



## OVERVIEW SULLA FIRMA DIGITALE

**La firma digitale viene rilasciata a tutto il personale docente e ricercatore, ai professori a contratto presenti in Ateneo, a tutti i Responsabili degli Uffici dell'Ateneo e di specifici procedimenti amministrativi individuati dall'Amministrazione.**

L'Ateneo, in qualità di Centro di Registrazione Locale (C.D.R.L.) effettua, in nome e per conto della Certification Authority Aruba PEC S.p.A., le attività di **registrazione** e **identificazione**<sup>1</sup> dei titolari di firma e – quando necessario – all'emissione di Certificati Digitali.

Ai fini del funzionamento del predetto C.D.R.L. sono nominati, per conto della "CA", gli "*Incaricati del servizio di firma digitale*" tra le unità di personale in servizio presso l'Amministrazione e le strutture dell'Università quali **Operatori di Registrazione** (ODR) oppure **Incaricato al Riconoscimento** (IR) per lo svolgimento delle attività inerenti il rilascio di servizi di certificazione digitale, con i compiti e le responsabilità indicate, tra l'altro, nelle "*Condizioni Generali di Contratto Servizi di Certificazione Digitale v. 2.2*", disponibile al link <https://www.praxis.unina.it/firma-digitale>.

Più in dettaglio, per quanto attiene alle emissioni di certificati di firma digitale "ad personam":

- gli ODR procedono al riconoscimento del titolare di firma (*de visu*, oppure, da remoto) e alla compilazione dei campi presenti nelle pagine della applicazione WEB messa a disposizione dalla "Certification Authority", ai fini della emissione del certificato di firma;
- Il titolare accetta per adesione le clausole contrattuali;
- la CA emette il certificato qualificato per la firma digitale e, nel caso di firma mediante token, anche quello di autenticazione "CNS like";
- nel caso di firma digitale su token, il dispositivo fisico prodotto viene consegnato all'Interessato dall'Incaricato\_firma preposto;
- i dati relativi al nominativo del Titolare e agli estremi del certificato di firma, con le date di emissione e scadenza del certificato sono quindi acquisite con frequenza giornaliera dall'Università e caricate nell'anagrafica dei certificati per la firma digitale;
- la CA gestirà tutti gli adempimenti normativi previsti per la gestione dei certificati qualificati per la firma digitale.

---

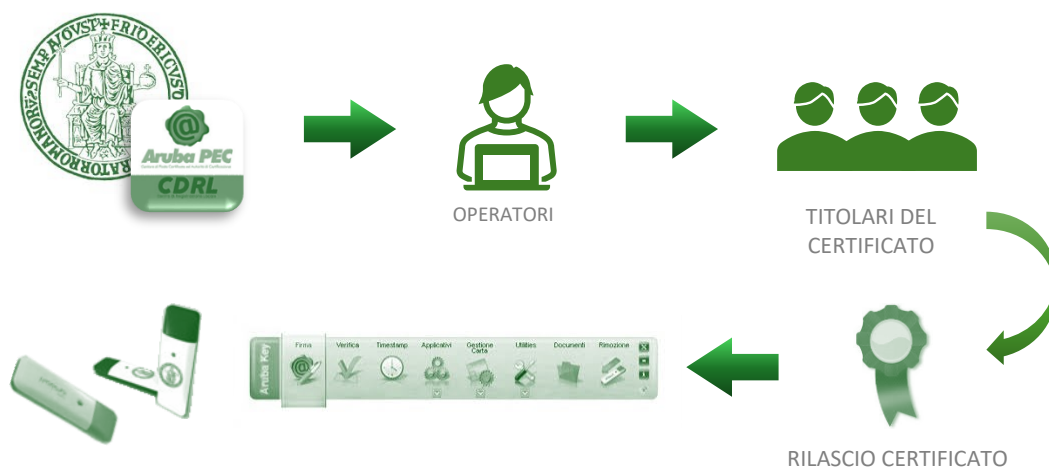
<sup>1</sup> Per quanto attiene agli aspetti relativi alla protezione dei dati personali, le attività di emissione, sospensione e revoca dei certificati di firma digitale, titolare autonomo del trattamento è la CA Aruba PEC S.p.A. società del Gruppo Aruba, (P.Iva 01879020517) con sede in Via Sergio Ramelli n. 8, 52100 Arezzo, iscritta negli elenchi pubblici dei Gestori di Posta Elettronica Certificata, dei Certificatori, dei Prestatori di Servizi Fiduciari e dei Conservatori accreditati predisposti, tenuti ed aggiornati dall'Agenzia per l'Italia Digitale. E-mail: [privacy@staff.aruba.it](mailto:privacy@staff.aruba.it). Il Responsabile della Protezione dei Dati (RPD) Aruba PEC è raggiungibile al seguente indirizzo: [dpo@staff.aruba](mailto:dpo@staff.aruba)

