

DOCUMENTO INFORMATICO, FIRMA ELETTRONICA E DIGITALE

Avv. Carlo Piana

Array <https://array.eu>

Milano, Bolzano, the Internet, 26 giugno 2020

DO PER SCONTATO!

- Cos'è EIDAS e a cosa serve
 - Cos'è il CAD
- Cos'è la Conservazione sostitutiva

IL DOCUMENTO INFORMATICO

Poco in Eidas

- Articolo 2.1.35

«documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

- Articolo 46 - Effetti giuridici dei documenti elettronici

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

- Documento elettronico a cui viene apposta una firma digitale o elettronica (art. 20 CAD) → **Forma Scritta**

FORMA SCRITTA PER UN DOCUMENTO ELETTRONICO

Qualità della firma:

- Avanzata → Art. 26 EIDAS
- Qualificata → Art. 29 EIDAS
- Digitale → Art. 24 CAD
- Firma Art. 20 CAD (SPID?)

COS'È UNA FIRMA ELETTRONICA?

«firma elettronica»: dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare (art. 3.1.10 EIDAS)




NO, DAVVERO, COS'È?

Un dispositivo logico e tecnico che consente di attribuire all'autore la paternità della sottoscrizione, perché solo lei/lui possedeva qualcosa e creare la firma.



FACCIAMO UN PASSO INDIETRO

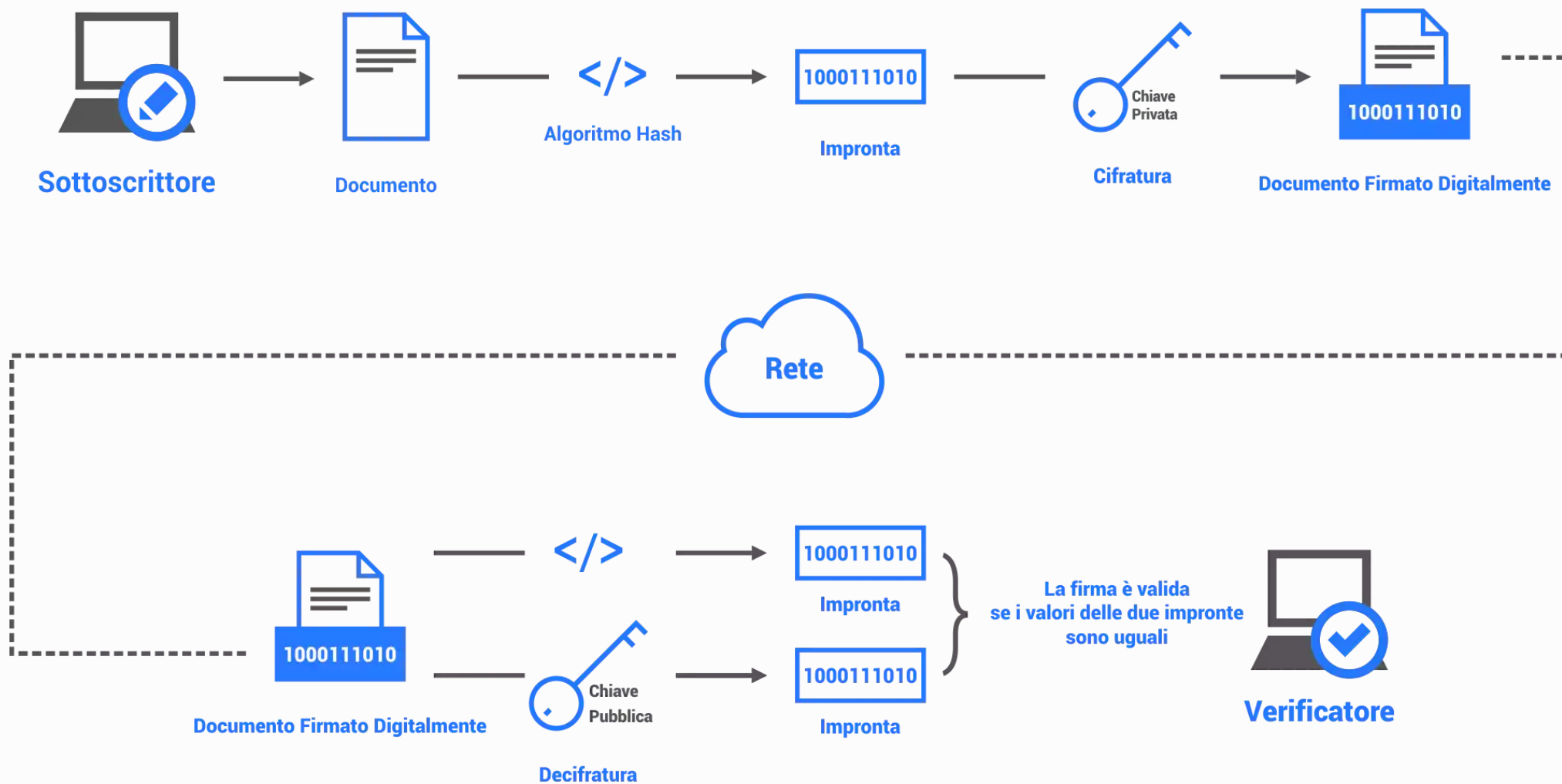
Cifratura a chiavi asimmetriche:

- Tizio ha un messaggio per Caio, che solo Caio deve poter aprire
- Caio rende **pubblica** una **chiave** con cui si può solo cifrare. Decifrare è praticamente impossibile
- Per decifrare occorre una chiave **privata**
- Caio ha la chiave privata che corrisponde alla chiave pubblicata
- **Bingo!** 

E LA FIRMA?

La firma è l'inverso della cifratura.

- La chiave **pubblica** è quella di **decifratura**
- La chiave **privata** è quella di **cifratura**
- Chi firma **cifra** il documento con la chiave privata
- Chi verifica la firma **decifra** la firma con la chiave pubblica
- Se la decifratura riesce, dimostra che il firmatario era in possesso della chiave privata
- Se riesce, significa che il messaggio non è stato alterato



COME SI AUTENTICA LA FIRMA?

Meccanismo della qualificazione:

- La firma contiene alcuni dati che **individuano** il sottoscrittore
- La firma è a sua volta **firmata** da un ente terzo (**Certification Authority**)
- Il certificato della Certification Authority è Pubblico
- L'elenco delle Certification Authority è pubblico ed esiste un'autorità di **root** (RootCA) che certifica i certificatori.
- In Italia, **DigitPA**.

FIRMA QUALIFICATA VALIDA ALLORCHÉ

- La firma si basa su un **certificato qualificato**
- Il certificato è qualificato quando è emesso da un ente certificatore autorizzato.
- La firma risulta apposta con tale certificato e corrisponde al documento (hash)
- Requisiti ulteriori

EFFETTI DELLA FIRMA VALIDA

- **Authenticity** Il messaggio proviene da una fonte autentica
- **Non repudiation** La fonte autentica non è in grado di dissociarsi da ciò che ha firmato
- **Integrity** Il contenuto del messaggio non è stato alterato

COSA SERVE PER “CONVALIDARE” UNA FIRMA?

- **Software di validazione**
- Il certificato della CA per convalidare il certificato del firmatario
- Il certificato della RootCA per convalidare il certificato della CA
- **!** La Certification Revocation List (**CRL**)
- **!!** Un orologio e un calendario



UN CERTIFICATO NON È PER SEMPRE

- Il possessore può perdere il certificato o questo può essere rubato
- Il possessore “denuncia” la perdita
- Il certificato viene inserito in un lista di revoca, la **CRL**
- Chi valida il certificato **deve** controllare la CRL (tipicamente ogni 24 ore)
- Una firma apposta con un certificato **revocato non è valida**

