Città metropolitana
di Roma Capitale

Piano formativo
«OpenID Connect – PNRR 1.4.4»

Comuni Area metropolitana di Roma Capitale

CAPITALE LAVORO
società di Città metropolitana di Roma Capitale

Con il supporto tecnico di

PA 3.26

LIVELLO NORMATIVO

LE FIRME ELETTRONICHE:
quali differenze tra tutte le tipologie

Docente:
Dott. **Rosario Carrisi**
Consulente di management
Esperto di governance, e-government delle P.A

UD: CAD-006-01 - Edizione 05-2024

Contenuti dell’unità didattica

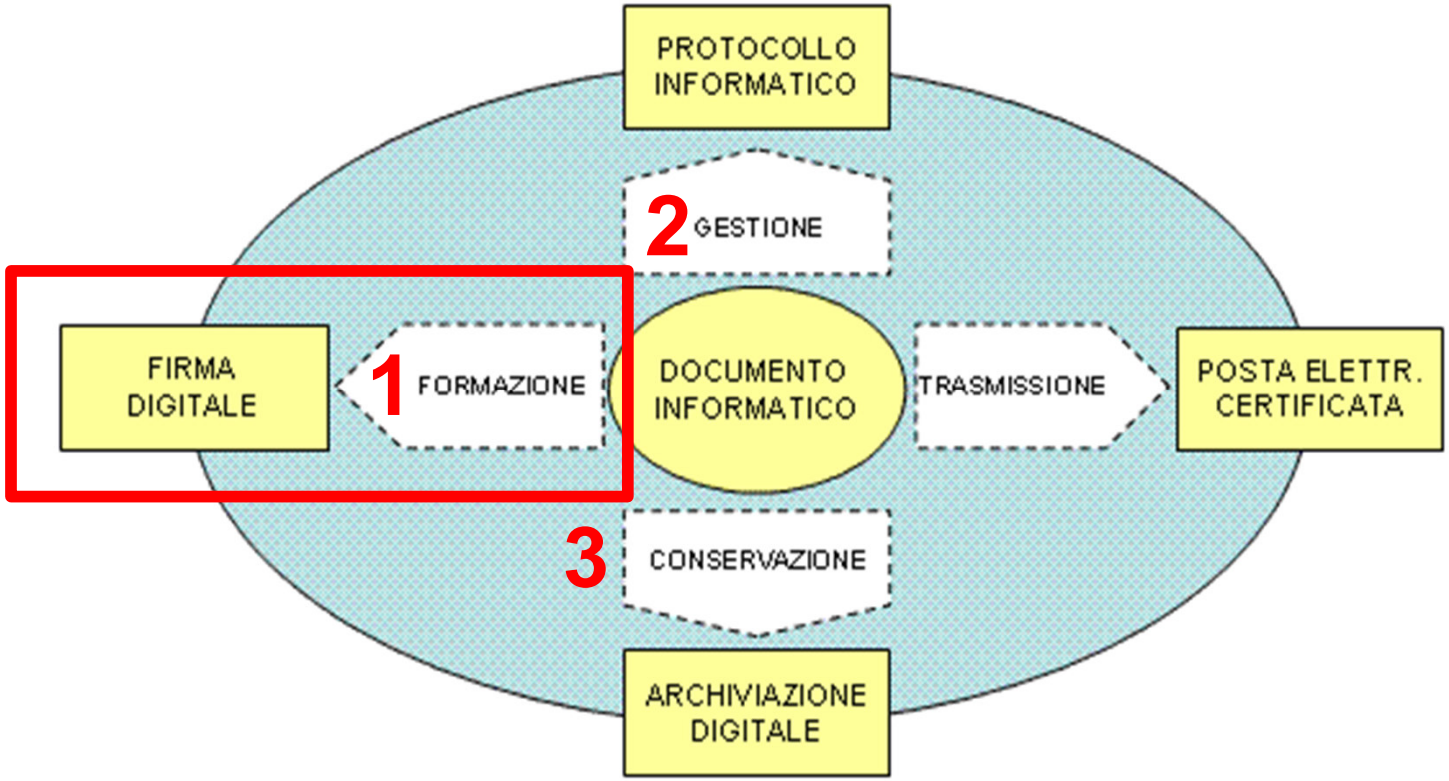
In questa unità didattica affronteremo i seguenti argomenti:

- **Analizzare il quadro normativo di riferimento delle firme elettroniche (europea e nazionale)**
- **Fare chiarezza e fugare i dubbi su cosa siano le firme elettroniche, quali tipologie esistono, quali differenze presentano e quale valenza giuridico probatoria è loro riconosciuta dalla normativa**

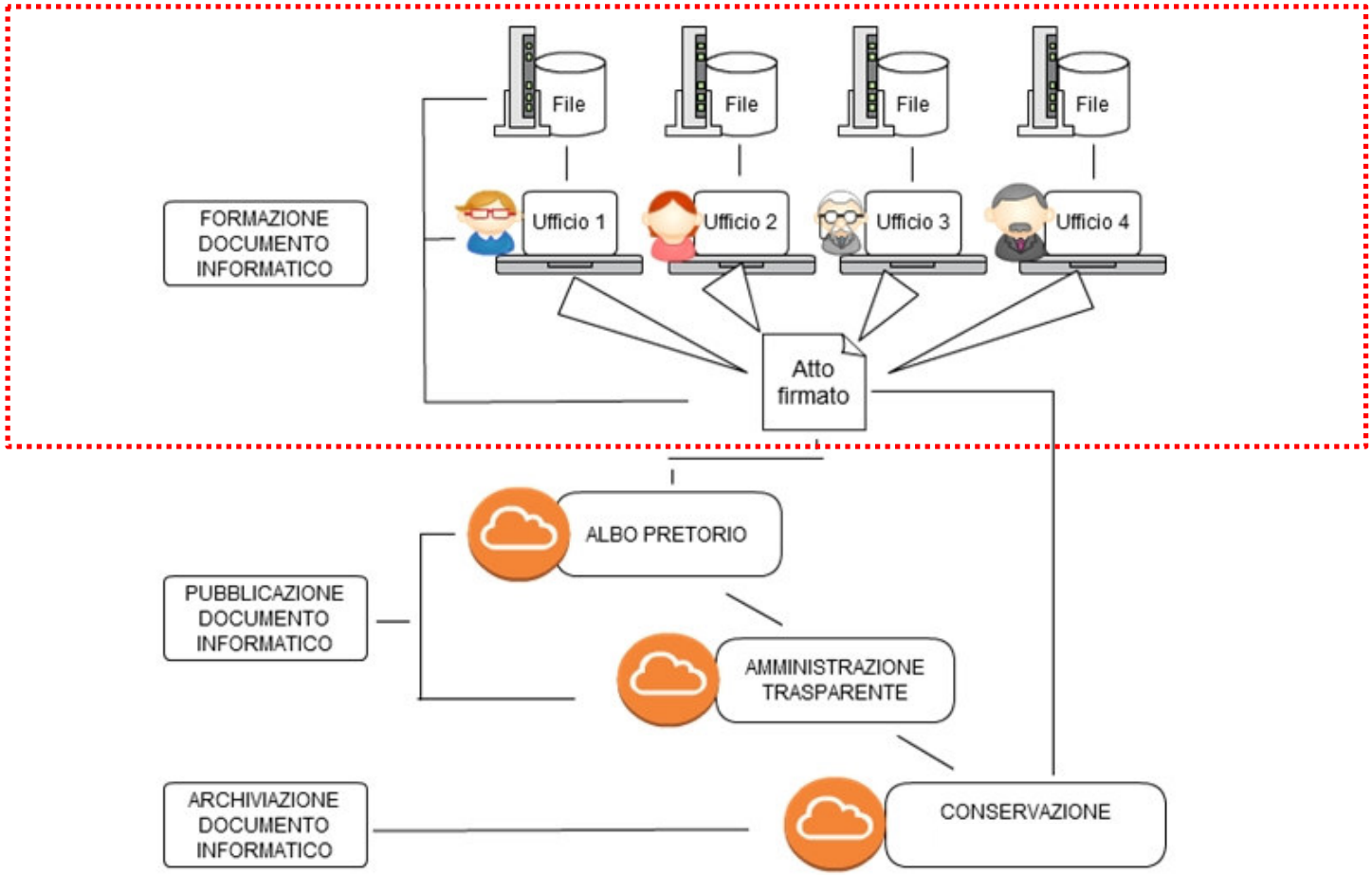
Contenuti dell'incontro

- La normativa di riferimento delle firme elettroniche;
- La tecnologia delle firme informatiche: *crittografia, funzioni di hash*;
- Definizioni, tipologie e caratteristiche delle firme elettroniche;
- Il sigillo elettronico
- Prestatori di servizi fiduciari (ex Certificatori)
- Efficacia probatoria dei documenti sottoscritti con firma elettronica
- Effetti giuridici del sigillo elettronico

Il ciclo di vita del documento informatico



Il ciclo di vita del documento informatico



LA NORMATIVA DI RIFERIMENTO DELLE FIRME ELETTRONICHE

Regolamento europeo 910/2024
in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE

Il regolamento eIDAS è stato emanato il 23 luglio 2014 e ha piena efficacia dal **1 luglio del 2016.**

eIDAS

Obiettivi del regolamento eIDAS

- Evidenziare l'esigenza di rafforzare la fiducia nelle transizioni informatiche nel mercato interno e di garantire il reciproco riconoscimento dell'identificazione elettronica, dell'autenticazione, delle firme e di altri servizi che vengono definiti «trusted» tradotti come «fiduciari» in italiano;

- Realizzare l'interoperabilità giuridica e tecnica degli strumenti elettronici di identificazione, autenticazione e sottoscrizione tra i Paesi della UE.

Obiettivo primario è quello di aumentare l'efficacia dei servizi online nel mercato interno europeo

