AGID
Agenzia per l'Italia Digitale

FormezPA

FORMAZIONE AGID – FORMEZ SULLA TRANSIZIONE DIGITALE DELLA PA

Progetto Informazione e formazione per la transizione digitale della PA nell'ambito del progetto «Italia Login – la casa del cittadino»

(A valere sul PON Governance e Capacità Istituzionale 2014-2020)

UNIONE EUROPEA
Dipartimento della Funzione Pubblica
PON
AGID Agenzia per l'Italia digitale

AGID
Agenzia per l'Italia Digitale

FormezPA

Ho visto firme che voi umani…

09-11-2022

Stefano Ianniello

UNIONE EUROPEA

Dipartimento della Funzione Pubblica

AGID Agenzia per l'Italia digitale

La Firma Digitale - FD

La Firma Digitale è il risultato di una procedura informatica che garantisce l'autenticità e l'integrità di messaggi e documenti scambiati e archiviati con mezzi informatici, al pari di quanto svolto dalla firma autografa per i documenti tradizionali

La Firma Digitale è nata con l'obbiettivo di trasferire su digitale il concetto di *firma autografa* su carta.

Attraverso la Firma Digitale si riescono quindi a garantire i seguenti 3 requisiti:

Autenticità	Con un documento firmato digitalmente si può essere certi dell'identità del sottoscrittore.
Integrità	Sicurezza che il documento informatico non è stato modificato dopo la sua sottoscrizione;
Non ripudio	Il documento informatico sottoscritto con firma digitale, ha piena validità legale e non può essere ripudiato dal sottoscrittore.

Accenni normativi – definizioni FD e FEQ

Codice dell'Amministrazione Digitale (D.Lgs. 7 marzo 2005 e s.m.i.)

Art. 1

***Firma Digitale*:** *un particolare tipo di firma qualificata basata su un su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.*

Regolamento (UE) 910/2014 - eIDAS

Art. 3

Firma elettronica qualificata*: una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche.*

Art. 25

2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.

In Italia "**firma elettronica qualificata**" e "**firma digitale**" sono sostanzialmente sinonimi.

Accenni normativi - mutuo riconoscimento negli Stati Membri

Con l'introduzione del Regolamento (UE) N. 910/2014 – eIDAS, assume particolare rilevanza la piena interoperabilità a livello comunitario di particolari tipologie di firme elettroniche e dei sistemi di validazione temporale note in Italia rispettivamente come ***firma digitale*** e ***marca temporale***.

Il Regolamento eIDAS all'art. 25 comma 3 prescrive che:
Una firma elettronica qualificata basata su un certificato qualificato rilasciato in uno Stato membro è riconosciuta quale firma elettronica qualificata in tutti gli altri Stati membri.

Ne deriva che obbligo di riconoscere le firme elettroniche qualificate (firma digitale) introdotto nel Regolamento eIDAS (art. 25, comma 3) deve essere onorato, altrimenti, oltre a non consentire l'esercizio di un diritto dei cittadini dell'unione, si incorre in una procedura di infrazione.

Accenni normativi - Elenchi di fiducia

A questo scopo il Regolamento eIDAS all'art. 22 ha introdotto gli **Elenchi di fiducia.**

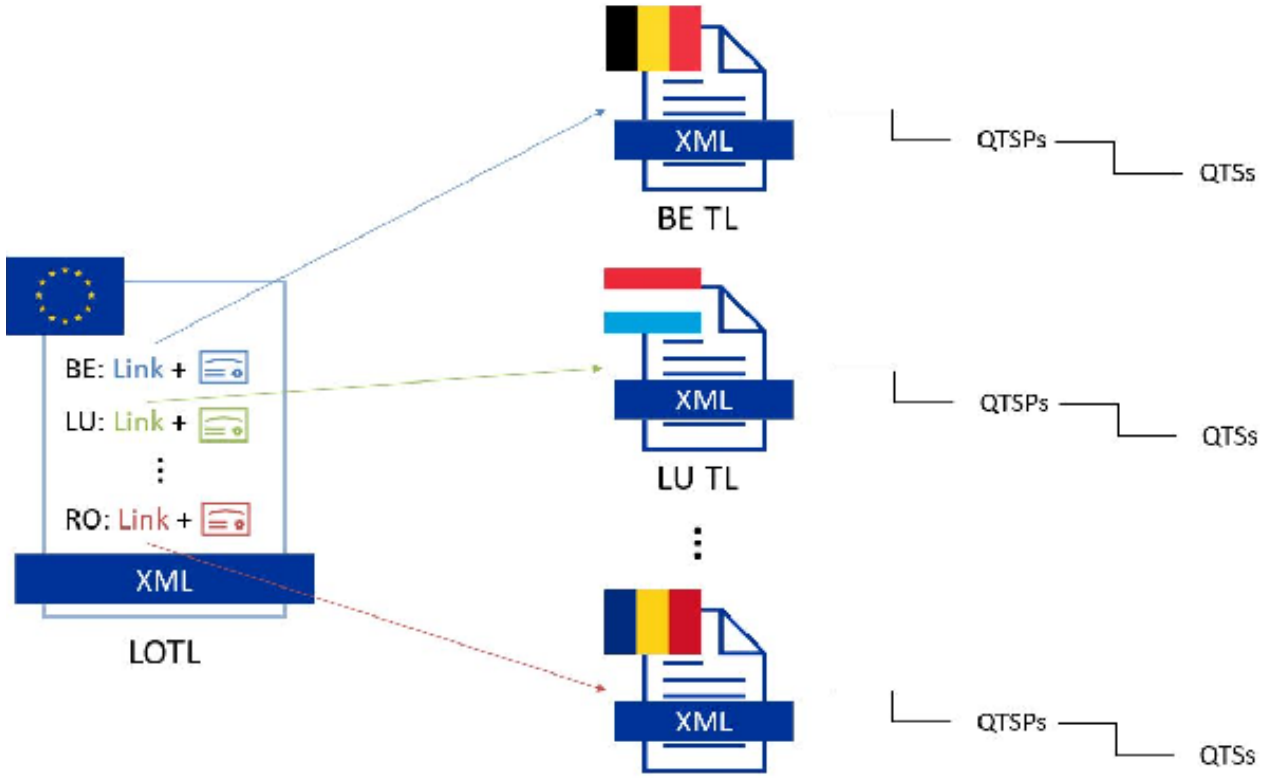
Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia, che includono le informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono responsabili, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati.

In altre parole un fornitore/servizio sarà qualificato solo se compare negli elenchi di fiducia. Di conseguenza, gli utenti (cittadini, imprese o pubbliche amministrazioni) beneficeranno dell'effetto giuridico associato a un determinato servizio fiduciario qualificato solo se quest'ultimo è elencato (come qualificato) negli Elenchi di fiducia.

La Commissione pubblica un elenco di questi elenchi di fiducia la **List of Trusted Lists** (LOTL) (https://esignature.ec.europa.eu/efda/tl-browser), strumento che consente a chiunque di consultare gli tutti gli elenchi di fiducia, nazionali ed europei, e cercare i servizi fiduciari disponibili nell'UE.

Accenni normativi - Elenchi di fiducia

La **List of Trusted Lists** (LOTL) è disponibile in un formato XML adatto all'elaborazione automatica. Questo formato della LOTL è firmato/sigillato digitalmente, il che consente di garantire l'autenticità e l'integrità della LOTL.

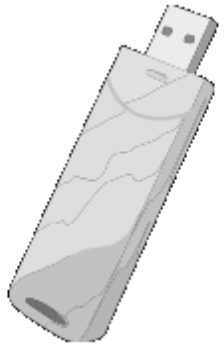


QTSPs – Prestatori di Servizi Fiduciari Qualificati
QTSs – Servizi Fiduciari Qualificati

Principio di funzionamento della FEQ o FD

- Per la creazione e la verifica delle firme digitali è necessario utilizzare un dispositivo di firma (ad es. smart card o token usb) in cui è custodita una **coppia di chiavi crittografiche**.