Infine, per le emissioni massive dei certificati per la firma digitale remota, l'Ateneo è accreditato presso la C.A. per l'utilizzo della procedura di validazione delle identità delle persone fisiche - **c.d. modalità "Datore di Lavoro"** - al fine di poter effettuare le operazioni in modalità semplificata, richiedendo in tal caso agli interessati solo di comunicare gli estremi di un documento di identità in corso di validità e il proprio numero di mobile per associarvi il meccanismo di OTP (One Time Password).

L'Ateneo sta inoltre attuando un piano graduale di migrazione dei certificati di firma digitale su token alla firma remota.

Il certificato di firma digitale remota ha una validità di anni 6 non rinnovabili

## FIRMA DIGITALE CON TOKEN ARUBA KEY

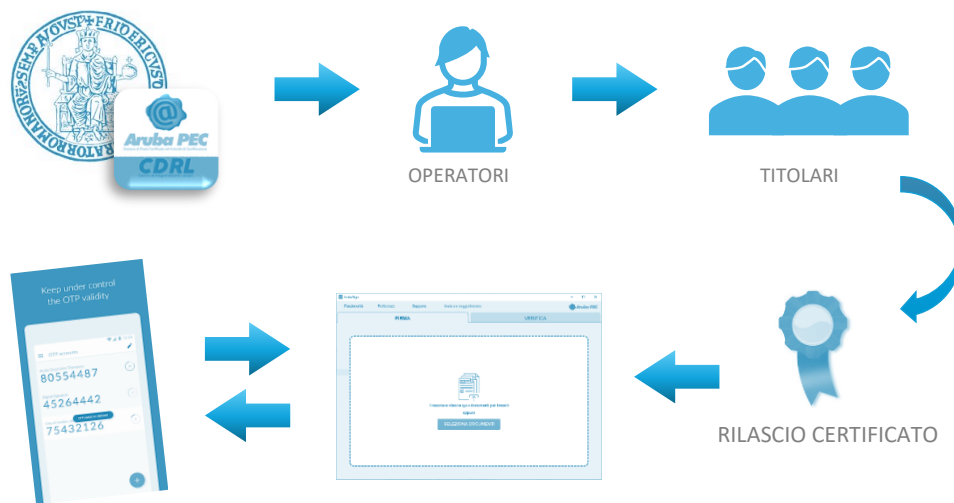


La firma digitale ArubaKey è un dispositivo USB (token) contenente una SIM Card nella quale è memorizzato il certificato di firma digitale a conclusione del processo di identificazione e di emissione svolto dagli Operatori di Registrazione (ODR) per conto della CA.

Per firmare è necessario utilizzare il dispositivo USB e il codice PIN della carta mediante l'applicazione ArubaKey disponibile sul dispositivo di firma, oppure l'applicazione ArubaSign (in tal caso, effettuando preventivamente l'operazione di import certificato), oppure l'applicazione Confirma integrata con le principali piattaforme istituzionali. Maggiori informazioni sull'utilizzo della firma su token sono disponibili nei manuali e nelle guide operative reperibili al seguente link:

[Praxis - UNINA - Menu Principale - Firma digitale - Guide e manuali](#)

## FIRMA DIGITALE REMOTA



La Firma Remota è una tipologia di Firma Digitale che non necessita dell'installazione di hardware, rendendone il suo utilizzo più semplice e veloce.

