>Il fascicolo è una aggregazione documentale informatica strutturata e univocamente identificata contenente atti, documenti o dati informatici prodotti e funzionali all'esercizio di una attività o allo svolgimento di uno specifico procedimento.</i></p> <p><i>Le serie documentarie sono costituite da documenti singoli accorpati per ragioni funzionali in base alla tipologia di riferimento.</i></p> <p><i>Le serie di fascicoli sono costituite da fascicoli accorpati per ragioni funzionali in base alla classe di riferimento o alla tipologia di fascicoli.</i></p>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
--------------	------------	----------------	-----------	----------------	-------------------

<b>Tipologia fascicolo</b>		Solo in caso di TipoAggregazione = 'Fascicolo' Tipologia del fascicolo: <ul style="list-style-type: none"> <li>• affare</li> <li>• attività</li> <li>• persona fisica</li> <li>• persona giuridica</li> <li>• procedimento amministrativo</li> </ul>	Alfanumerico	SI, solo in caso di TipoAggregazione = 'Fascicolo'	SI
----------------------------	--	---	--------------	--	----

**Definizione**

*I fascicoli sono organizzati per tipo:*

- *Tipo 1 - fascicolo per affare:* conserva i documenti relativi a una competenza non proceduralizzata, ma che nella consuetudine amministrativa la PA deve concretamente portare a buon fine. Il fascicolo per affare ha una data di apertura e una durata circoscritta.
- *Tipo 2 - fascicolo per persona fisica o giuridica:* comprende tutti i documenti, anche con classifiche diverse, che si riferiscono a una persona (fisica o giuridica). Quasi sempre i fascicoli intestati alle persone restano correnti per molti anni, costituendo serie aperte.
- *Tipo 3 - fascicolo per attività:* comprende i documenti prodotti nello svolgimento di un'attività amministrativa semplice che implica risposte obbligate o meri adempimenti, per la quale quindi non è prevista l'adozione di un provvedimento finale. Ha in genere durata annuale.
- *Tipo 4 - fascicolo per procedimento amministrativo:* conserva una pluralità di documenti che rappresentano azioni amministrative omogenee e destinate a concludersi con un provvedimento amministrativo.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Soggetti</b>					
	Ruolo	<ul style="list-style-type: none"> <li>• Amministrazione titolare</li> <li>• Amministrazioni partecipanti</li> <li>• Soggetto intestatario persona fisica</li> <li>• Soggetto intestatario persona giuridica</li> <li>• RUP (Solo in caso di</li> <li>• TipoAggregazione = 'Fascicolo')</li> </ul>	Alfanumerico	SI	SI

	Tipo soggetto	<ul style="list-style-type: none"> <li>• PF per Persona Fisica</li> <li>• PG per Organizzazione</li> <li>• PA per le Amministrazioni Pubbliche</li> </ul>	Alfanumerico	SI	SI
	Nominativo	<p>Nominativo:  se Tipo Soggetto = PF:  ✓ cognome e nome;</p> <p>se Tipo Soggetto = PG:  ✓ denominazione</p> <p>se Tipo Soggetto = PA:  ✓ denominazione Amministrazione \  denominazione AOO;</p>	Alfanumerico	SI	SI
	Codice	<p>Codice identificativo:  se Tipo Soggetto = PF  ✓ codice fiscale</p> <p>se Tipo Soggetto = PG:  ✓ codice fiscale</p> <p>se Tipo Soggetto = PA:  ✓ Codice IPA dell'Amministrazione \  Codice AOO</p>	Alfanumerico	SI	SI
	UOR	Unità Organizzativa di riferimento	Alfanumerico	Obbligatorio nel caso si stia indicando Ruolo = RUP	SI

## Definizione

Indica il metadato che consente di individuare le informazioni relative a tutti i Soggetti che, a vario titolo, sono coinvolti nella costituzione dell'aggregazione. Sono definiti quindi i seguenti attributi:

- **Ruolo:**
  - Amministrazione titolare
  - Amministrazioni partecipanti
  - Soggetto intestatario persona fisica
  - Soggetto intestatario persona giuridica
  - RUP (Solo in caso di TipoAggregazione = 'Fascicolo')
- **Tipo soggetto:** consente di tipizzare i soggetti come persone fisiche, giuridiche, amministrazioni pubbliche
- **Nominativo:** valorizzato a seconda del tipo soggetto.
- **Codice:** valorizzato a seconda del tipo soggetto.
- **UOR:** Nel caso in cui sia stato definito un Ruolo=RUP è obbligatorio indicare anche l'UOR corrispondente.

Il metadato ha una struttura ricorsiva

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Assegnazione</b>					
	Tipo assegnazione	<ul style="list-style-type: none"><li>• Per competenza</li><li>• Per conoscenza</li></ul>	Alfanumerico	SI, in caso di fascicolo	SI
	Ruolo	Definito come da <i>Ruolo</i> del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Tipo soggetto	Definito come da <i>Tipo soggetto</i> del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Codice	Definito come da <i>Codice</i> del metadato Soggetti.	Alfanumerico	SI, in caso di fascicolo	SI
	Data inizio assegnazione	Data inizio assegnazione	Datetime	SI, in caso di fascicolo	SI

	Data fine assegnazione	Data fine assegnazione	Datetime	NO	SI
<b>Definizione</b>					
<p>Indica il metadato che consente di individuare le informazioni relative all'assegnazione per conoscenza o per competenza. I Soggetti indicati in questo metadato devono essere stati dichiarati nel metadato Soggetti. Sono definiti quindi i seguenti attributi:</p> <ul style="list-style-type: none"> <li>• Tipo assegnazione</li> <li>• Ruolo</li> <li>• Tipo soggetto</li> <li>• Codice</li> <li>• Data inizio assegnazione</li> <li>• Data fine assegnazione</li> </ul> <p>Il metadato ha una struttura ricorsiva.</p>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
DataApertura		Data	Date	SI	SI
<b>Definizione</b>					
Data di apertura dell'aggregazione documentale.					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
--------------	------------	----------------	-----------	----------------	-------------------

Classificazione					
	Indice di classificazione	Codifica secondo il Piano di classificazione utilizzato	Alfanumerico	SI	SI
	Descrizione	Descrizione per esteso dell'Indice di classificazione indicato.	Alfanumerico	SI	SI
	Piano di classificazione	URI del Piano di classificazione pubblicato	Alfanumerico	SI	SI
Definizione					
<p><i>Classificazione dell'aggregazione:</i></p> <ul style="list-style-type: none"> <li>• <i>Indice di classificazione:</i> Codifica del documento secondo il Piano di classificazione utilizzato</li> <li>• <i>Descrizione:</i> Descrizione per esteso dell'Indice di classificazione indicato.</li> <li>• <i>Piano di classificazione:</i> se presente, riportare eventualmente l'URI di pubblicazione del Piano di classificazione</li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>Progressivo</b>			Numerico	SI	SI
Definizione					
<i>Progressivo numerico calcolato nell'ambito della chiave della classificazione o in ordine cronologico nell'ambito dell'anno</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
--------------	------------	----------------	-----------	----------------	-------------------

<b>Chiave descrittiva</b>					
	Oggetto	Testo libero	Alfanumerico	SI	SI
	Parole chiave	Testo libero	Alfanumerico	NO	SI
<b>Definizione</b>					
<p><i>Metadato funzionale volto a chiarirne la natura del fascicolo o della serie. È costituito da seguenti sottocampi:</i></p> <ul style="list-style-type: none"> <li>• <i>Oggetto: testo libero;</i></li> <li>• <i>Parole Chiave: da compilare facoltativamente con l'ausilio di attingendo da thesauri o da vocabolari controllati, per evitare ambiguità terminologiche e avere la possibilità di utilizzare il metadato come chiave di ricerca. Il metadato è ricorsivo fino ad un massimo di 5 occorrenze.</i></li> </ul>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>DataChiusura</b>		Data	Date	SI, quando l'aggregazione viene chiusa	SI
<b>Definizione</b>					
<i>Data di chiusura dell'aggregazione documentale.</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Procedimento Amministrativo</b>					

	Materia\Argomento\Struttura		Indicare la materia o l'argomento o la struttura per la quale sono stati catalogati i procedimenti amministrativi	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
	Procedimento		Denominazione del Procedimento	Alfanumerico	SI, nel caso Tipologia fascicolo = procedimento amministrativo.	SI
	Catalogo procedimenti		Uri di pubblicazione del catalogo	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
	Fasi		A sua volta suddiviso, in una struttura ricorsiva:		SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Tipo Fase	<ul style="list-style-type: none"> <li>• Preparatoria</li> <li>• Istruttoria</li> <li>• Consultiva</li> <li>• Decisoria o deliberativa</li> <li>• Integrazione dell'efficacia</li> </ul>	Alfanumerico	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Data inizio fase		Date	SI, nel caso di Tipologia fascicolo = procedimento amministrativo.	SI
		Data fine fase		Date	NO	SI

**Definizione**

Metadato funzionale volto ad indicare il procedimento a cui il fascicolo afferisce, nonché lo stato di avanzamento e le relative fasi.

Il sottocampo "Fase", a sua volta costituito da "Tipo Fase":

- Preparatoria
- Istruttoria
- Consultiva
- Decisoria o deliberativa
- Integrazione dell'efficacia

"Data inizio fase" e "Data fine fase" deve considerarsi dinamico, destinato ad essere aggiornato con lo stato di avanzamento dell'iter del procedimento\processo.

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>Indice documenti</b>		IdDoc		SI	NO, ma ridefinito
<b>Definizione</b>					
<i>Elenco degli identificativi dei documenti contenuti nell'aggregazione. Metadato ricorsivo</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>Posizione fisica Aggregazione Documentale</b>		Testo libero	Alfanumerico	SI, solo nel caso di fascicoli cartacei digitalizzati o di fascicoli ibridi	SI
<b>Definizione</b>					
<i>Posizione fisica dell'aggregazione. Nel caso di fascicoli ibridi indica la posizione della componente cartacea del fascicolo.</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>IdAggPrincipale</b>		Come da sistema di identificazione formalmente definito	Alfanumerico	NO	SI
<b>Definizione</b>					
<i>Identificativo univoco e persistente del livello superiore di fascicolazione nel caso in cui si stia definendo un sottofascicolo o una sottoserie</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova definizione
<b>Tempo di conservazione</b>		<ul style="list-style-type: none"> <li>• 9999</li> <li>• 5 anni</li> <li>• 10 anni</li> <li>• .....</li> </ul>	Numerico	NO	SI
<b>Definizione</b>					
<i>Tempo di conservazione dell'aggregazione desunto dal Piano di conservazione formalmente integrato al Piano di classificazione. Espresso in numero di anni, il valore 9999 indica un tempo di conservazione "Permanente".</i>					

Informazione	Sottocampi	Valori Ammessi	Tipo dato	Obbligatorietà	Nuova Definizione
<b>Note</b>		Testo Libero	Alfanumerico	NO	SI
<b>Definizione</b>					
<i>Eventuali indicazioni aggiuntive</i>					



## 4.1 XSD METADATI DELLE AGGREGAZIONI DOCUMENTALI INFORMATICHE

### Schema xsd:

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema xmlns:xs="http://www.w3.org/2001/XMLSchema" elementFormDefault="qualified">

  <xs:element name="AggregazioneDocumentaliInformatiche">
    <xs:complexType>
      <xs:sequence>
        <xs:element name="IdAgg" >
          <xs:complexType>
            <xs:sequence>
              <xs:element name="TipoAggregazione">
                <xs:simpleType>
                  <xs:restriction base="xs:string">
                    <xs:enumeration value="Fascicolo"/>
                    <xs:enumeration value="Serie
Documentale"/>
                    <xs:enumeration value="Serie Di
Fascicoli"/>
                  </xs:restriction>
                </xs:simpleType>
              </xs:element>
              <xs:element name="IdAggregazione" Type="xs:string" />
            </xs:sequence>
          </xs:complexType>
        </xs:element>
        <xs:element name="Tipologia" minOccurs="0">
          <xs:simpleType>
            <xs:restriction base="xs:string">
              <xs:enumeration value="affare"/>
              <xs:enumeration value="attivita"/>
              <xs:enumeration value="persona fisica"/>
              <xs:enumeration value="persona giuridica"/>
              <xs:enumeration value="procedimento amministrativo"/>
            </xs:restriction>
          </xs:simpleType>
        </xs:element>
      </xs:sequence>
    </xs:complexType>
  </xs:element>
</xs:schema>
```

```

        </xs:simpleType>
    </xs:element>
    <xs:element name="Soggetti" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="Ruolo">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="Amministrazione
titolare"/>
                            <xs:enumeration value="Amministrazioni
partecipanti"/>
                            <xs:enumeration value="Soggetto
intestatarario persona fisica"/>
                            <xs:enumeration value="Soggetto
intestatarario persona giuridica"/>
                            <xs:enumeration value="RUP" />
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="TipoSoggetto">
                    <xs:simpleType>
                        <xs:restriction base="xs:string">
                            <xs:enumeration value="PF"/>
                            <xs:enumeration value="PG"/>
                            <xs:enumeration value="PA"/>
                        </xs:restriction>
                    </xs:simpleType>
                </xs:element>
                <xs:element name="Nominativo" Type="xs:string" />
                <xs:element name="Codice" Type="xs:string" />
                <xs:element name="UOR" Type="xs:string" minOccurs="0" />
            </xs:sequence>
        </xs:complexType>
    </xs:element>
    <xs:element name="Assegnazione" minOccurs="0" maxOccurs="unbounded">
        <xs:complexType>
            <xs:sequence>
                <xs:element name="TipoAssegnazione">

```

```

        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Per competenza"/>
                <xs:enumeration value="Per conoscenza"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="Ruolo">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="Amministrazione
                <xs:enumeration value="Amministrazioni
                <xs:enumeration value="Soggetto
                <xs:enumeration value="Soggetto
                <xs:enumeration value="RUP" />
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="TipoSoggetto">
        <xs:simpleType>
            <xs:restriction base="xs:string">
                <xs:enumeration value="PF"/>
                <xs:enumeration value="PG"/>
                <xs:enumeration value="PA"/>
            </xs:restriction>
        </xs:simpleType>
    </xs:element>
    <xs:element name="Codice" Type="xs:string" />
    <xs:element name="DataInizioAssegnazione" Type="xs:dateTime"/>
    <xs:element name="DataFineAssegnazione" Type="xs:dateTime"
minOccurs="0"/>
        </xs:sequence>
    </xs:complexType>
</xs:element>
<xs:element name="DataApertura" Type="xs:date"/>

```