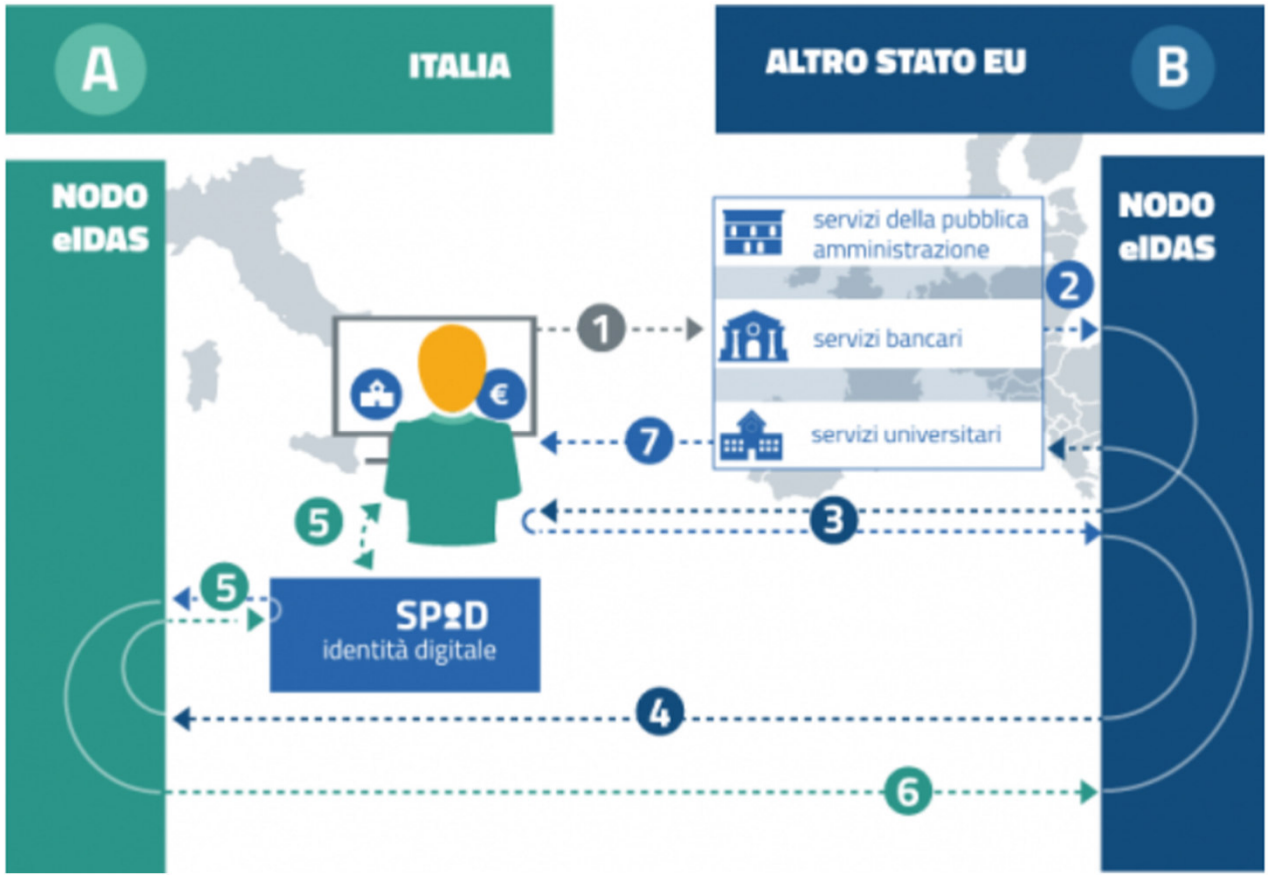
Nodo eIDAS italiano

Il progetto nazionale finanziato dalla Commissione Europea per la realizzazione del nodo eIDAS italiano.

FICEP è il primo "server trasfrontaliero italiano": la sua implementazione consente la circolarità delle identità digitali italiane fra tutti gli stati membri dell'Unione Europea.

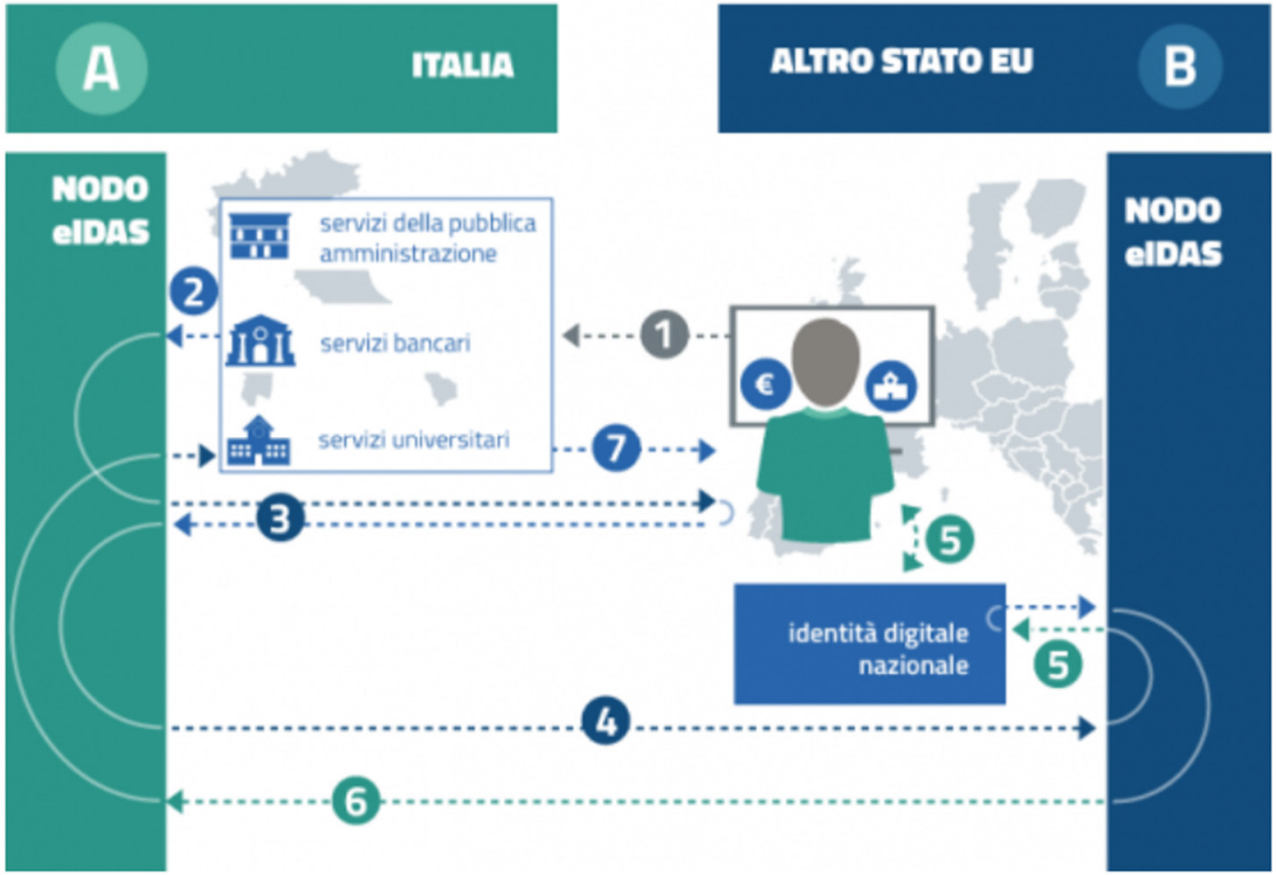
AgID, in raggruppamento con Infocert S.p.a., Politecnico di Torino, Telecom Italia S.p.a., si è aggiudicata con il bando CEF-Telecom eID 2014 un finanziamento per la realizzazione del nodo eIDAS italiano.

Modello semplificato del funzionamento nodo eIDAS



utente italiano richieda di fruire il servizio online di un altro stato membro UE

Modello semplificato del funzionamento nodo eIDAS

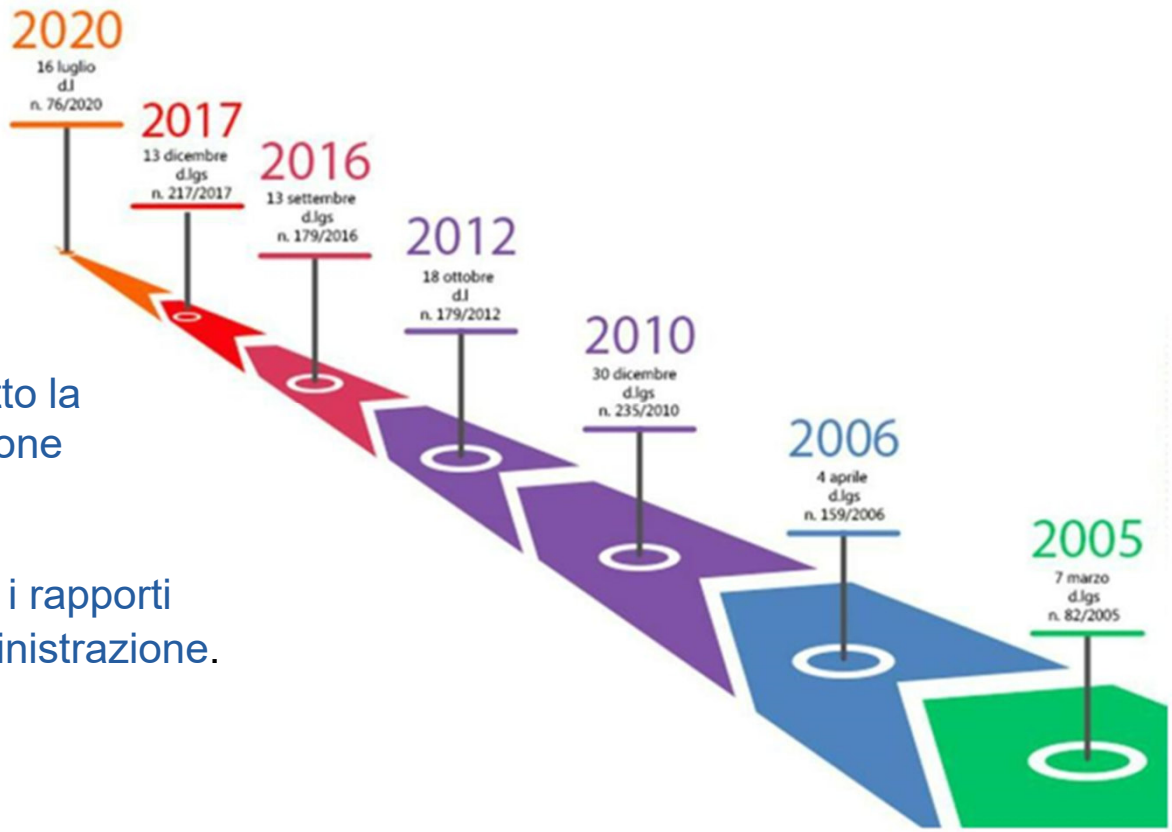


un cittadino UE che chieda di accedere a fornitori di servizi italiani, pubblici o privati utilizzando le credenziali fornitegli nel proprio stato e da questo notificate ai sensi del regolamento eIDAS

La normativa nazionale

D. Lgs. 7 marzo 2005, n. 82
Codice dell'Amministrazione Digitale

Ultima modifica
DL 2 marzo 2024 n. 19
convertito con la Legge 29
aprile 2024 n. 56



È la fonte del diritto che ha per oggetto la regolamentazione dell'informatizzazione della Pubblica Amministrazione

E' soprattutto una legge che governa i rapporti "digitali" tra cittadino e pubblica amministrazione.

Il contenuto del CAD

D. Lgs. 7 marzo 2005, n. 82
Codice dell'Amministrazione Digitale

Diritti digitali di cittadini e imprese: norme che introducono la "**carta della cittadinanza digitale**", definendo il perimetro dei diritti (e dei doveri) di cittadini e imprese nei rapporti con la PA

Obblighi a contenuto **digitale** per le **pubbliche amministrazioni**: norme che definiscono gli obblighi tecnologici e organizzativi di ogni amministrazione, anche con riferimento ai rapporti con gli utenti

Norme sull'**efficacia giuridica e probatoria** dei documenti informatici: norme che regolano il valore giuridico di contratti, dichiarazioni, istanze e atti amministrativi digitali

D. Lgs. 7 marzo 2005, n. 82
Codice dell'Amministrazione Digitale

Capo II - Documento informatico, firme elettroniche, servizi fiduciari e trasferimenti di fondi (art. 20 - 39)

- **Sezione I - Documento informatico**
- **Sezione II - Firme elettroniche, certificati e prestatori di servizi fiduciari**

Art. 20 - Validità ed efficacia probatoria dei documenti informatici

«**1-bis.** Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.»

Art. 2702 cc - (Efficacia della scrittura privata) – «La scrittura privata fa piena prova, fino a querela di falso, della provenienza delle dichiarazioni da chi l'ha sottoscritta, se colui contro il quale la scrittura è prodotta ne riconosce la sottoscrizione, ovvero se questa è legalmente considerata come riconosciuta.»

