Smart Card Owner Guide

Guida all'interfaccia αPeS™ ® per il titolare di una Smart Card di firma automatica

ver1.2

SECURE EDGE

your safety .net

Questo documento è disponibile all'indirizzo: www.secure-edge.com/Appliance_PeS/doc/
seguendo il link Signer Manual

Table of Contents

(blank page)

Destinatari del manuale

Questa guida è rivolta a qualsiasi persona fisica cui sia stata assegnata una smart card per la firma automatica di documenti.

Tale soggetto, detto titolare di smart card, è la persona che fisicamente firma i documenti su cui viene poi apposto il timbro digitale.

Per approfondire i concetti di firma digitale,certificati digitali e firma automatica si rimanda all'appendice in calce al presente documento.

Fatta questa premessa, passiamo alla descrizione delle attività che coinvolgono il titolare di smart card per poter generare un timbro digitale.

Assetto organizzativo

Una volta che si è stabilito l'ufficio o la divisione responsabile dell'emissione del documento a cui si vuole applicare il timbro digitale, lo stesso dovrebbe formalizzare la propria richiesta di servizio di creazione di timbro digitale indicando il tipo documento, i dati da firmare, i destinatari del documento nonchè il firmatario e titolare di smart card.

Prima di avviare un processo di produzione documentale con timbro digitale, sarebbe necessario predisporre una serie di procedure organizzative volte all'individuazione di ruoli e responsabilità per un utilizzo ottimale dell'applicazione.

Ruoli e Responsabilità

A tale scopo andrebbero individuati i seguenti ruoli:

- Responsabile Applicazione [RAp]: persona fisica/ufficio che fornisce le informazioni al Titolare di smart card relativamente al contenuto dei documenti che questo ultimo autorizzerà a firmare in modo automatico, con la smart card di cui risulta intestatario. In capo a tale figura ricade la responsabilità di definire gli ambienti che consentono di descrivere i documenti, i firmatari, le applicazioni informatiche che gestiscono tali informazioni (configurazioni).

- Amministratore dell'Appliance αPeS™ ® [PeSAdmin=PAdm]: amministratore della configurazione del Software Core Appliance αPeS™ 2D-Plus®, tale figura ha il compito di associare la smart card del Titolare alla configurazione definita in precedenza dal responsabile dell'applicazione; inoltre dovrà operare affinchè il titolare rimanga l'unico a poter attivare o disattivare la propria smart card e affinchè la stessa sia conservata in modo da non essere disponibile ad altri se non al titolare.

- Titolare della Smart Card: persona fisica, in possesso di una smart card con certificato di firma digitale automatica, cui è demandata la firma dei dati per l'apposizione del timbro digitale per il documento scelto. Qualora il titolare fosse già in possesso di una smart card

per la firma automatica, avrebbe facoltà di utilizzarla per firmare un ulteriore documento senza doverne richiedere una nuova.

La procedura di firma

Prima di proseguire con le operazioni di firma è necessario personalizzare ogni smart card ufficiale attraverso una cerimonia di sostituzione delle originali credenziali di attivazione della stessa.

In questa cerimonia, il titolare della smart card utilizza un PC off-line con un lettore di smart card inserito, per cambiare PIN e PUK assegnati inizialmente dal Certificatore Accreditato che l'ha rilasciata.

Una volta che la smart card è stata personalizzata in questo modo, può essere sottoposta al rilascio e all'attivazione presso il centro che ospita l'Appliance αPeS™

Assicurazione e controllo delle operazioni

Una volta formalizzata la volontà di applicare un timbro digitale ad un particolare documento (per evitare confusione, da qui in avanti IDD), devono essere svolti una serie di passi, sia per organizzare le attività per l'erogazione di questo nuovo servizio, sia per ottemperare agli obblighi legali.

Da qui in avanti, viene usato come guida organizzativa e modello di riferimento, il form "Dichiarazione Richiesta di Timbro Digitale" (DRT).


Richiesta Servizio Timbro Digitale - Sezione Tecnica/Applicativa

POLICY: Qualunque utilizzo di qualunque Smart Card presente nella Piattaforma αPeS™ 2D Plus™, deve essere autorizzato tramite questo modello.