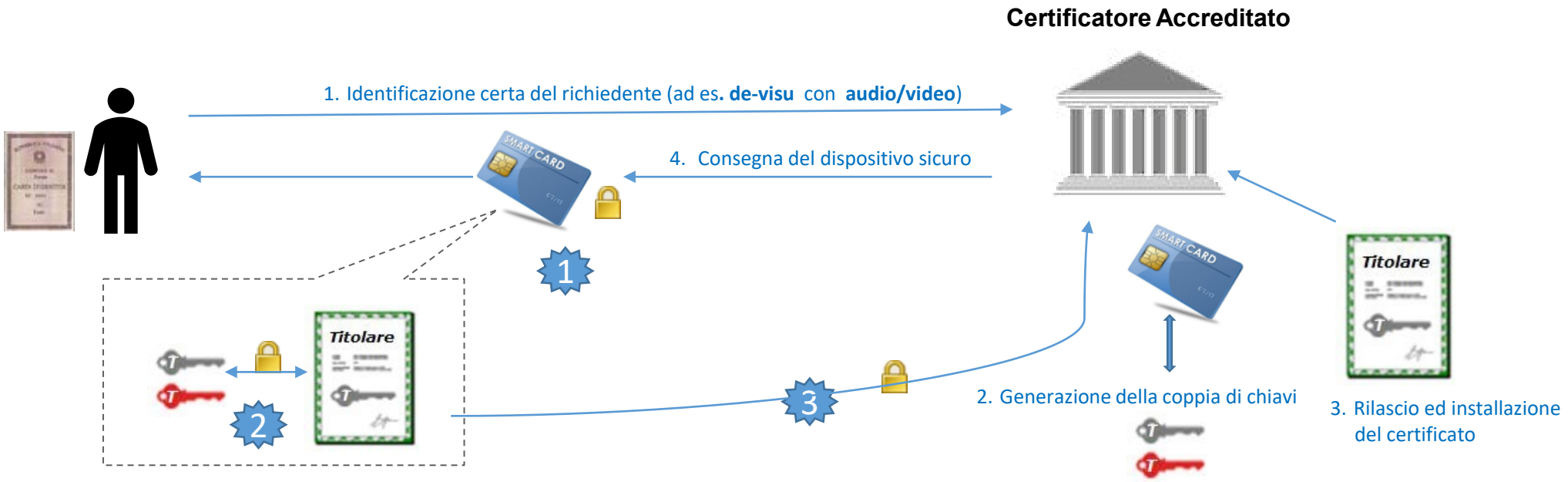
- La prima, **chiave privata**, destinata ad essere custodita solo dal Titolare, è utilizzata per la generazione della firma digitale, la seconda, **chiave pubblica**, viene utilizzata per verificare l'autenticità della firma.



- Caratteristica di tale metodo, detto crittografia a chiave asimmetrica, è che, una volta che il documento è stato firmato con la **chiave privata**, quella firma può essere verificata con successo esclusivamente con la corrispondente **chiave pubblica**.

- La sicurezza è garantita dalla **impossibilità** di ricostruire la chiave privata (segreta) a partire da quella pubblica, anche se le due sono collegate tra loro.

Rilascio della Firma Digitale



1. I dispositivi di firma sono dispositivi QSCD (**Q**ualified electronic **Si**gnature **C**reation **D**evices) certificati Common Criteria per il livello di garanzia EAL 4 + e garantisce l'unicità e l'inesportabilità della chiave privata.

2. La chiave pubblica del Certificato e quella privata custodita nel dispositivo sono uniche e correlate tra loro grazie ad una legge matematica.

3. La chiave pubblica ed i dati anagrafici contenuti nel Certificato sono garantiti dalla firma digitale della CA.

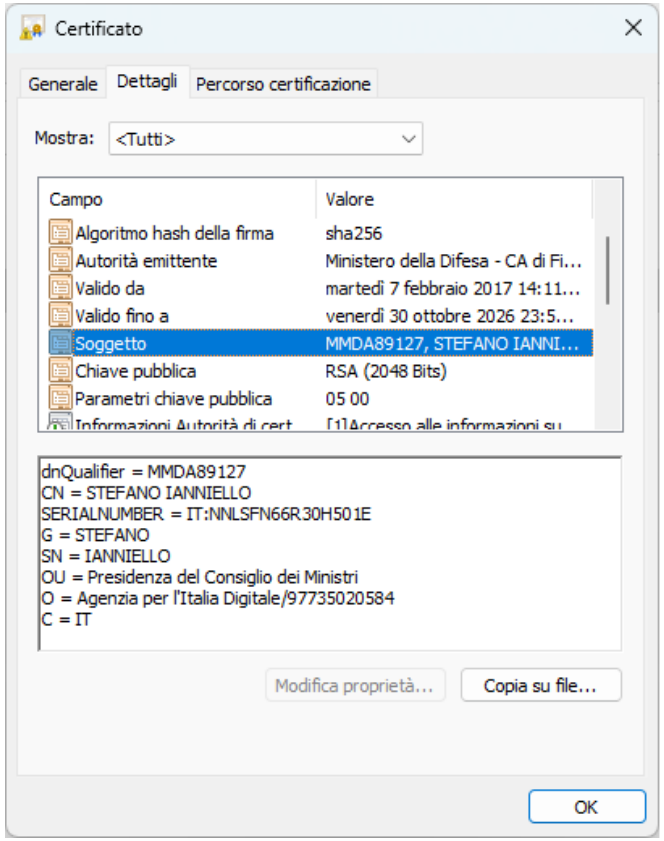
Caratteristiche del certificato

Un certificato qualificato è lo strumento che permette di distribuire pubblicamente le chiavi pubbliche rendendole note agli utenti finali con garanzia di autenticità e integrità.

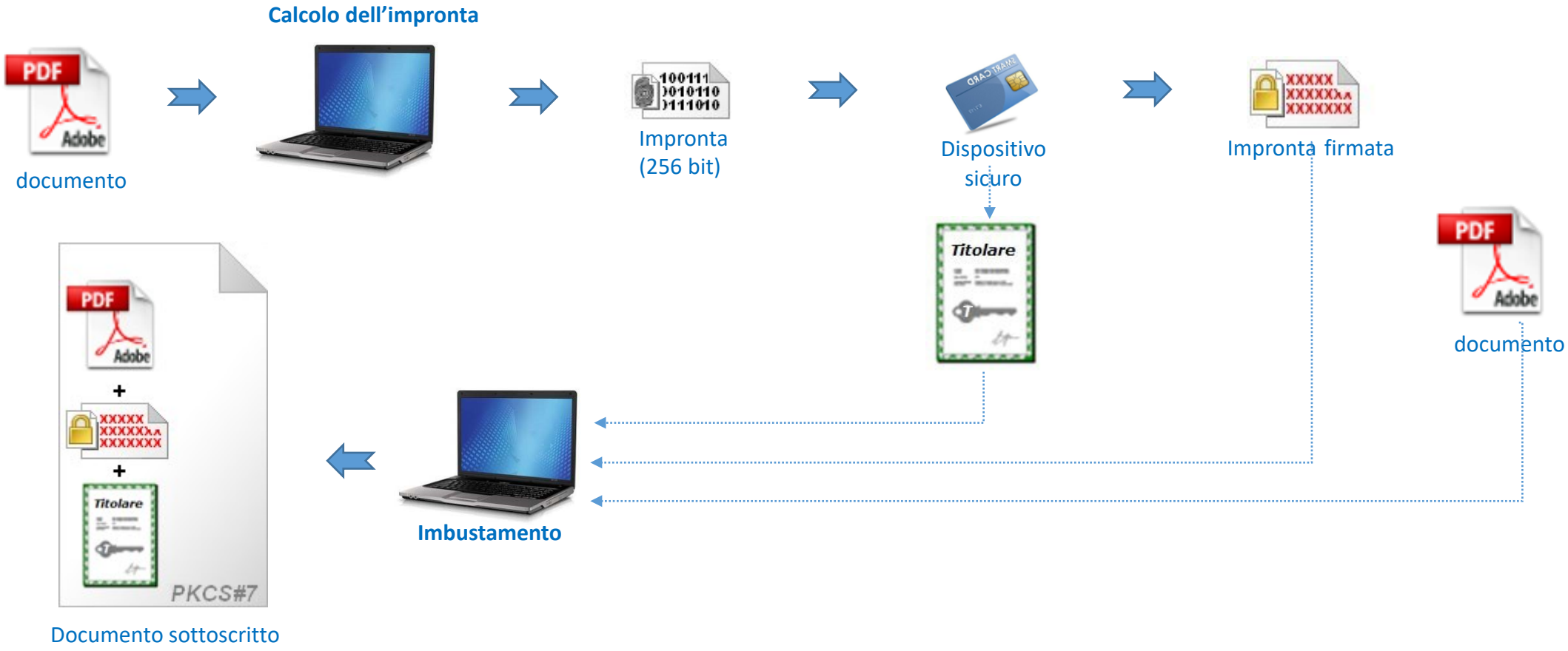
All'interno di un certificato qualificato troviamo le seguenti informazioni:

- Ragione sociale o denominazione dell'Ente che ha rilasciato il certificato;
- Dati del Titolare del certificato (nome, cognome, CF, Organizzazione di appartenenza, Titolo o Carica etc…);
- Durata del certificato (solitamente 3 anni);
- Chiave pubblica del Titolare del certificato;
- Firma Digitale dell'Ente Certificatore a garanzia dell'autenticità ed integrità di tutte le informazioni contenute nel certificato.

Le informazioni afferenti lo stato del certificato sono rese disponibili nel certificato attraverso il servizio OCSP ed eventualmente anche tramite liste di revoca (CRL).

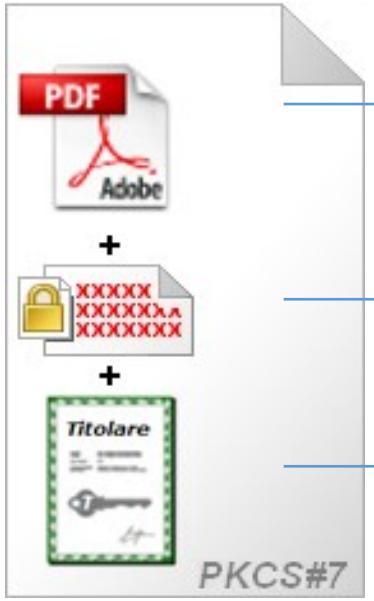


Generazione della Firma



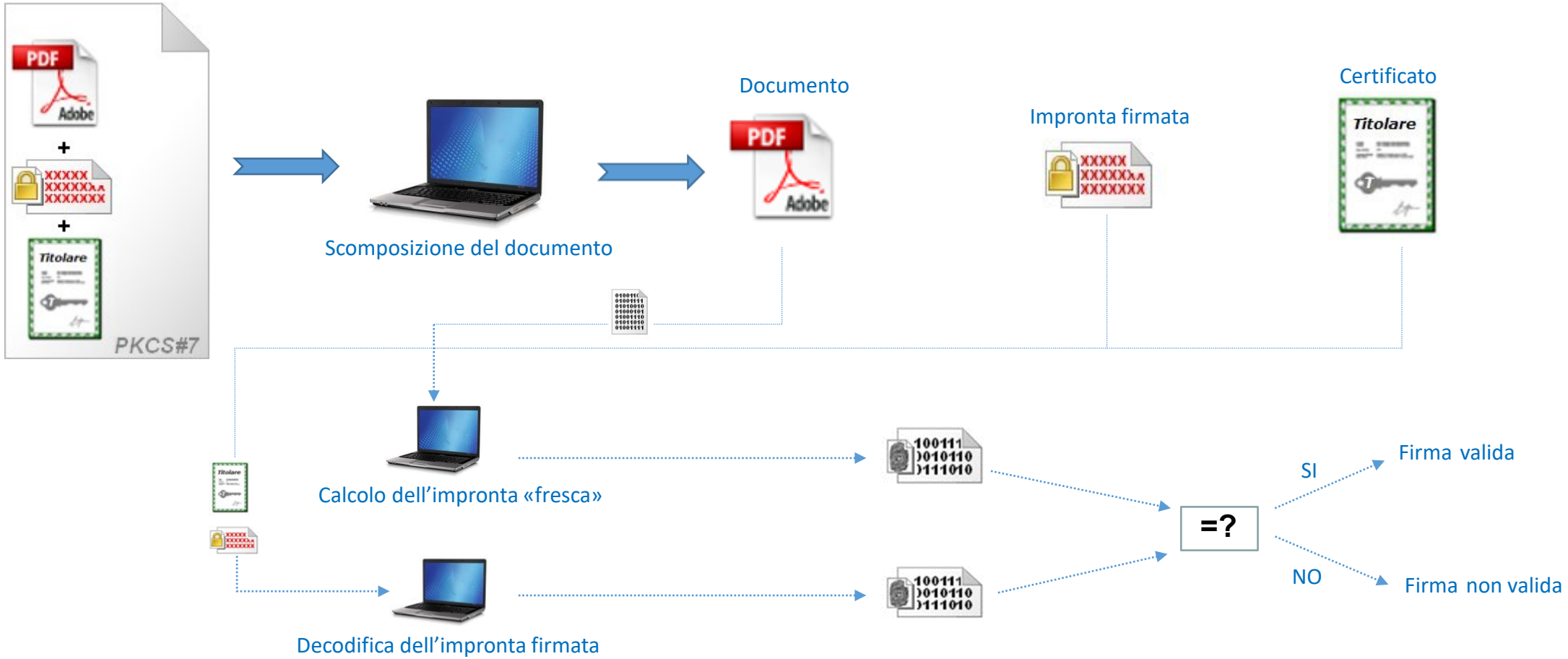
Documento firmato digitalmente

E’ un unico file prodotto dal software di firma ed è costituito da 4 componenti principali:

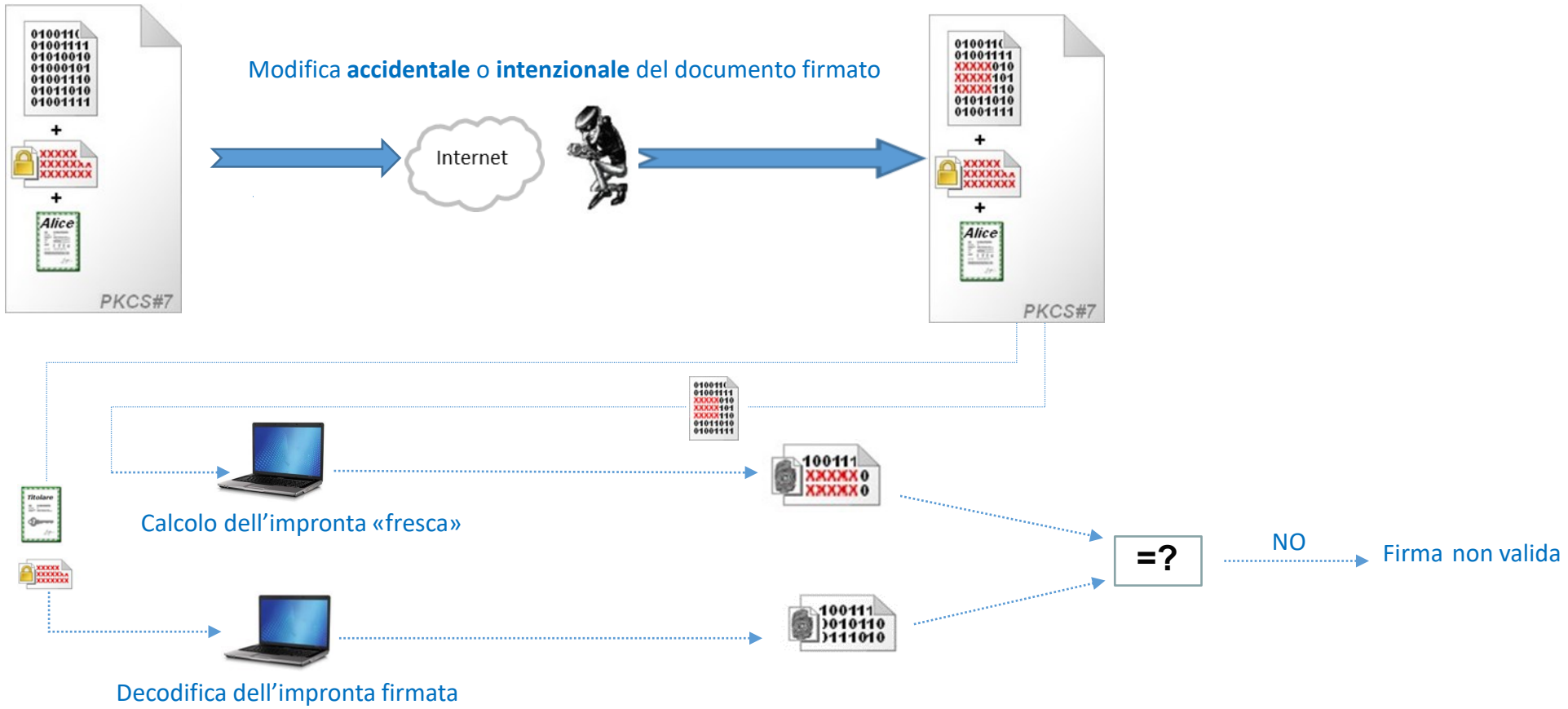


1. Il documento originale
2. la firma (ovvero impronta firmata dal sottoscrittore)
3. il certificato del sottoscrittore
4. l’involucro (struttura dati) contenitore

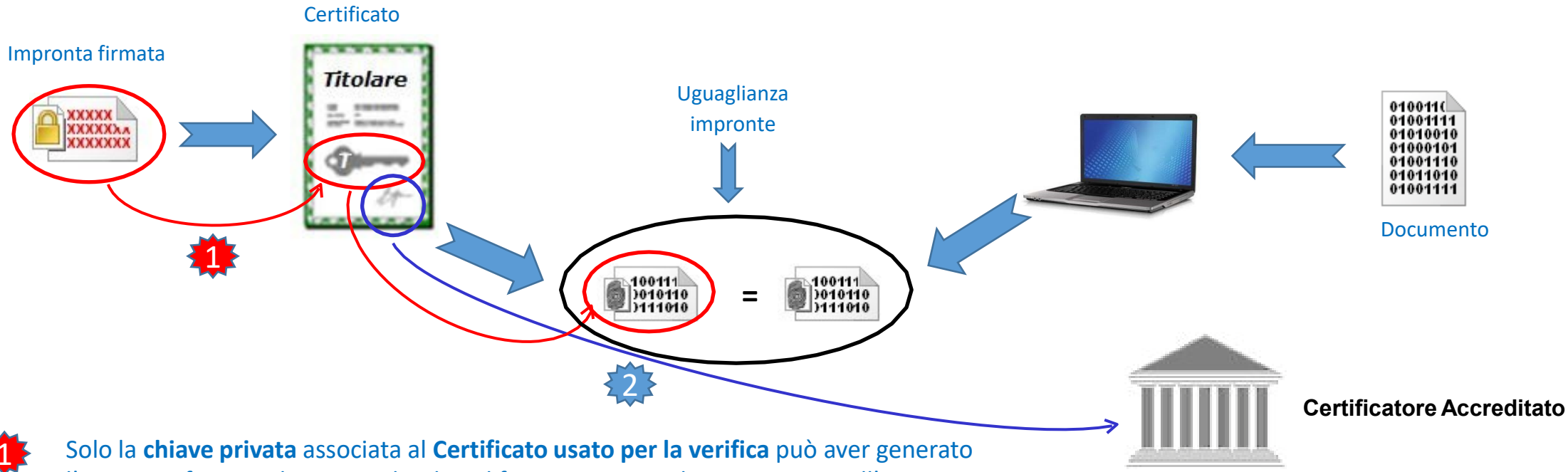
Processo di verifica di una Firma digitale



Verifica dell'integrità



Garanzia di autenticità



1 Solo la **chiave privata** associata al **Certificato usato per la verifica** può aver generato l'impronta firmata che, una volta decodificata, corrisponde esattamente all'impronta calcolata ex-novo

2 Se la **firma del Certificato è valida** allora lo stesso è stato emesso a fronte **dell'identificazione certa del Titolare** del dispositivo sicuro (QSCD) con cui è stata apposta la **Firma Digitale**

Formati di firma

La **Decisione di esecuzione (UE) 2015/1506 della Commissione** - Stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere (di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 - eIDAS).

CAdES (.p7m) → **C**MS **Ad**vanced **E**lectronic **S**ignature → ETSI TS 103 172 PAdES Baseline Profile → ETSI TS 101 733 CMS Advanced Electronic Signatures (CAdES)

PAdES (.pdf) → **P**DF **Ad**vanced **E**lectronic **S**ignature → ETSI TS 103 173 CAdES Baseline Profile → ETSI EN 319 142 PDF Advanced Electronic Signature Profiles (PAdES)

XAdES(.xml) → **X**ML **Ad**vanced **E**lectronic **S**ignature → ETSI TS 103 171 XAdES Baseline Profile → ETSI TS 101 903 XML Advanced Electronic Signatures (XAdES)