```

<xs:element name="Classificazione" >
  <xs:complexType>
    <xs:sequence>
      <xs:element name="IndiceDiClassificazione" Type="xs:string" />
      <xs:element name="Descrizione" Type="xs:string" />
      <xs:element name="PianoDiClassificazione" Type="xs:string"/>
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="Progressivo">
  <xs:simpleType>
    <xs:restriction base="Integer">
      <xs:minInclusive value="1"/>
      <xs:maxInclusive value="999999999"/>
    </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="ChiaveDescrittiva">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="Oggetto" Type="xs:string" />
      <xs:element name="ParoleChiave" Type="xs:string" minOccurs="0"
maxOccurs="5" />
    </xs:sequence>
  </xs:complexType>
</xs:element>
<xs:element name="DataChiusura" type="xs:date" minOccurs="0"/>
<xs:element name="ProcedimentoAmministrativo" minOccurs="0" >
  <xs:complexType>
    <xs:sequence>
      <xs:element name="MateriaArgomentoStruttura" Type="xs:string" />
      <xs:element name="Procedimento" Type="xs:string" />
      <xs:element name="CatalogoProcedimenti" Type="xs:string" />
      <xs:element name="Fase" minOccurs="1" maxOccurs="unbounded">
        <xs:complexType>
          <xs:sequence>
            <xs:element name="TipoFase" >
              <xs:simpleType>

```

```

base="xs:string">
value="Preparatoria"/>
value="Istruttoria"/>
value="Consultiva"/>
value="Decisoria o deliberativa"/>
value="Integrazione dell'efficacia"/>

type="xs:date"/>
type="xs:date" minOccurs="0"/>

name="ImprontaCrittograficaDelDocumento">
name="Impronta" Type="xs:base64Binary" />
name="Algoritmo" Type="xs:string" default="SHA-256"/>

<xs:restriction
  <xs:enumeration
  <xs:enumeration
  <xs:enumeration
  <xs:enumeration
  <xs:enumeration
  </xs:restriction>
  </xs:simpleType>
</xs:element>
<xs:element name="DataInizioFase"
  <xs:element name="DataFineFase"
  </xs:sequence>
</xs:complexType>
</xs:element>
</xs:sequence>
</xs:complexType>
</xs:element>
<xs:element name="IndiceDocumenti" minOccurs="1" maxOccurs="unbounded">
  <xs:complexType>
    <xs:sequence>
      <xs:element name="IdDoc">
        <xs:complexType>
          <xs:sequence>
            <xs:element
              <xs:complexType>
                <xs:sequence>
                  <xs:element
                    <xs:sequence>
                      <xs:element

```