Responsabile Applicazione:
- Cognome / Nome
- Ufficio
- Ruolo
- Telefono
- Fax
- E-mail

Dichiarazione:
Si dichiara che la Smart Card, *inserire identificativo Smart Card*, verrà utilizzata dalla Applicazione informatica *inserire identificativo applicazione*, quando questa Applicazione richiederà il servizio di Timbro Digitale utilizzando la Piattaforma αPeS™ 2D Plus™.
Il documento *inserire identificativo documento*, verrà firmato ed un Timbro Digitale verrà creato, utilizzando la configurazione: *inserire identificativo configurazione*.

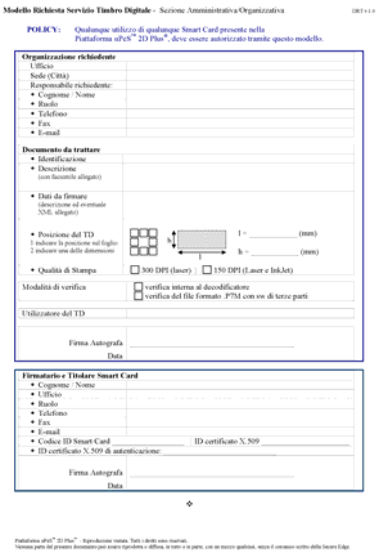
Identificativi
- Codice Applicazione — Descrizione
- Configurazione — Descrizione
- Host (ID certificato X.509) — Descrizione

Firma Autografa
Data

Amministratore Piattaforma αPeS™ 2D Plus™:
- Cognome / Nome
- Ufficio
- Ruolo
- Telefono
- Fax
- E-mail

Dichiarazione:
Si dichiara che la Smart Card, *inserire identificativo Smart Card*, contiene un certificato X509 *inserire ID X.509 di firma*.
Si dichiara che il Titolare *inserire nome e cognome Titolare Smart Card*, verrà identificato univocamente dalla piattaforma αPeS™ 2D Plus™, per mezzo del certificato di autenticazione *inserireID X.509 di autenticazione del Titolare*.

Firma Autografa
Data


Modello Richiesta Servizio Timbro Digitale - Sezione Amministrativa/Organizzativa

POLICY: Qualunque utilizzo di qualunque Smart Card presente nella Piattaforma αPeS™ 2D Plus™, deve essere autorizzato tramite questo modello.

Organizzazione richiedente
- Ufficio
- Sede (Città)

Responsabile richiedente:
- Cognome / Nome
- Ruolo
- Telefono
- Fax
- E-mail

Documento da trattare
- Identificazione
- Descrizione (con facsimile allegato)
- Dati da firmare (descrizione ed eventuale XML allegato)
- Posizione del TD (1 indicare la posizione nel foglio; 2 indicare una delle dimensioni): l = _____ (mm); h = _____ (mm)
- Qualità di Stampa: ☐ 300 DPI (laser) ; ☐ 150 DPI (Laser e InkJet)

Modalità di verifica: ☐ verifica interna al decodificatore; ☐ verifica del file formato .PTM con sw di terze parti

Utilizzatore del TD

Firma Autografa
Data

Firmatario e Titolare Smart Card
- Cognome / Nome
- Ufficio
- Ruolo
- Telefono
- Fax
- E-mail
- Codice ID Smart Card _____ ID certificato X.509 _____
- ID certificato X.509 di autenticazione _____

Firma Autografa
Data

Nella descrizione dei capitoli che seguono, gli elementi preceduti dal simbolo ↳ sono da considerarsi necessari ed obbligatori, anche se viene raccomandato la compilazione del form in ogni sua sezione.

