Addendum al Manuale Operativo Servizio Postecert Firma Digitale

MOP01 del 14/01/2013

Copia Archiviata Elettronicamente	File: MO_ADDT_01.pdf

Copia cartacea Controllata in distribuzione ad enti esterni	N°:
Rilasciata al	
Copia cartacea non Controllata in distribuzione ad enti esterni	N°:

Versione n.	Pagina n.	Motivo della revisione	Data
1.0		Prima elaborazione: Rilascio di certificati di Firma Digitale remota per dipendenti appartenenti al Ministero delle Infrastrutture e dei Trasporti	22/10/2014

Versione n.	Redazione	Verifica	Approvazione	Data
1.0	Marco Bongiovanni	Giuseppe Pellegrino Marco Vaccari Alfredo Terrone	Fabio Sensidoni	23/10/2014

Indice

1 Scopo ed Applicabilità

Il presente documento viene redatto con lo scopo di esporre le procedure e le modalità operative adottate dal Certificatore Postecom S.p.A. per il servizio di certificazione con generazione di chiavi asimmetriche all'interno del Dispositivo centralizzato, sito presso il Ministero delle Infrastrutture e dei Trasporti, per l'apposizione di firme digitali e/o firme elettroniche qualificate ed emissione dei relativi certificati qualificati di firma per i dipendenti del Ministero stesso.

I certificati emessi dal Certificatore Postecom nell'ambito di quanto definito nel presente Addendum verranno adottati esclusivamente per procedure di emissione di documenti aventi valenza esterna del Ministero delle Infrastrutture e dei Trasporti.

Attraverso il presente documento si intendono definire i processi e le modalità operative seguite dal Certificatore Postecom per l'emissione e l'utilizzo dei certificati sopra esposti; tale documento va ad integrare quanto già definito all'interno del Manuale Operativo Servizio Postecert Firma Digitale - MOP01 del 14/02/2013 il cui contenuto, per quanto non espressamente ivi richiamato, deve intendersi valido ed operante.

Il Certificatore Postecom intende quindi, attraverso la pubblicazione del presente documento, consentire a terzi di accedere alle modalità del servizio di certificazione svolto per i dipendenti del Ministero delle Infrastrutture e dei Trasporti.

2 Contesto Normativo

D.Lgs.82/2005	"Codice dell'amministrazione digitale" e s.m.
CNIPA/CR/48	Modalita' per presentare la domanda di iscrizione nell'elenco pubblico dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445.
D.Lgs. 159/2006	"Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale" e s.m.
D.P.C.M. 30/03/2009	"Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici." e s.m.
CNIPA 45/2009	"Regole per il riconoscimento e la verifica del documento informatico"
D.P.C.M. 22/02/2013	"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36, comma 2, e 71."
D.Lgs. 196/2003	"Codice in materia di protezione dei dati personali"

3 Definizioni

Si riportano di seguito le definizioni contenute all'interno del presente documento.

Le definizioni di cui al Manuale Operativo MOP01 del 14/01/2013, a cui si rimanda, vanno intese come interamente richiamate.

Firma Digitale Remota	Procedura di firma elettronica qualificata o di firma digitale, generata su Hardware Secure Module, che consente di garantire il controllo esclusivo delle proprie chiavi private da parte dei titolari delle stesse.
Hardware Secure Module	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.
One Time Password	meccanismo di autenticazione di tipo challenge-response che consente l'accesso controllato al dispositivo di firma HSM ed è validamente utilizzabile una sola volta.
Token	Dispositivo fisico necessario per dare luogo a una autenticazione
Portale	Portale del Ministero delle Infrastrutture e dei Trasporti

4 Acronimi

CA	Certification Authority
RA	Registration Authority
WS	Web Service
DB	Data Base
BP	Banco Posta
AgID	Agenzia per l'Italia Digitale
FDR	Firma Digitale Remota
SSO	Single sign-on
HSM	Hardware Secure Module
OTP	One Time Password
DT o Amministrazione o Organizzazione	Ministero delle Infrastrutture e dei Trasporti

5 Obiettivi

Il documento descrive la soluzione tecnica abilitante per l'implementazione delle funzionalità di Firma Digitale Remota e Strong Authentication presso il cliente Ministero Infrastrutture e Trasporti.