```
                </xs:simpleType>
            </xs:element>
            <xs:element name="Note" Type="xs:string" minOccurs="0" />
        </xs:sequence>
    </xs:complexType>
</xs:element>
</xs:schema>
```

# **Comunicazione tra AOO di Documenti Amministrativi Protocollati.**

*Allegato 6 al documento “Linee  
Guida sulla formazione, gestione e  
conservazione dei documenti  
informatici”.*

## Indice del documento

1. Scopo ed ambito di applicazione	3
1.1. Note di lettura del documento	4
2. Messaggio di protocollo	5
2.1. Struttura della segnatura di protocollo	6
2.1.1. Intestazione	6
2.1.2. Descrizione	6
2.1.3. Signature	7
2.2. Regole di processamento	7
3. Flussi di comunicazione	9
3.1. Regole di processamento	10
3.1.1. Inoltro di un messaggio protocollato	10
3.1.2. Annullamento protocollazione mittente	11
3.1.3. Annullamento protocollazione destinatario	12
4. APPENDICE A - XML Schema della segnatura di protocollo	13
4.1. Segnatura di protocollo XML Schema	13
5. APPENDICE B - Interfacce di servizio SOAP	22
5.1. protocollo-mittente.wsdl	22
5.2. protocollo-destinatario.wsdl	25
5.3. messaggio_protocollo.xsd	27

# 1. Scopo ed ambito di applicazione

Il “Sistema di Gestione Informatica dei Documenti” è utilizzato da una Pubbliche Amministrazioni (di seguito *PA*) per gestire il ciclo di vita dei “Documenti Amministrativi Informatici”, a partire dalla loro formazione/ricezione per giungere alla loro archiviazione e/o trasmissione, nell’esercizio delle proprie funzioni istituzionali.

Con “Protocollo Informatico” indichiamo la componente software del sistema di “Sistema di Gestione Informatica dei Documenti” che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo.

Nel dettaglio il “Protocollo Informatico” assicura le seguenti azioni:

- produzione della segnatura di protocollo, cioè l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione dalle pubbliche amministrazioni;
- registrazione di protocollo, cioè l'attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito dalle pubbliche amministrazioni.

La strategia per la digitalizzazione della PA, e non da ultimo le indicazioni riportate nel “Piano Triennale per l'Informatica nella Pubblica Amministrazione”, individuano l'esigenza di favorire l'interazione tra i sistemi informatici delle PA che, nel presente allegato, si concretizza nella comunicazione tra le Aree Organizzative Omogenee (AOO) della medesima PA o appartenenti a differenti PA.

Di seguito, quale presupposto all'esigenza di ricezione e spedizione espressa in precedenza, sono definite le tipologia e la rappresentazione (formati dati) delle informazioni associate ai documenti amministrativi informatici protocollati che costituiscono la segnatura di protocollo. La rappresentazione formale degli stessi è realizzata attraverso l'utilizzo degli XML Schema nel rispetto delle specifiche W3C:

- W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures<sup>1</sup>
- W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes<sup>2</sup>

In attuazione di quanto disposto dell'art. 47 del D.Lgs. 82/2005, relativamente alle comunicazione tra amministrazioni, di documenti amministrativi informatici protocollati, sono individuate le modalità tecniche per assicurare il trasporto di documenti amministrativi informatici tra AOO della pubblica amministrazione.

I formati dati e le modalità tecniche per il trasporto indicati nel presente allegato verranno adeguati in relazione all'evoluzione tecnologica e alle eventuali ulteriori esigenze che le amministrazioni dovessero manifestare a seguito della loro applicazione.

---

<sup>1</sup> <https://www.w3.org/TR/xmlschema11-1/>

<sup>2</sup> <https://www.w3.org/TR/xmlschema11-2/>

Il presente documento abroga e sostituisce la circolare 60/2103 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni".

### 1.1. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con RFC 2119<sup>3</sup> dell'Internet Engineering Task Force. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'è proibizione assoluta di implementazione di un determinato elemento di specifica.

---

<sup>3</sup> <https://www.ietf.org/rfc/rfc2119.txt>

## 2. Messaggio di protocollo

Lo scambio di documenti amministrativi protocollati tra AOO vede coinvolti:

- il *mittente*, l'AOO che invia i documenti amministrativi protocollati;
- il *destinatario*, l'AOO che riceve i documenti amministrativi protocollati.

Un *messaggio di protocollo*, l'elemento atomico di interesse per dare seguito allo scambio di documenti amministrativi protocollati tra AOO, è una struttura logica che:

- DEVE contenere il documento amministrativo informatico principale (di seguito *documento principale*);
- PUÒ contenere un numero qualsiasi di documenti amministrativi informatici allegati (di seguito *allegati*);
- DEVE contenere la segnatura di protocollo del messaggio protocollato (di seguito *segnatura di protocollo*).

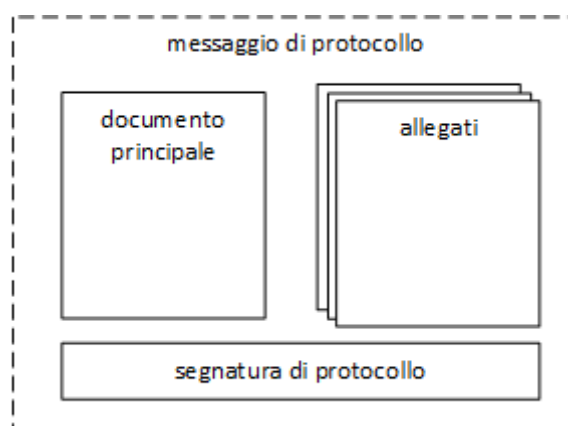


Figure 1. Struttura logica del "messaggio di protocollo"

Il *documento principale* e gli eventuali *allegati* DEVONO essere formati nel rispetto delle regole di formazione dei documenti amministrativi informatici.

La *segnatura di protocollo* DEVE essere formata nel rispetto di quanto indicato al successivo paragrafo [2.1 Struttura segnatura di protocollo](#).

La *segnatura di protocollo* DEVE essere associata in forma permanente al *documento principale* e agli *allegati* che con esso formano il *messaggio di protocollo*. A tal fine sistema informatico dell'AOO mittente:

- DEVE riportare nella *segnatura di protocollo* l'impronta del *documento principale* e, se presenti, degli *allegati*;
- DEVE assicurare l'autenticità e integrità della *segnatura di protocollo* attuando le regole tecniche in materia di firma elettronica dei documenti informatici emanate dall'AgID conformemente al regolamento UE n° 910/2014, nel dettaglio applicando un "sigillo elettronico qualificato" previsti alla sezione 5 del regolamento UE n° 910/2014 utilizzando il profilo XAdES baseline B level signatures definito in [ETSI EN 319 132-1 v1.1.1](#).

Il controllo della validità amministrativa del *documento principale*, degli *allegati* e dei dati riportati nella *segnatura di protocollo*:

- è di responsabilità della AOO mittente;
- DEVE essere effettuato prima della composizione del *messaggio di protocollo*.

Per assicurare la non ripudiabilità dello scambio tra AOO, le informazioni della *segnatura di protocollo* DEVONO essere memorizzate nel sistema di gestione dei documenti della AOO mittente e in quello delle AOO destinataria. L'indicata azione di memorizzazione è assicurata dalla registrazione di protocollo realizzata dal "Protocollo informatico".

### 2.1. Struttura della segnatura di protocollo

La *segnatura di protocollo* DEVE prevedere le seguenti sezioni:

- "Intestazione", contiene i dati identificativi e le informazioni fondamentali del messaggio;
- "Descrizione", contiene le informazioni descrittive riguardanti il contenuto del messaggio;
- "Signature" per permettere la firma della segnatura di protocollo conformemente al profilo XAdES baseline B level signatures.

Di seguito sono indicate la natura delle informazioni presenti nelle sezioni della *segnatura di protocollo*.

Le AOO mittenti che predispongono la *segnatura di protocollo* DEVONO assicurare la conformità rispetto all'XML Schema riportato nell'[Appendice A](#).

#### 2.1.1. Intestazione

La sezione "Intestazione" DEVE contenere gli elementi essenziali di identificazione e caratterizzazione amministrativa del *messaggio di protocollato*.

In particolare, la sezione contiene l'*Identificatore* della registrazione relativa al messaggio protocollato in uscita. Tale identificatore riporta i seguenti dati:

- a) indicazione della amministrazione mittente;
- b) indicazione della AOO mittente;
- c) indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
- d) numero progressivo di protocollo;
- e) data di registrazione;
- f) l'oggetto del messaggio di protocollo;
- g) la classificazione del messaggio di protocollo;
- h) il fascicolo del messaggio di protocollo.

#### 2.1.2. Descrizione

La sezione "Descrizione" DEVE contenere le informazioni che descrivono i corrispondenti (mittente e destinatario) interessati nello scambio e i riferimenti al *documento principale* e agli eventuali *allegati* del *messaggio di protocollo*.

In particolare, contiene l'impronta informatica del *documento principale* e degli eventuali *allegati* necessari per associarli in forma permanente alla *segnatura di protocollo*.

### 2.1.3. Signature

La sezione "Signature" DEVE contenere le informazioni per assicurare la firma della *segnatura di protocollo* da parte della AOO mittente per assicurare l'autenticità e integrità.

## 2.2. Regole di processamento

Il flusso di processamento che le AOO mittenti devono realizzare per assicurare la formazione del *messaggio di protocollo* è di seguito riportato:

- A. Formazione del *documento principale (document)*, ed eventuali *allegati (attachment<sub>i</sub>)*, DEVONO rispettare le regole di formazione dei documenti amministrativi elettronici, inclusa la classificazione.
- B. Calcolo dell'impronta del *documento principale (digest(document,algorithm))*, e degli eventuali *allegati (digest(attachment<sub>i</sub>,algorithm))*, che DEVONO utilizzare uno degli algoritmi indicati nella seguente tabella 1.
- C. Generazione del numero di protocollo da assegnare al *messaggio di protocollo*.
- D. Formazione della *segnatura di protocollo* che DEVE rispettare l'XML Schema indicato nell'[Appendice A](#), utilizzando le impronte *digest(document,algorithm)* e *digest(attachment<sub>i</sub>,algorithm)* create al passo B.
- E. Apposizione di un "sigillo elettronico qualificato" alla *segnatura di protocollo per* garantire l'integrità e autenticità che DEVE applicare il profilo XAdES baseline B level signatures definito in [ETSI EN 319 132-1 v1.1.1](#).

Nota: L'AOO mittente assicura l'atomicità<sup>4</sup> delle operazione da C a E.

Tabella 1 - Digest algorithm

SIGLA	URI
SHA-224	<a href="http://www.w3.org/2001/04/xmldsig-more#sha224">http://www.w3.org/2001/04/xmldsig-more#sha224</a>
SHA-256	<a href="http://www.w3.org/2001/04/xmlenc#sha256">http://www.w3.org/2001/04/xmlenc#sha256</a>
SHA-384	<a href="http://www.w3.org/2001/04/xmldsig-more#sha384">http://www.w3.org/2001/04/xmldsig-more#sha384</a>

<sup>4</sup> le operazioni sono eseguite in maniera indivisibile da un punto di vista logico, in breve o sono eseguite tutte o non è eseguita nessuna

**Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati**

SHA-512	<a href="http://www.w3.org/2001/04/xmlenc#sha512">http://www.w3.org/2001/04/xmlenc#sha512</a>
HMAC-SHA-224	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha224">http://www.w3.org/2001/04/xmldsig-more#hmac-sha224</a>
HMAC-SHA-256	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">http://www.w3.org/2001/04/xmldsig-more#hmac-sha256</a>
HMAC-SHA-384	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha384">http://www.w3.org/2001/04/xmldsig-more#hmac-sha384</a>
HMAC-SHA-512	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha512">http://www.w3.org/2001/04/xmldsig-more#hmac-sha512</a>

### 3. Flussi di comunicazione

Le esigenze di comunicazione tra AOO mittente e AOO destinataria per assicurare l'inoltro di un messaggio protocollato richiedono:

- *inoltro di un messaggio protocollato (MessaggioInoltro)* da una AOO mittente ad una AOO destinataria e la relativa conferma, anche la gestione dei due casi di annullamento possibili:
- *annullamento protocollazione mittente (AnnullamentoInoltroMittente)*, nel caso in cui successivamente all'inoltro l'AOO mittente adotti un provvedimento per il suo annullamento;
- *annullamento protocollazione destinatario (AnnullamentoInoltroDestinatario)*, nel caso in cui successivamente alla conferma di ricezione l'AOO destinataria adotti un provvedimento per il suo annullamento.

Le esigenze di comunicazione individuate sono sintetizzate nel seguente UML sequence diagram.



Figure 2. Comunicazioni tra AOO mittente e AOO destinatario

Per dare seguito alla comunicazione tra AOO mittente e AOO destinataria, le stesse possono adottare una delle modalità previste dalla norma:

- *posta elettronica*, in cui il *messaggio di protocollo* (documento, allegati e segnatura di protocollo) è trasportato come allegato della stessa e il contenuto del messaggio di posta elettronica NON DEVE intendersi come parte del *messaggio di protocollo*;
- *cooperazione applicativa*, utilizzando il Simple Object Access Protocol assicurando l'implementazione delle interfacce di servizio riportate nell'[Appendice B](#).

Per assicurare la comunicazione tra AOO le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA)<sup>5</sup> (di seguito IPA) con:

- indirizzo di *posta elettronica certificata*;
- *endpoint* di esposizione dei servizi indicati nell'[Appendice B](#).

### 3.1. Regole di processamento

I flussi di processamento che le AOO mittenti e destinatari devono realizzare per assicurare l'inoltro e ricezione dei messaggi protocollati sono riportate di seguito.

Si precisa che ogni flusso di seguito indicato è da ritenersi completo quando l'intero set di messaggi previsto dallo specifico flusso è stato scambiato. Si precisa che non è possibile avviare i flussi di annullamento (**AnnullamentoInoltroMittente** e **AnnullamentoInoltroDestinatario**) prima del completamento del flusso di inoltro (**MessaggioInoltro**).

#### 03.1.1. Inoltro di un messaggio protocollato

A. AOO mittente: Inoltro *messaggio di protocollo*

L'AOO mittente DEVE produrre il *messaggio di protocollo*, come indicato nel precedente [paragrafo 2](#) e inoltrare lo stesso alla AOO destinataria.

B. AOO destinatario: Riceve *messaggio di protocollo*

L'AOO destinatario ricevuto il *messaggio di protocollo* DEVE verificare la *segnatura di protocollo*, nel dettaglio:

- a. DEVE verificare la correttezza della firma della *segnatura di protocollo*;
- b. DEVE verificare la corrispondenza dell'impronta del *documento principale* presente nella *segnatura di protocollo* e il documento *principale* ricevuto;
- c. se presenti *allegati*, per ogni allegato DEVE verificare la corrispondenza dell'impronta dell'*allegato* presente nella *segnatura di protocollo* e l'allegato ricevuto.

Se l'AOO destinataria è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE rispondere indicando l'Identificatore associato dalla AOO mittente.

Se l'AOO destinataria non è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

- a. se la firma della *segnatura di protocollo* non è verificata DEVE restituire l'anomalia 001\_ValidazioneFirma;
- b. se almeno una delle impronte riportate nella *segnatura di protocollo* (*documento principale* e *allegati*) non è verificata DEVE restituire l'anomalia 002\_AnomaliaImpronta.

---

<sup>5</sup> <https://www.indicepa.gov.it/>

- C. AOO destinatario: Inoltro conferma di protocollazione del *messaggio di protocollo*  
L'AOO destinataria DEVE inoltrare conferma di protocollazione del *messaggio di protocollo* alla AOO mittente a conclusione del processo di protocollazione in ingresso.

L'AOO destinataria PUO' effettuare il controllo dei file ricevuti (*documento principale e allegati*) ed in caso di anomalie DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

- a. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta non leggibile DEVE restituire l'anomalia 003\_DocumentoAllegatiNonLeggibili.
- b. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta firmato e la validazione della stessa fallisce DEVE restituire l'anomalia 004\_DocumentoAllegatiErroreValidazioneFirma.
- c. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta con marca temporale e la validazione della stessa fallisce DEVE restituire l'anomalia 005\_DocumentoAllegatiErroreValidazioneMarcaTemporale.
- d. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta con sigillo elettronico e la validazione dello stesso fallisce DEVE restituire l'anomalia 006\_DocumentoAllegatiErroreValidazioneSigillo.

AOO destinataria DEVE verificare la ricevibilità del *messaggio di protocollo* ricevuto, ed in caso negativo DEVE restituire l'anomalia 000\_Irricevibile e l'indicazione della motivazione di irricevibilità.

AOO destinatario DEVE generare il numero di protocollo per *messaggio di protocollo* ricevuto e, contemporaneamente, memorizzare lo stesso nel registro di protocollo in ingresso.

L'AOO destinatario DEVE inoltrare la conferma di protocollazione del *messaggio di protocollo* ricevuto includendo l'Identificatore associato dal AOO mittente e l'Identificatore da essa associato.

- D. AOO mittente: Ricezione della conferma di protocollazione del *messaggio di protocollo*

Nel caso in cui l'AOO destinatario non segnali anomalie l'AOO mittente DEVE memorizzare la conferma di protocollazione del *messaggio di protocollo* nel registro di protocollo per assicurare la persistenza dello stesso.

Nel caso in cui l'AOO destinatario segnali anomalie l'AOO mittente DEVE ritenere la transazione non conclusa.

### 3.1.2. Annullamento protocollazione mittente

- A. AOO mittente: Inoltro messaggio annullamento

L'AOO mittente DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente inviato:

- indicando l'Identificatore associato da essa al momento dell'inoltro e l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

**B. AOO destinatario: Inoltro ricevuta annullamento**

L'AOO destinatario DEVE inoltrare la ricevuta di annullamento di un *messaggio di protocollo* precedentemente ricevuto.

L'AOO destinataria assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000\_Irricevibile indicando il motivo di irricevibilità;
- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l'anomalia 007\_ErroreIdentificatoreNonTrovato.

### 3.1.3. Annullamento protocollazione destinatario

**A. AOO destinatario: Inoltro messaggio annullamento**

L'AOO destinatario DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente ricevuto:

- indicando l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

**B. AOO mittente: Inoltro ricevuta annullamento**

L'AOO mittente DEVE inoltrare la ricevuta di annullamento di un *messaggio di protocollo* precedentemente inviato.

L'AOO mittente assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato da essa al momento dell'inoltro e l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000\_Irricevibile indicando il motivo di irricevibilità;
- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l'anomalia 007\_ErroreIdentificatoreNonTrovato.

## 4. APPENDICE A - XML Schema della segnatura di protocollo

Di seguito è riportato XML Schema della *segnatura di protocollo* che le AOO delle pubbliche amministrazioni adottano.

Per favorire l'utilizzo del XML Schema lo stesso è riportato nel repository github pubblico consultabile all'URL <https://github.com/AgID/protocollo-comunicazione-ao>.

### 4.1. Segnatura di protocollo XML Schema

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:prot="http://www.agid.gov.it/protocollo/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

  targetNamespace="http://www.agid.gov.it/protocollo/"

  elementFormDefault="qualified"
  attributeFormDefault="qualified"

  version="3.0"
  >

  <xs:element name="SegnaturaInformatica" type="prot:SegnaturaInformaticaType"/>

  <xs:complexType name="SegnaturaInformaticaType">
    <xs:annotation>
      <xs:documentation>
        La segnatura di protocollo contiene i dati relativi ad un
        messaggio di protocollo.

        Un messaggio di protocollo è determinato da:
        - documento principale
        - eventuali allegati
        - la segnatura di protocollo qui definita

        La segnatura di protocollo è associata in forma permanente al
        documento principale e agli allegati che con esso formano il messaggio di protocollo
        includendo nella segnatura di protocollo le impronte (digest)
        del documento principale e degli allegati e assicurando l'autenticità e integrità
        della segnatura di protocollo firmando la stessa implementando
        il profilo XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1.

        La segnatura di protocollo è caratterizzata da:
        - Intestazione, i dati necessari per individuare univocamente il
        messaggio di protocollo

        - Descrizione, i dati aggiuntivi del messaggio di protocollo
        - Signature, i dati e metadati della firma dell'XML (profilo
        XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1)
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="Intestazione" type="prot:IntestazioneType"/>

      <xs:element name="Descrizione" type="prot:DescrizioneType"/>

      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attribute name="versione" type="xs:NMTOKEN" fixed="3.0.0" use="required"/>
  </xs:complexType>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:attribute name="lang" type="xs:NMTOKEN" fixed="it" use="required"/>
</xs:complexType>

<xs:complexType name="IntestazioneType">
  <xs:annotation>
    <xs:documentation>
      L'intestazione contiene i dati essenziali per l'identificazione
      e caratterizzazione amministrativa del messaggio di protocollato.

      L'intestazione è caratterizzata da:
      - Identificatore, i dati per identificare univocamente il
      messaggio di protocollo conformemente in attuazione all'art. 55 del DPR 445/2000
      - Oggetto, sintesi dei contenuti di carattere giuridico,
      amministrativo e narrativo di un documento
      - Classifica, la categoria del Titolare di classificazione
      associato al messaggio di protocollo
      - Fascicolo, opzionalmente, il fascicolo entro cui è presente il
      messaggio di protocollo
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Identificatore" type="prot:IdentificatoreType"/>
    <xs:element name="Oggetto" type="xs:string"/>

    <xs:element name="Classifica" type="prot:ClassificaType" />

    <xs:element name="Fascicolo" type="prot:FascicoloType" minOccurs="0" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="IdentificatoreType">
  <xs:annotation>
    <xs:documentation>
      Contiene i dati identificativi della segnatura di protocollo.

      L'identificativo è caratterizzato da:
      - CodiceAmministrazione, il codice IPA
      dell'amministrazione
      - CodiceAOO, il codice IPA dell'AOO
      - CodiceRegistro, il codice del Registro
      - NumeroRegistrazione, il progressivo di protocollo
      - DataRegistrazione, la data di registrazione
      - OraRegistrazione, in maniera opzionale l'ora di
      registrazione
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="CodiceAmministrazione" type="prot:CodiceIPA"/>
    <xs:element name="CodiceAOO" type="prot:CodiceIPA"/>
    <xs:element name="CodiceRegistro" type="prot:CodiceRegistroType"/>
    <xs:element name="NumeroRegistrazione"
    type="prot:NumeroRegistrazioneType"/>
    <xs:element name="DataRegistrazione" type="xs:date"/>
    <xs:element name="OraRegistrazione" type="xs:time" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="CodiceIPA">
  <xs:annotation>
    <xs:documentation>
      Contiene il codice IPA dell'amministrazione o dell'AOO indica
      all'amministrazione e, in maniera opzionale, la descrizione della stessa.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="descrizione" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="FascicoloType">
  <xs:annotation>
    <xs:documentation>
      Il fascicolo riporta il riferimento al fascicolo prevedendo la
      Denominazione e il relativo CodiceFascicolo
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Denominazione" type="xs:string"/>
    <xs:element name="CodiceFascicolo" type="xs:string"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ClassificaType">
  <xs:annotation>
    <xs:documentation>
      La classificazione riporta il valore attribuito al messaggio di
      protocollo.

      La classificazione è caratterizzata da:
      - Denominazione, una descrizione della classificazione
      attribuita
      - In alternativa il codice di classificazione può essere
      rappresentato:
      - CodiceFlat, l'unione in un'unico element di categoria,
      classe ed eventuale sottoclasse
      es. <CodiceFlat>Titolo I.Classe 1</CodiceFlat>
      - CodicePath, la separazione in differenti element di
      categoria, classe ed eventuale sottoclasse
      es. <CodicePath>
          <Livello>Titolo I</Livello>
          <SubLivello>
            <Livello>Classe
            1</Livello>
          </SubLivello>
        </CodicePath>
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Denominazione" type="xs:string"/>
    <xs:choice>
      <xs:element name="CodiceFlat" type="xs:string"/>
      <xs:element name="CodicePath" type="prot:LivelloType"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="LivelloType">
  <xs:annotation>
    <xs:documentation>
      Il livello riporta i dati relativi alla categoria, classe ed
      eventuale sottoclasse

      Il livello è composto dal codice della categoria, classe ed
      eventuale sottoclasse e la relativa descrizione
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Livello">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```

                                                                 <xs:attribute name="descrizione"
type="xs:string"/>
                                                                 </xs:extension>
                                                                 </xs:simpleContent>
                                                                 </xs:complexType>
                                                                 </xs:element>
                                                                 <xs:element name="SubLivello" type="prot:LivelloType" minOccurs="0"/>
                                                                 </xs:sequence>
                                                                 </xs:complexType>

<xs:complexType name="DescrizioneType">
  <xs:annotation>
    <xs:documentation>
      La descrizione contiene i dati descrittivi del messaggio di
protocollato.

      La descrizione è caratterizzata da:
      - Mittente, riferimento del mittente (organizzazione o persona)
      - Destinatario, riferimento del destinatario (organizzazione o
persona)
      - DocumentoPrimario, riferimento al documento primario del
messaggio di protocollo
      - Allegato, riferimento ad uno degli allegati del messaggio di
protocollo se presente
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Mittente" type="prot:SoggettoType" minOccurs="0"/>
    <xs:element name="Destinatario" type="prot:SoggettoType" minOccurs="1"
maxOccurs="unbounded"/>
    <xs:element name="DocumentoPrimario" type="prot:DocumentoType"/>

    <xs:element name="Allegato" type="prot:DocumentoType" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="DocumentoType">
  <xs:annotation>
    <xs:documentation>
      Il documento contiene i dati per referenziare un documento
(documento primario o allegato) del messaggio di protocollo

      Il documento è caratterizzato da:
      - Descrizione, la descrizione del contenuto dello specifico
documento
      - Impronta, l'impronta digitale (digest) del documento
      - nomeFile, il nome del file relativo al documento
      - mimeType, il mime type (RFC 6838) associato al documento
      - firmatoDigitalmente, flag per indicare il documento è firmato
digitalmente (sezione 4 Regolamento UE 910/2014)
      - sigillatoElettronicamente, flag per indicare che al documento
è apposto un sigillo elettronico (sezione 5 Regolamento UE 910/2014)
      - marcaturaTemporale, flag per indicare che al documento è
apposta una marca temporale (sezione 6 Regolamento UE 910/2014)
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Descrizione" type="xs:string" minOccurs="0"/>
    <xs:element name="Impronta" type="prot:ImprontaType"/>

  </xs:sequence>
  <xs:attribute name="nomeFile" type="xs:string" use="required"/>
  <xs:attribute name="mimeType" type="xs:string" use="required"/>
  <xs:attribute name="firmatoDigitalmente" type="xs:boolean"/>
  <xs:attribute name="marcaturaTemporale" type="xs:boolean"/>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:attribute name="sigillatoElettronicamente" type="xs:boolean"/>
</xs:complexType>

<xs:complexType name="SoggettoType">
  <xs:annotation>
    <xs:documentation>
      Il soggetto contiene i dati per referenziare un corrispondente

      Sulla base delle necessità è possibile indicare:
      - una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPA">Organizzazione</Riferimento>
          </Organizzazione>

      - una specifica unità organizzativa di una
organizzazone
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPAOrganizzazione">Organizzazione</Riferimento>
          <UnitaOrganizzativa>
            <Descrizione
codiceIPA="codiceIPAUnitaOrganizzativa">UnitaOrganizzativa</Descrizione>
          </UnitaOrganizzativa>
          </Organizzazione>

      - una persona fisica
        es. <Persona>...</Persona>
      - una persona fisica relativa ad una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPA">Organizzazione</Riferimento>
          <Persona>...</Persona>
          </Organizzazione>

      - una persona fisica relativa ad una specifica unità
organizzativa di una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPAOrganizzazione">Organizzazione</Riferimento>
          <UnitaOrganizzativa>
            <Descrizione
codiceIPA="codiceIPAUnitaOrganizzativa">UnitaOrganizzativa</Descrizione>
          <Persona>...</Persona>
          </UnitaOrganizzativa>
          </Organizzazione>

      Il soggetto è caratterizzato da:
      - il alternativa:
        - Organizzazione, un'organizzazione
    </xs:documentation>
  </xs:annotation>
  <xs:choice>
    <xs:element name="Organizzazione" type="prot:OrganizzativaType"/>
    <xs:element name="Persona" type="prot:PersonaType"/>
  </xs:choice>
</xs:complexType>

<xs:complexType name="OrganizzativaType">
  <xs:annotation>
    <xs:documentation>
      L'organizzativa contiene i dati di un'unità organizzativa o
unità organizzativa

      L'unità organizzativa è caratterizzata da:
      - Nome, il nome dell'unità organizzativa
      - in alternativa:
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```

- UnitaOrganizzativa, una sottounità organizzativa di
livello inferiore
- Persona, il riferimento ad una persona fisica
</xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element name="Riferimento" type="prot:NomeOrganizzazioneType"/>
  <xs:choice minOccurs="0">
    <xs:element name="UnitaOrganizzativa"
type="prot:OrganizzativaType"/>
    <xs:element name="Persona" type=" prot:PersonaType "/>
  </xs:choice>
</xs:sequence>
</xs:complexType>

<xs:complexType name="NomeOrganizzazioneType">
  <xs:annotation>
    <xs:documentation>
      Il nome organizzazione contiene i riferimenti ad
un'organizzazione o unità organizzativa

      Il nome organizzazione è caratterizzata dal nome
dell'organizzazione o dell'unità organizzativa e, quando esiste, il codice IPA della stessa
    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="codiceIPA" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="IndirizzoPostaleType">
  <xs:annotation>
    <xs:documentation>
      L'indirizzo contiene i dati relativi ad un'indirizzo.

      L'indirizzo è caratterizzato da:
      - Toponimo, il riferimento al nome proprio del luogo
      - Civico, il riferimento assegnato allo specifico immobile
      - CAP, il codice di avviamento postale
      - Comune, il riferimento al Comune
      - Provincia, la provincia
      - Nazione, la denominazione della nazione e il codice ISO 3166-1
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Toponimo" type="prot:ToponimoType"/>
    <xs:element name="Civico" type="xs:string"/>
    <xs:element name="CAP" type="prot:CAPType"/>
    <xs:element name="Comune" type="prot:ComuneType"/>
    <xs:element name="Nazione" default="Italia">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute name="codice3166"
default="ITA"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ToponimoType">
  <xs:annotation>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:documentation>
    Il toponimo contiene il riferimento al nome proprio del luogo

    Il toponimo è caratterizzato da:
    - dug, denominazione urbanistica generica o qualificatore del
toponimo (e.g., via, viale, piazza, ecc.)
    - duf, denominazione urbanistica ufficiale o nome della strada
</xs:documentation>
</xs:annotation>
<xs:sequence>
    <xs:element name="dug" type="xs:string"/>
    <xs:element name="duf" type="xs:string"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="CAPType">
    <xs:annotation>
        <xs:documentation>
            Il CAP contiene il codice di avviamento postale
        </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{6}"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ComuneType">
    <xs:annotation>
        <xs:documentation>
            Il Comune contiene il riferimento al Comune

            Il Comune è caratterizzato dalla denominazione del Comune e il
relativo codice ISTAT a 6 cifre
        </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="CodiceISTAT"
type="prot:CodiceISTATComune6Type" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="CodiceISTATComune6Type">
    <xs:annotation>
        <xs:documentation>
            Il codice ISTAT del Comune a 6 cifre
        </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{6}"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ImprontaType">
    <xs:annotation>
        <xs:documentation>
            L'impronta contiene il digest di un documento elettronico

            L'impronta è caratterizzata dalla codifica base64 del digest
calcolato applicando l'algoritmo specifico
        </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
        <xs:extension base="xs:base64Binary">
            <xs:attribute name="algoritmo" type="xs:string" default="SHA-
256"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="PersonaType">
  <xs:annotation>
    <xs:documentation>
      La persona contiene i dati relativi ad una persona fisica

      La persona è caratterizzata da:
      - Nome, il nome
      - Cognome, il cognome
      - Titolo, il titolo (es. Sig., Dott., ...)
      - CodiceFiscale, il codice fiscale
      - Contatti, i contatti della persona
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Nome" type="xs:string"/>

    <xs:element name="Cognome" type="xs:string"/>

    <xs:element name="Titolo" type="xs:string" minOccurs="0"/>
    <xs:element name="CodiceFiscale" type="prot:CodiceFiscaleType"
minOccurs="0"/>

    <xs:element name="Contatti" type="prot:ContattiType">

      </xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ContattiType">
    <xs:annotation>
      <xs:documentation>
        L'insieme di contatti, e nel dettaglio:
        - IndirizzoPostale, un'indirizzo relativo
        - IndirizzoTelematico, un'indirizzo elettronico
        - Telefono, un contatto telefonico
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="IndirizzoPostale" type="prot:IndirizzoPostaleType"
minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="IndirizzoTelematico"
type="prot:IndirizzoTelematicoType" maxOccurs="unbounded"/>
      <xs:element name="Telefono" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="IndirizzoTelematicoType">
    <xs:annotation>
      <xs:documentation>
        Un'indirizzo telematico utilizzato per la trasmissione
telematica

        I tipi di indirizzi telematici sono:
        - smtp, nel caso della posta elettronica
        - url, nel caso di interfacce di servizio (API REST o SOAP)
        - other, in casi differenti dai precedenti
      </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="tipo" default="smtp">
          <xs:simpleType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="smtp"/>
    <xs:enumeration value="url"/>
    <xs:enumeration value="other"/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="note" type="xs:string"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:simpleType name="CodiceFiscaleType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Z]{6}[0-9LMNPQRSTUVWXYZ]{2}[ABCDEHLMPRST][0-9LMNPQRSTUVWXYZ]{2}[A-Z][0-9LMNPQRSTUVWXYZ]{3}[A-Z]"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IdentificativoType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Za-z0-9_\. \-]{1,16}"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="CodiceRegistroType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Za-z0-9_\. \-]{1,16}"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NumeroRegistrazioneType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{7,}"/>
    </xs:restriction>
</xs:simpleType>

</xs:schema>
```