La richiesta

L'ufficio responsabile del documento a cui applicare il Timbro Digitale (TD) imposta preliminarmente una Dichiarazione Richiesta di Timbro Digitale (DRT). In questo documento, per la parte di competenza dell'ufficio richiedente, vengono indicati:

- ✓ l'anagrafica dell'ufficio competente;
- ✓ il codice (IDD) del documento DT a cui verrà associato un timbro digitale;
- ✓ una descrizione dei dati da trattare, con un allegato contenente la loro rappresentazione finale o quanto altro necessario per consentire al TSC di identificare in modo certo il documento che andrà a firmare in modalità automatica;
- ✓ un' indicazione di massima della posizione del TD nel DT;
- ✓ la qualità di stampa prevista, che implicitamente definisce la densità in PPI (point-per-inch) del TD;
- ✓ una descrizione sull'utilizzo che verrà fatto del TD;

I dati del Titolare

L'ufficio responsabile del documento, una volta firmata la parte del DRT di sua competenza, dovrà identificare il firmatario del documento IDD d'interesse.

Il firmatario (TSC) a sua volta compilerà il DRT. Due sono le sezioni di sua competenza. Nella prima il TSC dovrà indicare:

- ✓ la sua anagrafica nel contesto aziendale;
- ✓ il codice riportato sulla smart card di ADS in suo possesso e utilizzata per firmare l'IDD indicato;
- ✓ il codice identificativo (XSG) del certificato di chiave pubblica, presente all'interno della smart card;
- ✓ il codice identificativo (XAT) del certificato di autenticazione, con il quale verrà autorizzato dalla piattaforma αPeS™ 2D-Plus® ad operare;

Il RAp e le Garanzie sull'applicazione informatica

Nel contesto attuale, i documenti (IDD) di cui si parla, sono tipicamente generati da una procedura informatica, cioè da un software, residente all'interno del sistema informatico dell'Azienda/Ente.

In un processo di ADS il software richiede ad una Smart Card di operare una firma digitale: come può un TSC, titolare di una smart card essere certo di cosa firma quest'ultima?

Per fornire le giuste garanzie di sicurezza al TSC, sarebbe opportuno che il responsabile dell'applicazione informatica [RAp] facesse una dichiarazione formale con il dettaglio di cosa viene firmato ed in quale contesto.

Il RAp, che ha la responsabilità dell'applicazione che genera l'IDD, deve quindi compilare e firmare una sezione della DRT a lui dedicata da presentare al TSC ed al PAdm.

Nella sezione di sua competenza:

- ✓ viene identificata in modo univoco [IDA] l'applicazione che genera il documento di cui viene fornito l'identificativo IDD;
- ✓ viene fornita la garanzia che l'applicazione IDA, richiederà la generazione del timbro digitale, esclusivamente per questo IDD;
- ✓ viene indicato l'XAA dell'host che ospita l'applicazione, il quale consentirà l'indentificazione certa dell'host richiedente, da parte dell'appliance;
- ✓ viene indicata la configurazione (ICP) che verrà utilizzata per richiedere all'appliance di generare un timbro digitale per questo IDD; questa configurazione, tra le altre cose, consente un'associazione certa tra la richiesta di timbro digitale per un particolare documento, l'applicazione richiedente e l'host che la ospita ed infine le smart card che potranno operare una ADS;

Il PAdm e le Garanzie sull'operatività dell'appliance

Affinchè tutte le policy di sicurezza e le assicurazioni sui processi descritti abbiano un riscontro sulle operazioni reali, l'amministratore dell'appliance (PAdm) dovrà a sua volta fornire una dichiarazione, di cui si assume la responsabilità, nella quale garantirà che:

- ✓ la smart card con il codice esterno identificato e riportato, contiene un certificato di ADS il cui identificativo è XSG;
- ✓ che questa smart card, è stata associata dal PAdm, a lavorare sulla configurazione ICP proposta dal RAp;
- ✓ che il TSC, verrà autenticato dalla piattaforma αPeS™ 2D-Plus®, per mezzo di un certificato di autenticazione il cui identificativo è XAT,
- ✓ che solo al TSC, autenticato con il suo certificato XAT, verrà dato accesso alla smart card contenente il certificato XSG;

Completamento del Form: Accettazione da parte del firmatario

Il TSC, con il DRT totalmente compilato e firmato dai vari responsabili, ha un corretto livello di assicurazione e di controllo, circa le attività di firma automatica, che verranno fatte operare dalla sua smart card (XSG).