La soluzione permette di dotare il DT di:

1. Una soluzione di Firma Digitale Remota che consenta lo scambio in rete di documenti con validità legale; la proposta è abilitante per la firma di documenti prodotti dalle Applicazioni Web in uso presso il Ministero delle Infrastrutture e dei Trasporti;
2. Una soluzione di Strong Authentication, basata su chiavi hardware OTP, che consente l'autenticazione forte del personale autorizzato ad utilizzare le applicazioni esposte sul Portale ed il servizio di firma digitale.

la soluzione di Firma su basa su un certificato digitale, generato dalla Certification Authority di postecom S.p.A. ed associato in modo univoco all'utente attraverso la fase detta di Enrollment.

Tale fase consiste nella registrazione dell'utente, sulla base di un processo autorizzativo interno al DT e nella emissione di un certificato digitale qualificato di firma remota a cura della CA di Postecom S.p.A., iscritta nell'elenco pubblico dei certificatori accreditati da AgID e riscontrabile nella TSL da questi pubblicata all'indirizzo https://applicazioni.cnipa.gov.it/TSL/IT_TSL_signed.xml.

Per quanto riguarda i sistemi Adobe il link utilizzabile è pubblicato dallo stesso AgID alla pagina http://www.agid.gov.it/identita-digitali/firmeelettroniche/firma-pdf.

A valle del completamento della fase di Enrollment, il certificato è archiviato in modo sicuro in un appliance hardware dedicato (HSM) e certificato dall'Organismo di Certificazione della Sicurezza Informatica (OCSI) ed AgID.

La presente soluzione tecnica prevede di generare una coppia di chiavi e un certificato per ogni utente, adottando una configurazione dei dispostivi HSM in alta affidabilità ai sensi dell'art. 8 comma 4 delle Regole Tecniche.

La disponibilità della soluzione di Strong Authentication è quindi un prerequisito importante per la realizzazione di una infrastruttura di Firma Digitale Remota. In tal modo il servizio di firma digitale risulta conforme al quadro normativo vigente ed allineato al Security Target dei dispositivi HSM certificati.

In particolare l'utilizzo dell'autenticazione forte per la firma digitale risponde in modo ottimale ai requisiti funzionali intrinsecamente connessi con il valore legale della firma digitale di:

- Sicurezza dell'identità del Titolare del Certificato Digitale (e della relativa chiave privata contenuta nell'appliance hardware gestito dal servizio);
- Volontà di apposizione delle firme digitali: l'attivazione della procedura di autenticazione mediante meccanismi che non possano essere resi completamente automatici, garantisce che, sia in caso di errori che per azioni malevole, non siano firmati digitalmente documenti senza che il Titolare del certificato sia consapevole dell'attivazione della procedura di firma stessa;
- Non ripudio: la firma digitale ha valore di sottoscrizione, essendo per legge equiparata alla firma autografa. La Strong Authentication contribuisce a garantire pertanto il livello di sicurezza sufficiente per cui la firma sia ritenuta legalmente valida fino a querela di falso, ai sensi del Codice per l'Amministrazione Digitale.

La soluzione proposta, limitando l'apposizione della firma digitale ai soli documenti creati ed emessi dalle applicazioni web dell'Amministrazione, di fatto inibisce l'utilizzo del certificato digitale all'esterno dell'Amministrazione stessa.

6 Descrizione della Soluzione

In questo capitolo sono brevemente descritti i singoli elementi della fornitura proposta organizzati nelle seguenti sezioni:

- Soluzione di firma digitale: comprende tutti gli elementi relativi alla funzionalità di firma digitale;
- Soluzione di Strong Authentication: comprende tutti gli elementi relativi alle funzionalità di autenticazione forte;

- Processo di enrollment: comprende i servizi di riconoscimento degli utenti e consegna delle credenziali per richiedere l'emissione del al certificato;
- Disegno dei processi del DT legati all'utilizzo della soluzione informatica e consistenti nella re-ingegnerizzazione o disegno ex-novo dei processi e nelle attività di Change Management collegate, necessarie alla piena adozione del modus operandi validato dall'Amministrazione.

