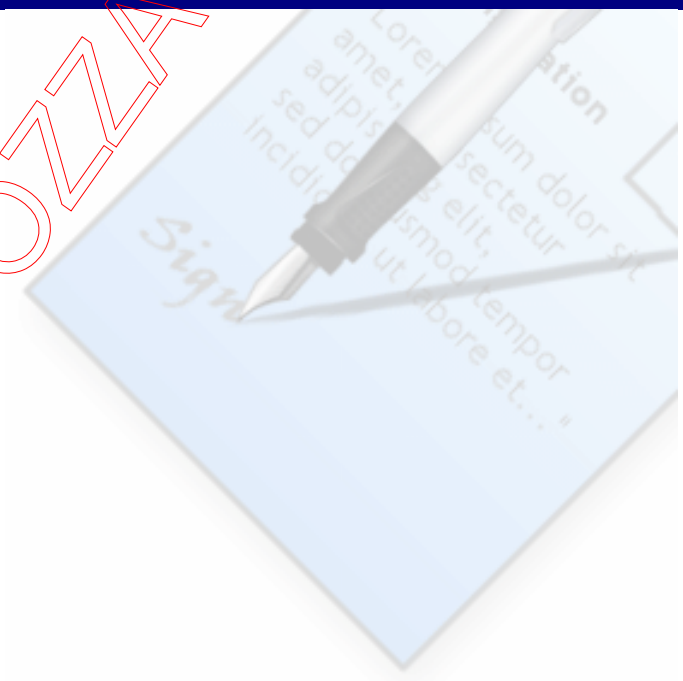
Interfaccia Amministratore αPeS

Guida all'interfaccia Amministratore αPeS™

Ver 2.0



SECURE EDGE
your safety .net

Sommario

Definizioni e acronimi

Sigla	Descrizione
[LR]	Last Release (questa sigla riportata a fianco di un documento ricorda che si fa riferimento all'ultima versione del documento stesso).
Configurazione	Una configurazione, di seguito indicata anche con l'abbreviazione "Conf", è una struttura dati che descrive un particolare attività che verrà svolta del server. La configurazione indica un profilo di applicazione autorizzato a richiedere il servizio, il o i certificati di firma da utilizzare e le caratteristiche dell'attività da svolgere.
HSM	Hardware Security Module, infrastruttura hardware che contiene e protegge un certificato di firma digitale.
HSM	Hardware Security Module generalmente utilizzato per indicare apparati di firma realizzati con schede per computer o sistemi dedicati. I sistemi HSM si caratterizzano per l'alta velocità di firma e/o dalla possibilità di ospitare un grande numero di certificati di firma (alcune migliaia) In linea di principio una Smart Card è un HSM.
MultiSSCD Box	Il MultiSSCD Box è un contenitore tamper evident di Smart Card. Il MultiSSCD Box viene in contro all'esigenza di ospitare molti certificati di firma in un contenitore compatto e proporzionalmente più conveniente di molti SCBox. Il MultiSSCD Box è fornito precaricato con i token crittografici ed essi non sono accessibili dall'esterno. Questa è la principale differenza con l'SCBox. Il MultiSSCD Box può ospitare fino a 98 certificati di firma saturando in questo modo le possibilità dell'appliance.
N.A.	Non Applicabile
PAdm	Nella soluzione Timbro Digitale di Secure Edge identifica il ruolo dell'amministratore dell'appliance αPeS
Profilo	Il Profilo è una struttura dati che associa un nome ad un certificato di autenticazione; vengono generati profili per TSC nel seguito anche P_TSC e per applicazioni nel seguito anche P_App. I profili TSC vengono associati ai certificati di firma mentre i profili applicazioni vengono associati alle configurazioni. P_TSC -> Cert_F (1 a n con n>= 0) P_App -> Conf (n a m con n e m > 0)