In queste condizioni può completare il DRT, firmando a sua volta la sua dichiarazione, nella quale accetta di fare operare firme digitali automatiche --dalla smart card contenente il certificato XSG precedentemente da lui identificata-- nel contesto indicato, firmato e garantito dai vari responsabili.

Processo di generazione dei timbri digitali

Definiti ruoli e responsabilità, individuato il titolare di firma e i documenti che lo stesso ha la responsabilità di firmare, è possibile apporre il timbro digitale attraverso l'appliance αPeS™.

L'Appliance αPeS™

αPeS™ è lo strumento ideato da Secure Edge, che permette di introdurre, con un impatto minimo sull'assetto informativo preesistente, l'uso del Timbro Digitale in modalità automatica nei normali processi di produzione documentale nel rispetto della normativa vigente.

L'appliance αPeS™ è un computer connesso ad una rete locale, al quale si possono richiedere una serie di servizi, dedicati alla creazione di timbri digitali basati sul codice grafico 2D- Plus® ed alla firma digitale. L'erogazione di tali servizi non prevede modifiche sostanziali alle applicazioni esistenti o l'istallazione di nuovi agenti software.

αPeS™ fornisce informazioni sullo stato dei suoi servizi tramite un'applicazione web ed una console di gestione molto semplice, con autenticazione basata su certificati digitali.

Tutte le operazioni di firma gestite da αPeS™ avvengono tramite un apparato sicuro di firma (Smart Card) o un HSM (Hardware Security Model), integrato con l'appliance.

La funzione di attivazione/disattivazione dell'HSM integrato in αPeS™ permette esclusivamente al titolare della chiave di sottoscrizione, contenuta nell'HSM, di esprimere la propria volontà di attivazione del processo di firma automatica, così come esplicitamente richiesto dalla normativa vigente.

Tutte le operazioni effettuate con αPeS™ avvengono in totale sicurezza tramite canale SSL.

Modalità multicard : SCBox

La presenza di più titolari, quindi di più smart card, aumenta la complessità della loro gestione sicura, che è molto importante, oltre che obbligatoria per legge.

A questo scopo, la Secure Edge mette a disposizione un apparato, con cui integrare l'Appliance αPeS™ 2D-Plus®, definito SCBox, che consente la gestione in aree fisiche separate ad accesso dedicato, delle smart card.

Questo SCBox può contenere da un minimo di una ad un massino di 12 smart card. La SCBox contiene al su interno le smart card che utilizza, sia per ragioni di sicurezza che in ottemperanza al Codice dell'Amministazione Digitale. Un Appliance αPeS™ 2D-Plus® può gestire fino a quattro SCBox.

Configurazione smart card

Cerimonia di rilascio smart card

Per ogni nuova smart card è buona prassi che il suo Titolare sostituisca le originali credenziali di attivazione: PIN e PUK. Il Titolare, utilizzando un PC off-line tramite il lettore di smart card ed il software fornito dal Certificatore Accreditato, dovrebbe cambiare PIN e PUK associati inizialmente alla smart card.

In genere il titolare è presente nella fase di inserimento della propria smart card nella SCBox, sia per certificare che questa sia stata inserita nell'apparato e nel luogo concordato, sia perchè successivamente all'inserimento fisico, il titolare dovrà fornire il PIN di sblocco allo scopo di completare il profilo di uso della smart card stessa.

Attenzione: per le caratteristiche elettriche dei lettori di Smart Card è necessario porre particolare attenzione a come vengono inserite le Smart Card nei lettori.

In caso di erroneo inserimento è possibile che il lettore risulti bloccato e l'unico modo per sbloccarlo è il riavvio dell'Appliance αPeS™ 2D-Plus® a cui è collegato con i problemi connessi alla riattivazione dei demoni di firma.

Le Smart Card vanno inserite con il chip rivolto verso il lettore e la faccia contenente il chip rivolta verso il lato destro dell'SCBox™
(vedi figura laterale)

Contemporaneamente il titolare dovrà fornire al PeS Administrator, il proprio certificato di autenticazione, in modo da poter successivamente accedere alla "Interfaccia Titolare" che l'Appliance mette a disposizione.