6.1 Soluzione di Firma Digitale Remota

La soluzione di Firma Digitale proposta è costituita dai seguenti componenti:

- Appliance HSM: è costituito da due appliance che custodiscono i certificati digitali per la firma remota e che effettuano l'apposizione della Firma Digitale Remota. Gli appliance saranno installati nel rispetto dei requisiti infrastrutturali e di rete dell'Amministrazione e dei vincoli di sicurezza relativi alla normativa vigente;
- Middleware di firma digitale: è il componente che ha il compito di gestire le richieste di apposizione della firma elettronica che gli utenti sottomettono tramite le applicazioni web;
- Applicativo di Enrollment e Gestione Certificati: è una applicazione web based, che, utilizzando gli specifici servizi della Certification Authority di Postecom S.p.A., attraverso la mediazione del Middleware di firma digitale, fornisce le funzioni necessarie per il caricamento dei certificati qualificati sugli HSM in modo semplice, sicuro e nel rispetto della normativa in materia. L'applicativo di enrollment consentirà agli operatori della Local Registration Authority, autenticati con meccanismi di autenticazione a tre fattori, di gestire il ciclo di vita dei certificati digitali funzionale alla firma digitale (emissione e sospensione[1]) in accordo con i processi aziendali di provisioning che saranno concordati in fase di analisi; da notare che tale applicativo sarà predisposto per essere integrato con l'applicazione di gestione del ciclo di vita delle utenze già in uso dall'Amministrazione;
- Certificati digitali per il personale del DT emessi dalla Certification Autority di Postecom S.p.a. (vedi par 6.1.4)

L'autenticazione degli Titolari dipendenti del DT viene effettuata utilizzando dei token hardware personali, marcati "OT", che generano One Time Password (OTP). Il sistema di Strong Authentication è descritto più approfonditamente nel par. 6.2)

6.1.1 Appliance

La proposta tecnica contempla la fornitura di appliance preposti alla conservazione delle chiavi private dei certificati di firma remota secondo la normativa corrente.

6.1.2 Certificati di Firma Digitale Remota

Nell'ambito del presente Addendum le funzioni dell'Ufficio Delegato sono svolte esclusivamente da Operatori appartenenti al Ministero delle Infrastrutture e dei trasporti.

I certificati che saranno rilasciati saranno personali e intestati alla persona fisica che sarà riconosciuta da un Operatore di Ufficio Delegato del DT (vedi par. 6.3).

Su richiesta del DT i certificati rilasciati saranno limitati all'uso del processo di sottoscrizione erogato dall'Ente, inserendo nel campo "organization" del certificato il nome dell'Ente, e nel campo "user notice" un'apposita clausola in accordo con l'art. 12, comma 6, lettera c) della Deliberazione CNIPA n. 45, affinché il certificato sia limitato per le sole funzioni ricoperte dal ruolo del titolare all'interno del DT.

Tutti i certificati saranno firmati da un certificato della Certification Authority di Postecom S.p.A. accreditata per il rilascio di certificati per la firma digitale.

[1] Il servizio di revoca è gestito da un processo manuale offline, non è erogato a livello applicativo

6.1.3 Caso d'uso per Firma Digitale Remota

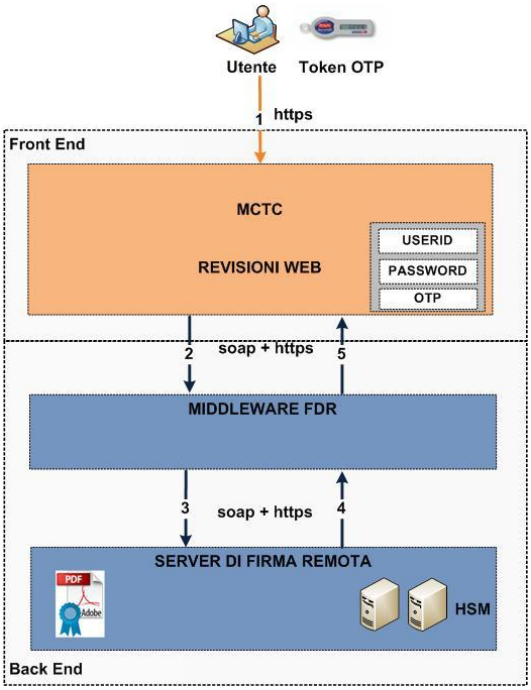
Un esempio del processo di firma digitale attivabile per le applicazioni che generano documenti, garantendone cosi la non ripudiabilità, è il seguente:

- l'utente accede all'applicazione del Portale utilizzando, se previsto dall'applicazione, una autenticazione forte ovvero fornendo username, password e codice OTP;
- l'utente esegue normalmente le proprie attività fino alla creazione del documento sul server;
- dopo la generazione del documento in formato pdf, l'applicazione richiede all'utente di firmarlo digitalmente;
- all'utente viene richiesto il PIN (codice numerico fisso associato alla chiavetta) e il codice OTP, assumendo che nella fase di Enrollment sul sistema di Firma Digitale il certificato dell'utente sia stato logicamente associato alla UserID del portale;
- I valori inseriti vengono verificati dalla piattaforma di Firma Digitale. Se le verifiche hanno esito positivo, il documento viene firmato digitalmente e può essere scaricato.

Come già precisato, la soluzione prevede che la firma possa essere applicata solo all'interno dei workflow delle applicazioni di DT, prevenendo così ogni possibile uso dei certificati stessi al di fuori degli ambienti dell'Amministrazione.

In particolare, sarà messa a disposizione degli utenti DT un'applicazione web che consente di effettuare il cambio pin del proprio certificato di firma.

Il flusso logico che segue il processo di firma è riportato nella figura seguente:



1. l'utente è già loggato al portale, ha perfezionato un documento PDF, vuole sottoporlo al sistema per firma; l'utente visualizza una interfaccia di apposizione Firma nella quale sono presenti:
    a. UserID: si propone la medesima utenza utilizzata per accedere al portale,
    b. PIN: l'utente deve digitare la propria password di Firma Digitale Remota,

c. OTP: l'utente deve digitare la One Time Password (password monouso);

2. il portale invia al Middleware di Firma la richiesta e il documento che deve essere firmato digitalmente;
3. il Middleware prende in carico il documento e invoca il Servizio di Firma sul Server di Firma Remota passando Documento, UserID, PIN e OTP;
4. il Server di FDR verifica il PIN e l'OTP, in caso positivo procede alla firma e restituisce al Middleware il Documento Firmato (PAdES);
5. il Middleware completa la sua attività restituendo il Documento Firmato (PAdES) al Portale Revisioni Web.

Il processo sopra descritto si conclude in maniera sincrona.

6.1.4 Security Audit

Al fine di garantire la massima sicurezza dell'intero processo di gestione dei certificati di firma Postecom, in qualità di Certificatore, verificherà la collocazione fisica degli appliance e le procedure di sicurezza applicate per la protezione degli apparati per certificarne la sicurezza logica e fisica.

A tale scopo viene inserita in offerta la seguente clausola di audit:

- il Certificatore, indirizzerà una richiesta formale di audit al Responsabile dei sistemi ICT del DT;
- nella richiesta verranno indicati ruoli e nominativi della/delle persona/persone appartenenti all'Ente Certificatore che eseguiranno la visita ispettiva;
- il periodo di preavviso in caso di audit è fissato dal Certificatore in 15 giorni;
- la visita ispettiva si svolgerà presso la sede del DT ove risiedono le macchine e si sostanziano i processi finalizzati all'erogazione del servizio di firma digitale attraverso l'appliance.

La costituzione del gruppo di audit sarà completata con la fornitura da parte del DT dei nominativi dei suoi funzionari, identificabili nelle figure del Responsabile delle verifiche e delle ispezioni (auditing) o suo delegato e del Responsabile dei sistema ICT o suo delegato.

La data dell'audit verrà concordata con DT durante la fase iniziale del progetto.

Postecom assume che i nominativi dei funzionari succitati siano comunicati da DT almeno 5 giorni prima della data prevista per l'Audit.

Il personale del Certificatore, insieme ai Responsabili indicati dal DT, avrà accesso ai locali ove sono mantenuti i server di cui si richiede la certificazione.

Postecom, nel suo ruolo di Certificatore, è responsabile della verifica dell'adozione di tutte le necessarie misure di sicurezza organizzative e tecniche nell'utilizzo e nella gestione del sistema di firma e dell'ambiente tecnologico che interagisce con questo.

