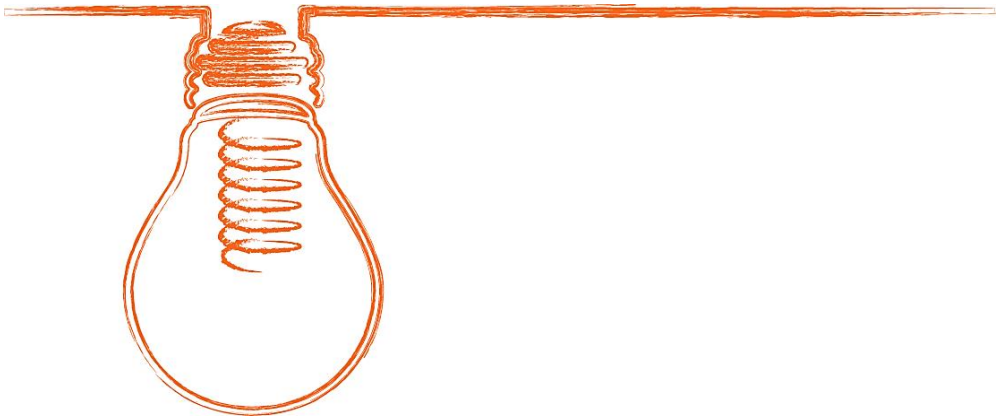
Agenzia Entrate Riscossione



Acquisto di certificati digitali HSM

Capitolato tecnico

SOMMARIO

1 PREMESSA

Agenzia delle entrate–Riscossione (di seguito anche AdeR) si è dotata da tempo di alcune soluzioni di firma digitale atte a soddisfare le esigenze di business correlate alla propria missione istituzionale. Per la firma digitale massiva associata ai processi di produzione documentale AdeR utilizza la firma remota.

La Firma Remota, è una modalità di firma digitale che, pur garantendo lo stesso grado di sicurezza e gli stessi effetti di legge della tradizionale firma digitale basata su smartcard o token USB, rispetto a quest'ultima offre diversi vantaggi specifici:

- non richiede l'installazione di hardware e driver dedicati, pertanto riduce virtualmente a zero i relativi problemi di incompatibilità hw/sw, supporto tecnico, ecc.;
- è sostanzialmente indipendente dall'ambiente operativo dell'utente (Windows, Mac, Linux, …);
- permette di generare firme digitali in ogni momento ed in ogni luogo.

In concreto, per "Firma Remota" si intende la firma digitale eseguita con una chiave privata non residente su un dispositivo personale dell'utente, quale ad es. una smartcard, bensì su un dispositivo remoto (normalmente un HSM – Hardware Security Module). I dati da firmare sono inviati all'HSM attraverso la rete, e la risposta ritorna all'utente sempre attraverso la rete.

2 DESCRIZIONE DELLE ATTIVITÀ

Le attività richieste sono le seguenti:

- Approvvigionamento di 200 certificati di firma remota/automatica validità 3 anni. Al cessare dei rapporti contrattuali, il Fornitore potrà revocare tutti i certificati qualificati emessi e AdeR si impegna a cancellare tutte le relative chiavi crittografiche presenti sui propri dispositivi HSM;
- Audit di Sicurezza, e aggiornamento del sistema di provisioning con integrazione in cooperazione applicativa,

2.1 ACQUISIZIONE DEI CERTIFICATI DI FIRMA REMOTA VALIDITÀ TRIENNALE

Sono richiesti 200 certificati di firma remota con validità 3 anni dal momento dell'attivazione del certificato.

Si specifica che i 200 certificati saranno intestati a titolari già censiti sul sistema Anagrafico Poste Italiane. Per questi titolari i certificati scadranno a partire dal

1° luglio 2023.

Per garantire la continuità operativa degli utenti sarà necessario avviare le attività di emissione del nuovo certificato prima della scadenza naturale dei certificati.

Sarà necessario, pertanto, predisporre il sistema di provisioning per l'emissione del nuovo certificato.

2.2 AUDIT DI SICUREZZA.

L'attività di audit certifica la conformità dell'infrastruttura, delle misure di sicurezza logica e fisica e dei processi ad essa afferenti.

2.3 SISTEMA DI PROVISIONING PER L'EMISSIONE DEI CERTIFICATI

I certificati digitali attualmente presenti nel dispositivo HSM in house sono stati emessi dalla Certification Authority di Poste Italiane.