LA TECNOLOGIA DELLE FIRME ELETTRONICHE

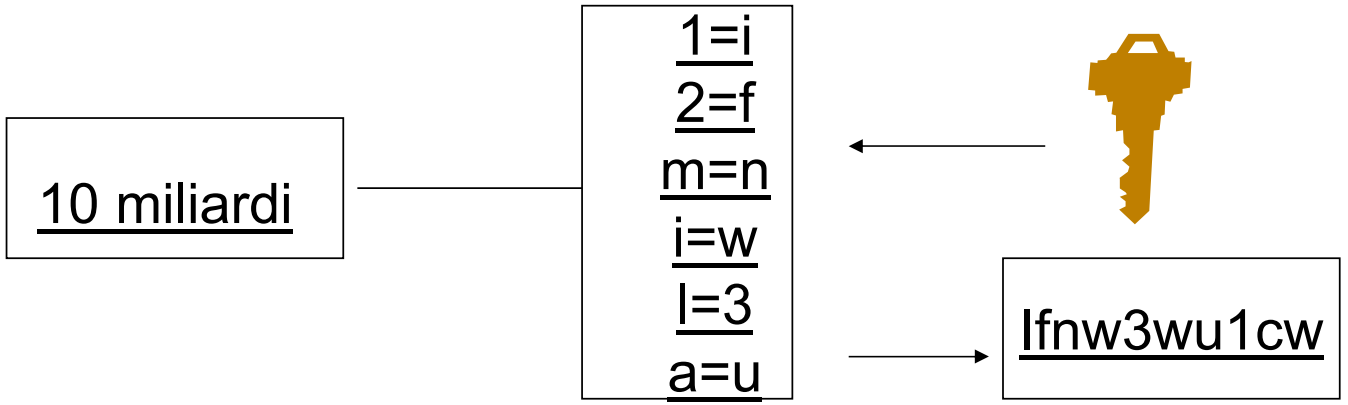
La crittografia

Non è possibile parlare di firma elettroniche senza descrivere in qualche modo la **crittografia** con le sue principali istanze nel mondo digitale, la crittografia simmetrica e quella asimmetrica.

La crittografia

Definizione:

- *Arte di proteggere il segreto di un testo mediante una scrittura convenzionale conosciuta solo da chi scrive e da chi legge.*



Elementi del sistema crittografico

- **Algoritmo:** "*complesso di operazioni che consente di rendere incomprensibile il messaggio scomponendolo in una sequenza di caratteri non immediatamente intellegibili*"
- **Chiave:** *"l'elemento che, associato ad un algoritmo crittografico, consente la crittazione e decrittazione del testo cifrato"*

Fonte: G. Taddei Elmi - Corso di informatica giuridica

La crittografia a chiave simmetrica

- In questo caso la stessa chiave serve per cifrare e decifrare il testo
- Svantaggi:
  - ✓ la comunicazione della chiave condivisa deve avvenire attraverso un canale sicuro
  - ✓ è necessaria una chiave diversa per ogni coppia di interlocutori

La crittografia a chiave asimmetrica

In questo sistema ogni utente ha una coppia di chiavi distinte e legate fra loro:

- la chiave pubblica, *divulgabile*
- la chiave privata, *conosciuta e custodita dal solo proprietario*

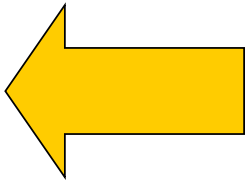
- Non si può decifrare il testo con la stessa chiave usata per cifrarlo
- Conoscendo una delle due chiavi, non c'è nessun modo di ricostruire l'altra

La crittografia a chiave asimmetrica

- Nel 1978 i ricercatori *Rivest, Shamir a Adleman* utilizzando particolari *proprietà formali dei numeri primi*, realizzano i primi cifrari a chiave asimmetrica (algoritmo RSA);
- Si moltiplicano tra loro due numeri primi ciascuno contenente fino a 80 cifre. Si cripta il messaggio con il numero composto ottenuto, che verrà reso pubblico mediante inserimento in apposito elenco, mentre si decripta utilizzando i due numeri primi iniziali da tenere segreti.
- *Ogni utente possiede una coppia chiave, una pubblica e una privata*

La crittografia a chiave asimmetrica

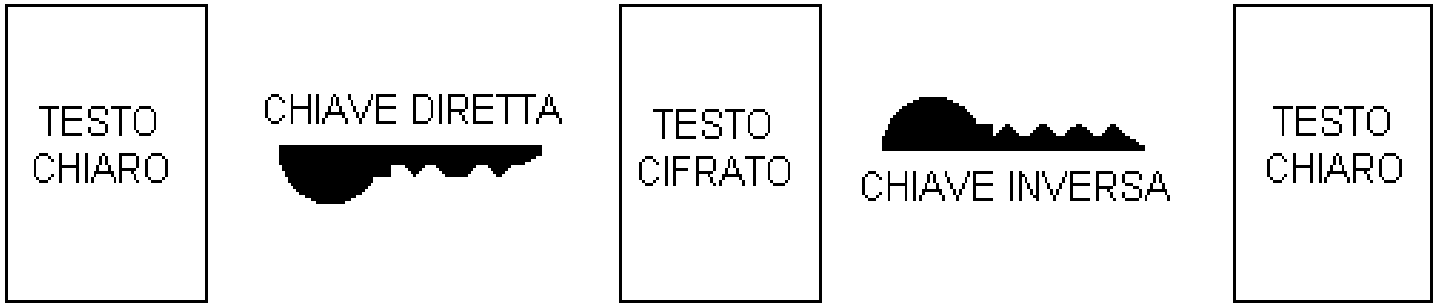
Esempio:
Numero composto ***589***
Fattori primi: ***31*** *e* ***19***



Un banale computer impiega qualche minuto per ricavare i numeri primi

- Perché il sistema funzioni occorre pubblicare un numero composto avente più di cento cifre. *La ricerca dei fattori primi durerebbe diversi anni*
- E' importante quindi la ***complessità computazionale***: non è impossibile decifrarlo, ma è ragionevolmente impossibile farlo in tempo utile

La crittografia a chiave asimmetrica

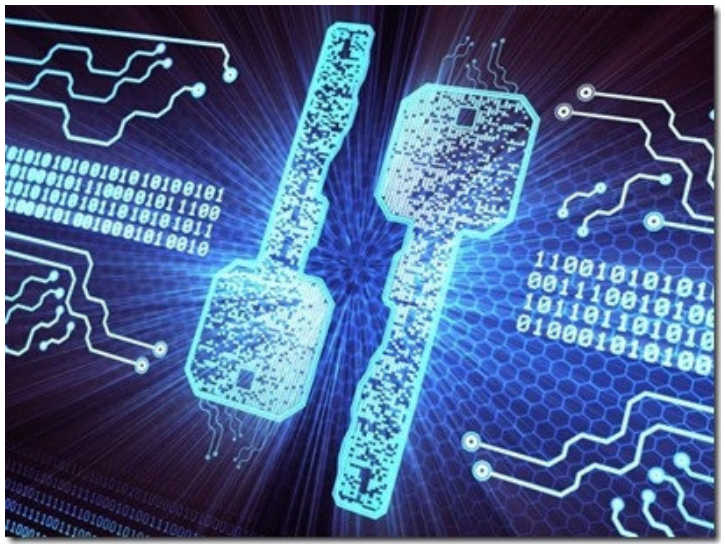


- Cifratura e decifratura di un documento con un cifrario a chiave asimmetrica

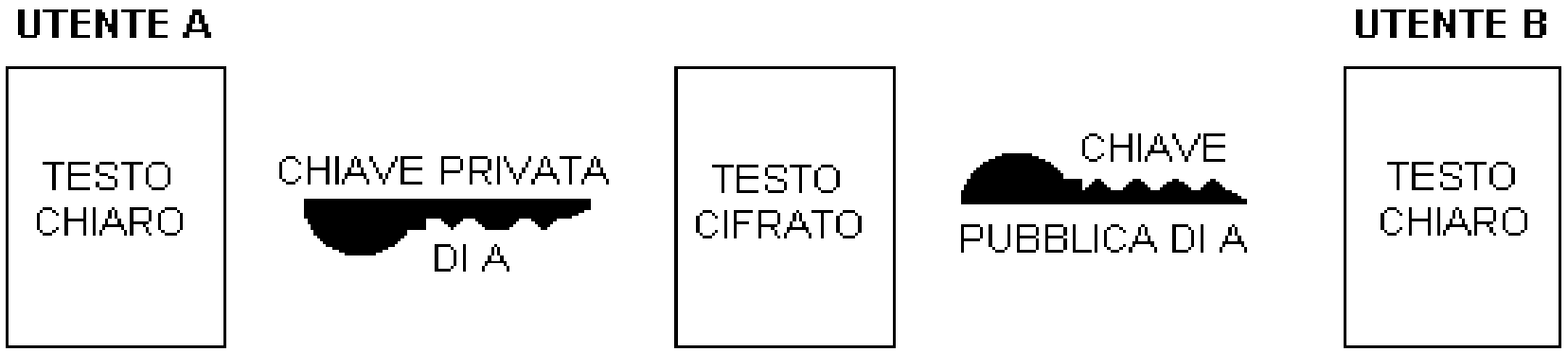
La crittografia a chiave asimmetrica

Questo sistema offre la possibilità a chiunque di inviare un messaggio segreto a chi renda pubblica una delle due chiavi.

- Generare con un software crittografico e generare la propria coppia di chiavi
- Rendere disponibile a chiunque la chiave pubblica
- Per mandare un messaggio segreto deve cifrarlo con la chiave pubblica del destinatario
- Solo il destinatario può decifrare il messaggio perché solo lui dispone della chiave privata



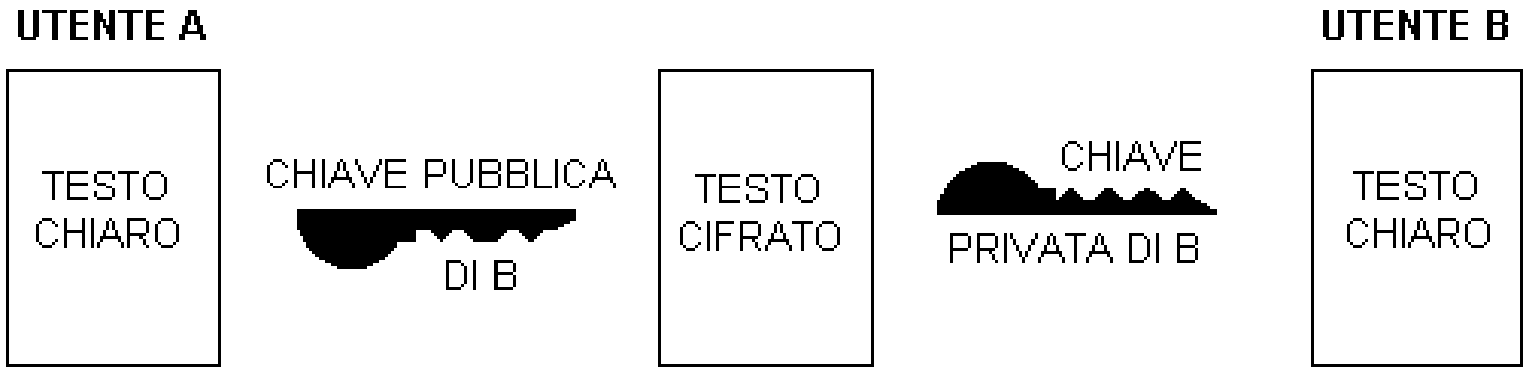
Il riconoscimento del mittente



TESTO CIFRATO CON LA CHIAVE PRIVATA DEL MITTENTE

- Se B riesce a decifrare il messaggio con la chiave pubblica di A, questi è certamente l'autore del testo