L'attività di audit di sicurezza sarà dunque finalizzata a:

- analizzare lo scenario nel quale il sistema di firma è inserito: sarà pertanto richiesta al Cliente la documentazione necessaria (politiche di qualità e sicurezza, procedure operative, procedure tecniche relative alla configurazione e gestione degli strumenti tecnologici utilizzati, quali antivirus, firewall, ecc.) e sarà esaminata in un tempo variabile dipendente dalla quantità e complessità della stessa.
- verificare l'effettiva adozione delle misure di sicurezza previste (logiche, fisiche e organizzativa): sarà pertanto fissato un incontro in loco con il Cliente, durante il quale il team di audit visiterà gli ambienti che ospiteranno il sistema e intervisterà il personale individuato per testare la conoscenza, diffusione e applicazione delle norme e delle politiche di sicurezza in vigore;
- verificare la conformità normativa degli apparati di firma previsti;

Al termine dell'audit verrà redatto un rapporto contenente la sintesi dei risultati ottenuti e, specificatamente, i punti d'attenzione e gli ambiti di miglioramento ove sarà necessario intervenire con appositi trattamenti preventivi/correttivi definiti e concordati con il Team di Audit del Certificatore, insieme alle tempistiche entro le quali dovranno necessariamente essere attuati.

Con cadenza periodica, e comunque almeno annuale, il Team di Audit del Certificatore svolgerà una verifica sulla conservazione del livello di sicurezza ottenuto a valle dell'audit stesso.

Le attività di Audit sono propedeutiche al rilascio di certificati del Certificatore sugli apparati ospitati presso la sede del DT.

6.2 Soluzioni di Strong Authentication

La presente soluzione si basa su una infrastruttura per la Strong Authentication, a servizio non esclusivo, della funzionalità di firma digitale, ed è realizzata ed integrata con l'infrastruttura di Identity e Access Management dell'Amministrazione.

La funzionalità di Strong Authentication è generalizzata e quindi resa disponibile per essere successivamente integrata con le applicazioni che il cliente riterrà maggiormente critiche.

Da notare che la componente server per la Strong Authentication è fornita già integrata nel middleware e ne condivide pertanto gli aspetti architetturali già descritti precedentemente.

La soluzione di Strong Authentication si basa sull'uso del token fisico Vasco, un dispositivo hardware che genera a intervalli regolari delle One Time Password (OTP) con le quali è possibile realizzare la Strong Authentication o abilitare la funzione di firma con il proprio certificato digitale.

L'autenticazione dell'utente può essere integrata nelle applicazioni dell'Amministrazione, cosicché queste richiedano, in fase di accesso al portale, oltre alle credenziali di accesso (userid, password), anche la OTP.

Il portale dell'Amministrazione, ottenute le credenziali dall'utente, invoca un servizio del Middleware passando la userid e la OTP; il Middleware accede, quindi, al modulo di SA passando le credenziali ricevute e in funzione della userid viene validato il valore del la OTP inserita.

Il servizio Middleware ritorna al sistema di Identity Management l'esito della verifica e in caso di riscontro positivo il portale consente l'accesso all'utente.

L'utilizzo delle SA è abilitato solo per quegli utenti a cui è stato rilasciato il token fisico di generazione della OTP. Tale attività avviene in una fase propedeutica ed è a carico dell'Amministrazione.

Durante tale fase all'utente è rilasciato il token Vasco che viene registrato sul server di SA per l'associazione della userid dell'utente al SID del token fisico; l'attività di associazione userid e token fisico avviene tramite un servizio esposto dal Middleware.

Con una singola pressione del tasto, il token visualizza una one-time password dinamica, per ogni volta che un utente accede in remoto ad un'applicazione o sito web.

Per l'abilitazione della funzione di firma, è prevista la creazione di un PIN aggiuntivo, associato al certificato, per ridurre il rischio di uso non autorizzato, qualora il dispositivo venisse perso o rubato.

6.3 Rilascio del certificato di Firma Digitale Remota

Il rilascio di un certificato digitale ad un Titolare deve avvenire secondo precise indicazioni fornite da Postecom, basate a loro volta sulle vigenti norme in materia di Firma Digitale.

La Convenzione è il documento che regola i rapporti tra il Certificatore ed il DT, indicando i reciproci impegni nell'esecuzione delle attività.

Nell'ambito della Convenzione sono "Referenti" i soggetti delegati dall'Organizzazione alla gestione dei rapporti con il Certificatore, alla richiesta di registrazione da parte degli appartenenti all'Organizzazione nonché all'inoltro della richiesta di revoca o sospensione dei certificati.