La maggior parte dei certificati presenti nell'HSM in house sono stati concessi in uso dall'Agenzia agli enti impositori per la firma dei Frontespizi dei ruoli.

La procedura di provisioning per la richiesta e l'emissione dei certificati digitali prevede l'integrazione a servizi tra i sistemi di back end dell'Agenzia e quelli della Certification Authority (CA). Pertanto, la predisposizione dei servizi necessari per l'integrazione con il back end di AdeR deve essere parte integrante del servizio offerto da parte del nuovo fornitore.

Il processo di gestione, di generazione e consegna dei certificati digitali deve prevedere i seguenti passi:

1. Acquisizione dei dati anagrafici del titolare tramite front end web – questa funzionalità prevede l'esposizione da parte della CA di un'applicazione Web con il form per l'inserimento dei dati anagrafici dell'utente;

2. Invio in back end dei dati della richiesta ad AdeR – questa funzionalità prevede la predisposizione da parte della CA di un client applicativo per l'invio dei i dati anagrafici dell'utente al web service esposto da AdeR;

3. Ricezione della richiesta di AdeR dell'emissione dei certificati (CSR) – questa funzionalità prevede l'esposizione da parte della CA di un web service per la ricezione delle CSR inviate da AdeR, la generazione ed il rilascio contestuale del certificato digitale;

4. Conferma dell'acquisizione del certificato digitale – questa funzionalità prevede l'invio da parte di AdeR della conferma di acquisizione del certificato digitale al web service della CA.

Per ogni utente attivato sui servizi di firma digitale, viene generato un certificato digitale, che sarà caricato sui due apparati HSM AdeR, configurati nel cluster High Availability.

Le funzionalità da predisporre da parte della CA per l'integrazione in modalità SOA[1], con il back end AdeR, sono le seguenti:

1. Predisposizione di una funzione di front end sulla quale l'utente, rediretto dal front end web AdeR, possa inserire i propri dati anagrafici;
2. Invio della send data da parte della CA: deve essere predisposta la funzionalità di back end per l'invio dei dati anagrafici dell'utente, da parte della CA, ai sistemi AdER. Per questo scopo AdeR espone apposito web service;
3. Invio della CSR alla CA per l'emissione del certificato digitale; funzionalità di back end, tramite la quale i sistemi AdeR inviano una request ad apposito web service esposto dalla CA; la CA alla ricezione della CSR genererà, in modalità sincrona, il certificato digitale; il certificato sarà caricato dal back end AdER nell'HSM.

Di seguito sono elencati i passi da compiere per richiedere l'emissione di un certificato di firma remota HSM:

1. L'interessato al rilascio del certificato digitale di firma automatica (denominato d'ora in poi "richiedente") chiede l'attivazione del servizio "Firma digitale" sulla propria utenza Portale AdeR;
2. Attivato il servizio Firma digitale, il richiedente contatta un incaricato al riconoscimento ed alla registrazione LRA[2] per avviare la procedura emissione.
3. L'operatore LRA prende appuntamento con il richiedente e lo incontra per il riconoscimento;
4. Con il supporto dell'operatore LRA il richiedente accede al servizio Firma digitale presente nel menù Servizi vari, nell'area riservata del portale, e compie le seguenti azioni:
    a. Inserimento casella email ordinaria dove saranno inviate le

[1] Service Oriented Application: architetture basate sui web-services che vengono richiamate dalle applicazioni per scambiarsi informazioni.

[2] LRA – local registration authoriry – gli LRA sono dipendenti Agenzia delle entrate - riscossione che in base alla convenzione sarà attivata tra AdeR stessa e Poste Italiane (certification authority) in sede di stipula del contratto, opereranno in nome e per conto di quest'ultima. Gli LRA hanno l'incarico di eseguire il riconoscimento "de visu" del richiedente certificato digitale, raccogliere la documentazione cartacea di registrazione sottoscritta dal richiedente e consegnarla a Poste Italiane.[2]

credenziali per il cambio password e le credenziali definitive;

b. Registrazione sul portale Poste Italiane per la richiesta di emissione del certificato digitale;

c. al termine della registrazione il portale Poste Italiane rende disponibile il contratto per la fornitura del certificato digitale; il titolare stampa il contratto, lo sottoscrive e lo consegna all'operatore LRA, unitamente ad una copia del documento d'identità e del codice fiscale; l'operatore LRA provvede ad inviare all'ufficio Registrazione di Poste Italiane la documentazione in formato elettronico e cartaceo;