Da sottolineare che il PIN digitato non viene memorizzato su disco né mantenuto nella memoria dell'appliance, pertanto successivamente a questa operazione, il PIN non è più disponibile all'appliance.

Verifica funzionale Smart Card: Timbri Digitali di prova

Alla fase precedente viene fatta seguire quella di verifica della funzionalità della smart card.

Questo processo vede coinvolti, oltre al titolare di smart card, ai responsabili operativi del centro, al PeS Administrator, anche il responsabile dell'applicazione che richiede il servizio del Timbro Digitale.

Il richiedente il servizio di Timbro Digitale in precedenza ha effettuato una serie di test utilizzando una smart card di test.

Il test di verifica funzionalità è progettato dal Responsabile dell'applicazione che richiede il servizio del Timbro Digitale; tipicamente si tratterà di richiedere la generazione di un Timbro Digitale la cui firma digitale verrà prodotta dalla smart card in questione.

Affinchè si possa valutare la funzionalità della smart card ufficiale, il titolare di smart card dovrà:

- ✓ accedere all' Interfaccia Titolare messa a disposizione dall'Appliance;
- ✓ selezionare la smart card di interesse;
- ✓ abilitare questa Smart alla configurazione (identificata con ICP) che deriva dal documento di Richiesta del Timbro Digitale,
- ✓ attivare la smart card

Al termine dei test, il titolare di smart card può disattivare nuovamente la Smart Card.

