



## **Identificazione e Sottoscrizione Digitale degli Studenti: strumenti attuali ed evoluzioni future in ottica europea**

---

**UniSTUD, 7° Coordinamento nazionale  
delle Segreterie Studenti**  
25 e 26 maggio 2023

# Agenda



---

## 01. Introduzione

Basi sulle firme.

Basi sull'identificazione e autenticazione.

---

## 02. In Italia

Come si firma in Italia, stato dell'arte.

---

## 03. In Europa

Il Regolamento 910/2014 (eIDAS) e lo stato dell'arte comunitario.

---

## 04. Novità

Il portafoglio europeo di identità digitale.

---

## 05. Chiusura

Lo scenario a breve termine

# Basi sulla firma

---

## La crittografia asimmetrica

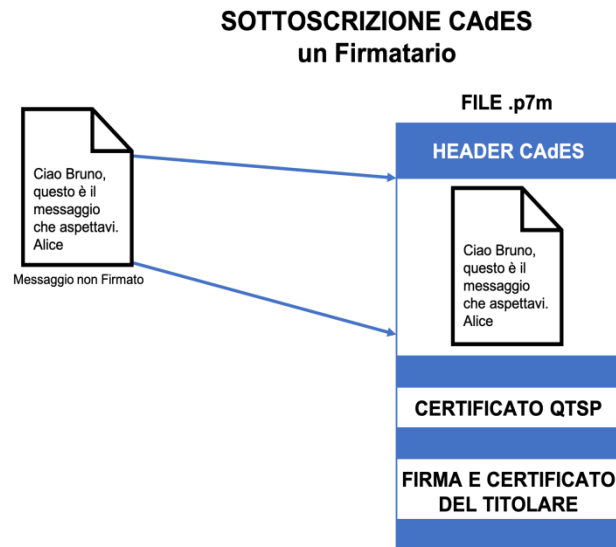
- Una coppia di chiavi crittografiche
- Ciascun firmatario ha una propria coppia
- Una chiave è pubblica
- La chiave pubblica è assegnata univocamente a un titolare tramite un certificato digitale
- La chiave privata è usata per firmare

## Cosa succede

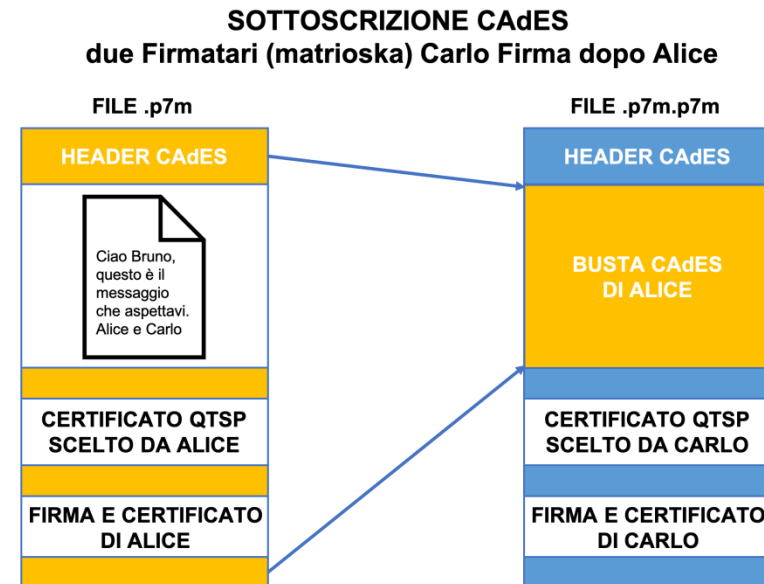
- Il documento informatico viene preparato per la firma
- Si calcola l'impronta del documento (funzione di hash)
- L'impronta viene cifrata con la chiave privata
- L'impronta viene decifrata con la chiave pubblica
- I formati di firma (CAAdES, XAdES, PAdES e JAdES) aggregano documento, firma, certificato e altre informazioni.

# Un paio di esempi

## Struttura firma CADES



## CADES due firmatari



# Identificazione

---

## Identificazione

- **eIDAS, identificazione elettronica:** il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica o un'unica persona fisica che rappresenta una persona giuridica.
- **eIDAS, dati di identificazione personale:** un insieme di dati che consente di stabilire l'identità di una persona fisica o giuridica o di una persona fisica che rappresenta una persona giuridica.