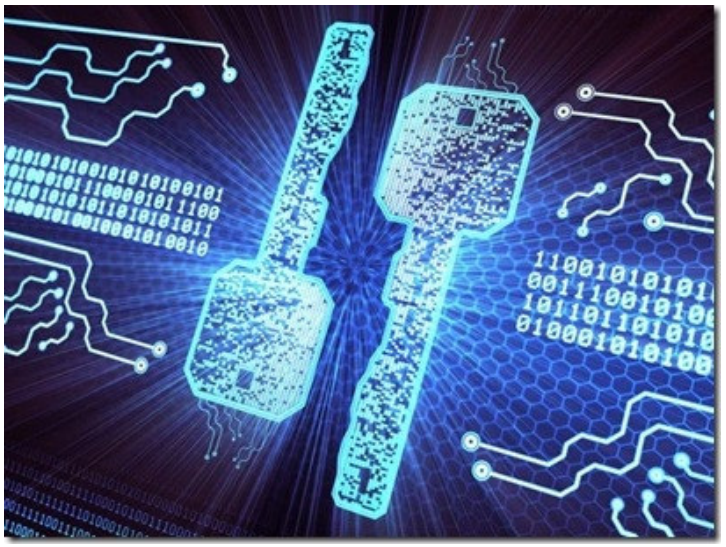
Informazioni segrete con cifratura asimmetrica



- **Invio di un messaggio cifrato con un sistema asimmetrico**
- **Il mittente cifra il testo con la chiave pubblica del destinatario, questi lo decifra con la propria chiave privata**

DOPPIA COMBINAZIONE

- Il mittente può inviare un messaggio segreto *(cifrato con la propria chiave privata e con la chiave pubblica del destinatario)*
- Si ottiene:
  - Sia la segretezza del testo
  - Sia la certezza dell'identità del mittente



Come si può dare
a un testo chiaro la certezza dell'identità del firmatario e dell'integrità del contenuto?

Come funziona la firma digitale?

- Un *documento cartaceo* può essere consegnato ad altri così come appare, visibile a tutti e quindi leggibile da chiunque, oppure inviato al destinatario in plico chiuso da spedire per raccomandata
- Nella telematica l'unica alternativa alla busta, intesa come strumento di garanzia della riservatezza e dell'integrità, è il ricorso a ***sistemi crittografici***

- *Riservatezza:* inviolabilità della corrispondenza
- *Integrità dei dati:* conformità del duplicato all'originale
- *Autenticazione:* effettiva provenienza del documento da colui che appare come mittente
- *Non ripudio*: chi trasmette non deve poter negare di aver trasmesso così come chi riceve non deve poter negare di aver ricevuto

Come funziona la firma digitale?

- Il sistema più elementare è inviare il testo in chiaro insieme ad una versione cifrata con la chiave privata del mittente
- Si opera con la chiave pubblica del mittente e se i due testi sono uguali si ottengono le certezze sulla identità e sulla integrità
- Questo sistema è molto lento perché è necessario cifrare e decifrare tutto il testo che potrebbe essere molto lungo

Funzione di hash

- Si ricorre ad un brevissimo riassunto del testo stesso ottenuto attraverso la

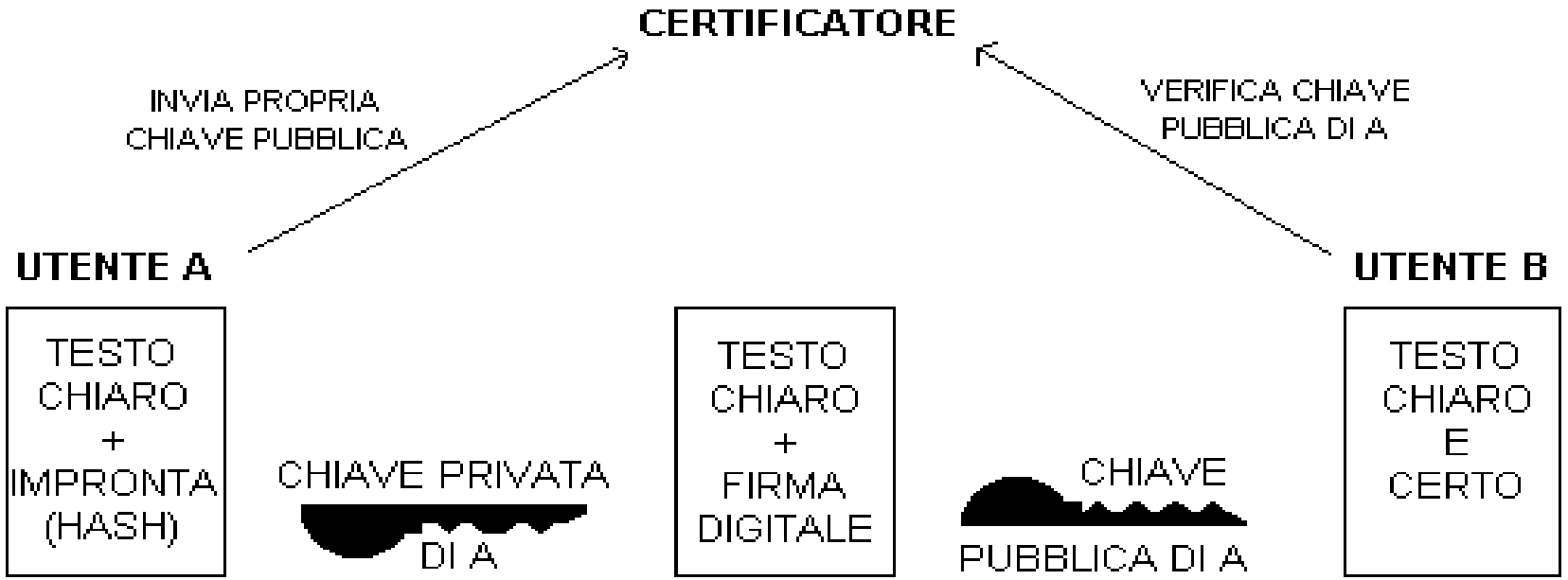
funzione di hash

- Pochi caratteri che costituiscono l'***impronta del testo***

Funzione di hash

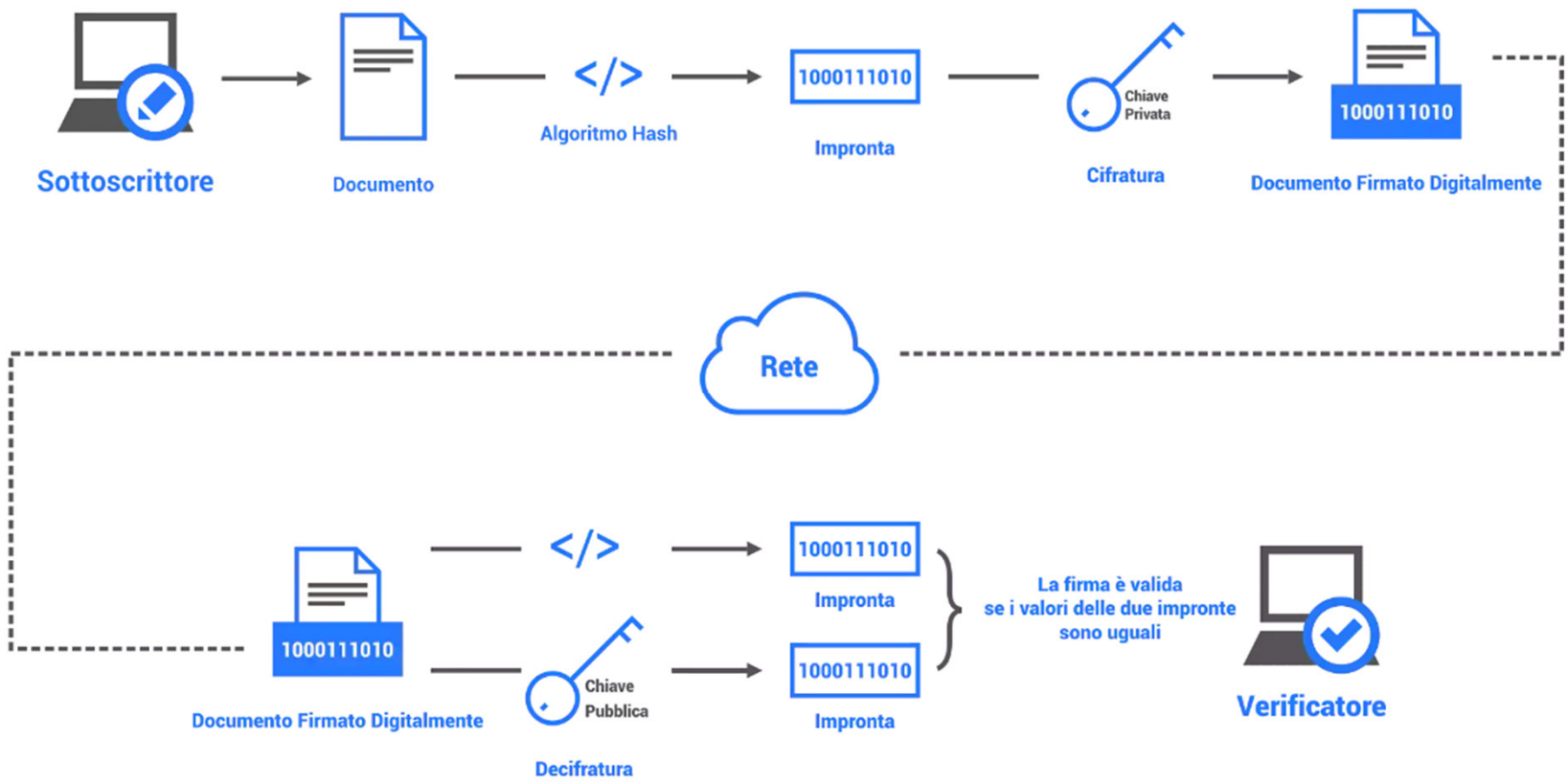
- Algoritmo matematico che, sulla base del numero e del tipo di caratteri, permette di generare *l'estratto*
- L'impronta è unica per ogni documento e basta cambiare anche un solo carattere del testo stesso per avere un'impronta diversa
- Se l'impronta che risulta dalla decifratura è uguale a quella che si ottiene applicando la funzione di hash al testo chiaro, vuol dire che esso non è stato alterato dopo la generazione della firma digitale
- Può sembrare complicato ma in realtà basta un semplice *clic* su un pulsante e il computer in pochi istanti fornisce la risposta

Generazione e verifica della firma



La firma digitale si genera applicando la propria chiave privata all'impronta del testo