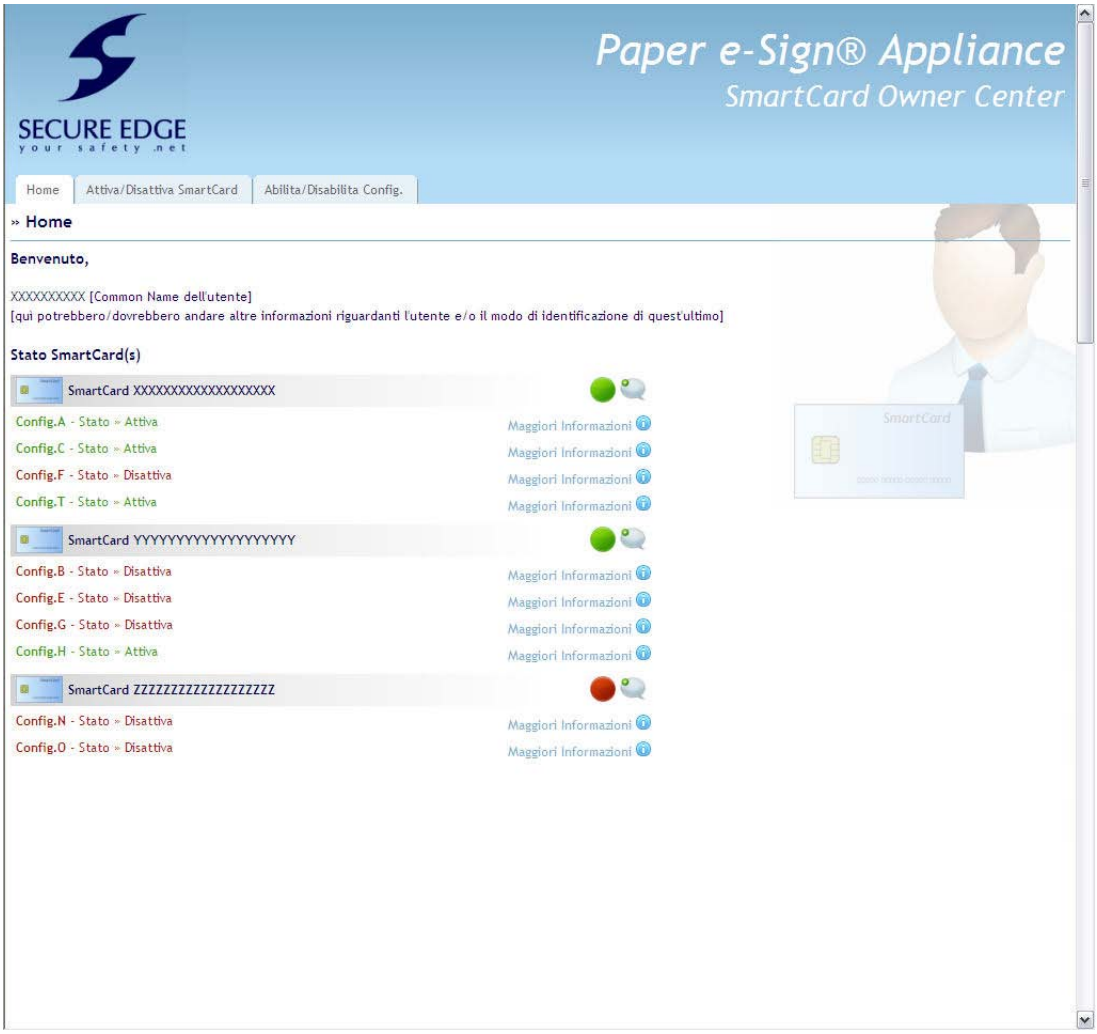
Descrizione interfaccia

Home page

L'accesso a tale interfaccia avviene soltanto se si è titolari di una o più Smart Card di firma automatica e solo previa autenticazione web per la quale è necessario che il titolare disponga di un certificato X.509 di autenticazione (XAT) da richiedere all'amministratore dell'appliance.

Sull' home page sono disponibili le seguenti informazioni:

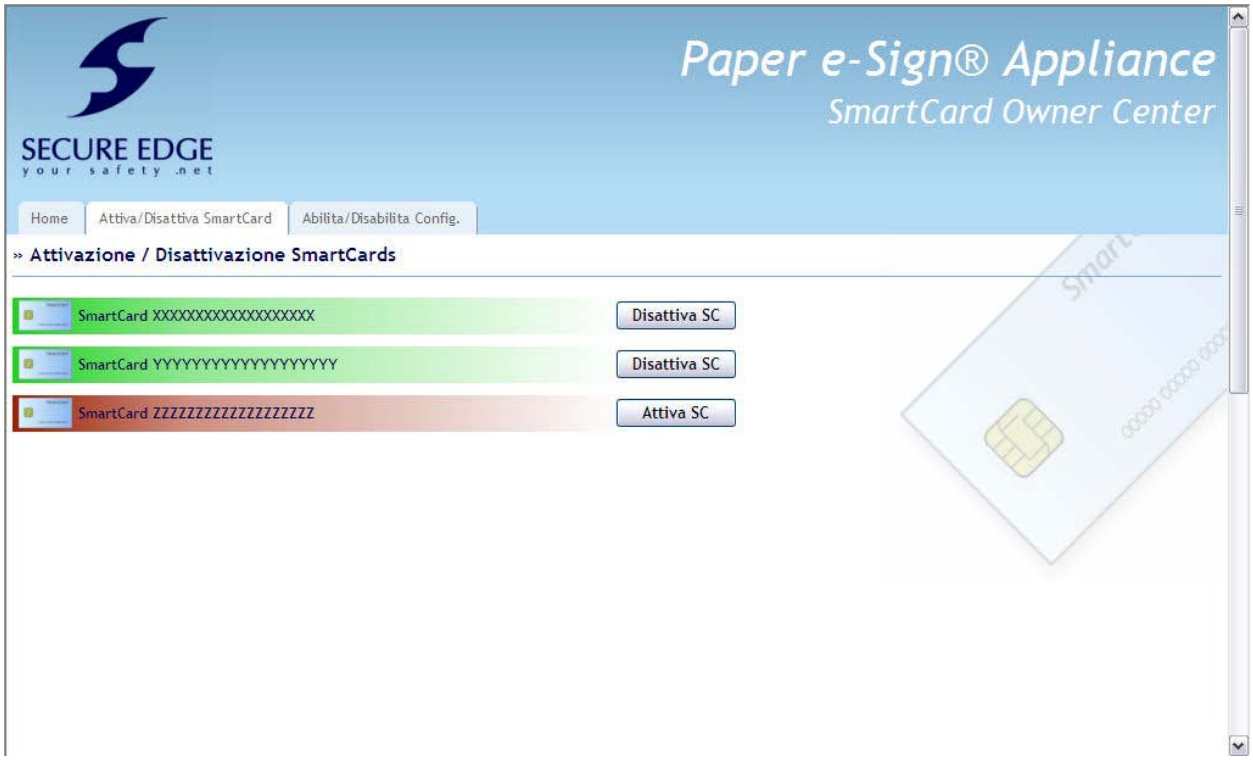
1. Dati Utente: in questa sezione vengono forniti i dati relativi al titolare della smart card. nome, cognome e altre informazioni (common name)
2. Numero di smart card associate all'utente: ogni utente può essere titolare di una o più smart card, in questa sezione è disponibile l'elenco di tutte le smart card associate all'utente;
3. Stato della smart card. Per ogni smart card di cui l'utente è titolare è possibile conoscere lo stato di attivazione. Nel caso in cui la smart card non risultasse attivata, le motivazioni potrebbero essere o che il certificato è scaduto, che la smart card non sia stata attivata dal titolare o che sia danneggiata. In tal caso è opportuno che il titolare la attivi.