L'Organizzazione potrà poi individuare degli Operatori da applicare all'Ufficio Delegato per svolere le attività di identificazione del Titolare nonché ogni attività definita all'interno del MOP01.

Nell'ambito del trattamento dei dati personali connessi all'espletamento delle attività previste dalla Convenzione, Postecom, in qualità di Titolare, nomina ai sensi dell'art. 29 del D.Lgs. 196/2003 l'Organizzazione quale Responsabile esterno del trattamento medesimo.

Al fine di procedere ad una puntuale esplicazione dei processi di identificazione e riconoscimento, Postecom erogherà corsi di formazione rivolti agli Operatori degli Uffici Delegati presso una o più sedi concordate con il DT. I corsi avranno generalmente durata di quattro ore e prevedono il rilascio del certificato all'Operatore e delle opportune credenziali che consentono l'accesso all'ambiente applicativo.

6.3.1 Registrazione

Il Referente si collega al Portale del Ministero delle Infrastrutture e dei Trasporti e, dopo essersi opportunamente autenticato attraverso l'applicazione "Gestione Utenti", richiede l'emissione del certificato per i dipendenti dell'Ufficio Provinciale di riferimento.

Ha così inizio il processo di Registrazione che si conclude con la generazione da parte della CA del certificato e con la consegna all'Utente, da parte dell'Operatore, del Token OTP (vedi par. 6.3.2).

A seguito della richiesta di certificato da parte del Referente, vengono recuperati applicativamente dai Data Base del DT i dati anagrafici del Titolare per il quale viene richiesta l'emissione del certificato ed effettuata una preregistrazione presso la Registration Authority del Certificatore. Il Titolare riceve, contestualmente alle credenziali, all'indirizzo e-mail specificato in fase di registrazione il codice di sospensione immediata definito dalla CA in fase di registrazione.

L'Operatore dell'Ufficio Delegato, selezionato da DT fra i dipendenti dell'Amministrazione e comunicato preventivamente a Postecom, riceve da parte dell'applicazione la notifica della pre-registrazione tramite e-mail, e collegandosi con meccanismi a tre fattori al portale del DT, interroga, tramite dei servizi offerti dal middleware, l'elenco delle prenotazioni afferenti al suo Ufficio Delegato di riferimento.

L'Operatore dell'Ufficio Delegato prende quindi appuntamento con il Titolare per la verifica ed il completamento dei dati di registrazione, in particolare:

- procede alle attività di identificazione de visu per mezzo di un documento d'identità valido;
- verifica la completezza e la correttezza dei dati e li completa sul portale del DT;

- consegna la busta contenente il token per la generazione del codice OTP e fornisce le informazioni necessarie per utilizzare il servizio di Firma Digitale;
- attiva la procedura di generazione del PIN di primo accesso al servizio che verrà inviato all'indirizzo email del Titolare;
- stampa, in duplice copia, la Scheda di Registrazione compilata in ogni sua parte e la sottopone contestualmente alla Condizioni Generali del Servizio di Certificazione ed ai relativi allegati al Titolare (formato pdf); Il Titolare dopo aver letto la documentazione presentata sottoscrive la Scheda di Registrazione per accettazione dell'intera documentazione contrattuale. L'Operatore dell'Ufficio Delegato procederà infine a compilare e sottoscrivere la parte della Scheda di registrazione (in entrambe le copie) ad esso riservato relativa alla compiuta fase di identificazione consegnerà una copia al Titolare;
- conserva una copia della documentazione contrattuale originale sottoscritta da Titolare.

Alla conclusione del processo verrà inviata automaticamente una notifica tramite e-mail al Titolare contenente le istruzioni per procedere autonomamente alla fase di emissione del certificato.

6.3.2 Emissione

Così come indicato nella e-mail di notifica il Titolare si collegherà al portale ivi indicato con le opportune credenziali di sicurezza. Gli verrà richiesto di inserire il PIN di primo accesso e, successivamente, di definire il PIN da utilizzare durante le operazioni di firma.

L'applicazione sottostante al portale opera in modo da:

- recuperare i dati di registrazione;
- comporre con tali dati la richiesta di certificato alla CA, avendo generato sull'HSM la coppia di chiavi, pubblica e privata;
- inviare via web service la richiesta di certificato alla CA;
- installare sull'HSM il certificato così ottenuto.

I certificati prodotti sono validi immediatamente e possono quindi essere fin da subito utilizzati.