5. Successivamente il sistema provvederà ad inviare (dalla casella mittente firmadigitale@agenziariscossione.gov.it) alla casella email inserita dal richiedente al passo "a." del punto 4, sopra descritto, due email contenenti le credenziali da utilizzare per il cambio password, descritto al punto 6 (n.b. una email contiene il "pin statico" e l'altra la password di primo accesso),
6. il richiedente accede al portale sul servizio Firma digitale, attiva la funzione "Cambio password" e compie le seguenti azioni:
   - Copia il pin statico, ricevuto per email, nell'apposito campo;
   - Copia la password di primo accesso, ricevuta per email, nell'apposito campo;
   - Digita la password personale prescelta nell'apposito campo, tenendo conto che:
     - Deve essere lunga 8 posizioni;
     - Deve contenere almeno un carattere alfabetico maiuscolo;
     - Deve contenere almeno un carattere alfabetico minuscolo;
     - Deve contenere almeno un numero;
   - Digita nuovamente la password personale nel campo "conferma";
   - Attiva il tasto "OK";
7. Il sistema emetterà il certificato digitale ed il richiedente riceverà una email con la password personalizzata;
8. Dal momento del ricevimento della email con la password personalizzata (la password personale prescelta al momento del cambio password), il richiedente sarà divenuto "titolare" di un certificato digitale di firma remota HSM (di durata triennale) che potrà utilizzare su tutte le piattaforme applicative AdeR alle quali sarà abilitato ad operare, che prevedono la firma digitale HSM in house (vedere elenco nel capitolo 2).
9. Per apporre la firma digitale il titolare, quando richiesto dai servizi di produzione documentale sui quali opera, dovrà inserire le proprie credenziali:

- Pin statico
- Password personalizzata.

3 REQUISITI ED ATTIVITA' DEL FORNITORE

Il Fornitore, autorità di certificazione, deve:

1) essere in possesso della certificazione a norma ISO27001:2005 valido per il perimetro delle attività di Certificazione;
2) essere in possesso di un set di procedure organizzative e tecniche atte a regolamentare le modalità di protezione dei sistemi su cui avvengono le attività di produzione/personalizzazione dei certificati e regolamentazione dei processi stessi;
3) assicurarsi che siano poste in atto tutte le necessarie azioni al fine di ridurre i rischi connessi alle seguenti minacce:
    - infrazioni della sicurezza dovute a carenze organizzative,
    - incidenti e avarie dei sistemi di elaborazione,
    - uso non autorizzato o improprio di impianti, sistemi di elaborazione delle informazioni, utilità di sistema o applicazioni, rimozione non autorizzata di oggetti,
    - accesso non autorizzato a informazioni o sistemi,
    - iniezione di codice doloso, worm, trojan e in generale qualsiasi tipo di virus informatico,
    - comportamenti scorretti o non conformi dell'utente,
    - ogni altro tipo di attacco proveniente della rete internet
    - utilizzo doloso dell'infrastruttura o delle applicazioni al fine di procurare danno a terzi;
4) raccogliere segnalazioni e formalizzare tempestivi rapporti su tutte le infrazioni della sicurezza, vere o presunte;
5) dare garanzia della continuità dei servizi, nel rispetto dei livelli di servizio contrattuali;
6) effettuare l'analisi dei rischi quando cambino le condizioni organizzative, ambientali e tecniche oggetto del presente bando di gara;
7) garantire lo svolgimento delle verifiche periodiche annuali anche in modalità congiunta qualora il dispositivo ospiti certificati qualificati afferenti a diversi certificatori;
8) garantire che il personale adibito alle verifiche ispettive sia in possesso della qualifica di Lead Auditor ISO/IEC 27001 conseguito attraverso corsi certificati da IRCA;

9) qualora i certificati siano installati su un dispositivo che ospiti certificati emessi da altro certificatore, il fornitore deve garantire il rispetto delle politiche di sicurezza preesistenti all'atto della installazione dei nuovi certificati. Qualora fosse necessario procedere all'aggiornamento del piano per la sicurezza con impatto sugli aspetti inerenti l'ambito di protezione del dispositivo di firma, i certificatori dovranno operare in collaborazione fornendo a AdeR un unico documento.