La firma CAdES

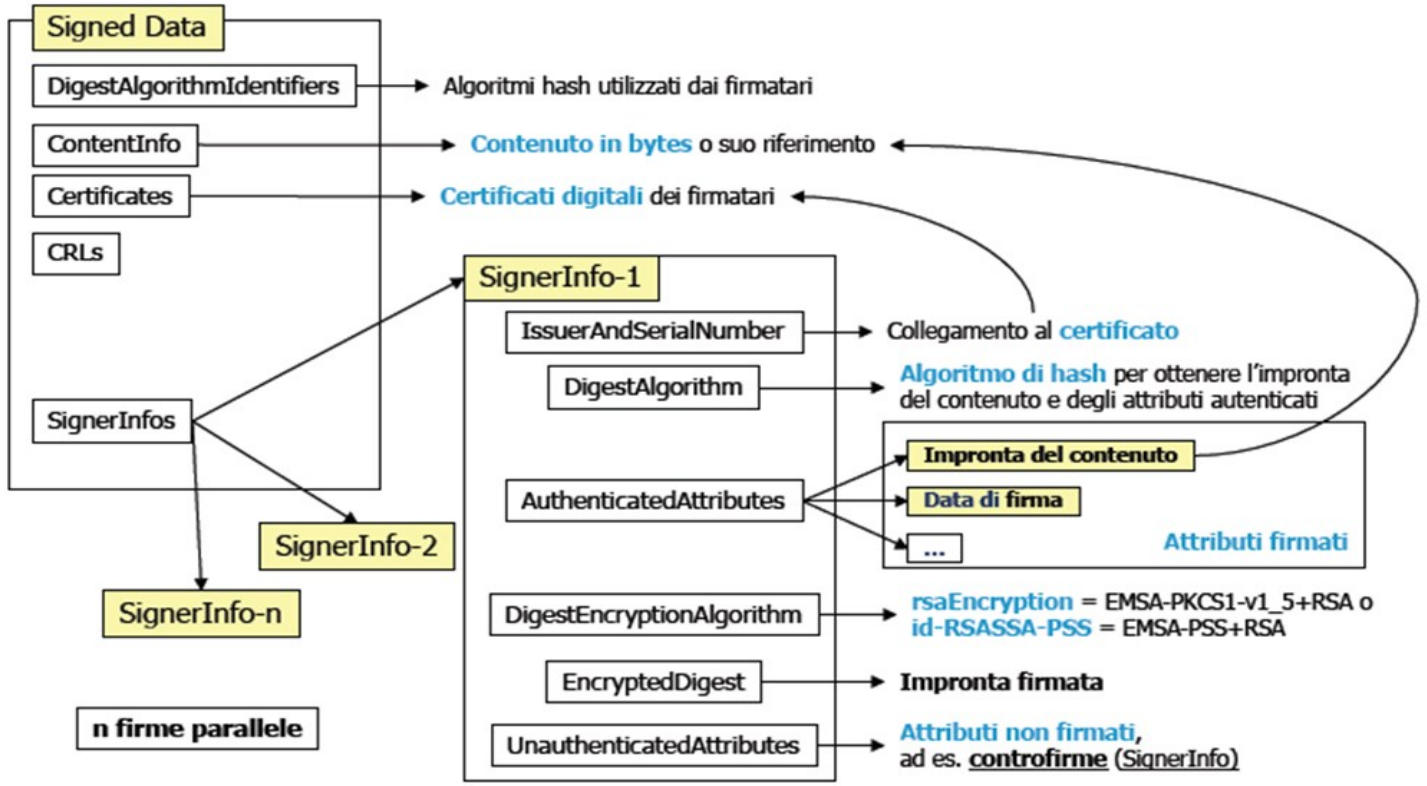
PKCS#7 o P7M

La busta CAdES è un file con estensione **.p7m**, il cui contenuto è visualizzabile solo attraverso idonei software (software di verifica) in grado di "sbustare" il documento sottoscritto.

Tale formato permette di firmare qualsiasi tipo di file, ma presenta lo svantaggio di non consentire di visualizzare il documento oggetto della sottoscrizione in modo agevole. Infatti, è necessario utilizzare un'applicazione specifica.

Il formato consente di apporre tutte le tipologie di firma:

- Firma singola - modalità di firma classica.
- Firma parallela o congiunta - più firmatari appongo la propria firma al medesimo documento.
- Controfirma - il firmatario appone la firma al documento e le successive firme sono calcolate sulla firma iniziale (sorta di validazione gerarchica).
- Firma Enveloped (Matrioska) – con cui è possibile firmare l'intera busta crittografica.p7m, che al suo interno conterrà un documento già sottoscritto digitalmente, ottenendo così un file di estensione.p7m.p7m.



La firma CAdES

Per il formato CAdES l'apposizione di due o più firme può essere effettuata in due modi:

- re-imbustando in una nuova busta CAdES la busta generata dalla sottoscrizione precedente (c.d. controfirma o "*firma matrioska*"), come mostrato in figura 1;
- oppure aggiungendo nella busta ulteriori firme, accompagnate dai relativi certificati (c.d. firme congiunte), come mostrato in figura 2.

.

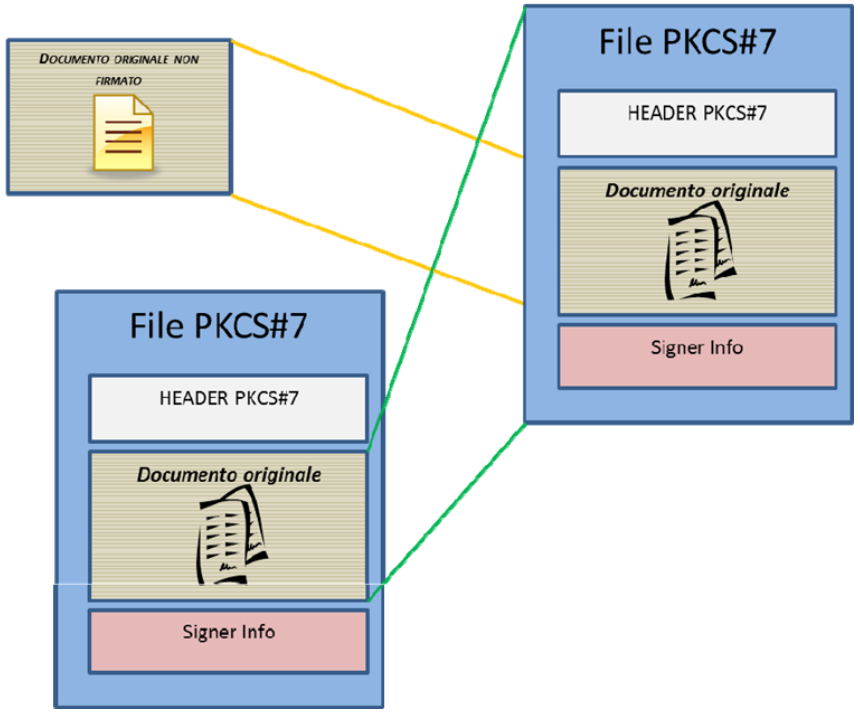


Figura 1 – Firma a matriosca – ogni firma afferisce al documento e alle firme precedenti formato CAdES