## 5. APPENDICE B - Interfacce di servizio SOAP

Le AOO mittente e AOO destinataria, per dare seguito alla comunicazione di messaggi protocollati utilizzando il Simple Object Access Protocol, implementano le interfacce di servizio descritte nei seguenti Web Services Description Language.

Nello specifico:

- la AOO mittente DEVE implementare protocollo-mittente.wsdl;
- la AOO destinataria DEVE implementare protocollo-destinatario.wsdl.

Per favorire l'utilizzo dei WSDL gli stessi sono riportati nel repository github pubblico consultabile all'URL <https://github.com/AgID/protocollo-comunicazione-aoa>.

Per l'inoltro di binary data nei messaggi SOAP si assume l'adozione del W3C Message Transmission Optimization Mechanism<sup>6</sup>.

Per l'autenticazione delle parti si adotta il profilo di iterazione "Bloccante RPC"<sup>7</sup> e la "Soluzione per confidenzialità ed autenticazione del soggetto fruitore"<sup>8</sup> per la tecnologia SOAP individuata nel modello di interoperabilità della PA assumendo l'utilizzo di certificati qualificati per il riconoscimento delle PA/AOO.

### 5.1. protocollo-mittente.wsdl

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:tns="http://ws.protocollo.comunicazione.aoa.mittente/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soapbind="http://schemas.xmlsoap.org/soap/http"
  name="ProtocolloDestinatarioService"
  targetNamespace="http://ws.protocollo.comunicazione.aoa.mittente/">

  <wsdl:types>

    <xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
      xmlns:prot="http://www.agid.gov.it/protocollo/"
      xmlns:tns="http://ws.protocollo.comunicazione.aoa.mittente/"
      targetNamespace="http://ws.protocollo.comunicazione.aoa.mittente/"
      elementFormDefault="qualified" version="1.0">

      <xs:element name="RequestConfermaMessaggioInoltro"
        type="tns:RequestConfermaMessaggioInoltroType"/>
      <xs:element name="ResponseConfermaMessaggioInoltro"
        type="tns:ResponseConfermaMessaggioInoltroType"/>
    </xs:schema>
  </wsdl:types>
</wsdl:definitions>
```

<sup>6</sup> <https://www.w3.org/TR/soap12-mtom/>

<sup>7</sup> <https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/profili-di-interazione/profilo-bloccante-rpc.html> (in via di pubblicazione)

<sup>8</sup> [https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/doc\\_04/soluzioni-di-sicurezza.html](https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/doc_04/soluzioni-di-sicurezza.html) (in via di pubblicazione)

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:element name="RequestAnnullamentoInoltroDestinatario"
type="tns:RequestAnnullamentoInoltroDestinatarioType"/>
<xs:element name="ResponseAnnullamentoInoltroDestinatario"
type="tns:ResponseAnnullamentoInoltroDestinatarioType"/>

<xs:complexType name="RequestConfermaMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:choice>
      <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
      <xs:element name="Anomalia" type="tns:AnomalieConfermaType" />
    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseConfermaMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="RequestAnnullamentoInoltroDestinatarioType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element name="RiferimentoProvvedimento" type="xs:string"/>
    <xs:element name="Note" type="xs:string"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseAnnullamentoInoltroDestinatarioType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieAnnullamentoType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AnomalieConfermaType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieConfermaEnum">
      <xs:attribute name="info" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieConfermaEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibile"/>
    <xs:enumeration value="003_DocumentoAllegatiNonLeggibili"/>
    <xs:enumeration value="004_DocumentoAllegatiErroreValidazioneFirma"/>
    <xs:enumeration value="005_DocumentoAllegatiErroreVaidazioneMarcaTemporale"/>
    <xs:enumeration value="006_DocumentoAllegatiErroreValidazioneSigillo"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AnomalieAnnullamentoType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieAnnullamentoEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:simpleType name="AnomalieAnnullamentoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibilita"/>
    <xs:enumeration value="007_ErroreIdentificatoreNonTrovato"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>

</wsdl:types>

<wsdl:message name="RequestConfermaMessaggioInoltro">
  <wsdl:part element="tns:RequestConfermaMessaggioInoltro" name="parameters"/>
</wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseConfermaMessaggioInoltro">
  <wsdl:part element="tns:ResponseConfermaMessaggioInoltro" name="parameters"/>
</wsdl:part>
</wsdl:message>

<wsdl:message name="RequestAnnullamentoInoltroDestinatario">
  <wsdl:part element="tns:RequestAnnullamentoInoltroDestinatario" name="parameters"/>
</wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseAnnullamentoInoltroDestinatario">
  <wsdl:part element="tns:ResponseAnnullamentoInoltroDestinatario" name="parameters"/>
</wsdl:part>
</wsdl:message>

<wsdl:portType name="ProtocolloMittentePortType">

  <wsdl:operation name="ConfermaMessaggioInoltro">
    <wsdl:input message="tns:RequestConfermaMessaggioInoltro"
name="RequestConfermaMessaggioInoltro">
      </wsdl:input>
    <wsdl:output message="tns:ResponseConfermaMessaggioInoltro"
name="ResponseConfermaMessaggioInoltro">
      </wsdl:output>
    </wsdl:operation>

    <wsdl:operation name="AnnullamentoInoltroDestinatario">
      <wsdl:input message="tns:RequestAnnullamentoInoltroDestinatario"
name="RequestAnnullamentoInoltroDestinatario">
        </wsdl:input>
      <wsdl:output message="tns:ResponseAnnullamentoInoltroDestinatario"
name="ResponseAnnullamentoInoltroDestinatario">
        </wsdl:output>
      </wsdl:operation>

  </wsdl:portType>

<wsdl:binding name="ProtocolloMittenteServiceBinding" type="tns:ProtocolloMittentePortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>

  <wsdl:operation name="ConfermaMessaggioInoltro">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestConfermaMessaggioInoltro">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseConfermaMessaggioInoltro">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
</wsdl:service>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</wsdl:output>
</wsdl:operation>

<wsdl:operation name="AnnullamentoInoltroDestinatario">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="RequestAnnullamentoInoltroDestinatario">
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="ResponseAnnullamentoInoltroDestinatario">
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>

</wsdl:binding>

<wsdl:service name="ProtocolloMittenteService">
  <wsdl:port binding="tns:ProtocolloMittenteServiceBinding"
name="ProtocolloMittenteService">
    <soap:address location="http://localhost:8080/proto-test/protocollo/mittente"/>
  </wsdl:port>
</wsdl:service>

</wsdl:definitions>
```