	Conf -> Cert_F (n a m con n e m > 0)
RAp	Responsabile dell'applicazione che richiede i Timbri Digitali
Mini SCBox	Il Mini Security Box è un contenitore tamper evident di lettori USB per Smart Card (token USB crittografici). Un Mini SC Box può contenere fino a 7 lettori, collegati direttamente e ad uso esclusivo sull'appliance αPeS. In situazioni in cui i TSC sono molti o i certificati di firma con limitazione d'uso specifica sono tanti è possibile collegare internamente fino ad un massimo di 4 Mini SCBox per appliance.
SCBox	Il Security Box è un contenitore tamper evident di lettori di Smart Card. Un SCBox può contenere fino a 6+6 lettori che possono essere collegati ad uno o due appliance αPeS. I lettori di Smart Card sono in uso esclusivo all'appliance αPeS a cui sono collegati. In situazioni in cui i TSC sono molti o i certificati di firma con limitazione d'uso specifica sono tanti è possibile collegare gli SCBox in cascata fino ad un massimo di 8 SCBox per appliance.
SE	Secure Edge
TSC	Nella soluzione Timbro Digitale di Secure Edge identifica il ruolo del Titolare del certificato di firma digitale automatica che verrà utilizzato per firmare i documenti. Tipicamente il certificato di firma è conservato in una mart Card.
SSCD	Secure Signature Creation Device è un apparato per effettuare firme digitali conforme alla direttiva Europea sulla firma elettronica 1999/93/UE, tipicamente una Smart Card

Documentazione di riferimento

Titolo del documento Descrizione del documento Eventuale nome file
SCBox User Guide Manuale di utilizzo della SCBox. [SE_T-08-0054] T I MAN SCBox User Guide [1.9].pdf
Procedure Operative Manuale che presenta un insieme di procedure operative per la gestione dell'appliance αPeS. [SE_T-07-0049] T I DST proc operative aPeS [1.5]

Introduzione

Il presente documento è parte della documentazione prodotta per supportare gli utilizzatori della piattaforma di Timbro Digitale 2DPlus della Secure Edge srl; tutta la documentazione può essere scaricata dal sito:

www.timbrodigitale.com.

Questo manuale illustra l'interfaccia di amministrazione dell'appliance αPeS ed è destinato principalmente all'amministratore dell'appliance, nel seguito denominato **PAdm**, ma illustra anche l'interfaccia di gestione per il titolare della Smart Card., nel seguito denominato **TSC**.

Per una descrizione generale del servizio si rimanda alla documentazione presente in rete ed in particolare al manuale "***Introduzione alla soluzione Timbro Digitale***".

Per una illustrazione veloce dei passi operativi vedere il capitolo **Procedure Operative: Quick Start**.

Descrizione della piattaforma

La seguente descrizione della piattaforma di Timbro Digitale 2DPlus ha il solo scopo di offrire una visione generale del contesto nel quale opera il PAdm e il TSC quando utilizzano l'interfaccia di amministrazione dell'appliance αPeS.

La piattaforma consiste in strumenti hardware, applicazioni software e processi organizzativi che sintetizziamo nei paragrafi seguenti.

Scopo della Piattaforma

La piattaforma di Timbro Digitale 2DPlus può produrre Timbri Digitali, documenti PDF contenenti Timbri Digitali o Firme Digitali. La piattaforma di Timbro Digitale 2DPlus può anche codificare un Timbro Digitale a partire da dati generici forniti dall'applicazione.

Timbro Digitale è la denominazione adottata dal CNIPA nel documento "*Il timbro digitale: una soluzione tecnologica per l'autenticazione di documenti stampati*" - Versione 2.0 - 18 dicembre 2006 per una soluzione tecnologia inventata da Secure Edge e presentata alla XXXIX conferenza annuale del AICA nel settembre del 2001.

Un Timbro Digitale nella soluzione di Secure Edge srl è un codice a barre bidimensionale che contiene il documento firmato digitalmente.

Con l'adozione della piattaforma Timbro Digitale di Secure Edge si possono produrre documenti di cui si può verificate l'autenticità e l'integrità anche nella forma stampata.