UN CERTIFICATO NON È PER SEMPRE, RELOADED

- Il certificato **scade**
- Il certificato **può venire revocato**
- Dunque è necessario conoscere il **tempo della firma**
- Firma apposta **prima** della **scadenza** e della **revoca**
è salva



RIFERIMENTO TEMPORALE

Colloca la firma in un orizzonte temporale precedente la revoca o la scadenza



Firma valida

VALIDI RIFERIMENTI TEMPORALI

Art. 41 delle Regole Tecniche (Dpcm 22/2/2013 n. 68380)

- Marca temporale (41.1)
- Segnatura di protocollo (41.1.a)
- **Conservazione sostitutiva** (41.1.b)
- Messaggio di PEC (ma anche quello scade) (41.1.c)
- Marcatura postale elettronica (41.1.d)

MA QUALE FIRMA?

RICAPITOLANDO

- Avanzata → Art. 26 EIDAS
- Qualificata → Art. 29 EIDAS
- Digitale → Art. 24 CAD
- Firma Art. 20 CAD (SPID?)

FIRMA AVANZATA

Articolo 26

Requisiti di una firma elettronica avanzata

Una firma elettronica avanzata soddisfa i seguenti requisiti:

- a) è connessa unicamente al firmatario;
- b) è idonea a identificare il firmatario;
- c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
- d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

FIRMA QUALIFICATA

«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;

Requisiti: Allegato II EIDAS

FIRMA DIGITALE

- Art. 1.1.s e 24 CAD (= Italiana)
- È una firma elettronica qualificata basata su chiavi asimmetriche e certificati qualificati.

FIRME EU

Art. 25.3 EIDAS

3. 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.

Art. 27 EIDAS: Firme nel settore pubblico

1. Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato di firma elettronica e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

[...]

3. Gli Stati membri non richiedono, per un utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, una firma elettronica dotata di un livello di garanzia di sicurezza più elevato di quello della firma elettronica qualificata.

FIRME NON EU

STATO DELL'OPERA

- Estremamente complessa
- Per EIDAS va riconosciuta se vi sono accordi di reciprocità (art. 14.1)
- WTO, art. 49 Dlgs 50/2016 “condizioni non meno favorevoli”
- Reso parere ad ACP



IL PARERE ACP

«In caso di operatori stabiliti al di fuori dell'Unione Europea e senza una rappresentanza stabile nel territorio dell'Unione, sempreché lo Stato di stabilimento non abbia concluso un accordo ai sensi dell'art. 14.1 EIDAS, il requisito di firma potrà essere soddisfatto utilizzando una firma elettronica avanzata secondo gli standard internazionalmente riconosciuti, purché vi sia evidenza che quella firma sia accettata nel paese di origine in caso di gare per [indicare il tipo di appalto, gara, avviso in corso]. In tal caso l'operatore economico dovrà fornire, in un documento anche non firmato, le modalità tramite le quali sia possibile per la stazione appaltante verificare l'autenticità della firma tramite una connessione online con l'autorità di certificazione.

In mancanza di tale indicazione, l'Amministrazione potrebbe non essere in grado di verificare l'autenticità della sottoscrizione, con conseguente esclusione.»

CONVALIDA

SERVIZIO FANTASMA

- Art. 32 Eidas
- Recentemente pubblicate linee guida (laconiche)
- Fornisce un'attestazione affidabile e sottoscritta del risultato di convalida
- Attualmente non sono noti servizi di convalida

NEL FRATTEMPO...

- applicazioni realizzate da alcuni fornitori
 - Dike (Infocert)
 - Arubasign
- Servizi (Namirial)
- DSS <https://joinup.ec.europa.eu/dss-webapp/validation> (va e non va...)
- Molta fantasia e arte, soprattutto con le firme EIDAS

THANK YOU!

Thank
you



This work is licensed under a [Creative Commons - Attribution - ShareAlike](#)
Presentation made using [Reveal.js](#) and a [Markdown](#) workflow with [reveal-md](#)