## Metodi di identificazione

- **eIDAS, mezzi di identificazione elettronica:** un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online
- **CAD, identità digitale:** la rappresentazione informatica della corrispondenza tra un utente e i suoi attributi identificativi, verificata attraverso l'insieme di dati raccolti e registrati in forma digitale secondo le modalità fissate nel decreto attuativo dell'articolo 64
- Nell'articolo 64 sono stabilite le regole per SPID
- L'accesso ai servizi può avvenire anche tramite Carta Nazionale dei Servizi e Carta di Identità Elettronica.

# Autenticazione

---

## Autenticazione

- Conferma della propria identificazione. L'individuo è chi sostiene di essere.
  - ✓ Autenticazione a un fattore
  - ✓ Autenticazione a due fattori
  - ✓ Autenticazione con strumenti hardware

## Metodi di Autenticazione

- Password
- One Time Password (OTP)
- Smart Card, Token crittografico.
- Biometria: impronta digitale, riconoscimento facciale, retina, sistema venoso della mano, ecc.
- Prove a conoscenza zero.

# Il Regolamento 910/2014 (eIDAS)

## Stato dell'arte comunitario

- Alla data sono attivi 235 servizi fiduciari qualificati
- 166 soggetti per l'emissione di certificati qualificati per la firma.
- 140 soggetti per l'emissione di marche temporali
- Altri dati sono disponibili al seguente collegamento:
- <https://eidas.ec.europa.eu/efda/tlbrowser/#/screen/statistics>

## Numeri sulla diffusione dei servizi fiduciari

- I servizi elettronici di recapito certificato (la cosiddetta PEC europea sono 35.
- I sistemi utilizzano architetture proprietarie (non utilizzano gli standard ETSI).
- Non ci sono soggetti italiani.
- Un'azienda italiana è qualificata all'estero per i servizi di certificati di firma e sigillo.
- Un'altra è in fase di qualifica.

# Come si firma in Italia

## Numeri sulla diffusione

- Dati AgID aggiornati a dicembre 2022
- 82 % circa firme remote
- Oltre 29 milioni di certificati qualificati firma
- Circa 5 milioni e mezzo di certificati qualificati sigillo
- 3 miliardi di firme nel periodo

## Metodi di apposizione

- Firma remota
- Firma grafometrica
- Firma elettronica avanzata (FEA)
- Firma con token crittografico
- Firma con Smart Card (compresa la FEA con CIE)



# SPID e CIE

---

## Sistema Pubblico di Identità Digitale

- Attivo dall'8 marzo 2016.
- Utilizzato fino a un miliardo accessi nel 2022.
- Obbligatorio per l'accesso ai servizi online delle PPAA
- Il mercato offre servizi di firma qualificata con attivazione da remoto tramite SPID.

## Carta di Identità Elettronica

- Interagisce con una interfaccia NFC (Near Field Communication) senza contatti.
- Il lettore della carta può essere uno smartphone.
- E' possibile utilizzare la CIE per accedere a servizi online anche senza tessera (Livello 2 delle credenziali).
- Firma elettronica avanzata (FEA) tramite tessera conforme alle RRTT stabilite nel DPCM 22 febbraio 2013.

# Sistemi di DTM

## Digital Transaction Management

- Sono sistemi basati su una piattaforma *cloud* che consente la completa gestione delle transazioni basate su documenti informatici.
- La piattaforma più diffusa è DocuSign.
- Tramite essa si gestiscono transazioni digitali e, di base, si sottoscrive con un firma elettronica semplice.
- Esistono realizzazioni di DTM che sono in grado di produrre firme avanzate o firme qualificate.
- Il problema della validità legale della firma si manifesta nelle relazioni internazionali.

## Validità delle firme nei DTM

- La firma elettronica semplice non ha un valore giuridico e un'efficacia probatoria a priori.
- E' liberamente valutabile in giudizio in relazione alle caratteristiche di sicurezza. Integrità e immodificabilità
- Scegliere o accettare questa tipologia di firma è accettabile in ambito «corrente» quando non c'è l'obbligo legale della firma qualificata o la fiducia nell'identità del sottoscrittore è adeguata nel contesto dell'analisi del rischio.
- Lo scenario DocuSign si applica anche agli altri prodotti di mercato di classe DTM.
- Tutti questi prodotti hanno la possibilità di utilizzare la firma digitale (firma elettronica qualificata).