Attiva/Disattiva smart card

In questa sezione è possibile attivare e disattivare la/le smart card associate al titolare ed è inoltre possibile visualizzare lo stato di attivazione della/delle smart card: verde se attivata, rossa se disattivata. La disattivazione della smart card potrebbe essere causata da:

- Smart card danneggiata
- Mancata attivazione da parte del titolare
- Certificato scaduto

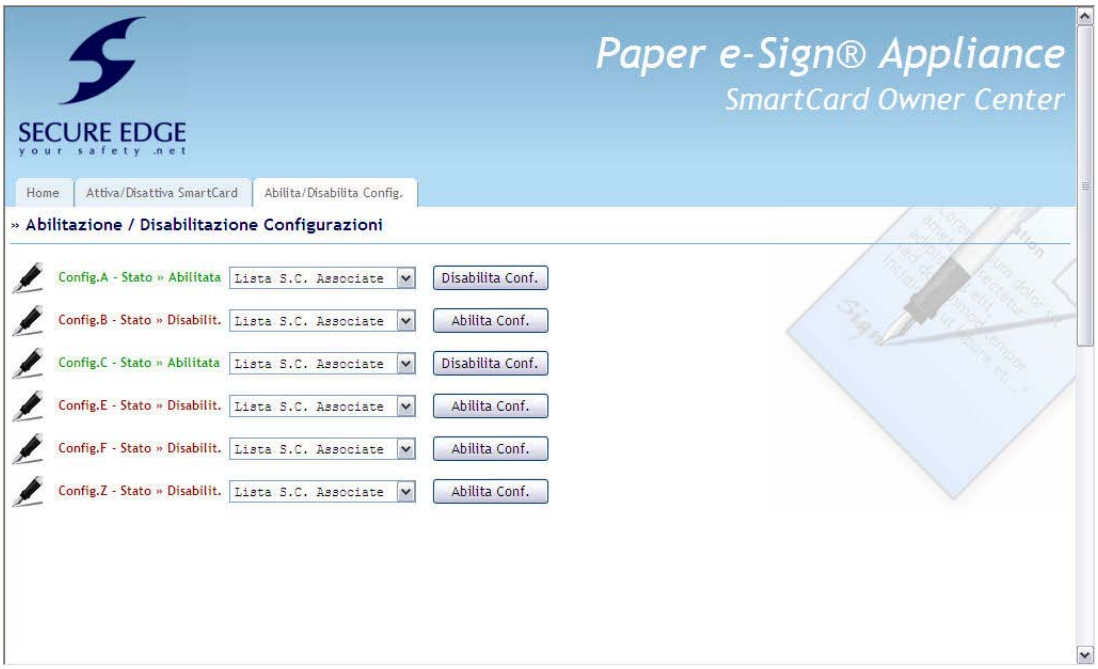


Abilita/disabilita configurazioni

In questa maschera sono elencate le configurazioni, vale a dire la tipologia di documenti che il titolare di smart card può firmare e la/le smart card associate ad ogni configurazione.

