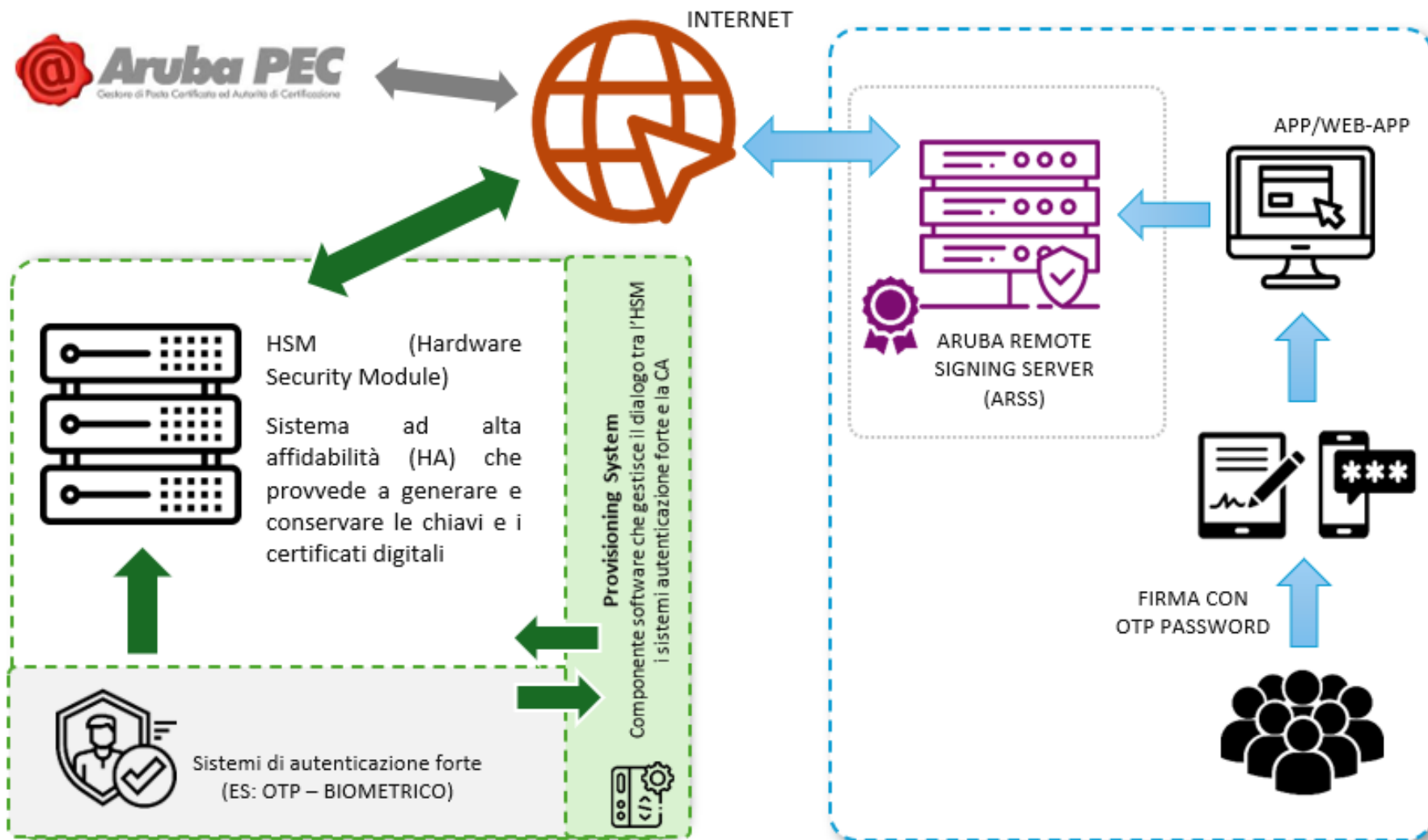


# Il processo di diffusione della firma digitale remota



# La firma digitale remota: cos'è e come funziona

- La **Firma Digitale Remota** è un particolare tipo di Firma Digitale che consente di **sottoscrivere online un documento elettronico direttamente da PC, tablet o cellulare**, senza bisogno di avere un Token USB o una Smart Card con lettore.
- Richiede **solo una connessione Internet e il proprio cellulare per ricevere l'OTP da utilizzare per apporre la firma digitale**.
- La chiave privata e il certificato digitale sono conservati sui server remoti sicuri **HSM** (Hardware Security Module) della CA.
- L'integrazione della firma digitale remota con i sistemi di gestione documentale interni all'Università è realizzata mediante l'invocazione applicativa dei servizi attestati sull'**ARSS** (Aruba Remote Signing Service).
- Il **processo di firma remota di un documento informatico** prevede le seguenti fasi (dopo inserimento del nome utente, password e codice OTP):
  - ✓ L'applicazione genera l'hash del documento;
  - ✓ L'applicazione invia l'hash ai server remoti della CA;
  - ✓ La CA firma digitalmente l'hash;
  - ✓ L'hash firmato digitalmente torna all'applicazione di firma che assembla il documento firmato e lo rende disponibile all'utente.
- ✓ In alternativa, l'applicazione invia ai server remoti della CA su canale crittografato il documento informatico da firmare e lo riceve sottoscritto digitalmente nel formato richiesto.



L'elemento principale in questo scenario è l'**HSM** (Hardware Security Module) che è definito nel DPCM 22 febbraio 2013 (regole tecniche vigenti in Italia) come: "insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche".

# Il valore giuridico della firma digitale remota

- Il **Regolamento eIDAS 2** (EU 2024/1183) ha, tra l'altro, aggiunto all'elenco dei servizi fiduciari qualificati il servizio per la gestione di dispositivi per la creazione di firme/sigilli elettronici qualificati a distanza per conto degli utenti, attribuendogli così **la massima validità legale a livello europeo**, confermandolo valido strumento legale per firmare documenti a distanza, con un valore legale equiparabile a una firma autografa.
- Nel corso del 2025 è stata data attuazione a tale ambito mediante l'entrata in vigore di un apposito Regolamento che mira a **rafforzare la sicurezza e l'affidabilità del servizio di firma digitale a distanza (o remota)**, attraverso
  - ✓ requisiti più stringenti per i prestatori di servizi fiduciari qualificati,
  - ✓ maggiori garanzie per l'identificazione e l'autenticazione del firmatario,