Piattaforma Hardware

La Piattaforma di Timbro Digitale 2DPlus si compone di almeno un appliance αPeS e uno o più HSM; tipicamente gli HSM utilizzati con l'appliance αPeS sono Smart Card.

Per rispettare i requisiti di legge che richiedono di conservare l'apparato di firma con diligenza la Secure Edge ha realizzato una serie di apparati/contenitori che consentono di conservare le Smart Card in modo da evidenziare eventuali manomissioni. Gli apparati SSCD realizzati e/o gestiti sono:

- il Mini SCBox è un contenitore sicuro di Smart Card nel quale è possibile inserire fino a 7 card è integrato all'interno dell'appliance; un appliance può contenere fino a quattro Mini SCBox.
- l'SCBox. è un contenitore sicuro di Smart Card nel quale è possibile inserire 6 + 6 card.
- L'MSBox è un contenitore sicuro di Smart Card che ospita fino a 49 + 49 card non rimovibili (Smart Card Embedded).
- Il µSCBox è un contenitore sicuro di Smart Card nel quale è possibile inserire una singola card. Questo contenitore è integrabile all'interno del mini appliance che può quindi contenere fino a due µSCBox.
- Apparati HSM ad alte prestazioni.

I diversi apparati SSCD gestiti si differenziano nella modalità di caricamento del certificato di firma. Tipicamente le Smart Card sono inizializzate da una CA emittente, mentre le Smart Card "embedded" necessitano di una procedura di richiesta del certificato; successivamente alla richiesta tale certificato deve essere caricato sulla card. Nulla osta a gestire la fase di richiesta e caricamento anche per le Smart Card. Per quanto riguarda gli apparati HSM ad alte prestazioni, la fase di caricamento del certificato viene realizzata direttamente sull'apparato. Quando tale HSM viene predisposto, viene gestito dall'appliance come se si trattasse di una Smart Card.

La piattaforma di Timbro Digitale 2DPlus è progettata in modo da garantire la continuità del servizio. L'appliance αPeS può essere configurato in modalità High Availability in hot-standby utilizzando i servizi offerti dalla piattaforma, oppure in load-balancing utilizzando hardware di bilanciamento esterno alla piattaforma di Timbro Digitale.

La piattaforma nasce per offrire il servizio di produzione di Timbri Digitali o di Firma Digitale automatica. Deve quindi essere interfacciata con una infrastruttura che richieda il servizio per realizzare l'applicazione di interesse.

Piattaforma Software

Per produrre un Timbro Digitale, l'applicazione "client" instaura un colloquio HTTPS con l'appliance αPeS. L'appliance dispone di diverse interfacce software in modo da semplificare l'integrazione della soluzione con l'infrastruttura del cliente.

La produzione di Timbri Digitali comporta l'acquisizione dei dati, la loro firma e quindi la codifica all'interno del codice a barre bidimensionale 2DPlus. In ultimo avviene la restituzione al chiamante del file contenente il Timbro Digitale. L'esecuzione delle firme Digitali all'interno dell'appliance è delegata ai "demoni di firma". I "demoni di firma" si occupano di colloquiare con gli HSM, tipicamente le smart card, per le operazioni di crittografia. Ogni demone di firma è configurato per utilizzare una specifica smart card attraverso una procedura detta "cerimonia di inizializzazione del certificato".

Piattaforma Organizzativa

L'adozione della Piattaforma di Timbro Digitale 2DPlus da parte di un cliente comporta necessariamente l'adozione di una serie di procedure organizzative mirate a soddisfare i requisiti di legge relativi all'utilizzo della firma digitale.

Anche in assenza di norme specifiche circa le modalità di utilizzo della firma digitale, è necessario rispettare delle procedure di sicurezza, affinché la soluzione tecnica possa essere efficace.

La Secure Edge srl ha pubblicato il documento "*[SE_T-07-0049] T I DST proc operative aPeS [1.5]*" in cui si illustra una procedura Organizzativa conforme ai dettami della legge Italiana sulla firma digitale.