Hash, Impronta, coppia di chiavi simmetriche, firma e verifica

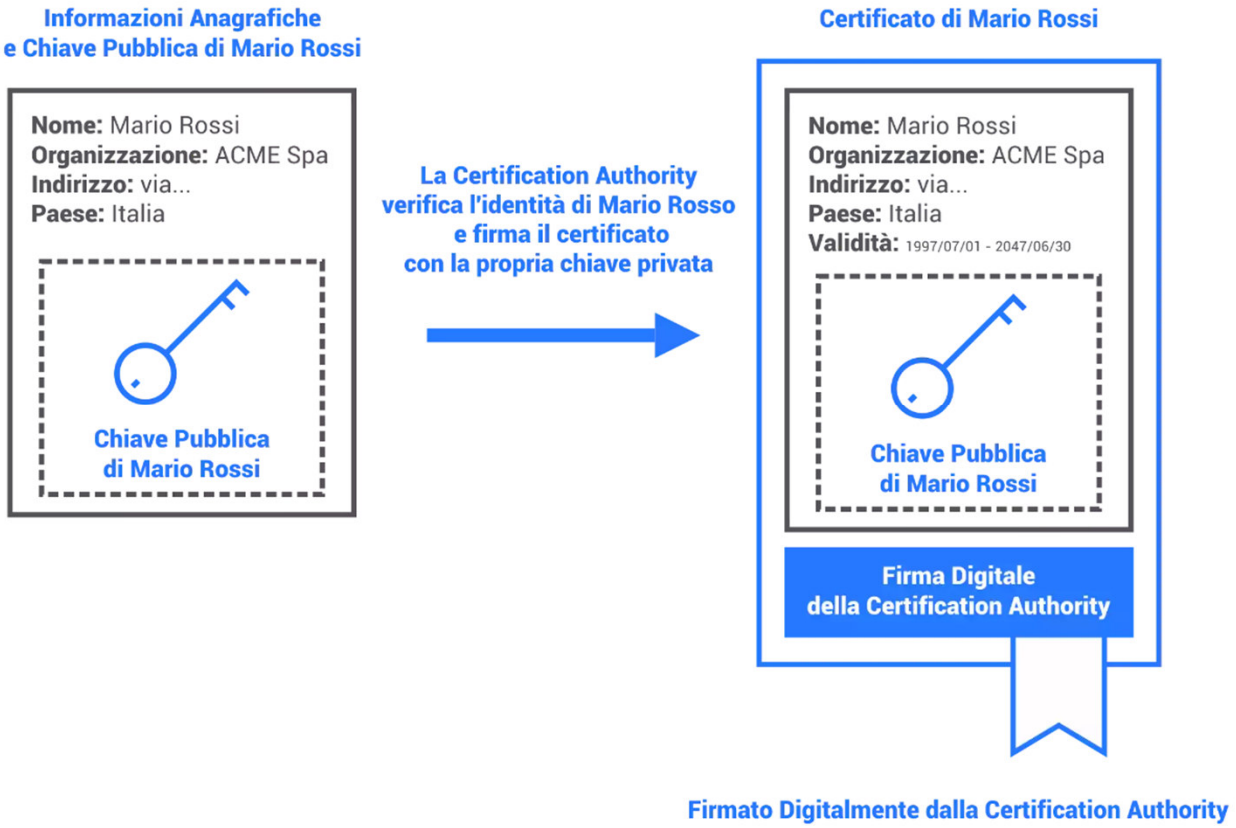


Tecnologie delle firme elettroniche

1. Il sottoscrittore prepara il documento da firmare
2. Il software di firma applica un algoritmo di hash standard e ne deriva **un'impronta** (una stringa di bit di lunghezza fissa, più facile da manipolare dell'intero documento)
3. Il software a questo punto usa la **chiave privata** del sottoscrittore per **cifrare** (con algoritmo di cifratura asimmetrica) l'impronta del documento: il risultato di questa cifratura (un'altra stringa di bit) è la **firma digitale**.
4. La firma digitale è associata al documento, che viene in generale trasmesso a un destinatario
5. In fase di verifica il destinatario (verificatore) elabora il documento con un software che:
6. Calcola l'impronta del documento con lo stesso algoritmo di hash usato dal sottoscrittore.
7. Decifra la firma digitale con la chiave pubblica associata alla chiave privata usata per firmare: il risultato deve essere ancora l'impronta
8. Se le due copie di impronta così ricavate sono uguali allora la firma è valida e il documento è integro

Certificato di chiave pubblica

Per verificare efficacemente le firme elettroniche si ricorre al Certificato di Chiave Pubblica



Certificato di chiave pubblica

- Il Certificato è un file, in formato standard, che contiene i dati anagrafici del proprietario della coppia di chiavi e una copia della chiave pubblica stessa.
- Un soggetto giudicato attendibile si accerta dell'identità del titolare del certificato e lo autentica apponendovi la propria firma: **la Certification Authority.**
- Il certificato è normalmente inserito nel documento insieme alla stringa di bit che ne costituisce la firma.
- Così il verificatore avrà subito a disposizione la chiave pubblica da impiegare nella verifica e potrà verificarne l'autenticità (questo è possibile verificando preventivamente la firma della Certification Authority: è un procedimento ricorsivo, di non facile comprensione, ma efficace)

DEFINIZIONI E TIPOLOGIE DI FIRME ELETTRONICHE

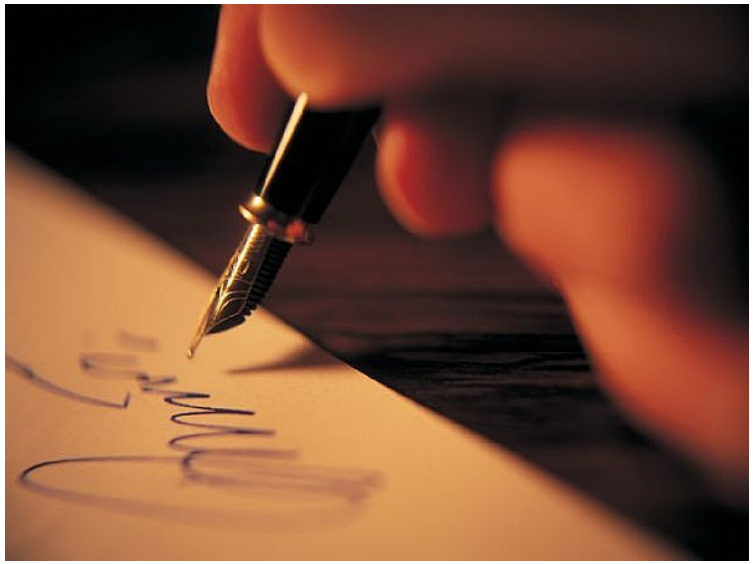
La firma elettronica

Definizione

Il D.lgs. 179/2026 ha soppresso le lettere g); g- bis) e r) del CAD relative alla definizione di firma elettronica, firma elettronica avanzata e firma elettronica qualifica

Art. 3 Regolamento europeo eIDAS

- 10) «**firma elettronica**», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

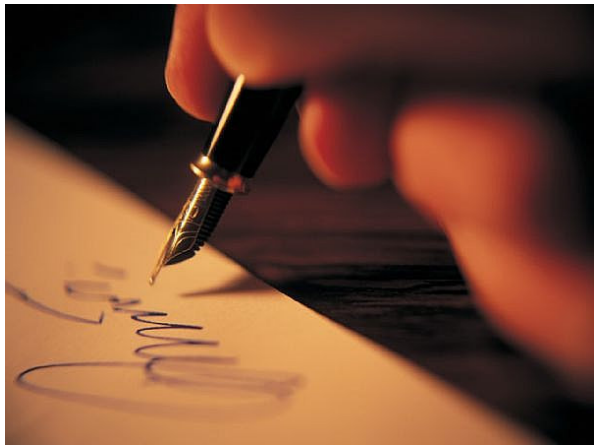


La firma elettronica avanzata

Definizione

Art. 3 Regolamento europeo eIDAS

- 11) «**firma elettronica avanzata**», una firma elettronica che soddisfi i requisiti di cui all'articolo 26 del regolamento;



Art. 26 /eIDAS – Requisiti delle firma elettronica avanzata
«Una firma elettronica avanzata soddisfa i seguenti requisiti:

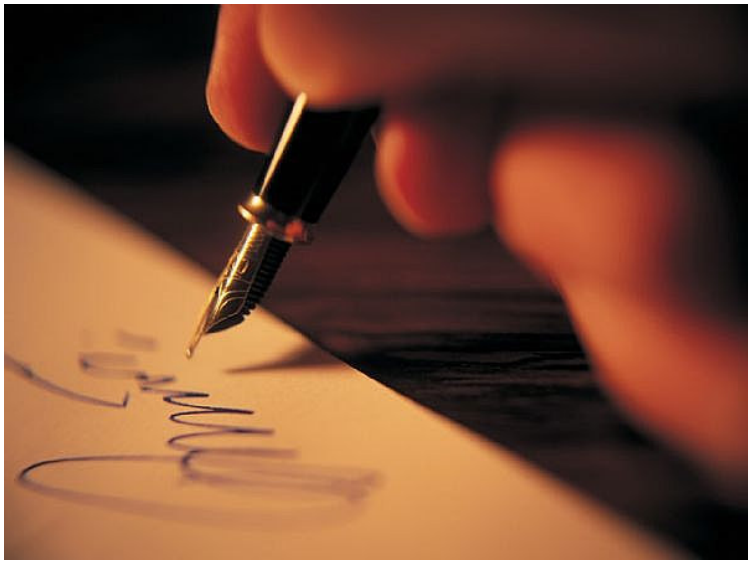
a) è connessa unicamente al firmatario;
b) è idonea a identificare il firmatario;
c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo;
d) è collegata ai dati sottoscritti in modo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

La firma elettronica avanzata

Definizione

Art. 3 Regolamento europeo eIDAS

- 12) «**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;