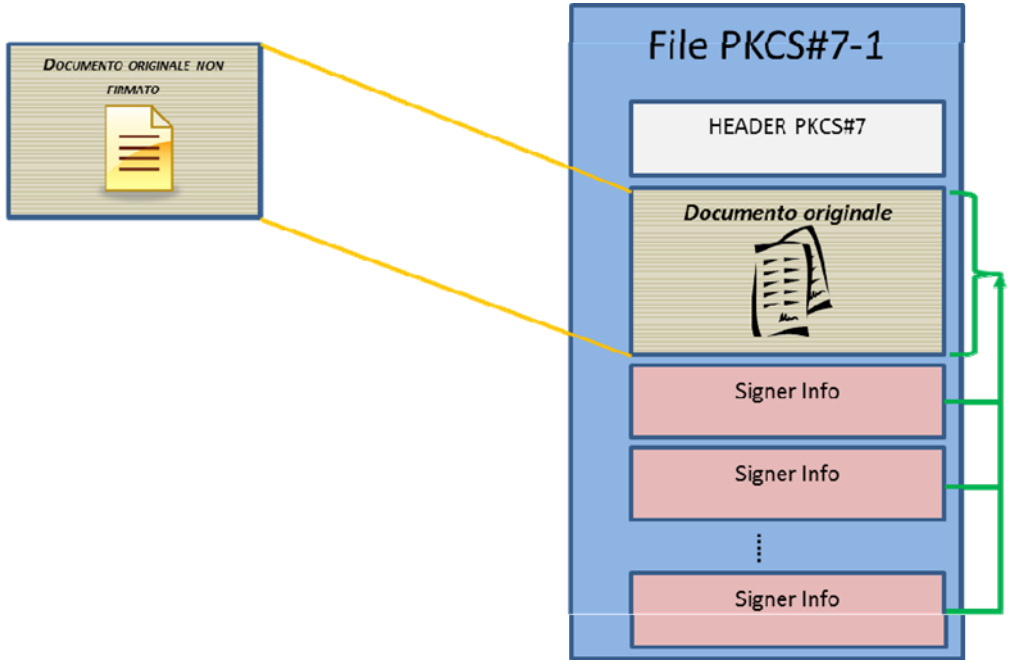


Figura 2 - Firme congiunte CAdES – ogni firma afferisce al documento

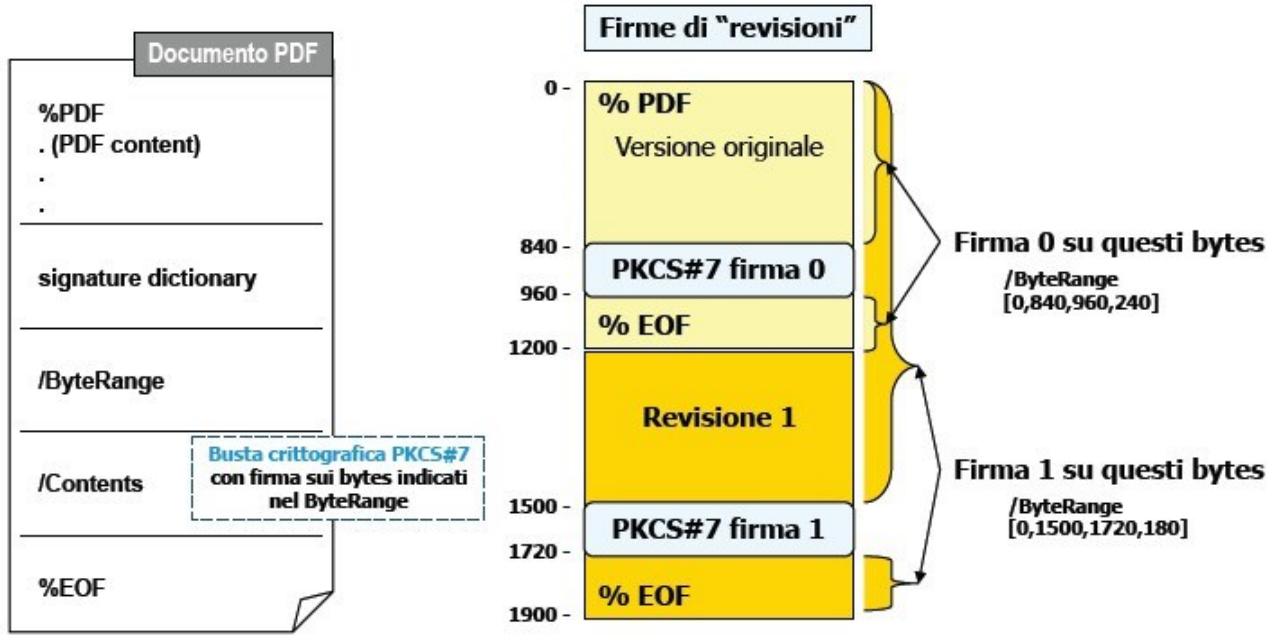
La firma PAdES

PDF

La firma digitale in formato PAdES è un file con estensione *.pdf*, leggibile con i comuni reader disponibili per questo formato.
Questa tipologia di firma, per la natura stessa del formato, consente di apporre solo firme di tipo enveloped. Tuttavia i file generati hanno una struttura pseudo- binaria che ben si presta a rappresentare informazioni crittografiche e a gestire revisioni successive di un documento firmato.
I file devono assumere l'estensione *.pdf* e sono leggibili dalla maggior parte dei visualizzatori PDF, primo tra tutti Adobe Reader.

Il formato consente di apporre tutte le tipologie di firma:

- Firma singola - modalità di firma classica.
- Firma parallela o congiunta - più firmatari appongo la propria firma al medesimo documento.



Ogni modifica al documento (ulteriore firma o aggiunta di testo o immagini) produce, infatti, una nuova versione che contiene la versione originale non modificata

La firma PAdES

Tale caratteristica della busta PAdES rende questo formato particolarmente idoneo anche nel caso in cui si renda necessario apportare delle modifiche al documento dopo averlo sottoscritto, ad esempio per riportarvi delle annotazioni, come i dati degli estremi di protocollo che sono disponibili solo successivamente alla sottoscrizione del documento stesso.
Ad una prima analisi, un documento sottoscritto sul quale sono riportate tali annotazioni potrebbe apparire corrotto in quanto modificato dopo la firma (figura 1), tuttavia nella busta PAdES è presente ed è accessibile anche la versione non modificata del documento (figura 2), che pertanto conserva piena efficacia giuridica. Non devono, infatti trarre in inganno i messaggi mostrati dal reader del documento "*Almeno una delle firme non è valida*" e "*Il documento dopo la firma è stato modificato o si è danneggiato*", in quanto è comunque possibile accedere alla versione del documento correttamente sottoscritta, coerentemente con quanto previsto dalle regole tecniche di cui al D.P.C.M. del 22 febbraio 2013.

.

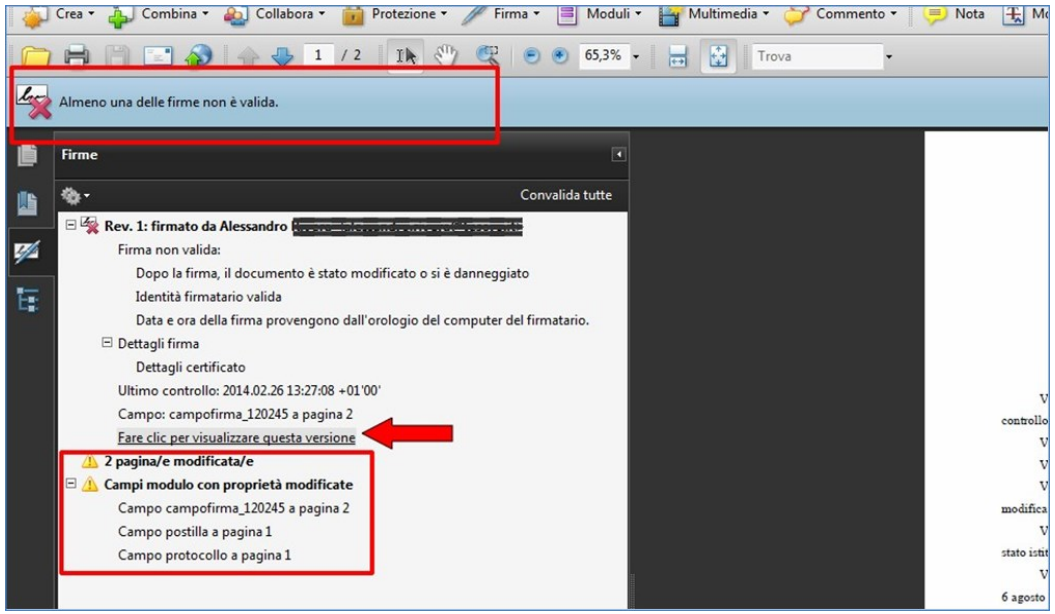


Figura 1 – accesso alla versione non modificata del documento firmato – formato PAdES

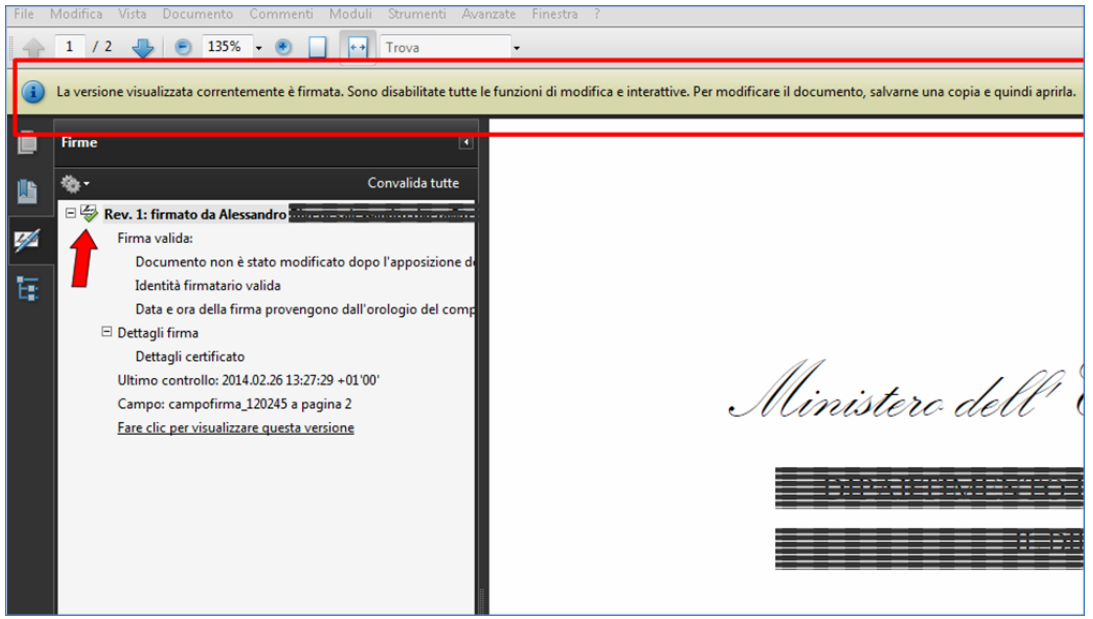


Figura 2 – busta formato PAdES- versione non modificata del documento sottoscritto digitalmente