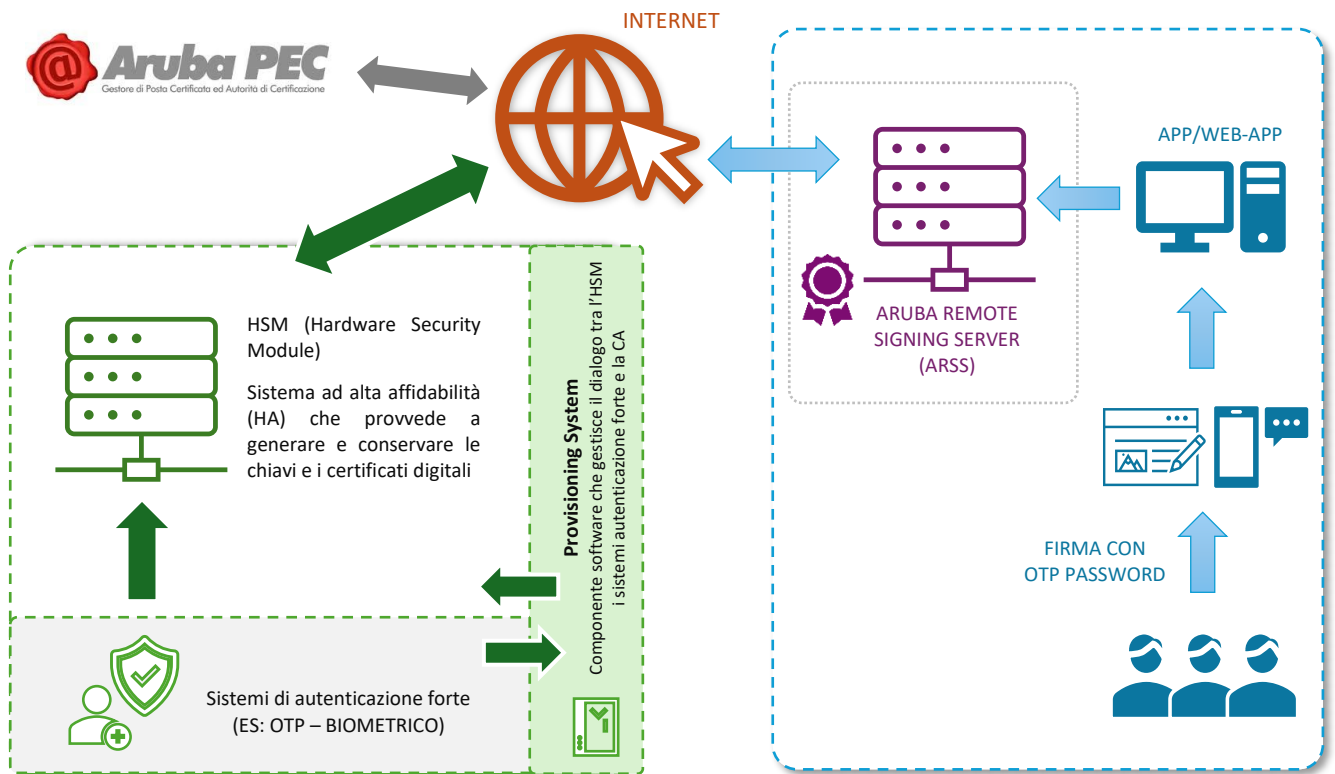
La Firma Remota è composta da un certificato di firma e da un OTP (*One Time Password*), ovvero una password momentanea (scade alcuni secondi dopo essere stata generata) per la quale non è necessaria la sua memorizzazione.

Il sistema OTP, in versione Mobile, consente di generare le password OTP dal proprio smartphone con l'app Aruba OTP.

L'app Aruba OTP, gratuita per tutti i clienti Aruba, consente di generare in modo sicuro codici OTP direttamente dallo smartphone senza l'utilizzo di dispositivi aggiuntivi.

La firma sui documenti digitali avviene tramite l'utilizzo del software ArubaSign, oppure l'applicazione Confirma integrata con le principali piattaforme istituzionali.

L'architettura di servizio prevede in tal caso l'utilizzo del servizio ARSS (erogato dalla CA in cloud) che fa da intermediario tra l'utente, l'applicazione di firma utilizzata e i servizi tenuti remotamente dalla CA di autenticazione a due livelli e di gestione della firma digitale e custodia del certificato di firma dell'utente.



Per maggiori informazioni visita la sezione [Firma digitale remota](#)