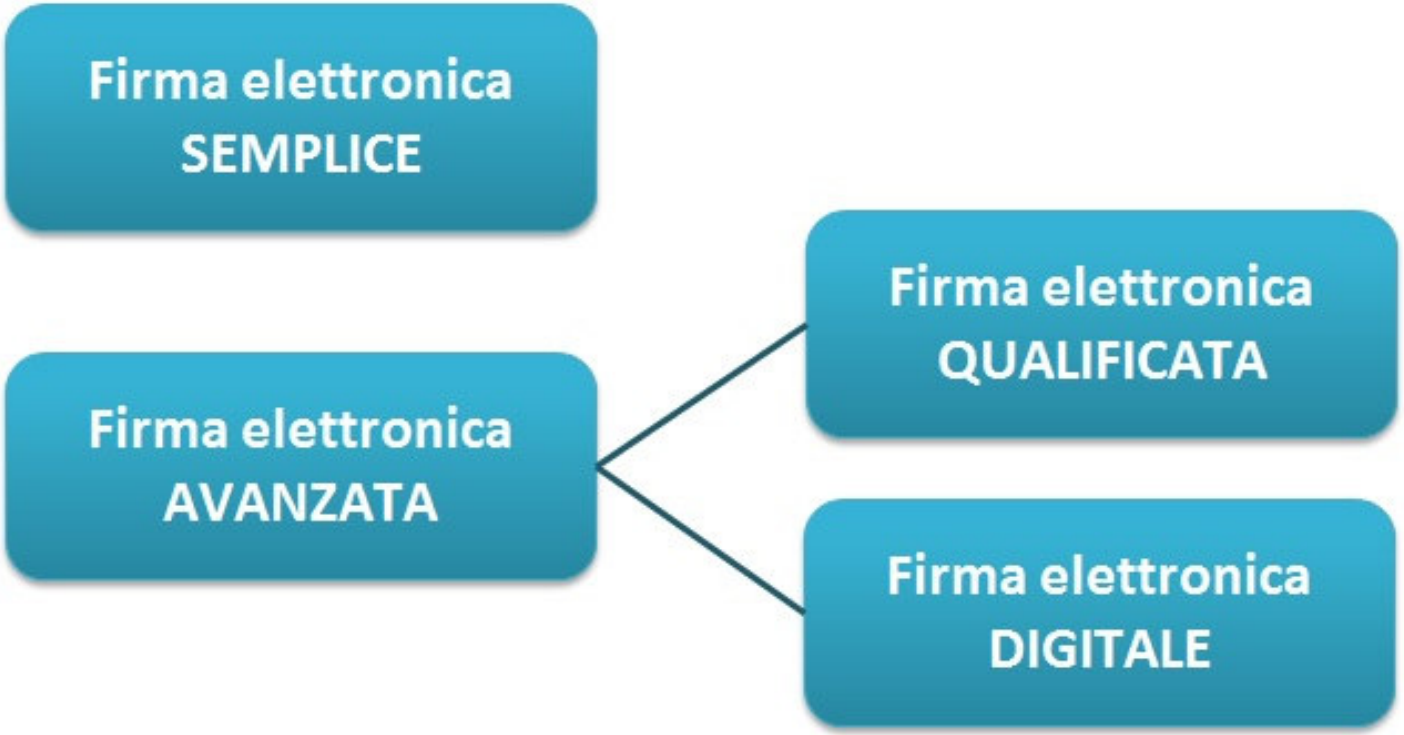
La firma elettronica avanzata

Definizione

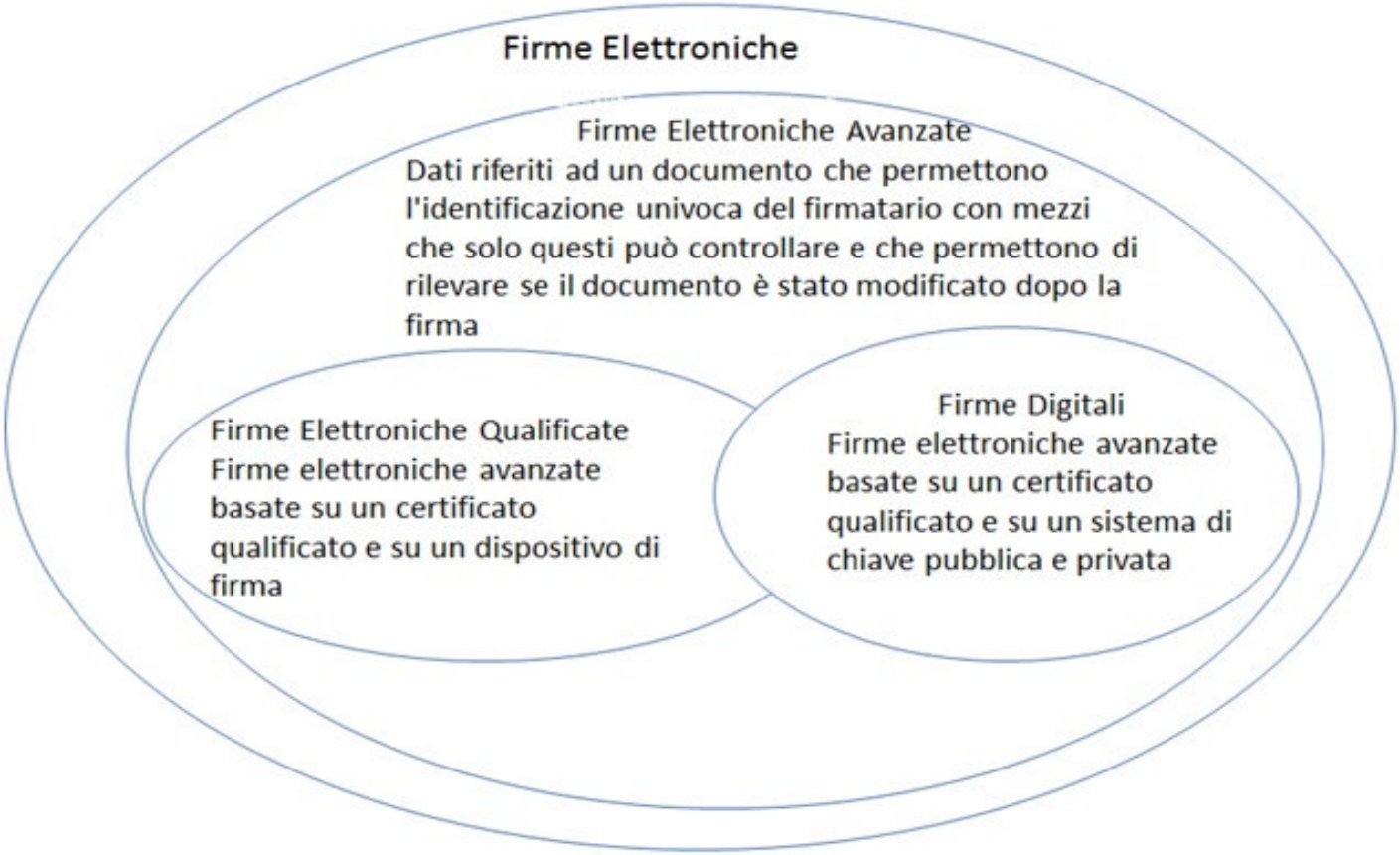
Art. 1 CAD

- s) **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 tramite la chiave privata e al destinatario 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

Tipologie di firme elettroniche



Varie tipologie di firme



La firma elettronica (semplice)

Firma elettronica:

- Ricomprende qualsiasi tipo di identificazione che in qualche modo consenta una qualsiasi associazione logica tra un determinato soggetto e determinati dati:
  - *PIN del bancomat,*
  - *normali credenziali di accesso costituite da nome utente e password;*
  - *etc*
- Firma e documento in ogni caso rimangono sempre entità distinte, ancorché logicamente associate

Firma elettronica leggera o semplice

La firma elettronica avanzata (FEA)

***Firma elettronica avanzata (FEA)*,**

- Consente di identificare in modo univoco il firmatario garantendo anche l'evidenza di modifiche all'oggetto firmato, apportate dopo la sottoscrizione;
- Si caratterizza per il fatto di essere "collegata ai dati" a cui si riferisce, in modo da consentire di rilevare eventuali alterazioni successive.
- Firma e documento quindi si fondono in un'unica entità, e vengono separate solo al momento della verifica della firma. Che poi nella prassi, per economia di calcolo, si firmi non direttamente il documento, ma la sua impronta, non rileva ai nostri fini perché ogni variazione del documento si ripercuote direttamente sulla sua impronta

Esempio di FEA: Firma grafometrica

La firma elettronica qualificata (FEQ)

***Firma elettronica qualificata (FEQ)*,**

- Evidenzia l'evoluzione della fattispecie di sottoscrizione verso livelli di sicurezza superiori. Con la firma elettronica qualificata questi livelli sono il massimo possibile rispetto al regolamento eIDAS
- Il dispositivo citato per la creazione della FEQ deve sodisfare una pluralità di requisiti che vengono dettagliati in modo puntuale nell'allegato II del regolamento eIDAS

Esempio di FEQ: Firma digitale

Il dispositivo di firma

Nell'impiego della firma digitale è obbligatorio usare un ***"dispositivo di firma"***, per tutte le operazioni sia di generazione delle chiavi, sia di sottoscrizione dei documenti

Il dispositivo di firma

- *"**dispositivo di firma**", un apparato elettronico programmabile solo all'origine, facente parte del sistema di validazione, in grado almeno di conservare in modo protetto le chiavi private e generare al suo interno le firme digitali.*

Il dispositivo: smart cart o token USB

- Smart card o token USB
- Sono memorizzate:
  - *Chiave pubblica*
  - *Chiave privata*
  - *Certificato*
- *Il PIN (Personal Identification Number)* attiva la smart card
- *Il PUK* – Blocca la smart card
- Nel chip vengono effettuati tutti i calcoli di cifratura che utilizzano la chiave privata
- Le informazioni relative alla chiave privata non escono dal chip

L’uso della firma digitale

Vi sono due modalità di utilizzare la firma digitale:

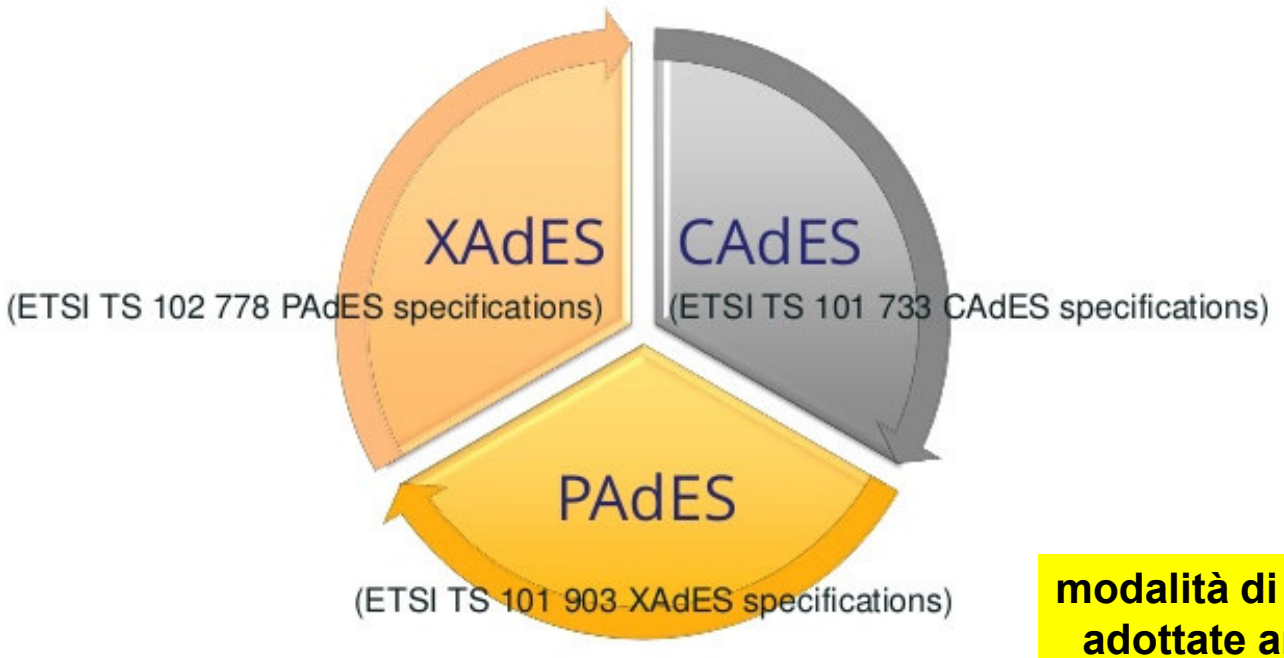
- **in "locale":** si intende la firma digitale generata in uno strumento nel possesso fisico del titolare, smartcard o token

- **da "remoto":** si intende la firma digitale generata usando strumenti di autenticazione (tipicamente user id+ password +OTP o telefono cellulare) che consentono la generazione della propria firma su un dispositivo (HSM) custodito dal certificatore (in terminologia europea, prestatore del servizio fiduciario qualificato).