# Il Portafoglio Europeo di Identità Digitale - 1

## Le modifiche al Regolamento eIDAS

- Portafoglio Europeo di Identità Digitale
- Attestazione elettronica degli attributi
- Sistemi di firma e sigillo a distanza (remote)
- Archiviazione digitale

## Le funzioni del Portafoglio

- *Definizione: un mezzo di identificazione personale, che in modo sicuro memorizza, gestisce e convalida dati di identità e attestazioni elettroniche di attributi, per fornirli su richiesta alle parti facenti affidamento e altri utenti dell'EDIW, e abilitare la generazione di firme e sigilli elettronici qualificati.*
- Interazione con le parti facenti affidamento in modo conforme alla protezione dei dati personali che è richiesta ad un livello di totale controllo dell'utente.
- Il Portafoglio interagisce anche con un suo pari e un titolare può avere più di Portafoglio con la possibilità di scambiare dati tra di essi

# Il Portafoglio Europeo di Identità Digitale - 2

Two horizontal green bars, one on the left and one on the right, positioned below the title.

## Nuovi servizi fiduciari

- Archiviazione elettronica: un servizio che assicura la custodia (*preservation*) di dati o documenti elettronici al fine di garantire la loro integrità, la precisione della loro origine e le caratteristiche legali per tutto il periodo di conservazione.
- La gestione dei dispositivi per la generazione a distanza di firme e sigilli.
- Gli altri servizi fiduciari stabiliti nel Regolamento eIDAS vigente rimangono inalterati.

# Come firmare i documenti

## Tipologie di sottoscrizione

- Firma elettronica semplice (Es. PIN, email)
- Firma elettronica avanzata (Es. CIE, grafometrica)
- Firma elettronica qualificata (FEQ)
- La FEQ è equivalente ad una sottoscrizione autografa
- La FEA italiana ha valore legale diverso da quello comunitario.

## Metodi di apposizione

- Smart card, token USB, token wireless
- Firma remota (a distanza)
- Grafometrica
- Server crittografico
- Piattaforme cloud DTM
- Ecc.

# Opportunità per gli Atenei

## Opportunità

- Firma grafometrica
- Firma disposable
- Firma remota (tramite SPID)
- Firma semplice con DTM o PIN
- Portafoglio europeo

## Cose da evitare, per quanto possibile

- Firme semplici con soggetti di identità non adeguatamente certa
- Firme elettroniche multiple con procedimenti non controllati.
- Firme ibride (digitale e carta)
- Stampa di documenti firmati elettronicamente senza copia digitale - analogica

# Lo scenario a breve termine

## Scenario Nazionale

- Ampliamento delle funzionalità della CIE
- Firma FEA con CIE
- Evoluzione dello SPID
- Portafoglio di identità italiano

## Scenario europeo

- Lo scenario europeo sarà totalmente riferibile al Portafoglio Europeo di Identità Digitale
- Tra le funzioni obbligatorie del Portafoglio Europeo c'è la sottoscrizione qualificata
- Nello schema di regolamento in fase di trilogò (discussione informale tra Commissione, Consiglio e Parlamento) è stabilito che la firma qualificata è disponibile all'utente gratuitamente.
- Quest'ultimo punto è oggetto di dibattito tra istituzioni e stakeholder europei.

# Conclusioni

---

## L'impatto del Portafoglio

- Il Portafoglio italiano e quello europeo avranno impatti anche nella sottoscrizione di documenti informatici.
- L'utilizzo della firma sarà sempre più diffuso e l'omogeneizzazione e il coordinamento degli strumenti potrebbe portare anche a una maggiore interoperabilità organizzativa.
- Le varie tipologie e modalità di firma non saranno modificate significativamente da questo nuovo scenario
- La carta può essere eliminata con una attenta organizzazione documentale.

## Usi per gli Atenei

- Firma disponibile per le persone non dotate di firma qualificata (quando c'è l'obbligo di legge)
- Firma grafometrica per gli sportelli dello studente
- Firma (FEA) per i titolari di CIE (APP dell'IPZS o privata)
- Firma tramite SPID per semplificare il cosiddetto onboarding del titolare



# Contatto del relatore

Two horizontal green lines, one on the left and one on the right, positioned below the title.

Posta elettronica:

[gmanca@land.it](mailto:gmanca@land.it)