Amministrazione dell'Appliance αPeS

L'amministratore può operare sull'appliance esclusivamente tramite interfaccia WEB. La connessione è cifrata, e all'amministratore è richiesto di autenticarsi con un certificato (mutua autenticazione forte con protocollo HTTPS). Per utilizzare in maniera corretta l'interfaccia di amministrazione, nel browser deve essere abilitato il supporto JavaScript.

L'appliance αPeS viene fornito unitamente ad un CD contenente il certificato di amministratore (.crt) precaricato sull'appliance e la relativa chiave privata (.p12) da caricare all'interno di un certificato crittografico.

E' comunque possibile caricare qualunque tipologia di certificati, in formato X509, emessi da qualsiasi CA pubblica o privata. Qualora di decidesse di utilizzare certificati emessi da una CA diversa da quella di SE si dovrà caricare il certificato della CA utilizzata. Per il dettaglio di questa operazione riferirsi al capitolo "*Authentication: Caricamento Certificati di autenticazione*"

Le pagine di amministrazione presentano dei brevi testi sullo scopo dei vari moduli interattivi ("form") e dei relativi vincoli di sicurezza.

La maggior parte dei bottoni dei form sono realizzati in modo tale da chiedere conferma prima dell'esecuzione delle operazioni richieste. Per alcune operazioni, sono invece presenti delle pagine "intermedie" di conferma.

Attenzione l'appliance viene consegnato con password di accesso standard che deve essere modificate prima di effettuare qualsiasi operazione !!

Per il cambio della password riferirsi al capitolo "*Web Pass: Modifica password di accesso*" a pagina 29

Amministrazione Concetti base

L'interfaccia di amministrazione dell'appliance αPeS presenta tre aree operative logicamente distinte così denominate: Administrator, Token Owner, Open Area.

La presenza sull'appliance αPeS di tre aree distinte identifica tre tipologie di utenti riconosciuti dal sistema, che sono:

- Amministratore PAdm (la versione attuale ammette uno solo amministratore)
- Titolare di Smart Card TSC (uno o più)
- Chiunque possa raggiungere l'appliance

L’area Amministrator è accessibile solo dal PAdm del sistema che viene riconosciuto dal suo certificato X509.

L’area Token Owner è accessibile dai TSC che possono operare sui certificati di firma. I certificati di firma sono consegnati da un Incaricato all’Identificazione. Nella consegna di ciscun certificato di firma, il TSC è tenuto a controfirmare un modulo presentato dall’Incaricato all’Identificazione. Ciascun TSC viene riconosciuto dal certificato X509 che presenta. Tutti i certificati di firma sono contenuti entro un HSM: per essere attivati richiedono uno specifico PIN noto solo al titolare. Eventuali possibili errori di configurazione non compromettono la sicurezza del sistema.

L’Open Area è aperta a chiunque possa raggiungere l’indirizzo dell’appliance. Quest’area espone delle informazioni di servizio che possono essere utili a ruoli diversi dal PAdm o TSC quali, ad esempio, il responsabile dell’applicazione che richiede i timbri, nel seguito indicato anche l’acronimo di **Rap**.

L'amministratore ha i seguenti compiti principali:

- imposta tutti i principali parametri relativi al sistema: parametri di rete, orario di sistema, accesso a tutti i log, download del file relativo allo stato del sistema (“Status Pack”), configurazione dell’agent di system management “Zabbix”, l’invio di alert tramite eamil, l’attivazione del supporto per le varie tipologie di Token crittografico (smart card)
- installa i pacchetti di aggiornamento al sistema, quando rilasciati.
- crea/rimuove i profili per i titolari dei certificati TSC e per le applicazioni
- associa i profili delle applicazioni alle configurazioni PeS
- associa i TSC ai relativi certificati di firma, presenti all’interno di smart card o dispositivi HSM (Luna SA)
- esegue la creazione, la modifica, la cancellazione, l’esportazione e l’importazione di una configurazione PeS
- esegue la pre associazione dei certificati di firma alle configurazioni
- esegue il caricamento di file XSL (per il processamento XSL-PDF, e quindi la generazione direttamente sull’appliance di documenti PDF contenenti il timbro digitale) e la successiva associazione alle varie configurazioni di firma
- gestisce le licenze per la firma associate a ciascun profilo
- modifica le credenziali predefinite per il profilo di Amministratore per l’accesso web alla gestione dei certificati di autenticazione
- interrompe il meccanismo di firma di uno o più certificati.