  - ✓ l'introduzione di standard tecnici uniformi a livello EU, atti a migliorarne la interoperabilità transfrontaliera.
- La soluzione **ARUBAPEC** per la firma digitale remota, adottata da UniNA per le sue caratteristiche tecnico-economiche, **è pienamente conforme al Regolamento eIDAS 2.**

# Alcuni riferimenti normativi in ambito UE

- [1] **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, in particolare l'articolo 29 bis, paragrafo 2, e l'articolo 39 bis.
- [2] **Regolamento (UE) 2024/1183** del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (in vigore dal 20.05.2024).
- [3] **Regolamento di esecuzione (UE) 2025/1567** della Commissione del 29 luglio 2025 recante modalità di applicazione del regolamento (UE) 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e dispositivi qualificati per la creazione di un sigillo elettronico a distanza come servizi fiduciari qualificati (applicato a partire dal 19.08.2027).

# L'avvio del percorso di passaggio alla firma digitale remota

- Il processo si è avviato a partire da luglio 2025, a seguito della circolare del Direttore Generale PG/2025/82402 del 23.06.2025.
- A partire da luglio 2025, tutti i certificati per la firma digitale sono emessi su dispositivo di firma digitale remota emesso dalla CA ARUBAPEC S.p.A..
- L'obiettivo è la sostituzione di tutte le firme digitali su dispositivo di firma USB con firme digitali remote, auspicabilmente entro il 2026.
- I certificati, emessi su dominio dedicato @frUnina, hanno validità pari a 6 anni e non sono rinnovabili.
- L'autenticazione ai servizi di firma avviene mediante OTP mobile.

# La migrazione dalla firma con token alla firma digitale remota

Il piano di massima per la migrazione da firma locale su token USB a firma digitale remota è così articolato:

- **Fase 1** – Emissione certificato di firma digitale remota per **tutti i titolari di certificato in scadenza e non rinnovabile** (in quanto già rinnovato, oppure su SIM obsoleta):
  - ✓ Per gli strutturati, tale attività sarà svolta dagli ODR afferenti agli Uffici UPDR, URP e UPTA (ciascuno per la propria competenza), in **modalità massiva** "Datore di Lavoro«, oppure (a seconda del numero di emissioni da effettuare) in **modalità *ad personam da remoto***;
  - ✓ Per i docenti a contratto, tale attività sarà svolta sempre in **modalità *ad personam da remoto*** dall'ODR della struttura che ha conferito l'incarico di insegnamento, previa verifica della sussistenza dei requisiti contrattuali.
- **Fase 2** – Emissione certificato di firma digitale remota **per i restanti titolari di certificato di firma su token** (il cui certificato scade dopo il 2026) purché in servizio oppure con contratto di docenza attivo.