La firma XAdES

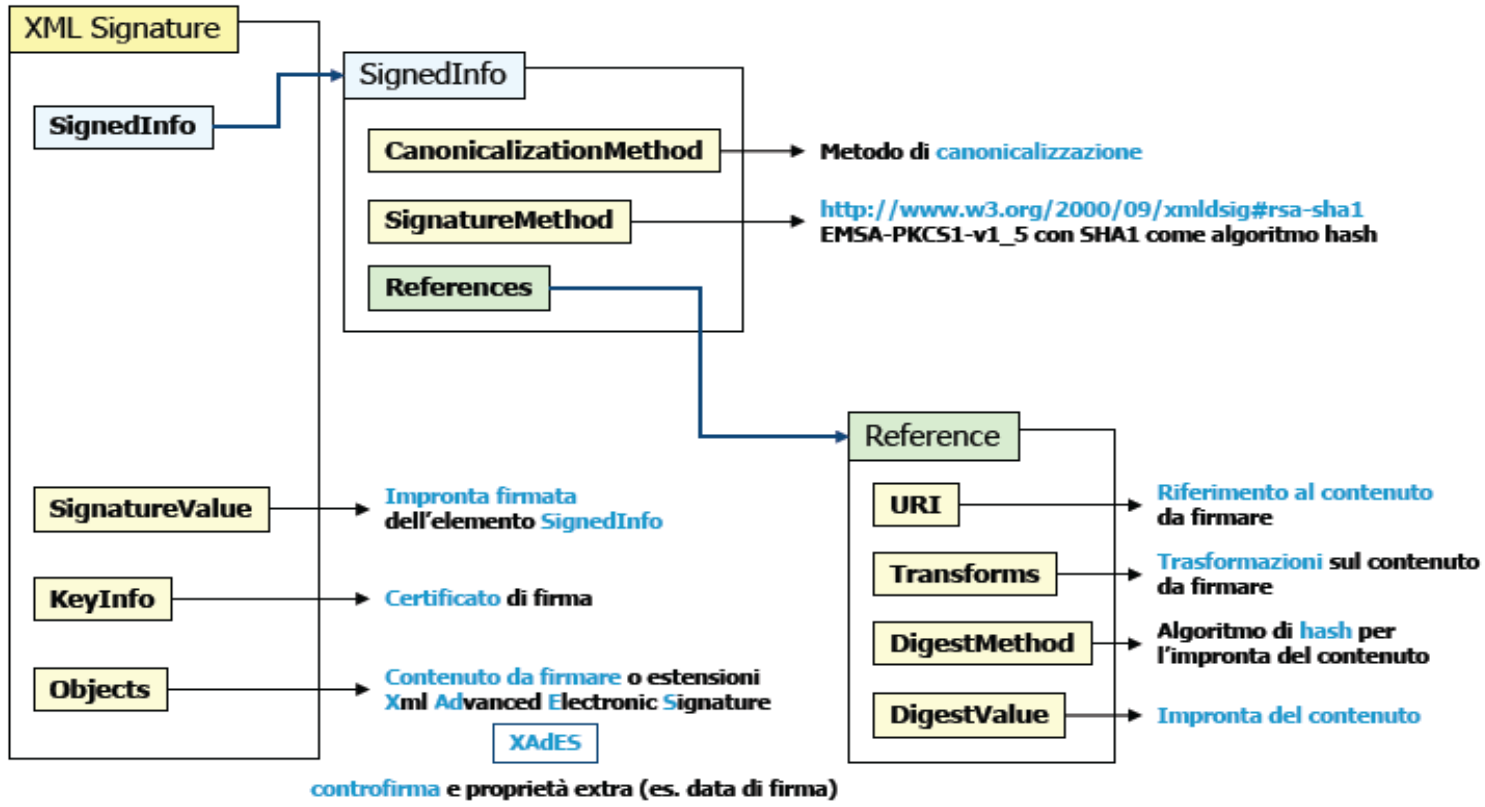
XML

E’ il tipo di firma digitale definito all’interno della specifica XML mantenuta dal W3C. Lo standard di riferimento è l’XML-Signature Syntax and Processing e l’ETSI 101 903 meglio nota come XAdES.

Questa tipologia di firma consente di apporre tutte le tipologie di firma previste dalla normativa.

I file prodotti hanno una struttura gerarchica con rappresentazione alfa numerica.
I file **devono** assumere l’estensione **.xml** e sono leggibili dalla maggior parte dei *parser XML*.

Al momento non è garantita l’interoperabilità a causa delle grandi potenzialità offerte da questo formato.
Viene utilizzato principalmente in documenti elettronici in ambito sanitario e finanziario, fatture elettroniche.



Software di verifica della firma

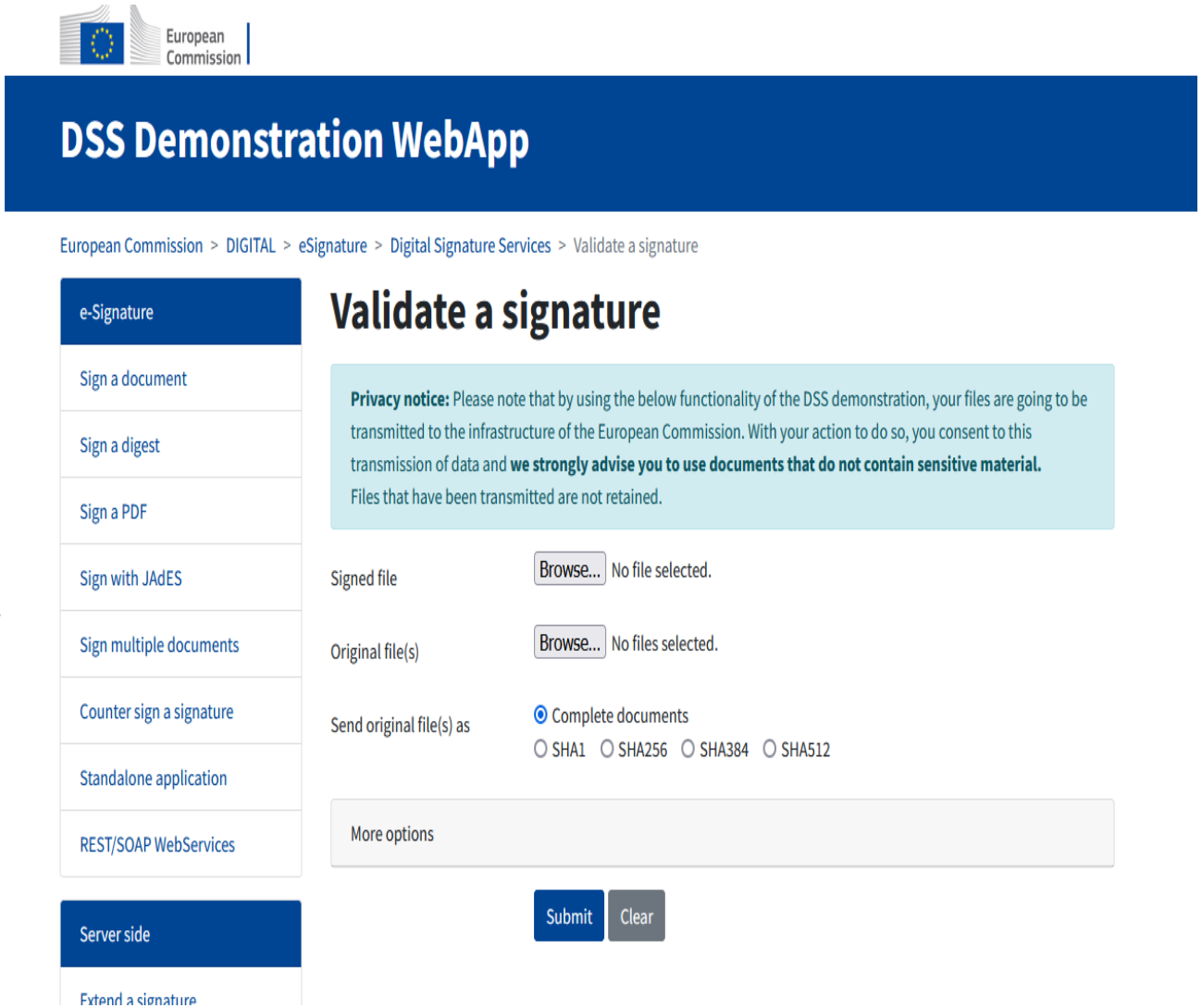
L'AgID espone sul proprio sito all'indirizzo https://www.agid.gov.it/it/piattaforme/firma-elettronica-qualificata/software-verifica alcuni software di verifica della firma che posso essere scaricati ed istallati o utilizzabili online.