## 5.2. protocollo-destinatario.wsdl

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:tns="http://ws.protocollo.comunicazione.aoo.destinatario/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soapbind="http://schemas.xmlsoap.org/soap/http"
  name="ProtocolloDestinatarioService"
  targetNamespace="http://ws.protocollo.comunicazione.aoo.destinatario/">

  <wsdl:types>

    <xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
      xmlns:prot="http://www.agid.gov.it/protocollo/"
      xmlns:tns="http://ws.protocollo.comunicazione.aoo.destinatario/"
      targetNamespace="http://ws.protocollo.comunicazione.aoo.destinatario/"
      elementFormDefault="qualified" version="1.0">

      <xs:element name="RequestMessageInoltro" type="tns:RequestMessaggioInoltroType"/>
      <xs:element name="ResponseMessageInoltro" type="tns:ResponseMessaggioInoltroType"/>

      <xs:element name="RequestAnnullamentoInoltroMittente"
type="tns:RequestAnnullamentoInoltroMittenteType"/>
      <xs:element name="ResponseAnnullamentoInoltroMittente"
type="tns:ResponseAnnullamentoInoltroMittenteType"/>

      <xs:complexType name="RequestMessaggioInoltroType">
        <xs:complexContent>
          <xs:extension base="msgprot:MessaggioProtocolloType"/></xs:extension>
        </xs:complexContent>
      </xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:complexType name="ResponseMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieInoltroType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="RequestAnnullamentoInoltroMittenteType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element name="RiferimentoProvvedimento" type="xs:string"/>
    <xs:element name="Note" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseAnnullamentoInoltroMittenteType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieAnnullamentoType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AnomalieInoltroType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieInoltroEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieInoltroEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="001_ValidazioneFirma"/>
    <xs:enumeration value="002_AnomaliaImpronte"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AnomalieAnnullamentoType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieAnnullamentoEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieAnnullamentoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibilita"/>
    <xs:enumeration value="007_ErroreIdentificatoreNonTrovato"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>
</wsdl:types>

<wsdl:message name="RequestMessageInoltro">
  <wsdl:part element="tns:RequestMessageInoltro" name="parameters"> </wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseMessageInoltro">
  <wsdl:part element="tns:ResponseMessageInoltro" name="parameters"> </wsdl:part>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</wsdl:message>

<wsdl:message name="RequestAnnullamentoInoltroMittente">
  <wsdl:part element="tns:RequestAnnullamentoInoltroMittente" name="parameters">
</wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseAnnullamentoInoltroMittente">
  <wsdl:part element="tns:ResponseAnnullamentoInoltroMittente" name="parameters">
</wsdl:part>
</wsdl:message>

<wsdl:portType name="ProtocolloDestinatarioPortType">
  <wsdl:operation name="MessaggioInoltro">
    <wsdl:input message="tns:RequestMessageInoltro" name="RequestMessageInoltro">
</wsdl:input>
    <wsdl:output message="tns:ResponseMessageInoltro" name="ResponseMessageInoltro">
</wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="AnnullamentoInoltroMittente">
    <wsdl:input message="tns:RequestAnnullamentoInoltroMittente"
name="RequestAnnullamentoInoltroMittente"> </wsdl:input>
    <wsdl:output message="tns:ResponseAnnullamentoInoltroMittente"
name="ResponseAnnullamentoInoltroMittente"> </wsdl:output>
  </wsdl:operation>
</wsdl:portType>

<wsdl:binding name="ProtocolloDestinatarioServiceBinding"
type="tns:ProtocolloDestinatarioPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="MessaggioInoltro">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestMessageInoltro">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseMessageInoltro">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="AnnullamentoInoltroMittente">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestAnnullamentoInoltroMittente">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseAnnullamentoInoltroMittente">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:service name="ProtocolloDestinatarioService">
  <wsdl:port binding="tns:ProtocolloDestinatarioServiceBinding"
name="ProtocolloDestinatarioService">
    <soap:address location="http://localhost:8080/proto-test/protocollo/destinatario"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

### 5.3. messaggio\_protocollo.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
  xmlns:prot="http://www.agid.gov.it/protocollo/"
  targetNamespace="http://www.agid.gov.it/protocollo/messaggi/"
  elementFormDefault="qualified"
  attributeFormDefault="qualified"
  >

  <xsd:complexType name="MessaggioProtocolloType">
    <xsd:sequence>
      <xsd:element name="Segnatura" type="prot:SegnaturaInformaticaType"/>
      <xsd:element name="Documento" type="msgprot:FileType"/>
      <xsd:element name="Allegato" type="msgprot:FileType" minOccurs="0"
maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="FileType">
    <xsd:simpleContent>
      <xsd:extension base="xsd:base64Binary">
        <xsd:attribute name="nomeFile" type="xsd:string" use="required"/>
        <xsd:attribute name="mimeType" type="xsd:string" use="required"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