# La modalità di identificazione come Datore di Lavoro

- L'Ateneo ha concluso il percorso di certificazione presso ARUBA per poter essere autorizzato dalla CA a identificare i titolari di firma con la modalità "Datore di lavoro", per procedere con l'emissione massiva dei certificati di firma.
- Questa modalità prevede il caricamento (da parte di ODR abilitati) di un file csv con dati anagrafici dei soggetti a cui rilasciare un certificato di firma remota, in modo tale da avviare le successive operazioni (di norma, svolte in autonomia dall'utente) per l'emissione e l'attivazione dei certificati di firma remota.
- Tra i metadati, oltre a quelli contenuti nella anagrafica CSA, sono presenti anche gli estremi di un documento di riconoscimento in corso di validità e un recapito di mobile per l'attivazione del dispositivo OTP, dati forniti dall'interessato e validati dall'ufficio del personale competente.

# Flusso di lavoro

Individuazione  
certificati da  
emettere

- Il CSI individua i certificati da emettere nel corso del mese successivo (selezionando solo il personale strutturato e non in quiescenza), in quanto prossimi alla scadenza e/o non più rinnovabili per SIM obsoleta.
- Il CSI fornisce l'elenco all'Ufficio UPDR/UPTA.

Comunicazione  
al dipendente e  
validazione dati

- UPDR/UPTA invia una mail a ciascun dipendente, chiedendo all'interessato di compilare i dati su Cerdi e fornendogli un range di date per effettuare il riconoscimento *de visu* (in presenza o da remoto) e la validazione, nonché le istruzioni per l'attivazione del certificato.
- L'incaricato dell'Ufficio contatta il dipendente e, in teleconferenza oppure in presenza, verifica il documento di identità e valida i dati su Cerdi.