Da segnalare che a livello europeo, la Commissione sta cercando di favorire il pieno riconoscimento dei documenti informatici sottoscritti nei diversi Stati Membri.

La Commissione ha reso disponibile il Digital Signature Service (DSS), un software di firma e verifica che può essere gratuitamente utilizzato online o scaricato ed istallato, maggiori info:

- https://ec.europa.eu/digital-building-blocks/code/projects/ESIG/repos/dss-demos/browse/README.md ;
- https://github.com/esig/dss-demonstrations .

Caricando il documento firmato si procede alla verifica.

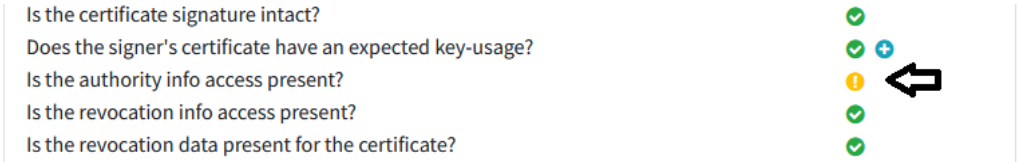


Software di verifica della firma

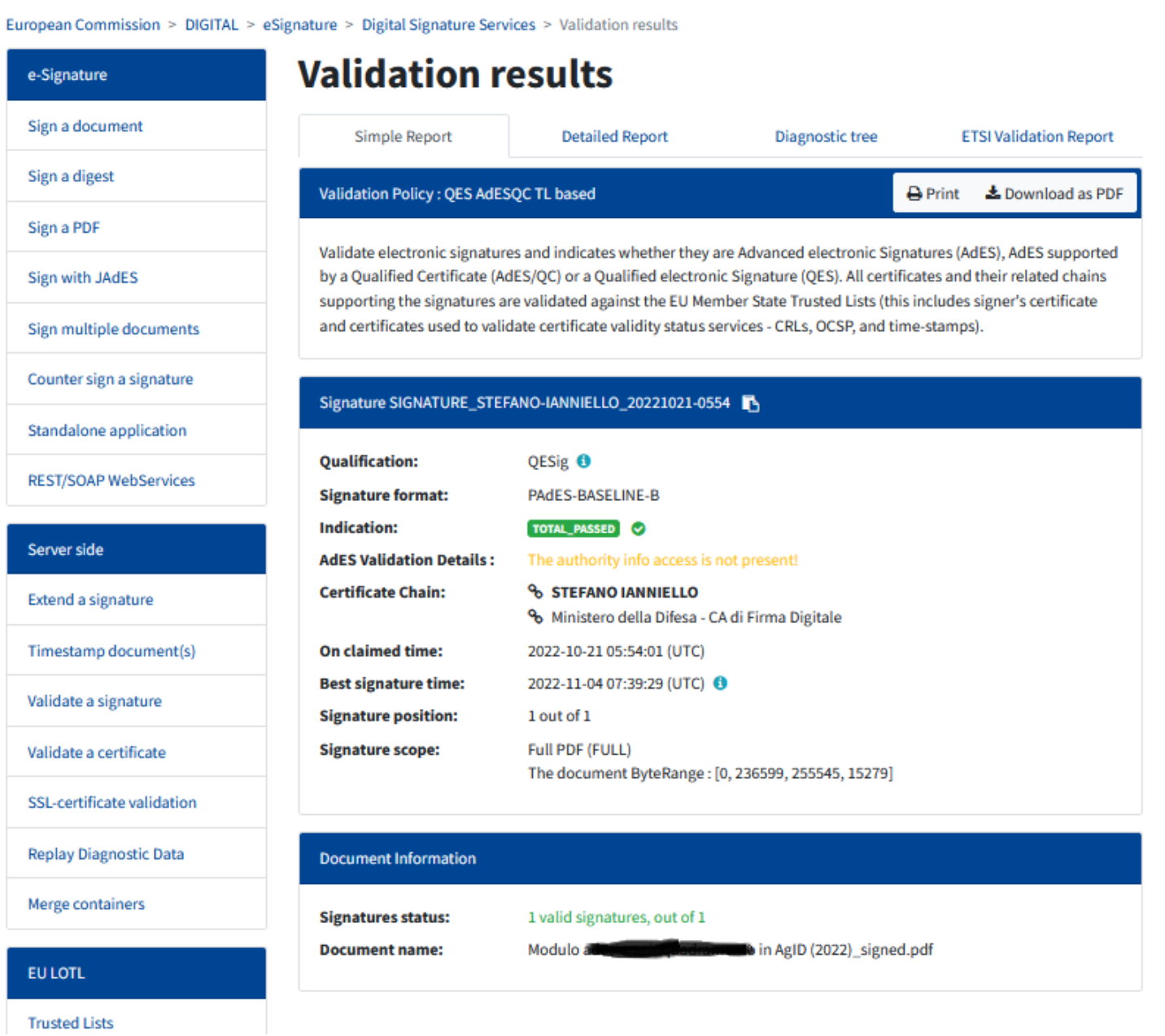
Una volta sottomesso il documento, l'applicazione restituisce un report semplificato che con l'indicazione «***TOTAL_PASSED***» conferma la validità della firma apposta al documento .

Se necessario, l'applicativo permette di visualizzare (si può scaricare il report) maggiori dettagli in merito alla validità della firma e sullo stato del documento caricato (non modificato dopo la sua sottoscrizione).
In alcuni casi nel report di dettagliato (voce *Detailed Report*) posso essere presenti alcuni avvisi segnalati in giallo, ad esempio:
"The authority info access is not present!"

Si evidenzia che gli avvisi in giallo (peculiarità di tutti i software di verifica) sono comunicazioni, non cambia il valore della firma apposta (la firma è valida).



Esempio di Avviso segnalato come warning nel «*Detailed Report*»



www.agid.gov.it

Riferimenti dei docenti - ianniello@agid.gov.it