In una configurazione sono presenti una serie di dati che permettono di verificare se la richiesta fatta all'appliance sia corretta, quale host/applicazione può fruire dei servizi associati alla configurazione richiesta, cosa e come operare sui dati allo scopo di realizzare un timbro digitale, che cosa restituire ed in che formato e così via.

Da questa interfaccia è possibile abilitare disabilitare singolarmente le configurazioni associate alle smart card dei titolari.



Appendice

La firma digitale

In Italia il Codice dell'Amministrazione Digitale (D. Lgs. 85/2005) prevede la firma digitale come soluzione tecnica per garantire ai documenti elettronici lo stesso valore legale della firma tradizionale. La firma digitale è associata ad un documento informatico e ne garantisce l'autenticità l'integrità e il non ripudio.

Per generare una firma digitale è necessario utilizzare una coppia di chiavi digitali asimmetriche, attribuite in maniera univoca ad un soggetto detto Titolare della coppia di chiavi. La prima, detta chiave privata destinata ad essere conosciuta solo dal Titolare, è utilizzata per la generazione della firma digitale da apporre al documento, la seconda, chiave pubblica, viene utilizzata per verificare l'autenticità della firma. Caratteristica di tale metodo, detto crittografia a doppia chiave, è che, firmato il documento con la chiave privata, la firma può essere verificata con successo esclusivamente con la corrispondente chiave pubblica.

Possono dotarsi di firma digitale tutte le persone fisiche (cittadini, amministratori e dipendenti di società e pubbliche amministrazioni) che ne facciano richiesta a Certificatori accreditati. Questi ultimi sono soggetti pubblici e privati che hanno ottenuto l'autorizzazione da parte di un Ente a ciò preposto (il CNIPA) a svolgere la funzione di garante dell'identità dei soggetti che utilizzano la firma digitale.

Il certificato digitale

L' elemento di rilievo del sistema di firma è rappresentato dal certificato digitale di sottoscrizione che il Certificatore rilascia al titolare di un dispositivo di firma (una smart card o token USB).

Il certificato di sottoscrizione è un file generato seguendo precise indicazioni e standard stabiliti per legge (al suo interno sono conservate informazioni che riguardano l'identità del titolare, la chiave pubblica attribuitagli al momento del rilascio, il periodo di validità del certificato stesso oltre ai dati dell'Ente Certificatore).

Il certificato digitale ha lo scopo di garantire che una chiave pubblica sia associata alla vera identità del soggetto che la rivendica come propria. Per poter generare una firma digitale è necessario disporre del kit di firma digitale fornito dal Cerificatore che comprende un dispositivo sicuro di generazione della firma (smartcard o token USB), un eventuale lettore di smartcard ed il software di firma in grado di utilizzare lo specifico dispositivo di cui si è dotati. Il caso che si prende in considerazione nel presente manuale contempla la sola generazione di firma tramite smart card.

La firma automatica

In numerose situazioni il procedimento di sottoscrizione può coinvolgere un elevato numero di documenti.

Non è quindi efficiente in tali procedimenti l'utilizzo della sottoscrizione "documento per documento" anche per evitare la digitazione del PIN di sblocco della smart card di firma a ogni sottoscrizione.

L'utilizzo di procedure automatiche di sottoscrizione è previsto dalla normativa vigente che obbliga a particolari cautele.

In particolare, è necessario che quando il titolare appone la sua firma mediante una procedura automatica utilizzi una coppia di chiavi diversa da tutte le altre in suo possesso.

Ogni dispositivo di firma utilizzato per procedure automatiche deve disporre di coppie di chiavi differenti, una per dispositivo, anche se il titolare è sempre lo stesso.

L'utilizzo di dispositivi di firma particolari denominati HSM (Hardware Security Module) garantisce migliori prestazioni rispetto alle smart card.

❖