Il TSC, titolare di un certificato, ha i seguenti compiti:

- Prende il controllo del certificato di firma eseguendo la “cerimonia”
- conferma l’assegnazione del proprio certificato all’applicazione
- attiva o disattiva la firma per ogni certificato, potendo limitare la firma ad una data e/o ad un numero di firme per ciascuna configurazione a cui è associata
- Gestisce la Smart Card potendo cambiare il PIN e il PUK associato alla card

L'amministratore e i titolari di certificato accedono all'interfaccia di amministrazione autenticandosi con un certificato X509 (mutua autenticazione).

Le aree di accesso dell'interfaccia di amministrazione sono:

- area Administrator
  - System
  - PeS Admin
  - PeS Cfg parameters
  - Special Tasks
- area Token Owners
- area “open” (non richiede autenticazione)
- pagine riepilogativa di aiuto

Gestione richiesta certificati per MSBox

La procedura per la richiesta dei certificati da caricare sulle Smart Card “embedded” presenti nel MSBox è descritta dettagliatamente nel manuale d’uso della procedura CRSS. Nel presente manuale viene illustrato il processo generale al fine di fornire una visione d’insieme della procedura e viene presentata l’interazione con l’appliance.

In questa procedura vengono riconosciuti i seguenti cinque attori:

- Richiedente è la persona che richiede il certificato di firma digitale che può essere diverso dal titolare.
- Titolare (TSC) è l’intestatario del certificato di firma.
- ODR è il … della CA emittente i certificati
- Identificatore è la persona incaricata dall’ODR di identificate il titolare prima di consegnare il certificato.
- PAdm è l’amministratore dell’appliance.

In questa procedura entrano anche i seguenti due sistemi:

- CRSS è il sistema Certificate Request Support System che permette la gestione delle informazioni per richiedere un certificato.
- L’appliance è il sistema che caricherà il certificato nella Smart Card embedded.

Il processo viene attivato dal richiedente che contatta l’ODR indicando la necessità di ottenere un certificato; l’ODR crea un accesso al sistema CRSS e riporta le credenziali al richiedente.

Il richiedente con le credenziali di accesso e la collaborazione del titolare, opera sul sistema CRSS fornendo tutte le informazioni necessarie al rilascio del certificato. Al termine della procedura di caricamento dati, il richiedente esegue il completamento delle informazioni.

L’ODR verifica le informazioni inserite dal richiedente. Se non si riscontrano anomalie, prepara il pacchetto di pre-richiesta del certificato (pre-CSR pack) che viene inviato all’identificatore. L’identificatore lo consegnerà personalmente al titolare per effettuare il riconoscimento “de visu”.

Il titolare accede sull’appliance e carica il pacchetto “pre-CSR” (richiesta certificato) operando quindi con una Smart Card vuota a lui assegnata dal PAdm. L’appliance produce il pacchetto CSR che viene scaricato dal titolare e che lo invierà per posta elettronica all’ODR.

L’ODR verifica nuovamente tutte le informazioni: se non riscontra problemi richiede il certificato alla CA. La CA provvede ad emettere il certificato e lo restituise all’ODR. Infine l’ODR lo restituisce al titolare sotto forma di “certificate pack”.

Il titolare può finalmente caricarlo sulla Smart Card che gli è stata assegnata.

Interfaccia di Amministrazione

La URL di accesso all'interfaccia è la seguente: **https://<appliance IP>/**

L'appliance viene inviata con un indirizzo IP sull'interfaccia "eth0" pari a 192.168.41.231 per il primo nodo, 192.168.41.232 per il secondo nodo 192.168.41.233 per l'indirizzo virtuale di HA e subnet mask 255.255.255.0

Quella che segue è la home page dell'interfaccia di amministrazione dell'appliance. Dalla home page si può accedere all'area desiderata.