</xsd:schema>
```

# **Comunicazione tra AOO di Documenti Amministrativi Protocollati.**

*Allegato 6 al documento “Linee  
Guida sulla formazione, gestione e  
conservazione dei documenti  
informatici”.*

## Indice del documento

1. Scopo ed ambito di applicazione	3
1.1. Note di lettura del documento	4
2. Messaggio di protocollo	5
2.1. Struttura della segnatura di protocollo	6
2.1.1. Intestazione	6
2.1.2. Descrizione	6
2.1.3. Signature	7
2.2. Regole di processamento	7
3. Flussi di comunicazione	9
3.1. Regole di processamento	10
3.1.1. Inoltro di un messaggio protocollato	10
3.1.2. Annullamento protocollazione mittente	11
3.1.3. Annullamento protocollazione destinatario	12
4. APPENDICE A - XML Schema della segnatura di protocollo	13
4.1. Segnatura di protocollo XML Schema	13
5. APPENDICE B - Interfacce di servizio SOAP	22
5.1. protocollo-mittente.wsdl	22
5.2. protocollo-destinatario.wsdl	25
5.3. messaggio_protocollo.xsd	27

# 1. Scopo ed ambito di applicazione

Il “Sistema di Gestione Informatica dei Documenti” è utilizzato da una Pubbliche Amministrazioni (di seguito *PA*) per gestire il ciclo di vita dei “Documenti Amministrativi Informatici”, a partire dalla loro formazione/ricezione per giungere alla loro archiviazione e/o trasmissione, nell’esercizio delle proprie funzioni istituzionali.

Con “Protocollo Informatico” indichiamo la componente software del sistema di “Sistema di Gestione Informatica dei Documenti” che assicura la gestione contemporanea della registrazione di protocollo e segnatura di protocollo.

Nel dettaglio il “Protocollo Informatico” assicura le seguenti azioni:

- produzione della segnatura di protocollo, cioè l'apposizione o l'associazione all'originale del documento, in forma permanente non modificabile, dei metadati riguardanti il documento stesso funzionali alla ricezione o spedizione dalle pubbliche amministrazioni;
- registrazione di protocollo, cioè l'attività di memorizzazione dei dati necessari a conservare le informazioni per ogni documento ricevuto o spedito dalle pubbliche amministrazioni.

La strategia per la digitalizzazione della PA, e non da ultimo le indicazioni riportate nel “Piano Triennale per l'Informatica nella Pubblica Amministrazione”, individuano l'esigenza di favorire l'interazione tra i sistemi informatici delle PA che, nel presente allegato, si concretizza nella comunicazione tra le Aree Organizzative Omogenee (AOO) della medesima PA o appartenenti a differenti PA.

Di seguito, quale presupposto all'esigenza di ricezione e spedizione espressa in precedenza, sono definite le tipologia e la rappresentazione (formati dati) delle informazioni associate ai documenti amministrativi informatici protocollati che costituiscono la segnatura di protocollo. La rappresentazione formale degli stessi è realizzata attraverso l'utilizzo degli XML Schema nel rispetto delle specifiche W3C:

- W3C XML Schema Definition Language (XSD) 1.1 Part 1: Structures<sup>1</sup>
- W3C XML Schema Definition Language (XSD) 1.1 Part 2: Datatypes<sup>2</sup>

In attuazione di quanto disposto dell'art. 47 del D.Lgs. 82/2005, relativamente alle comunicazione tra amministrazioni, di documenti amministrativi informatici protocollati, sono individuate le modalità tecniche per assicurare il trasporto di documenti amministrativi informatici tra AOO della pubblica amministrazione.

I formati dati e le modalità tecniche per il trasporto indicati nel presente allegato verranno adeguati in relazione all'evoluzione tecnologica e alle eventuali ulteriori esigenze che le amministrazioni dovessero manifestare a seguito della loro applicazione.

---

<sup>1</sup> <https://www.w3.org/TR/xmlschema11-1/>

<sup>2</sup> <https://www.w3.org/TR/xmlschema11-2/>

Il presente documento abroga e sostituisce la circolare 60/2103 dell'AgID in materia di "Formato e definizione dei tipi di informazioni minime ed accessorie associate ai messaggi scambiati tra le Pubbliche Amministrazioni".

### 1.1. Note di lettura del documento

Nella definizione dei requisiti, delle specifiche e delle regole descritte nei documenti precedentemente indicati sono utilizzate le parole chiave DEVE, NON DEVE, OBBLIGATORIO, VIETATO, DOVREBBE, CONSIGLIATO, NON DOVREBBE, SCONSIGLIATO, POTREBBE, OPZIONALE che devono essere interpretate in conformità con RFC 2119<sup>3</sup> dell'Internet Engineering Task Force. In particolare:

- DEVE, OBBLIGATORIO significano che la definizione è un requisito assoluto, la specifica deve essere implementata, la consegna è inderogabile.
- DOVREBBE, CONSIGLIATO significano che in particolari circostanze possono esistere validi motivi per ignorare un requisito, non implementare una specifica, derogare alla consegna, ma che occorre esaminare e valutare con attenzione le implicazioni correlate alla scelta.
- PUÒ, OPZIONALE significano che un elemento della specifica è a implementazione facoltativa.
- NON DOVREBBE, SCONSIGLIATO significano che in particolari circostanze possono esistere validi di motivi per cui un elemento di specifica è accettabile o persino utile, ma, prima di implementarlo, le implicazioni correlate dovrebbero essere esaminate e valutate con attenzione.
- NON DEVE, VIETATO significano che c'è proibizione assoluta di implementazione di un determinato elemento di specifica.

---

<sup>3</sup> <https://www.ietf.org/rfc/rfc2119.txt>

## 2. Messaggio di protocollo

Lo scambio di documenti amministrativi protocollati tra AOO vede coinvolti:

- il *mittente*, l'AOO che invia i documenti amministrativi protocollati;
- il *destinatario*, l'AOO che riceve i documenti amministrativi protocollati.

Un *messaggio di protocollo*, l'elemento atomico di interesse per dare seguito allo scambio di documenti amministrativi protocollati tra AOO, è una struttura logica che:

- DEVE contenere il documento amministrativo informatico principale (di seguito *documento principale*);
- PUÒ contenere un numero qualsiasi di documenti amministrativi informatici allegati (di seguito *allegati*);
- DEVE contenere la segnatura di protocollo del messaggio protocollato (di seguito *segnatura di protocollo*).

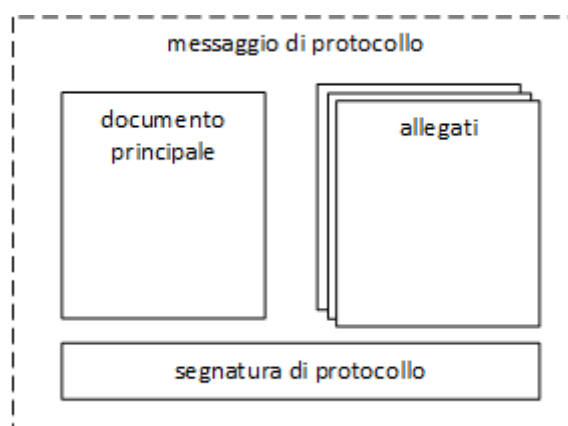


Figure 1. Struttura logica del "messaggio di protocollo"

Il *documento principale* e gli eventuali *allegati* DEVONO essere formati nel rispetto delle regole di formazione dei documenti amministrativi informatici.

La *segnatura di protocollo* DEVE essere formata nel rispetto di quanto indicato al successivo paragrafo [2.1 Struttura segnatura di protocollo](#).

La *segnatura di protocollo* DEVE essere associata in forma permanente al *documento principale* e agli *allegati* che con esso formano il *messaggio di protocollo*. A tal fine sistema informatico dell'AOO mittente:

- DEVE riportare nella *segnatura di protocollo* l'impronta del *documento principale* e, se presenti, degli *allegati*;
- DEVE assicurare l'autenticità e integrità della *segnatura di protocollo* attuando le regole tecniche in materia di firma elettronica dei documenti informatici emanate dall'AgID conformemente al regolamento UE n° 910/2014, nel dettaglio applicando un "sigillo elettronico qualificato" previsti alla sezione 5 del regolamento UE n° 910/2014 utilizzando il profilo XAdES baseline B level signatures definito in [ETSI EN 319 132-1 v1.1.1](#).

Il controllo della validità amministrativa del *documento principale*, degli *allegati* e dei dati riportati nella *segnatura di protocollo*:

- è di responsabilità della AOO mittente;
- DEVE essere effettuato prima della composizione del *messaggio di protocollo*.

Per assicurare la non ripudiabilità dello scambio tra AOO, le informazioni della *segnatura di protocollo* DEVONO essere memorizzate nel sistema di gestione dei documenti della AOO mittente e in quello delle AOO destinataria. L'indicata azione di memorizzazione è assicurata dalla registrazione di protocollo realizzata dal "Protocollo informatico".

### 2.1. Struttura della segnatura di protocollo

La *segnatura di protocollo* DEVE prevedere le seguenti sezioni:

- "Intestazione", contiene i dati identificativi e le informazioni fondamentali del messaggio;
- "Descrizione", contiene le informazioni descrittive riguardanti il contenuto del messaggio;
- "Signature" per permettere la firma della segnatura di protocollo conformemente al profilo XAdES baseline B level signatures.

Di seguito sono indicate la natura delle informazioni presenti nelle sezioni della *segnatura di protocollo*.

Le AOO mittenti che predispongono la *segnatura di protocollo* DEVONO assicurare la conformità rispetto all'XML Schema riportato nell'[Appendice A](#).

#### 2.1.1. Intestazione

La sezione "Intestazione" DEVE contenere gli elementi essenziali di identificazione e caratterizzazione amministrativa del *messaggio di protocollato*.

In particolare, la sezione contiene l'*Identificatore* della registrazione relativa al messaggio protocollato in uscita. Tale identificatore riporta i seguenti dati:

- a) indicazione della amministrazione mittente;
- b) indicazione della AOO mittente;
- c) indicazione del registro nell'ambito del quale è stata effettuata la registrazione;
- d) numero progressivo di protocollo;
- e) data di registrazione;
- f) l'oggetto del messaggio di protocollo;
- g) la classificazione del messaggio di protocollo;
- h) il fascicolo del messaggio di protocollo.

#### 2.1.2. Descrizione

La sezione "Descrizione" DEVE contenere le informazioni che descrivono i corrispondenti (mittente e destinatario) interessati nello scambio e i riferimenti al *documento principale* e agli eventuali *allegati* del *messaggio di protocollo*.

In particolare, contiene l'impronta informatica del *documento principale* e degli eventuali *allegati* necessari per associarli in forma permanente alla *segnatura di protocollo*.

### 2.1.3. Signature

La sezione "Signature" DEVE contenere le informazioni per assicurare la firma della *segnatura di protocollo* da parte della AOO mittente per assicurare l'autenticità e integrità.

## 2.2. Regole di processamento

Il flusso di processamento che le AOO mittenti devono realizzare per assicurare la formazione del *messaggio di protocollo* è di seguito riportato:

- A. Formazione del *documento principale (document)*, ed eventuali *allegati (attachment<sub>i</sub>)*, DEVONO rispettare le regole di formazione dei documenti amministrativi elettronici, inclusa la classificazione.
- B. Calcolo dell'impronta del *documento principale (digest(document,algorithm))*, e degli eventuali *allegati (digest(attachment<sub>i</sub>,algorithm))*, che DEVONO utilizzare uno degli algoritmi indicati nella seguente tabella 1.
- C. Generazione del numero di protocollo da assegnare al *messaggio di protocollo*.
- D. Formazione della *segnatura di protocollo* che DEVE rispettare l'XML Schema indicato nell'[Appendice A](#), utilizzando le impronte *digest(document,algorithm)* e *digest(attachment<sub>i</sub>,algorithm)* create al passo B.
- E. Apposizione di un "sigillo elettronico qualificato" alla *segnatura di protocollo per* garantire l'integrità e autenticità che DEVE applicare il profilo XAdES baseline B level signatures definito in [ETSI EN 319 132-1 v1.1.1](#).

Nota: L'AOO mittente assicura l'atomicità<sup>4</sup> delle operazione da C a E.

Tabella 1 - Digest algorithm

SIGLA	URI
SHA-224	<a href="http://www.w3.org/2001/04/xmldsig-more#sha224">http://www.w3.org/2001/04/xmldsig-more#sha224</a>
SHA-256	<a href="http://www.w3.org/2001/04/xmlenc#sha256">http://www.w3.org/2001/04/xmlenc#sha256</a>
SHA-384	<a href="http://www.w3.org/2001/04/xmldsig-more#sha384">http://www.w3.org/2001/04/xmldsig-more#sha384</a>

<sup>4</sup> le operazioni sono eseguite in maniera indivisibile da un punto di vista logico, in breve o sono eseguite tutte o non è eseguita nessuna

**Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati**

SHA-512	<a href="http://www.w3.org/2001/04/xmlenc#sha512">http://www.w3.org/2001/04/xmlenc#sha512</a>
HMAC-SHA-224	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha224">http://www.w3.org/2001/04/xmldsig-more#hmac-sha224</a>
HMAC-SHA-256	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha256">http://www.w3.org/2001/04/xmldsig-more#hmac-sha256</a>
HMAC-SHA-384	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha384">http://www.w3.org/2001/04/xmldsig-more#hmac-sha384</a>
HMAC-SHA-512	<a href="http://www.w3.org/2001/04/xmldsig-more#hmac-sha512">http://www.w3.org/2001/04/xmldsig-more#hmac-sha512</a>

### 3. Flussi di comunicazione

Le esigenze di comunicazione tra AOO mittente e AOO destinataria per assicurare l'inoltro di un messaggio protocollato richiedono:

- *inoltro di un messaggio protocollato (MessaggioInoltro)* da una AOO mittente ad una AOO destinataria e la relativa conferma, anche la gestione dei due casi di annullamento possibili:
- *annullamento protocollazione mittente (AnnullamentoInoltroMittente)*, nel caso in cui successivamente all'inoltro l'AOO mittente adotti un provvedimento per il suo annullamento;
- *annullamento protocollazione destinatario (AnnullamentoInoltroDestinatario)*, nel caso in cui successivamente alla conferma di ricezione l'AOO destinataria adotti un provvedimento per il suo annullamento.

Le esigenze di comunicazione individuate sono sintetizzate nel seguente UML sequence diagram.



Figure 2. Comunicazioni tra AOO mittente e AOO destinatario

Per dare seguito alla comunicazione tra AOO mittente e AOO destinataria, le stesse possono adottare una delle modalità previste dalla norma:

- *posta elettronica*, in cui il *messaggio di protocollo* (documento, allegati e segnatura di protocollo) è trasportato come allegato della stessa e il contenuto del messaggio di posta elettronica NON DEVE intendersi come parte del *messaggio di protocollo*;
- *cooperazione applicativa*, utilizzando il Simple Object Access Protocol assicurando l'implementazione delle interfacce di servizio riportate nell'[Appendice B](#).

Per assicurare la comunicazione tra AOO le Amministrazioni DEVONO registrare e mantenere aggiornato, per ogni AOO individuata nella propria organizzazione, l'Indice dei domicili digitali delle pubbliche amministrazioni e dei gestori di pubblici servizi (IPA)<sup>5</sup> (di seguito IPA) con:

- indirizzo di *posta elettronica certificata*;
- *endpoint* di esposizione dei servizi indicati nell'[Appendice B](#).

### 3.1. Regole di processamento

I flussi di processamento che le AOO mittenti e destinatari devono realizzare per assicurare l'inoltro e ricezione dei messaggi protocollati sono riportate di seguito.

Si precisa che ogni flusso di seguito indicato è da ritenersi completo quando l'intero set di messaggi previsto dallo specifico flusso è stato scambiato. Si precisa che non è possibile avviare i flussi di annullamento (**AnnullamentoInoltroMittente** e **AnnullamentoInoltroDestinatario**) prima del completamento del flusso di inoltro (**MessaggioInoltro**).

#### 03.1.1. Inoltro di un messaggio protocollato

##### A. AOO mittente: Inoltro *messaggio di protocollo*

L'AOO mittente DEVE produrre il *messaggio di protocollo*, come indicato nel precedente [paragrafo 2](#) e inoltrare lo stesso alla AOO destinataria.

##### B. AOO destinatario: Riceve *messaggio di protocollo*

L'AOO destinatario ricevuto il *messaggio di protocollo* DEVE verificare la *segnatura di protocollo*, nel dettaglio:

- DEVE verificare la correttezza della firma della *segnatura di protocollo*;
- DEVE verificare la corrispondenza dell'impronta del *documento principale* presente nella *segnatura di protocollo* e il documento *principale* ricevuto;
- se presenti *allegati*, per ogni allegato DEVE verificare la corrispondenza dell'impronta dell'*allegato* presente nella *segnatura di protocollo* e l'allegato ricevuto.

Se l'AOO destinataria è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE rispondere indicando l'Identificatore associato dalla AOO mittente.

Se l'AOO destinataria non è riuscita a verificare il *messaggio di protocollo* ricevuto DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

- se la firma della *segnatura di protocollo* non è verificata DEVE restituire l'anomalia 001\_ValidazioneFirma;
- se almeno una delle impronte riportate nella *segnatura di protocollo* (*documento principale* e *allegati*) non è verificata DEVE restituire l'anomalia 002\_AnomaliaImpronta.

---

<sup>5</sup> <https://www.indicepa.gov.it/>

- C. AOO destinatario: Inoltro conferma di protocollazione del *messaggio di protocollo*  
L'AOO destinataria DEVE inoltrare conferma di protocollazione del *messaggio di protocollo* alla AOO mittente a conclusione del processo di protocollazione in ingresso.

L'AOO destinataria PUO' effettuare il controllo dei file ricevuti (*documento principale e allegati*) ed in caso di anomalie DEVE segnalare alla AOO mittente l'anomalia riscontrata è nel dettaglio:

- a. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta non leggibile DEVE restituire l'anomalia 003\_DocumentoAllegatiNonLeggibili.
- b. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta firmato e la validazione della stessa fallisce DEVE restituire l'anomalia 004\_DocumentoAllegatiErroreValidazioneFirma.
- c. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta con marca temporale e la validazione della stessa fallisce DEVE restituire l'anomalia 005\_DocumentoAllegatiErroreValidazioneMarcaTemporale.
- d. se almeno uno dei file ricevuto (*documento principale e allegati*) risulta con sigillo elettronico e la validazione dello stesso fallisce DEVE restituire l'anomalia 006\_DocumentoAllegatiErroreValidazioneSigillo.

AOO destinataria DEVE verificare la ricevibilità del *messaggio di protocollo* ricevuto, ed in caso negativo DEVE restituire l'anomalia 000\_Irricevibile e l'indicazione della motivazione di irricevibilità.

AOO destinatario DEVE generare il numero di protocollo per *messaggio di protocollo* ricevuto e, contemporaneamente, memorizzare lo stesso nel registro di protocollo in ingresso.

L'AOO destinatario DEVE inoltrare la conferma di protocollazione del *messaggio di protocollo* ricevuto includendo l'Identificatore associato dal AOO mittente e l'Identificatore da essa associato.

- D. AOO mittente: Ricezione della conferma di protocollazione del *messaggio di protocollo*

Nel caso in cui l'AOO destinatario non segnali anomalie l'AOO mittente DEVE memorizzare la conferma di protocollazione del *messaggio di protocollo* nel registro di protocollo per assicurare la persistenza dello stesso.

Nel caso in cui l'AOO destinatario segnali anomalie l'AOO mittente DEVE ritenere la transazione non conclusa.

### 3.1.2. Annullamento protocollazione mittente

- A. AOO mittente: Inoltro messaggio annullamento

L'AOO mittente DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente inviato:

- indicando l'Identificatore associato da essa al momento dell'inoltro e l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

**B. AOO destinatario: Inoltro ricevuta annullamento**

L'AOO destinatario DEVE inoltrare la ricevuta di annullamento di un *messaggio di protocollo* precedentemente ricevuto.

L'AOO destinataria assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000\_Irricevibile indicando il motivo di irricevibilità;
- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l'anomalia 007\_ErroreIdentificatoreNonTrovato.

### 3.1.3. Annullamento protocollazione destinatario

**A. AOO destinatario: Inoltro messaggio annullamento**

L'AOO destinatario DEVE inoltrare la richiesta di annullamento di un *messaggio di protocollo* precedentemente ricevuto:

- indicando l'Identificatore associato dalla AOO mittente al momento dell'inoltro e l'Identificatore associato da esso indicato nella ricevuta di ricezione del *messaggio di protocollo* inoltrata al mittente;
- riportando il riferimento al provvedimento che determina il presupposto amministrativo per l'annullamento.

**B. AOO mittente: Inoltro ricevuta annullamento**

L'AOO mittente DEVE inoltrare la ricevuta di annullamento di un *messaggio di protocollo* precedentemente inviato.

L'AOO mittente assicura che nella ricevuta di annullamento:

- DEVE indicare l'Identificatore associato da essa al momento dell'inoltro e l'Identificatore associato dal destinatario indicato nella ricevuta di ricezione del *messaggio di protocollo*;
- nel caso di irricevibilità dell'annullamento DEVE restituire l'anomalia 000\_Irricevibile indicando il motivo di irricevibilità;
- nel caso in cui non risulti il *messaggio di protocollo* DEVE restituire l'anomalia 007\_ErroreIdentificatoreNonTrovato.

## 4. APPENDICE A - XML Schema della segnatura di protocollo

Di seguito è riportato XML Schema della *segnatura di protocollo* che le AOO delle pubbliche amministrazioni adottano.

Per favorire l'utilizzo del XML Schema lo stesso è riportato nel repository github pubblico consultabile all'URL <https://github.com/AgID/protocollo-comunicazione-ao>.

### 4.1. Segnatura di protocollo XML Schema

```
<?xml version="1.0" encoding="UTF-8" standalone="no"?>
<xs:schema
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:prot="http://www.agid.gov.it/protocollo/"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"

  targetNamespace="http://www.agid.gov.it/protocollo/"

  elementFormDefault="qualified"
  attributeFormDefault="qualified"

  version="3.0"
  >

  <xs:element name="SegnaturaInformatica" type="prot:SegnaturaInformaticaType"/>

  <xs:complexType name="SegnaturaInformaticaType">
    <xs:annotation>
      <xs:documentation>
        La segnatura di protocollo contiene i dati relativi ad un
        messaggio di protocollo.

        Un messaggio di protocollo è determinato da:
        - documento principale
        - eventuali allegati
        - la segnatura di protocollo qui definita

        La segnatura di protocollo è associata in forma permanente al
        documento principale e agli allegati che con esso formano il messaggio di protocollo
        includendo nella segnatura di protocollo le impronte (digest)
        del documento principale e degli allegati e assicurando l'autenticità e integrità
        della segnatura di protocollo firmando la stessa implementando
        il profilo XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1.

        La segnatura di protocollo è caratterizzata da:
        - Intestazione, i dati necessari per individuare univocamente il
        messaggio di protocollo

        - Descrizione, i dati aggiuntivi del messaggio di protocollo
        - Signature, i dati e metadati della firma dell'XML (profilo
        XAdES baseline B level signatures definito in ETSI EN 319 132-1 v1.1.1)
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="Intestazione" type="prot:IntestazioneType"/>

      <xs:element name="Descrizione" type="prot:DescrizioneType"/>

      <xs:element ref="ds:Signature"/>
    </xs:sequence>
    <xs:attribute name="versione" type="xs:NMTOKEN" fixed="3.0.0" use="required"/>
  </xs:complexType>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:attribute name="lang" type="xs:NMTOKEN" fixed="it" use="required"/>
</xs:complexType>

<xs:complexType name="IntestazioneType">
  <xs:annotation>
    <xs:documentation>
      L'intestazione contiene i dati essenziali per l'identificazione
      e caratterizzazione amministrativa del messaggio di protocollato.

