

## FIRMA AUTOMATICA

La **Firma Automatica** è una modalità di firma remota qualificata che consente di firmare automaticamente e massivamente documenti, tramite il processo di delega, in assenza di un presidio puntuale e continuo da parte del firmatario, cioè senza dover inserire le credenziali di firma a ogni operazione.

Il servizio è appositamente studiato per la clientela enterprise e viene utilizzato nei processi che richiedono un elevato numero di firme al secondo, come per esempio quelli adottati in ambito bancario, assicurativo, Pubblica Amministrazione e in generale in tutti quei processi time critical, oppure nei processi che non richiedono un presidio puntuale e continuo da parte del firmatario.

I documenti firmati tramite soluzione di Firma Automatica Massiva conservano le caratteristiche di autenticità, integrità, non ripudio e validità legale in piena conformità alla normativa nazionale (DPCM 22 febbraio 2013) e alla normativa europea (Regolamento UE n. 910/2014 del 23 luglio 2013 – EIDAS). Nel certificato qualificato di firma automatica è possibile, oltre a quanto già previsto dalla normativa vigente, inserire come opzione una ulteriore limitazione d'uso al fine di definire lo specifico ambito di validità della firma.

## COME FUNZIONA

A seguito dell'attivazione del servizio di firma automatica il titolare, al fine di sottoscrivere in modo automatico i documenti, dovrà autorizzare, mediante un processo di delega, l'utilizzo del proprio certificato da parte di specifici applicativi designati. Il processo di delega avviene mediante un'applicazione web in grado di gestire le associazioni tra firmatari e applicativi consentendo al titolare di mantenere il pieno controllo della delega all'utilizzo del certificato.

L'integrazione con il servizio di firma automatica avviene mediante semplici interfacce applicative di tipo Web Service (SOAP/REST) esposte dal componente software ATP (Aruba Trusted Platform).

La soluzione, estremamente modulare, flessibile e scalabile, prevede più modalità di erogazione che permettono di adattarsi alle reali esigenze del cliente.

- **On-premise** | Viene fornita completa di HSM (Hardware Security Module) e dei componenti software necessari per l'erogazione di tutte le funzionalità del sistema; in questa modalità può essere configurata la ridondanza affiancando più nodi identici, per realizzare soluzioni in HA (High Availability) o predisporre siti di disaster recovery. In caso di erogazione on-premise, il dispositivo HSM è custodito e gestito dal cliente sotto la propria responsabilità, a seconda della casistica specifica:

- dall'organizzazione di appartenenza dei titolari dei certificati che ha richiesto i certificati medesimi;
- dall'organizzazione che richiede al certificatore di fornire certificati qualificati ad altri soggetti al fine di dematerializzare lo scambio documentale con gli stessi.

Per ottemperare a quanto previsto dalle norme vigenti negli scenari sopra riportati, l'organizzazione (cliente) che custodisce e gestisce il dispositivo sicuro per la generazione delle firme (HSM) è tenuta ad adottare la specifica "Policy di sicurezza per soluzioni di firma in-house" che stabilisce i requisiti tecnici e organizzativi che devono essere soddisfatti al fine di preservare la conformità del prodotto e/o delle soluzioni che abilitano l'erogazione di certificati qualificati di firma e/o di sigillo sotto la responsabilità del cliente. Il cliente è inoltre tenuto a sottoscrivere la "*Dichiarazione di sussistenza dei requisiti*".

Per una descrizione dettagliata delle attività e delle responsabilità del certificatore e delle parti delegate si rimanda al contratto, di cui la suddetta policy di sicurezza è parte integrante e sostanziale.

- **Cloud** | Viene erogata dai Data Center Aruba attraverso una **piattaforma condivisa**, configurata in modalità HA nativa e con disaster recovery geografico;

A seconda della modalità individuata, è possibile attivare le componenti ATP presso i locali tecnici del cliente (modalità On-premise) o nei Data Center Aruba, sia dedicati che condivisi (modalità Cloud).

Al fine di permettere la definizione di processi di rilascio di certificati digitali che meglio possano adattarsi alle esigenze di business del cliente, Actalis e Aruba PEC, in qualità di Trust Service Provider Qualificati eIDAS, sono in grado di autorizzare il cliente come Centro di Registrazione Locale (CDRL), delegando tutte le attività di identificazione, rilascio e attivazione del servizio in totale autonomia.

## CARATTERISTICHE TECNICO – FUNZIONALI

### COMPLIANCE

<b>Normativa di riferimento</b>	<b>D.P.C.M. 22 febbraio 2013</b>   Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali <b>C.A.D. 7 marzo 2005</b>   Codice dell'Amministrazione Digitale <b>Regolamento UE n. 910/2014 del 23 luglio 2014</b>   Identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno
<b>Autorità di Certificazione</b>	<b>Actalis S.p.A. e Aruba PEC S.p.A.</b> sono i certificatori qualificati per la fornitura di servizi fiduciari qualificati iscritti all'elenco dei prestatori di servizi fiduciari stabiliti in Italia, tenuto presso l'AglID (Agenzia per l'Italia Digitale) e reso pubblico dalla Commissione europea attraverso un proprio elenco
<b>Garanzia</b>	I documenti così sottoscritti assumono piena efficacia probatoria

### CARATTERISTICHE DEL SERVIZIO

<b>Scalabilità</b>	Orizzontale con bilanciamento e <i>fault tolerance</i> - L'architettura del sistema consente una scalabilità orizzontale, permettendo di aggiungere, in modo trasparente, ulteriori linee di erogazione sia nella componente di <i>front end</i> ATP che in quelle di <i>back end</i> : è quindi sempre possibile garantire adeguate performance all'aumentare dei volumi.
<b>Disponibilità del servizio</b>	<b>High Availability &amp; Disaster Recovery</b> - Il sistema garantisce requisiti continuità operativa e bilanciamento di carico poiché ogni componente (sia fisico che applicativa) dell'architettura può essere ridondato al fine di escludere singoli punti di <i>failure</i> . Nelle soluzioni dedicate, on premise o in cloud, dipende dalla configurazione acquistata.  Qualificati in standard X.509 conformi al Regolamento UE n. 910/2014 del 23 luglio 2013 – EIDAS – e alle Linee guida AgID (Determinazione 147 del 4 giugno 2019)
<b>Certificati</b>	
<b>Tipologia di firma</b>	CadES, PadES (visibile e invisibile), XAdES
<b>Marca temporale</b>	Attached, Detached
<b>Verifica documenti firmati</b>	Integrazione applicativa tramite il modulo aggiuntivo di validazione online

### SERVICE LEVEL AGREEMENT (SLA)

<b>SLA di disponibilità del servizio</b>	Uptime garantito del 99,95%
<b>SLA di performance</b>	<ul style="list-style-type: none"> <li><b>Sistema condiviso:</b> performance garantite da un minimo di 2 ad un massimo di 50 firme al secondo sul sistema condiviso</li> <li><b>Sistema dedicato:</b> soluzioni personalizzate per raggiungere performance fino a migliaia di firme al secondo</li> </ul>
<b>Incident management e Service Request</b>	<ul style="list-style-type: none"> <li>Vale quanto previsto ed indicato nella scheda relativa al servizio di Assistenza Enterprise</li> </ul>

I servizi effettivamente offerti sono esclusivamente quelli espressamente indicati nell'Offerta Economica.