Tipi di sottoscrizione delle firma digitale

Tutte le firme “AdES” sono considerate “firme elettroniche qualificate

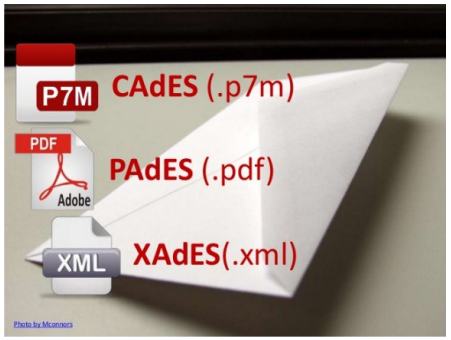
Gli standard europei prevedono tre tipi di sottoscrizione digitale, identificati dagli acronimi CAdES, PAdES e XAdES



modalità di sottoscrizione adottate anche in Italia.

Tipi di sottoscrizione delle firma digitale

CAdES	**Cryptographic Message Syntax Advanced Electronic Signature** *Il file sottoscritto conserva il suo nome e la sua estensione originale, al quale viene aggiunta l'estensione .p7m* *(ad esempio: nomedocumento.pdf.p7m)*
PAdES	**PDF Advanced Electronic Signature.** *File con estensione .pdf.* *Questo formato è leggibile con i comuni reader disponibili per questo formato*
XAdES	**XML Advanced Electronic Signature** *File con estensione .xml*



La firma CAdES

La firma **CAdES** (CMS Advanced Electronic Signatures) è una firma digitale che può essere apposta su qualsiasi tipo di file, con la CAdES si possono firmare file di testo comunque generati (Microsoft Word, OpenOffice Writer, semplici file di testo, etc.), fogli di calcolo (Microsoft Excel, OpenOffice Calc), file immagine (JPEG, GIF, PNG, etc.), ovviamente è possibile firmare anche dei PDF, insomma basta che sia un file ed è possibile mettere la firma digitale CAdES.

L'apposizione di una firma CAdES su un qualsiasi file genera una busta crittografica contenente il file originale che si presenta come un file la cui estensione (la parte finale del nome del file che succede il punto) è P7M

Tipi di sottoscrizione delle firma digitale

La firma CAdES

Pregi	Difetti
• può essere apposta su qualsiasi tipo di file, file di testo (Microsoft Word, OpenOffice Writer, semplici file di testo, etc.), fogli di calcolo (Microsoft Excel, OpenOffice Calc), file immagine (JPEG, GIF, PNG, etc.), PDF.	• per potere aprire la busta "p7m" è necessario avere a disposizione un software specifico, come DiKE, File Protector, ArubaSign, che riesca che si trova all'interno di un lettore/scrittore di smart card. • per effettuare più firme sullo stesso documento è necessario re-imbustare in una nuova busta CAdES la prima "busta" contenente la firma con un effetto detto "matrioska". • non è possibile aggiungere una firma grafica visibile sul documento[45].

Tipi di sottoscrizione delle firma digitale

La firma PAdES

La firma **PAdES** (PDF Advanced Electronic Signatures) è una firma che può essere apposta su un solo tipo di file, il PDF che è lo standard di riferimento per quanto riguarda i documenti in formato digitale.

L'apposizione di una firma PAdES su un file .pdf genera un nuovo file la cui estensione (la parte finale del nome del file che succede il punto) è ancora PDF

Pregi	Difetti
• non è necessario alcun tipo di software e lettore specifico per aprire la busta che si apre in PDF • è possibile firmare un documento senza l'effetto matrioska e senza invalidare le sottoscrizioni precedentemente apposte. • è possibile aggiungere una firma grafica visibile sul documento, oltre quella digitale, potendo quindi essere inserita nel punto desiderato del documento	• è possibile firmare solo PDF.

Come scelgo la firma?

La domanda è ovvia, perché dovrei usare la firma PAdES quando potrei utilizzare indifferentemente la firma CAdES per tutti i documenti?
Perché utilizzando la firma PAdES il file firmato può essere letto utilizzando qualsiasi lettore di file PDF (il più diffuso è Adobe Reader in precedenza noto come Acrobat), mentre utillizando la firma CAdES sarà necessario disporre di un software specifico per l'apertura della *busta crittografica* (il file .p7m) che contiene il documento per poterli visualizzare.

La firma PAdES, inoltre, permette di aggiungere una firma grafica visibile sul documento, oltre alla firma digitale.
Quindi se dobbiamo inviare un documento firmato ad un soggetto che non conosciamo sarà meglio utilizzare una firma PAdES, non sappiamo infatti se sarebbe in grado di aprire un documento firmato con CAdES.

Verifica della firma digitale

La **verifica della firma digitale** e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in modo conforme.

I produttori dei seguenti **software** rendono disponibili per il download i propri prodotti gratuitamente:

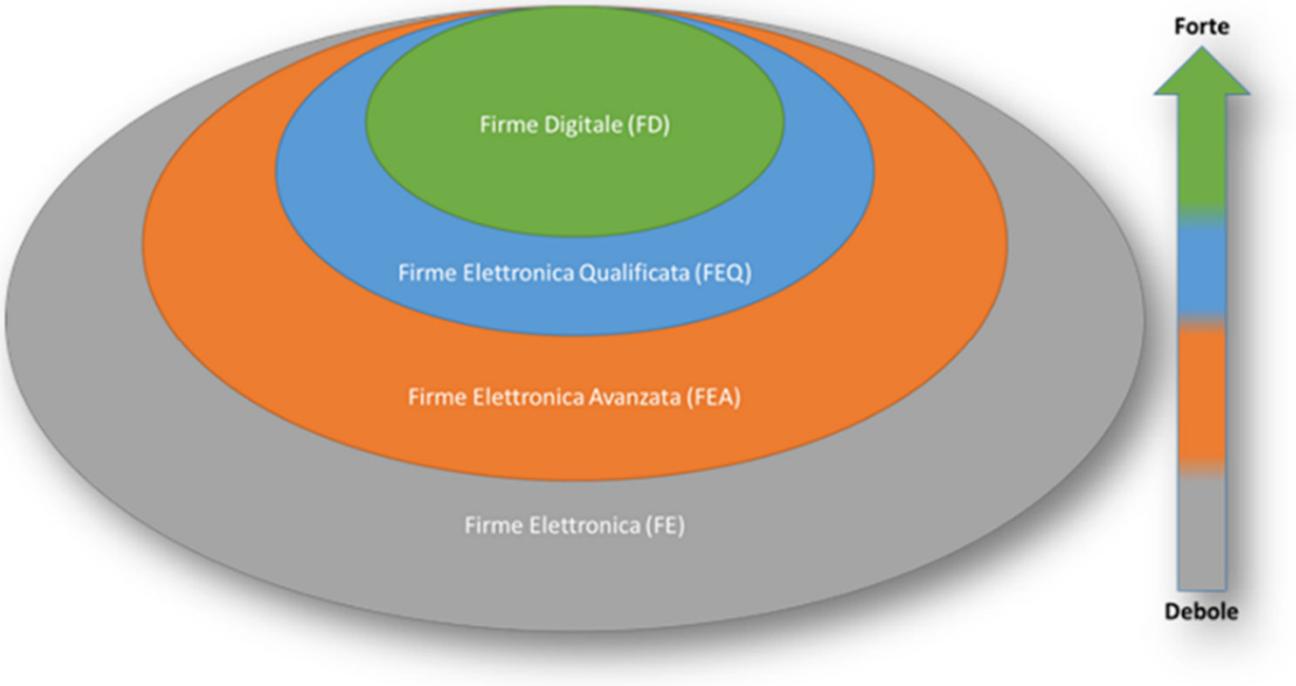
- Digital Signature Service
- DigitalSign Reader
- Firma OK!
- PkNet
- GoSign
- Namirial Sign
- Acrobat Reader DC
- ArubaSign
- GeniuSign
- Globo.Signer
- ……

Peculiarità della firma elettronica qualificata (o digitale)

- **Autenticità**: l'identità del sottoscrittore digitale è certa
- **Integrità:** la verifica positiva della firma attesta che il documento è integro
- **Non disconoscibilità (non ripudio):** la firma può essere disconosciuta dal presunto firmatario con la produzione da pare dello stesso della prova che non ha utilizzato il dispositivo di firma elettronica qualificata (o digitale). Si utilizza anche l'espressione «non ripudio» della sottoscrizione
- **Validità temporale:** al documento sottoscritto può essere associata una validazione temporale per attestarne l'esistenza in quello stato (es.: documento sottoscritto) a quella data ed ora.

Firme deboli e forti

Pensando ad uno schema, le varie firme esaminate possono essere rappresentate come:



Responsabile del titolare di firma digitale

Art. 21 co.2.

- «<*omissis*> . L'utilizzo del dispositivo di firma elettronica qualificata o digitale si presume riconducibile al titolare, salvo che questi dia prova contraria.»

Art. 32 co.1

- Il titolare del certificato di firma è tenuto ad assicurare la custodia del dispositivo di firma o degli strumenti di autenticazione informatica per l'utilizzo del dispositivo di firma da remoto, e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma.

Modificato dal D.Lgs. 29/08/2016 nr. 179

Certificato elettronico revocato, scaduto o sospeso

CAD - Art. 24 – Firma digitale

4-bis. L'apposizione a un documento informatico di una firma digitale o di un altro tipo di firma elettronica qualificata basata su un certificato elettronico

- revocato,
- scaduto
- sospeso

equivale a mancata sottoscrizione, salvo che lo stato di sospensione sia stato annullato.

Certificato elettronico revocato, scaduto o sospeso

DPCM 22/02/2013 – Art. 62 Valore delle firme elettroniche qualificate e digitali nel tempo

Le firme elettroniche qualificate e digitali, ancorché sia scaduto, revocato o sospeso il relativo certificato qualificato del sottoscrittore, **sono valide se alle stesse è associabile un riferimento temporale opponibile ai terzi** che collochi la generazione di dette firme rispettivamente in un momento precedente alla scadenza, revoca o sospensione del suddetto certificato.

Certificato elettronico revocato, scaduto o sospeso

DPCM 22/02/2013 – Art. 41 Riferimenti temporali opponibili a terzi

Costituiscono validazione temporale:

- ✓ Marca temporale
- ✓ Segnatura di protocollo
- ✓ Conservazione digitale a norma
- ✓ PEC
- ✓ Marcatura postale elettronica

Allungano la validità della firma digitale

Firma digitale autenticata

- L'autenticazione consiste nell'attestazione, da parte del pubblico ufficiale, che la firma sia stata apposta in sua presenza dal titolare, previo accertamento della sua identità personale, della validità del certificato elettronico utilizzato e del fatto che il documento sottoscritto non sia in contrasto con l'ordinamento giuridico
- A differenza del documento cartaceo l'autenticazione non è limitata alla presenza del titolare per la firma ma è estesa alla validità del certificato rilasciato al titolare della firma

Le proprietà della firma digitale (1/2)

La firma digitale supera in sicurezza ed affidabilità ogni sistema di certificazione tradizionale in quanto:

- La firma digitale è separata dal documento cui si riferisce e non lo modifica in alcun modo.
- La firma digitale non può essere apposta in bianco. Essa infatti deve far riferimento ad un "contenuto" , se il documento non esiste la firma non può essere calcolata.
- La firma digitale è differente da un documento all'altro. Essa dipende infatti dal contenuto del documento cui si riferisce. *(ciò significa che non è possibile falsificare o imitare la firma digitale, né duplicarla su un documento differente pur prelevandola da un documento valido)*
- La validità della firma digitale può essere verificabile da chiunque in modo certo e ripetibile. Non servono esperti e non vi è nessun margine di incertezza

Le proprietà della firma digitale (2/2)

- La firma digitale rivela eventuali modifiche al testo originale fatte dopo la apposizione.
  Se il testo è stato modificato anche minimamente, il suo contenuto non sarà uguale a quello calcolato dalla firma originale.
- La firma digitale non può essere ripudiata.
  La firma non può essere generata se non dal suo legittimo proprietario, pertanto non può in nessun modo sostenere di non essere stato lui a generarla.