      L'intestazione è caratterizzata da:
      - Identificatore, i dati per identificare univocamente il
      messaggio di protocollo conformemente in attuazione all'art. 55 del DPR 445/2000
      - Oggetto, sintesi dei contenuti di carattere giuridico,
      amministrativo e narrativo di un documento
      - Classifica, la categoria del Titolare di classificazione
      associato al messaggio di protocollo
      - Fascicolo, opzionalmente, il fascicolo entro cui è presente il
      messaggio di protocollo
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Identificatore" type="prot:IdentificatoreType"/>
    <xs:element name="Oggetto" type="xs:string"/>

    <xs:element name="Classifica" type="prot:ClassificaType" />

    <xs:element name="Fascicolo" type="prot:FascicoloType" minOccurs="0" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="IdentificatoreType">
  <xs:annotation>
    <xs:documentation>
      Contiene i dati identificativi della segnatura di protocollo.

      L'identificativo è caratterizzato da:
      - CodiceAmministrazione, il codice IPA
      dell'amministrazione
      - CodiceAOO, il codice IPA dell'AOO
      - CodiceRegistro, il codice del Registro
      - NumeroRegistrazione, il progressivo di protocollo
      - DataRegistrazione, la data di registrazione
      - OraRegistrazione, in maniera opzionale l'ora di
      registrazione
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="CodiceAmministrazione" type="prot:CodiceIPA"/>
    <xs:element name="CodiceAOO" type="prot:CodiceIPA"/>
    <xs:element name="CodiceRegistro" type="prot:CodiceRegistroType"/>
    <xs:element name="NumeroRegistrazione"
    type="prot:NumeroRegistrazioneType"/>
    <xs:element name="DataRegistrazione" type="xs:date"/>
    <xs:element name="OraRegistrazione" type="xs:time" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="CodiceIPA">
  <xs:annotation>
    <xs:documentation>
      Contiene il codice IPA dell'amministrazione o dell'AOO indica
      all'amministrazione e, in maniera opzionale, la descrizione della stessa.
    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="descrizione" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="FascicoloType">
  <xs:annotation>
    <xs:documentation>
      Il fascicolo riporta il riferimento al fascicolo prevedendo la
      Denominazione e il relativo CodiceFascicolo
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Denominazione" type="xs:string"/>
    <xs:element name="CodiceFascicolo" type="xs:string"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ClassificaType">
  <xs:annotation>
    <xs:documentation>
      La classificazione riporta il valore attribuito al messaggio di
      protocollo.

      La classificazione è caratterizzata da:
      - Denominazione, una descrizione della classificazione
      attribuita
      - In alternativa il codice di classificazione può essere
      rappresentato:
      - CodiceFlat, l'unione in un'unico element di categoria,
      classe ed eventuale sottoclasse
      es. <CodiceFlat>Titolo I.Classe 1</CodiceFlat>
      - CodicePath, la separazione in differenti element di
      categoria, classe ed eventuale sottoclasse
      es. <CodicePath>
          <Livello>Titolo I</Livello>
          <SubLivello>
            <Livello>Classe
            1</Livello>
          </SubLivello>
        </CodicePath>
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Denominazione" type="xs:string"/>
    <xs:choice>
      <xs:element name="CodiceFlat" type="xs:string"/>
      <xs:element name="CodicePath" type="prot:LivelloType"/>
    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="LivelloType">
  <xs:annotation>
    <xs:documentation>
      Il livello riporta i dati relativi alla categoria, classe ed
      eventuale sottoclasse

      Il livello è composto dal codice della categoria, classe ed
      eventuale sottoclasse e la relativa descrizione
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Livello">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```

                                                                 <xs:attribute name="descrizione"
type="xs:string"/>
                                                                 </xs:extension>
                                                                 </xs:simpleContent>
                                                                 </xs:complexType>
                                                                 </xs:element>
                                                                 <xs:element name="SubLivello" type="prot:LivelloType" minOccurs="0"/>
                                                                 </xs:sequence>
                                                                 </xs:complexType>

<xs:complexType name="DescrizioneType">
  <xs:annotation>
    <xs:documentation>
      La descrizione contiene i dati descrittivi del messaggio di
protocollato.

      La descrizione è caratterizzata da:
      - Mittente, riferimento del mittente (organizzazione o persona)
      - Destinatario, riferimento del destinatario (organizzazione o
persona)
      - DocumentoPrimario, riferimento al documento primario del
messaggio di protocollo
      - Allegato, riferimento ad uno degli allegati del messaggio di
protocollo se presente
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Mittente" type="prot:SoggettoType" minOccurs="0"/>
    <xs:element name="Destinatario" type="prot:SoggettoType" minOccurs="1"
maxOccurs="unbounded"/>
    <xs:element name="DocumentoPrimario" type="prot:DocumentoType"/>

    <xs:element name="Allegato" type="prot:DocumentoType" minOccurs="0"
maxOccurs="unbounded"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="DocumentoType">
  <xs:annotation>
    <xs:documentation>
      Il documento contiene i dati per referenziare un documento
(documento primario o allegato) del messaggio di protocollo

      Il documento è caratterizzato da:
      - Descrizione, la descrizione del contenuto dello specifico
documento
      - Impronta, l'impronta digitale (digest) del documento
      - nomeFile, il nome del file relativo al documento
      - mimeType, il mime type (RFC 6838) associato al documento
      - firmatoDigitalmente, flag per indicare il documento è firmato
digitalmente (sezione 4 Regolamento UE 910/2014)
      - sigillatoElettronicamente, flag per indicare che al documento
è apposto un sigillo elettronico (sezione 5 Regolamento UE 910/2014)
      - marcaturaTemporale, flag per indicare che al documento è
apposta una marca temporale (sezione 6 Regolamento UE 910/2014)
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Descrizione" type="xs:string" minOccurs="0"/>
    <xs:element name="Impronta" type="prot:ImprontaType"/>

  </xs:sequence>
  <xs:attribute name="nomeFile" type="xs:string" use="required"/>
  <xs:attribute name="mimeType" type="xs:string" use="required"/>
  <xs:attribute name="firmatoDigitalmente" type="xs:boolean"/>
  <xs:attribute name="marcaturaTemporale" type="xs:boolean"/>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:attribute name="sigillatoElettronicamente" type="xs:boolean"/>
</xs:complexType>

<xs:complexType name="SoggettoType">
  <xs:annotation>
    <xs:documentation>
      Il soggetto contiene i dati per referenziare un corrispondente

      Sulla base delle necessità è possibile indicare:
      - una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPA">Organizzazione</Riferimento>
          </Organizzazione>

      - una specifica unità organizzativa di una
organizzazone
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPAOrganizzazione">Organizzazione</Riferimento>
          <UnitaOrganizzativa>
            <Descrizione
codiceIPA="codiceIPAUnitaOrganizzativa">UnitaOrganizzativa</Descrizione>
          </UnitaOrganizzativa>
          </Organizzazione>

      - una persona fisica
        es. <Persona>...</Persona>
      - una persona fisica relativa ad una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPA">Organizzazione</Riferimento>
          <Persona>...</Persona>
          </Organizzazione>

      - una persona fisica relativa ad una specifica unità
organizzativa di una organizzazione
        es. <Organizzazione>
          <Riferimento
codiceIPA="codiceIPAOrganizzazione">Organizzazione</Riferimento>
          <UnitaOrganizzativa>
            <Descrizione
codiceIPA="codiceIPAUnitaOrganizzativa">UnitaOrganizzativa</Descrizione>
          <Persona>...</Persona>
          </UnitaOrganizzativa>
          </Organizzazione>

      Il soggetto è caratterizzato da:
      - il alternativa:
        - Organizzazione, un'organizzazione
    </xs:documentation>
  </xs:annotation>
  <xs:choice>
    <xs:element name="Organizzazione" type="prot:OrganizzativaType"/>
    <xs:element name="Persona" type="prot:PersonaType"/>
  </xs:choice>
</xs:complexType>

<xs:complexType name="OrganizzativaType">
  <xs:annotation>
    <xs:documentation>
      L'organizzativa contiene i dati di un'unità organizzativa o
unità organizzativa

      L'unità organizzativa è caratterizzata da:
      - Nome, il nome dell'unità organizzativa
      - in alternativa:
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```

- UnitaOrganizzativa, una sottounità organizzativa di
livello inferiore
- Persona, il riferimento ad una persona fisica
  </xs:documentation>
</xs:annotation>
<xs:sequence>
  <xs:element name="Riferimento" type="prot:NomeOrganizzazioneType"/>
  <xs:choice minOccurs="0">
    <xs:element name="UnitaOrganizzativa"
type="prot:OrganizzativaType"/>
    <xs:element name="Persona" type=" prot:PersonaType "/>
  </xs:choice>
</xs:sequence>
</xs:complexType>

<xs:complexType name="NomeOrganizzazioneType">
  <xs:annotation>
    <xs:documentation>
      Il nome organizzazione contiene i riferimenti ad
un'organizzazione o unità organizzativa

      Il nome organizzazione è caratterizzata dal nome
dell'organizzazione o dell'unità organizzativa e, quando esiste, il codice IPA della stessa
    </xs:documentation>
  </xs:annotation>
  <xs:simpleContent>
    <xs:extension base="xs:string">
      <xs:attribute name="codiceIPA" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:complexType name="IndirizzoPostaleType">
  <xs:annotation>
    <xs:documentation>
      L'indirizzo contiene i dati relativi ad un'indirizzo.

      L'indirizzo è caratterizzato da:
      - Toponimo, il riferimento al nome proprio del luogo
      - Civico, il riferimento assegnato allo specifico immobile
      - CAP, il codice di avviamento postale
      - Comune, il riferimento al Comune
      - Provincia, la provincia
      - Nazione, la denominazione della nazione e il codice ISO 3166-1
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Toponimo" type="prot:ToponimoType"/>
    <xs:element name="Civico" type="xs:string"/>
    <xs:element name="CAP" type="prot:CAPType"/>
    <xs:element name="Comune" type="prot:ComuneType"/>
    <xs:element name="Nazione" default="Italia">
      <xs:complexType>
        <xs:simpleContent>
          <xs:extension base="xs:string">
            <xs:attribute name="codice3166"
default="ITA"/>
          </xs:extension>
        </xs:simpleContent>
      </xs:complexType>
    </xs:element>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ToponimoType">
  <xs:annotation>

```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:documentation>
    Il toponimo contiene il riferimento al nome proprio del luogo

    Il toponimo è caratterizzato da:
    - dug, denominazione urbanistica generica o qualificatore del
toponimo (e.g., via, viale, piazza, ecc.)
    - duf, denominazione urbanistica ufficiale o nome della strada
</xs:documentation>
</xs:annotation>
<xs:sequence>
    <xs:element name="dug" type="xs:string"/>
    <xs:element name="duf" type="xs:string"/>
</xs:sequence>
</xs:complexType>

<xs:simpleType name="CAPType">
    <xs:annotation>
        <xs:documentation>
            Il CAP contiene il codice di avviamento postale
        </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{6}"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ComuneType">
    <xs:annotation>
        <xs:documentation>
            Il Comune contiene il riferimento al Comune

            Il Comune è caratterizzato dalla denominazione del Comune e il
relativo codice ISTAT a 6 cifre
        </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
        <xs:extension base="xs:string">
            <xs:attribute name="CodiceISTAT"
type="prot:CodiceISTATComune6Type" use="required"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="CodiceISTATComune6Type">
    <xs:annotation>
        <xs:documentation>
            Il codice ISTAT del Comune a 6 cifre
        </xs:documentation>
    </xs:annotation>
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{6}"/>
    </xs:restriction>
</xs:simpleType>

<xs:complexType name="ImprontaType">
    <xs:annotation>
        <xs:documentation>
            L'impronta contiene il digest di un documento elettronico

            L'impronta è caratterizzata dalla codifica base64 del digest
calcolato applicando l'algoritmo specifico
        </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
        <xs:extension base="xs:base64Binary">
            <xs:attribute name="algoritmo" type="xs:string" default="SHA-
256"/>
        </xs:extension>
    </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:complexType name="PersonaType">
  <xs:annotation>
    <xs:documentation>
      La persona contiene i dati relativi ad una persona fisica

      La persona è caratterizzata da:
      - Nome, il nome
      - Cognome, il cognome
      - Titolo, il titolo (es. Sig., Dott., ...)
      - CodiceFiscale, il codice fiscale
      - Contatti, i contatti della persona
    </xs:documentation>
  </xs:annotation>
  <xs:sequence>
    <xs:element name="Nome" type="xs:string"/>

    <xs:element name="Cognome" type="xs:string"/>

    <xs:element name="Titolo" type="xs:string" minOccurs="0"/>
    <xs:element name="CodiceFiscale" type="prot:CodiceFiscaleType"
minOccurs="0"/>

    <xs:element name="Contatti" type="prot:ContattiType">

      </xs:element>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="ContattiType">
    <xs:annotation>
      <xs:documentation>
        L'insieme di contatti, e nel dettaglio:
        - IndirizzoPostale, un'indirizzo relativo
        - IndirizzoTelematico, un'indirizzo elettronico
        - Telefono, un contatto telefonico
      </xs:documentation>
    </xs:annotation>
    <xs:sequence>
      <xs:element name="IndirizzoPostale" type="prot:IndirizzoPostaleType"
minOccurs="0" maxOccurs="unbounded"/>
      <xs:element name="IndirizzoTelematico"
type="prot:IndirizzoTelematicoType" maxOccurs="unbounded"/>
      <xs:element name="Telefono" type="xs:string" minOccurs="0"
maxOccurs="unbounded"/>
    </xs:sequence>
  </xs:complexType>

  <xs:complexType name="IndirizzoTelematicoType">
    <xs:annotation>
      <xs:documentation>
        Un'indirizzo telematico utilizzato per la trasmissione
telematica

        I tipi di indirizzi telematici sono:
        - smtp, nel caso della posta elettronica
        - url, nel caso di interfacce di servizio (API REST o SOAP)
        - other, in casi differenti dai precedenti
      </xs:documentation>
    </xs:annotation>
    <xs:simpleContent>
      <xs:extension base="xs:string">
        <xs:attribute name="tipo" default="smtp">
          <xs:simpleType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:restriction base="xs:NMTOKEN">
    <xs:enumeration value="smtp"/>
    <xs:enumeration value="url"/>
    <xs:enumeration value="other"/>
</xs:restriction>
</xs:simpleType>
</xs:attribute>
<xs:attribute name="note" type="xs:string"/>
</xs:extension>
</xs:simpleContent>
</xs:complexType>

<xs:simpleType name="CodiceFiscaleType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Z]{6}[0-9LMNPQRSTUVWXYZ]{2}[ABCDEHLMPRST][0-9LMNPQRSTUVWXYZ]{2}[A-Z][0-9LMNPQRSTUVWXYZ]{3}[A-Z]"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="IdentificativoType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Za-z0-9_\. \-]{1,16}"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="CodiceRegistroType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[A-Za-z0-9_\. \-]{1,16}"/>
    </xs:restriction>
</xs:simpleType>

<xs:simpleType name="NumeroRegistrazioneType">
    <xs:restriction base="xs:string">
        <xs:pattern value="[0-9]{7,}"/>
    </xs:restriction>
</xs:simpleType>

</xs:schema>
```

## 5. APPENDICE B - Interfacce di servizio SOAP

Le AOO mittente e AOO destinataria, per dare seguito alla comunicazione di messaggi protocollati utilizzando il Simple Object Access Protocol, implementano le interfacce di servizio descritte nei seguenti Web Services Description Language.