Si rappresenta inoltre che:

1. il certificato avrà validità 3 anni dalla data di richiesta di singola attivazione che sarà via via effettuata;
2. i certificati dovranno essere necessariamente associati a chiavi di lunghezza non inferiore a 2048 bit, in linea con il Target di Sicurezza di cui all'Attestato di Conformità rilasciato da OCSI.;
3. i sistemi interessati, quindi l' HSM di AdeR presso il data center SOGEI e i sistemi della Certification Authority dovranno essere conformi alle linee guida specificate nel documento allegato "Linee Guida HSM_v1 1.pdf".

4 CONDIZIONI E MODALITÀ DI ESECUZIONE

4.1 PIANIFICAZIONE ATTIVITA' DI AUDIT

Con riferimento al servizio, il Fornitore dovrà predisporre, nel corso dell'affidamento, la pianificazione delle attività di audit che andrà concordata con AdeR.

4.2 RESPONSABILE DI PROGETTO E MODALITÀ DI COMUNICAZIONE

Al fine di assicurare il coordinamento di tutte le attività attinenti alla fornitura del servizio, il Fornitore comunicherà ad AdeR il nominativo ed i contatti della risorsa individuata come del contratto, e delle eventuali altre risorse di riferimento. Tali risorse dovranno assicurare la propria reperibilità negli orari di esecuzione delle attività e comunque ogni giorno lavorativo dal lunedì al venerdì dalle ore 09:00 alle ore 18:00.

4.3 AVVIO DEL PROGETTO

Entro 10 gg. solari dalla sottoscrizione del contratto, il Responsabile del contratto del Fornitore parteciperà alla prima riunione, ovvero al cosiddetto kick off delle attività presso AdeR, al fine di esaminare congiuntamente la pianificazione delle attività.

Il Fornitore raccoglierà tutte le informazioni e i documenti necessari all'avvio del progetto e, sulla base di quanto discusso e concordato, consegnerà entro i 15 gg. solari successivi la pianificazione di dettagliato.

L'avvio delle attività avverrà a valle dell'approvazione di AdeR del piano di progetto, entro e non oltre i successivi 10 gg. solari.

4.4 LIVELLI DI SERVIZIO E PENALI

Livello di Servizio	**Valore soglia**	**Penali**	**Periodo di osservazione per calcolo penali**
Tempo massimo di presa in carico della richiesta di emissione certificato	2 ore	0,5‰ dell'intero valore contrattuale per ogni ora di ritardo maggiore al valore soglia	Tutto il periodo contrattuale
Ripristino delle normali funzionalità del Sistema di Provisioning	4 ore	0,5‰ dell'intero valore contrattuale per ogni ora di ritardo maggiore al valore soglia	Tutto il periodo contrattuale
Indisponibilità del Sistema di Provisioning	1 volta ogni 3 mesi	per ogni caso eccendente al valore di soglia si applica una penale del 1‰ dell'intero valore contrattuale	Tutto il periodo contrattuale

5 VERIFICA DELL'ESECUZIONE DEL CONTRATTO

Il DEC, valutato il mancato rispetto delle obbligazioni contrattuali e delle disposizioni impartite per la corretta esecuzione delle prestazioni affidate, nessuna esclusa, segnala al RUP, le inadempienze riscontrate, anche al fine dell'applicazione delle penali di cui al paragrafo "Penali" del presente Capitolato, ovvero della risoluzione dello stesso per inadempimento, dopodiché provvede a formulare le relative contestazione al Fornitore a mezzo PEC all'indirizzo indicato nel contratto, assegnando a quest'ultimo un termine per la presentazione delle proprie controdeduzione e per rimuovere gli inadempimenti riscontrati non inferiore a 15 giorni naturali e consecutivi, salvo i

casi d'urgenza in cui il predetto termine non potrà essere inferiore a 10 giorni naturali e consecutivi.

Ad ogni modo, nei termini indicati nella segnalazione, il Fornitore dovrà trasmettere ad AdeR le proprie eventuali controdeduzioni; trascorso tale termine, la stazione appaltante adotterà i provvedimenti conseguenti.

Il Responsabile del Procedimento

Maurizio Cereda

(Firmato digitalmente)