Le differenze

Documento cartaceo

- Dopo la formazione può essere facilmente modificato
- Immediatamente accessibile
- Rimane accessibile nel tempo
- I legami tra documenti possono dipendere dalla posizione fisica (collocazione nel medesimo fascicolo)
- La sottoscrizione e la segnatura possono essere apposte direttamente sul documento

Documento informatico

- Non può essere modificato (se si adottano tecnologie specifiche)
- Accessibile tramite attrezzature e procedure idonee
- l'invecchiamento tecnologico richiede passaggi periodici
- I legami tra documenti dipendono dall'organizzazione logica (attribuzione dello stesso codice di classificazione)
- La sottoscrizione e la segnatura di protocollo devono essere associate al documento attraverso procedure specifiche

Firma ex art 20/CAD (firma tramite SPID)

La firma tramite SPID trova origine nell’art. 20 comma 1-bis del CAD

«**1-bis.** Il documento informatico soddisfa il requisito della forma scritta e ha l'efficacia prevista dall'articolo 2702 del Codice civile quando vi è apposta una firma digitale, altro tipo di firma elettronica qualificata o una firma elettronica avanzata o, comunque, è formato, previa identificazione informatica del suo autore, attraverso un processo avente i requisiti fissati dall'AgID ai sensi dell'articolo 71 con modalità tali da garantire la sicurezza, integrità e immodificabilità del documento e, in maniera manifesta e inequivoca, la sua riconducibilità all'autore. In tutti gli altri casi, l'idoneità del documento informatico a soddisfare il requisito della forma scritta e il suo valore probatorio sono liberamente valutabili in giudizio, in relazione alle caratteristiche di sicurezza, integrità e immodificabilità. La data e l'ora di formazione del documento informatico sono opponibili ai terzi se apposte in conformità alle Linee guida.»

Linee guida emesse da AgID con determinazione 157/2020 intitolate «Linee guida per la sottoscrizione elettronica di documenti ai sensi dell’art. 20 del CAD»

spid
Sistema Pubblico
di Identità Digitale

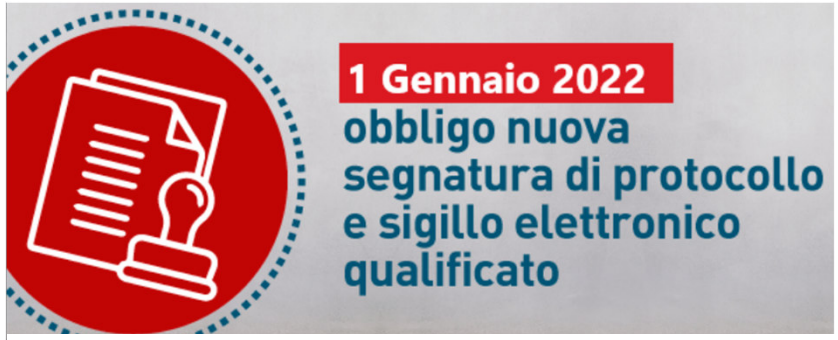
IL SIGILLO ELETTRONICO

Sigillo elettronico

Definizione (Art. 3 - Regolamento eIDAS)

25) **«sigillo elettronico»,** 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

Il **sigillo elettronico** è ancora oggi relativamente poco utilizzato. Eppure, emerge quando si parla di documenti digitali.



Altre definizioni relative al sigillo elettronico (art. 3/eIDAS)

24) **«creatore di un sigillo»,** una persona giuridica che crea un sigillo elettronico;
25) …
26) **«sigillo elettronico avanzato»**, un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;
27) **«sigillo elettronico qualificato»**, un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;
28) **«dati per la creazione di un sigillo elettronico»**, i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;
29) **«certificato di sigillo elettronico»**, un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;
30) **«certificato qualificato di sigillo elettronico»**, un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;
31) **«dispositivo per la creazione di un sigillo elettronico»**, un software o hardware configurato utilizzato per creare un sigillo elettronico;
32) **«dispositivo per la creazione di un sigillo elettronico qualificato»**, un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

Creatore del «Sigillo elettronico»

Analogamente a quanto previsto nell'ambito della firma elettronica, il Regolamento eIDAS prevede che ci sia un creatore del sigillo ovvero *"una persona giuridica che crea un sigillo elettronico*", utilizza dei dati unici in forma elettronica per creare il sigillo elettronico, realizzando l'associazione con i dati del documento elettronico che si vuole "sigillare" al fine di garantirne l'integrità e la paternità.

art. 3 paragrafo 24

Il Sigillo elettronico diventa uno *"strumento da utilizzare per certificare la qualità e l"affidabilità dei dati gestiti da una persona giuridica e rilasciati a un cittadino, un'impresa, o trasmessi da un sistema a un altro con i meccanismi dell' interoperabilità e cooperazione applicativa"*.

Tipologie di «Sigillo elettronico»

Esistono due grandi tipologie, che variano secondo i requisiti di sicurezza intrinseci, di sigillo elettronico.

Nello specifico:

- **avanzato;**
- **qualificato.**

Certificato qualificato di «Sigillo elettronico»

Per **“certificato qualificato di sigillo elettronico**”, si intende un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica confermando il nome di tale soggetto,

Il certificato è rilasciato da un prestatore di servizi fiduciari qualificato nonché è conforme a particolari requisiti, che indicano quali sono gli elementi che tali certifica e devono obbligatoriamente contenere.

A tal proposito si veda il Regolamento (UE) 910/2014, art. 3, paragrafi 29 e 30, nonché Allegato III.

Il Sigillo elettronico serve per…

Fatturazione Elettronica SDI XML

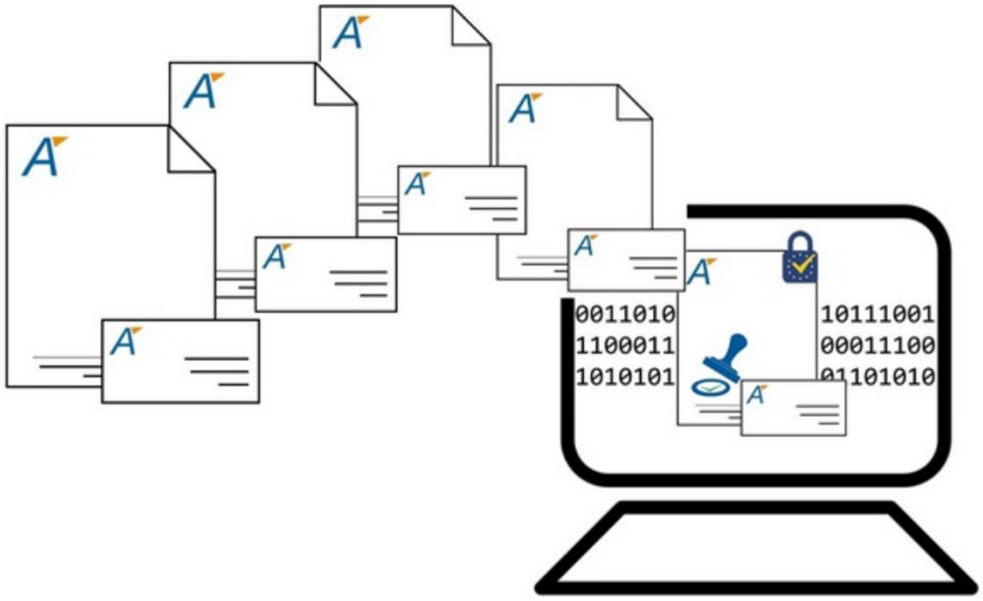
eProcurement System

CDP Certificato di Proprietá Digitale ACI PRA

Protocollo Informatico

Il Sigillo elettronico serve per…

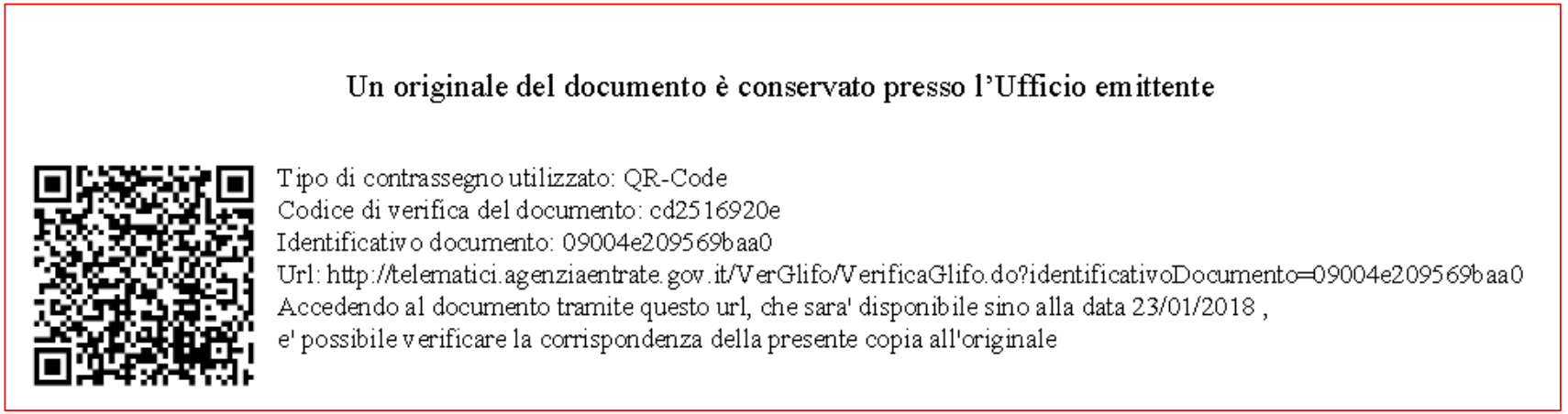
Digitalizzare la carta intestata e la comunicazione della organizzazione con il sigillo elettronico qualificato
Il sigillo elettronico è l'equivalente digitale del classico timbro aziendale che **certifica e tutela l'origine e l'affidabilità dei dati**.



Il «glifo»

Servizio di verifica dei documenti con "glifo" inviati dall'Agenzia

Questa funzione consente di verificare la corrispondenza tra i documenti originali e le copie inviate al contribuente sulle quali è stato apposto il "glifo" in conformità all'articolo 23, comma 2-bis della Legge 82/2005 (Codice dell'Amministrazione Digitale).



Un originale del documento è conservato presso l'Ufficio emittente

Tipo di contrassegno utilizzato: QR-Code
Codice di verifica del documento: cd2516920e
Identificativo documento: 09004e209569baa0
Url: http://telematici.agenziaentrate.gov.it/VerGlifo/VerificaGlifo.do?identificativoDocumento=09004e209569baa0
Accedendo al documento tramite questo url, che sara' disponibile sino alla data 23/01/2018 ,
e' possibile verificare la corrispondenza della presente copia all'originale

Il servizio di verifica on line è disponibile fino alla data indicata sul documento.

«[ ] se non v'è dispiaciuta affatto, vogliatene bene a chi l'ha scritta, e anche un pochino a chi l'ha raccomodata. Ma se in vece fossimo riusciti ad annoiarvi, credete che non s'è fatto apposta.»

Cap. XXXVIII – I Promessi Sposi

Grazie