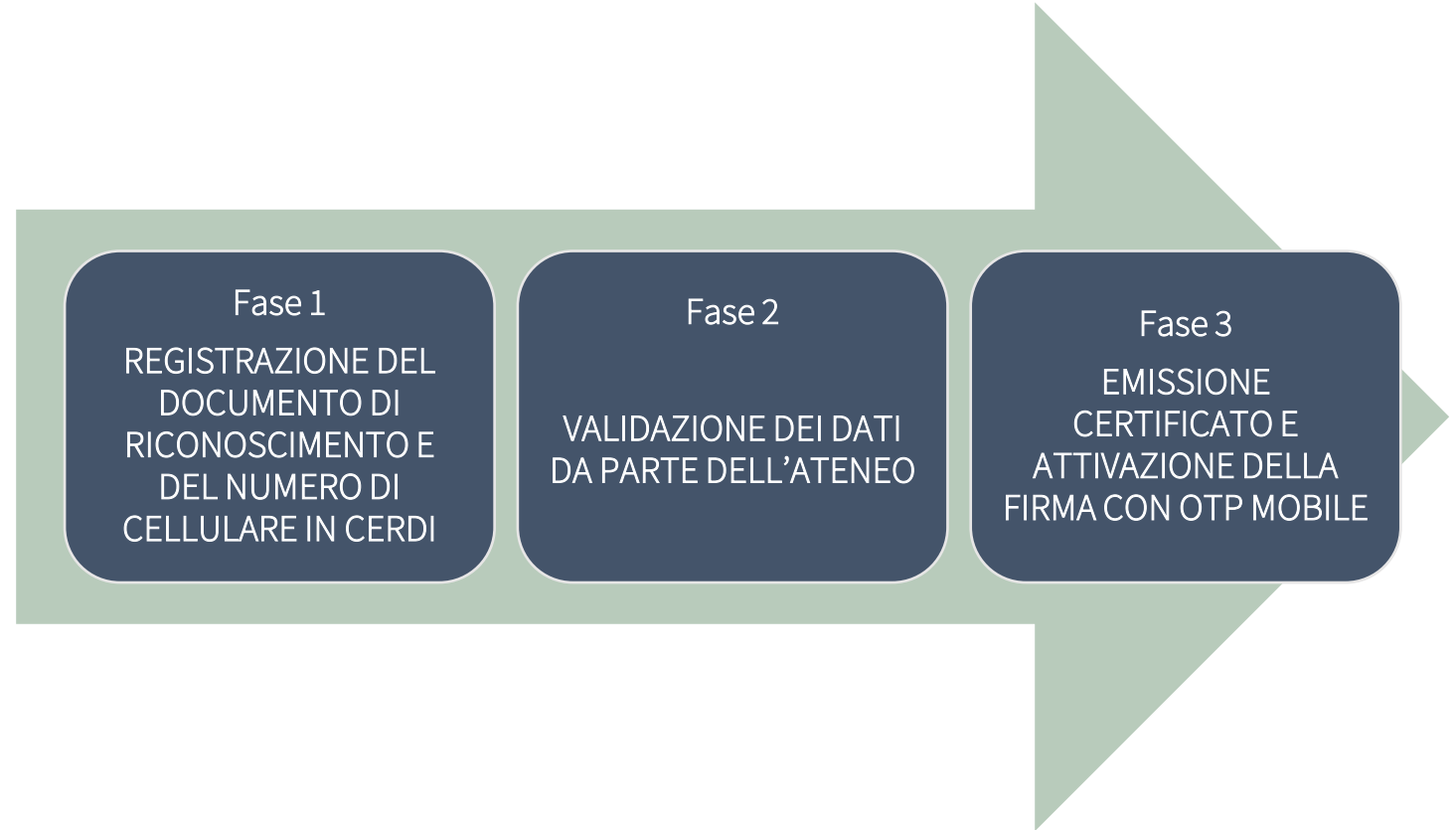
Creazione csv

- UPDR/UPTA genera, mediante una funzionalità Cerdi, il csv da trasmettere alla ARUBA che conterrà solo le occorrenze validate e non ancora scaricate.

Upload del csv  
e attivazione  
certificati

- L'ODR presso UPDR/UPTA effettua l'upload del csv sul CMS Aruba e ne monitora la corretta elaborazione.
- Ciascun interessato riceverà dalla CA le mail per procedere all'emissione del proprio certificato di firma qualificata e all'attivazione del dispositivo OTP mobile.

# Il processo di attivazione per il titolare del certificato



Questo processo è descritto più dettagliatamente nella pagina [Praxis - UNINA - Firma digitale remota](#)

# Gli strumenti per apporre la firma digitale remota su un documento informatico

- L'applicazione locale da utilizzare per la firma dei documenti informatici è **ArubaSign**, previa personalizzazione del dominio di firma (quello dell'Ateneo è **frUnina**).
- In ciascuna applicazione istituzionale (eDocumento, Verbali digitali esame e Web docenti) è stato **modificato il wizard di firma**, in modo tale da consentire anche l'apposizione della firma digitale remota.
- In ogni caso, l'utente dovrà utilizzare come generatore di OTP il cellulare fornito alla Aruba in fase di registrazione e di attivazione.
- Le guide operative sono disponibili all'indirizzo:  
[Praxis - UNINA - Menu Principale - Firma digitale - Guide e manuali](#)

## FAQ

D. Chi deve emettere il certificato di firma remota di un dipendente strutturato (in modalità datore di lavoro, oppure *ad personam*)?

R. Gli ODR dell'Amministrazione Centrale, ciascuno per la propria competenza.

D. Per quanto riguarda le nuove assunzioni (strutturati e non ), valgono le stesse regole che si seguivano per l'emissione su token USB?

R. Sì.

D. Si potranno emettere ancora firme su token USB?

R. No, salvo casi specifici, autorizzati dalla Direzione Generale.

D. Il personale cessato può ricevere la firma digitale (remota)?

R. No, in nessun caso. Il requisito è quello di essere titolare di un contratto attivo.

D. Il titolare della firma che ha dubbi o necessità di supporto sulle modalità di rinnovo/emissione/utilizzo della firma remota, a chi può rivolgersi?

R. Ciascun titolare deve rivolgersi all'Incaricato\_firma presso la propria struttura e, in caso di difficoltà tecnica, al CSI tramite Contact Center.