Nello specifico:

- la AOO mittente DEVE implementare protocollo-mittente.wsdl;
- la AOO destinataria DEVE implementare protocollo-destinatario.wsdl.

Per favorire l'utilizzo dei WSDL gli stessi sono riportati nel repository github pubblico consultabile all'URL <https://github.com/AgID/protocollo-comunicazione-ao>.

Per l'inoltro di binary data nei messaggi SOAP si assume l'adozione del W3C Message Transmission Optimization Mechanism<sup>6</sup>.

Per l'autenticazione delle parti si adotta il profilo di iterazione "Bloccante RPC"<sup>7</sup> e la "Soluzione per confidenzialità ed autenticazione del soggetto fruitore"<sup>8</sup> per la tecnologia SOAP individuata nel modello di interoperabilità della PA assumendo l'utilizzo di certificati qualificati per il riconoscimento delle PA/AOO.

### 5.1. protocollo-mittente.wsdl

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:tns="http://ws.protocollo.comunicazione.ao.mittente/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soapbind="http://schemas.xmlsoap.org/soap/http"
  name="ProtocolloDestinatarioService"
  targetNamespace="http://ws.protocollo.comunicazione.ao.mittente/">

  <wsdl:types>

    <xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
      xmlns:prot="http://www.agid.gov.it/protocollo/"
      xmlns:tns="http://ws.protocollo.comunicazione.ao.mittente/"
      targetNamespace="http://ws.protocollo.comunicazione.ao.mittente/"
      elementFormDefault="qualified" version="1.0">

      <xs:element name="RequestConfermaMessaggioInoltro"
        type="tns:RequestConfermaMessaggioInoltroType"/>
      <xs:element name="ResponseConfermaMessaggioInoltro"
        type="tns:ResponseConfermaMessaggioInoltroType"/>
    </xs:schema>
  </wsdl:types>
</wsdl:definitions>
```

<sup>6</sup> <https://www.w3.org/TR/soap12-mtom/>

<sup>7</sup> <https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/profili-di-interazione/profilo-bloccante-rpc.html> (in via di pubblicazione)

<sup>8</sup> [https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/doc\\_04/soluzioni-di-sicurezza.html](https://docs.italia.it/italia/piano-triennale-ict/lq-modellointeroperabilita-docs/it/bozza/doc/doc_04/soluzioni-di-sicurezza.html) (in via di pubblicazione)

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:element name="RequestAnnullamentoInoltroDestinatario"
type="tns:RequestAnnullamentoInoltroDestinatarioType"/>
<xs:element name="ResponseAnnullamentoInoltroDestinatario"
type="tns:ResponseAnnullamentoInoltroDestinatarioType"/>

<xs:complexType name="RequestConfermaMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:choice>
      <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
      <xs:element name="Anomalia" type="tns:AnomalieConfermaType" />
    </xs:choice>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseConfermaMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="RequestAnnullamentoInoltroDestinatarioType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element name="RiferimentoProvvedimento" type="xs:string"/>
    <xs:element name="Note" type="xs:string"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseAnnullamentoInoltroDestinatarioType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieAnnullamentoType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AnomalieConfermaType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieConfermaEnum">
      <xs:attribute name="info" type="xs:string"/>
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieConfermaEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibile"/>
    <xs:enumeration value="003_DocumentoAllegatiNonLeggibili"/>
    <xs:enumeration value="004_DocumentoAllegatiErroreValidazioneFirma"/>
    <xs:enumeration value="005_DocumentoAllegatiErroreVaidazioneMarcaTemporale"/>
    <xs:enumeration value="006_DocumentoAllegatiErroreValidazioneSigillo"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AnomalieAnnullamentoType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieAnnullamentoEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:simpleType name="AnomalieAnnullamentoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibilita"/>
    <xs:enumeration value="007_ErroreIdentificatoreNonTrovato"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>

</wsdl:types>

<wsdl:message name="RequestConfermaMessaggioInoltro">
  <wsdl:part element="tns:RequestConfermaMessaggioInoltro" name="parameters">
  </wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseConfermaMessaggioInoltro">
  <wsdl:part element="tns:ResponseConfermaMessaggioInoltro" name="parameters">
  </wsdl:part>
</wsdl:message>

<wsdl:message name="RequestAnnullamentoInoltroDestinatario">
  <wsdl:part element="tns:RequestAnnullamentoInoltroDestinatario" name="parameters">
  </wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseAnnullamentoInoltroDestinatario">
  <wsdl:part element="tns:ResponseAnnullamentoInoltroDestinatario" name="parameters">
  </wsdl:part>
</wsdl:message>

<wsdl:portType name="ProtocolloMittentePortType">

  <wsdl:operation name="ConfermaMessaggioInoltro">
    <wsdl:input message="tns:RequestConfermaMessaggioInoltro"
name="RequestConfermaMessaggioInoltro">
    </wsdl:input>
    <wsdl:output message="tns:ResponseConfermaMessaggioInoltro"
name="ResponseConfermaMessaggioInoltro">
    </wsdl:output>
  </wsdl:operation>

  <wsdl:operation name="AnnullamentoInoltroDestinatario">
    <wsdl:input message="tns:RequestAnnullamentoInoltroDestinatario"
name="RequestAnnullamentoInoltroDestinatario">
    </wsdl:input>
    <wsdl:output message="tns:ResponseAnnullamentoInoltroDestinatario"
name="ResponseAnnullamentoInoltroDestinatario">
    </wsdl:output>
  </wsdl:operation>

</wsdl:portType>

<wsdl:binding name="ProtocolloMittenteServiceBinding" type="tns:ProtocolloMittentePortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>

  <wsdl:operation name="ConfermaMessaggioInoltro">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestConfermaMessaggioInoltro">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseConfermaMessaggioInoltro">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
</wsdl:service>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</wsdl:output>
</wsdl:operation>

<wsdl:operation name="AnnullamentoInoltroDestinatario">
  <soap:operation soapAction="" style="document"/>
  <wsdl:input name="RequestAnnullamentoInoltroDestinatario">
    <soap:body use="literal"/>
  </wsdl:input>
  <wsdl:output name="ResponseAnnullamentoInoltroDestinatario">
    <soap:body use="literal"/>
  </wsdl:output>
</wsdl:operation>

</wsdl:binding>

<wsdl:service name="ProtocolloMittenteService">
  <wsdl:port binding="tns:ProtocolloMittenteServiceBinding"
name="ProtocolloMittenteService">
    <soap:address location="http://localhost:8080/proto-test/protocollo/mittente"/>
  </wsdl:port>
</wsdl:service>

</wsdl:definitions>
```

## 5.2. protocollo-destinatario.wsdl

```
<?xml version='1.0' encoding='UTF-8'?>
<wsdl:definitions
  xmlns:xs="http://www.w3.org/2001/XMLSchema"
  xmlns:wsdl="http://schemas.xmlsoap.org/wsdl/"
  xmlns:tns="http://ws.protocollo.comunicazione.aoo.destinatario/"
  xmlns:soap="http://schemas.xmlsoap.org/wsdl/soap/"
  xmlns:soapbind="http://schemas.xmlsoap.org/soap/http"
  name="ProtocolloDestinatarioService"
  targetNamespace="http://ws.protocollo.comunicazione.aoo.destinatario/">

  <wsdl:types>

    <xs:schema
      xmlns:xs="http://www.w3.org/2001/XMLSchema"
      xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
      xmlns:prot="http://www.agid.gov.it/protocollo/"
      xmlns:tns="http://ws.protocollo.comunicazione.aoo.destinatario/"
      targetNamespace="http://ws.protocollo.comunicazione.aoo.destinatario/"
      elementFormDefault="qualified" version="1.0">

      <xs:element name="RequestMessageInoltro" type="tns:RequestMessaggioInoltroType"/>
      <xs:element name="ResponseMessageInoltro" type="tns:ResponseMessaggioInoltroType"/>

      <xs:element name="RequestAnnullamentoInoltroMittente"
type="tns:RequestAnnullamentoInoltroMittenteType"/>
      <xs:element name="ResponseAnnullamentoInoltroMittente"
type="tns:ResponseAnnullamentoInoltroMittenteType"/>

      <xs:complexType name="RequestMessaggioInoltroType">
        <xs:complexContent>
          <xs:extension base="msgprot:MessaggioProtocolloType"/></xs:extension>
        </xs:complexContent>
      </xs:complexType>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xs:complexType name="ResponseMessaggioInoltroType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieInoltroType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="RequestAnnullamentoInoltroMittenteType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element name="RiferimentoProvvedimento" type="xs:string"/>
    <xs:element name="Note" type="xs:string" minOccurs="0"/>
  </xs:sequence>
</xs:complexType>

<xs:complexType name="ResponseAnnullamentoInoltroMittenteType">
  <xs:sequence>
    <xs:element name="IdentificatoreMittente" type="prot:IdentificatoreType"/>
    <xs:element name="IdentificatoreDestinatario" type="prot:IdentificatoreType"/>
    <xs:element minOccurs="0" name="Anomalia" type="tns:AnomalieAnnullamentoType" />
  </xs:sequence>
</xs:complexType>

<xs:complexType name="AnomalieInoltroType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieInoltroEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieInoltroEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="001_ValidazioneFirma"/>
    <xs:enumeration value="002_AnomaliaImpronte"/>
  </xs:restriction>
</xs:simpleType>

<xs:complexType name="AnomalieAnnullamentoType">
  <xs:simpleContent>
    <xs:extension base="tns:AnomalieAnnullamentoEnum">
      <xs:attribute name="info" type="xs:string" />
    </xs:extension>
  </xs:simpleContent>
</xs:complexType>

<xs:simpleType name="AnomalieAnnullamentoEnum">
  <xs:restriction base="xs:string">
    <xs:enumeration value="000_Irricevibilita"/>
    <xs:enumeration value="007_ErroreIdentificatoreNonTrovato"/>
  </xs:restriction>
</xs:simpleType>

</xs:schema>
</wsdl:types>

<wsdl:message name="RequestMessageInoltro">
  <wsdl:part element="tns:RequestMessageInoltro" name="parameters"> </wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseMessageInoltro">
  <wsdl:part element="tns:ResponseMessageInoltro" name="parameters"> </wsdl:part>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
</wsdl:message>

<wsdl:message name="RequestAnnullamentoInoltroMittente">
  <wsdl:part element="tns:RequestAnnullamentoInoltroMittente" name="parameters">
</wsdl:part>
</wsdl:message>

<wsdl:message name="ResponseAnnullamentoInoltroMittente">
  <wsdl:part element="tns:ResponseAnnullamentoInoltroMittente" name="parameters">
</wsdl:part>
</wsdl:message>

<wsdl:portType name="ProtocolloDestinatarioPortType">
  <wsdl:operation name="MessaggioInoltro">
    <wsdl:input message="tns:RequestMessageInoltro" name="RequestMessageInoltro">
</wsdl:input>
    <wsdl:output message="tns:ResponseMessageInoltro" name="ResponseMessageInoltro">
</wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="AnnullamentoInoltroMittente">
    <wsdl:input message="tns:RequestAnnullamentoInoltroMittente"
name="RequestAnnullamentoInoltroMittente"> </wsdl:input>
    <wsdl:output message="tns:ResponseAnnullamentoInoltroMittente"
name="ResponseAnnullamentoInoltroMittente"> </wsdl:output>
  </wsdl:operation>
</wsdl:portType>

<wsdl:binding name="ProtocolloDestinatarioServiceBinding"
type="tns:ProtocolloDestinatarioPortType">
  <soap:binding style="document" transport="http://schemas.xmlsoap.org/soap/http"/>
  <wsdl:operation name="MessaggioInoltro">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestMessageInoltro">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseMessageInoltro">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
  <wsdl:operation name="AnnullamentoInoltroMittente">
    <soap:operation soapAction="" style="document"/>
    <wsdl:input name="RequestAnnullamentoInoltroMittente">
      <soap:body use="literal"/>
    </wsdl:input>
    <wsdl:output name="ResponseAnnullamentoInoltroMittente">
      <soap:body use="literal"/>
    </wsdl:output>
  </wsdl:operation>
</wsdl:binding>
<wsdl:service name="ProtocolloDestinatarioService">
  <wsdl:port binding="tns:ProtocolloDestinatarioServiceBinding"
name="ProtocolloDestinatarioService">
    <soap:address location="http://localhost:8080/proto-test/protocollo/destinatario"/>
  </wsdl:port>
</wsdl:service>
</wsdl:definitions>
```

### 5.3. messaggio\_protocollo.xsd

```
<?xml version="1.0" encoding="UTF-8"?>
```

## Allegato 6 - Comunicazione tra AOO di Documenti Amministrativi Protocollati

```
<xsd:schema
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:msgprot="http://www.agid.gov.it/protocollo/messaggi/"
  xmlns:prot="http://www.agid.gov.it/protocollo/"
  targetNamespace="http://www.agid.gov.it/protocollo/messaggi/"
  elementFormDefault="qualified"
  attributeFormDefault="qualified"
  >

  <xsd:complexType name="MessaggioProtocolloType">
    <xsd:sequence>
      <xsd:element name="Segnatura" type="prot:SegnaturaInformaticaType"/>
      <xsd:element name="Documento" type="msgprot:FileType"/>
      <xsd:element name="Allegato" type="msgprot:FileType" minOccurs="0"
maxOccurs="unbounded"/>
    </xsd:sequence>
  </xsd:complexType>

  <xsd:complexType name="FileType">
    <xsd:simpleContent>
      <xsd:extension base="xsd:base64Binary">
        <xsd:attribute name="nomeFile" type="xsd:string" use="required"/>
        <xsd:attribute name="mimeType" type="xsd:string" use="required"/>
      </xsd:extension>
    </xsd:simpleContent>
  </xsd:complexType>

</xsd:schema>
```