Dalla home page dell'appliance è possibile accedere direttamente alle quattro sotto-aree dell'Amministratore:

- **System** amministrazione del sistema operativo
- **PeS** amministrazione delle funzionalità di firma
- **Config** amministrazione delle configurazioni
- **Special** operazioni speciali (caricamento certificati di autenticazione, CA e modifica del parametro di rinegoziazione SSL)

System Area: Configurazione del sistema

La configurazione degli aspetti sistemistici e di rete dell'appliance viene realizzata nell'area "***Administrator***" e quindi nel menu "***System***", presente in home page. Questo menu consente di accedere alla gestione delle seguenti funzioni:

- *System info*: consente di accedere al completo dettaglio delle principali configurazioni di sistema e di eseguire l'accesso ai relativi log;
- *Network*: consente di accedere alle configurazioni delle interfaccia di rete "eth0" ed ai parametri di configurazione del servizio di High Availabity
- *Ping*: consente di accedere alla funzione di invio di pacchetti "*icmp echo request*" (vedi paragrafo "*Open Area => Ping: Operazioni di troubleshooting*" a pagina 99)
- *Traceroute*: consente di accedere alla funzione di invio di pacchetti UDP per la visualizzazione dei sistemi intermedi fra appliance αPeS e altre infrastrutture remote (vedi paragrafo "*Open Area => Traceroute: Operazioni di troubleshooting*" a pagina 101)
- *Routing*: consente di accedere alle configurazioni del routing dell'appliance (inserire rotte statiche a livello di singolo host o sottorete)

- *Date / time*: consente di accedere alle configurazioni di data e ora di sistema o di impostare l'indirizzo di un server NTP
- *Agents*: consente di accedere alla configurazione del software di system management "Zabbix", per l'invio delle informazioni di funzionamento ad un omologo server Zabbix centralizzato; nelle versioni più recenti dell'interfaccia di amministrazione in quest'area è possibile indicare anche i parametri per l'invio automatico di email di alert, per avvisare l'amministratore di situazioni anomale
- *Cripto support*: abilitare il supporto crittografico per le varie tipologie di Smart Card supportate
- *Web Pass*: aggiornamento delle password per l'amministratore per accedere alla funzione speciale "*Authentication: Caricamento Certificati di autenticazione*"
- *Shutdown*: consente di accedere alla funzione per lo spegnimento completo dell'appliance
- *http on / off*: consente di abilitare o disabilitare il funzionamento dell'appliance con il protocollo http, sia per l'amministrazione, sia per il collegamento al "gateway" cgi-bin da parte delle applicazioni che contattano il servizio di firma.

System Info: Informazioni di sistema

Questo menu visualizza un riepilogo di tutte le principali configurazioni del sistema operativo dell'appliance, tra cui:

- hostname
- ID appliance
- Data/ora
- Configurazione delle interfacce di rete
- Routing
- Server DNS impostati
- Accesso all'elenco dei servizi in esecuzione

Inoltre attraverso quest'area è possibile accedere a tutta una serie di log, quali:

- Log di sistema operativo e dell'applicativo αPeS (in questa schermata convergono sia i log del sistema operativo, sia il log del software di firma; in caso di errori durante i processi di firma, è utile consultare i log presenti in questa pagina)
- Log del servizio web in chiaro (http) (consente di accedere alla lettura del file di log relativo alle operazioni del servizio Apache "in chiaro" (http); all'interno di questo file vengono riportate anche le attività di amministrazione svolte con il protocollo http

- Log del servizio web in SSL (https) (consente di accedere alla lettura del file di log relativo alle operazioni del servizio Apache su canale cifrato (SSL); all'interno di questo file vengono riportate anche le attività di amministrazione svolte con il protocollo https
- Log del web application server per la produzione da XSL-FO

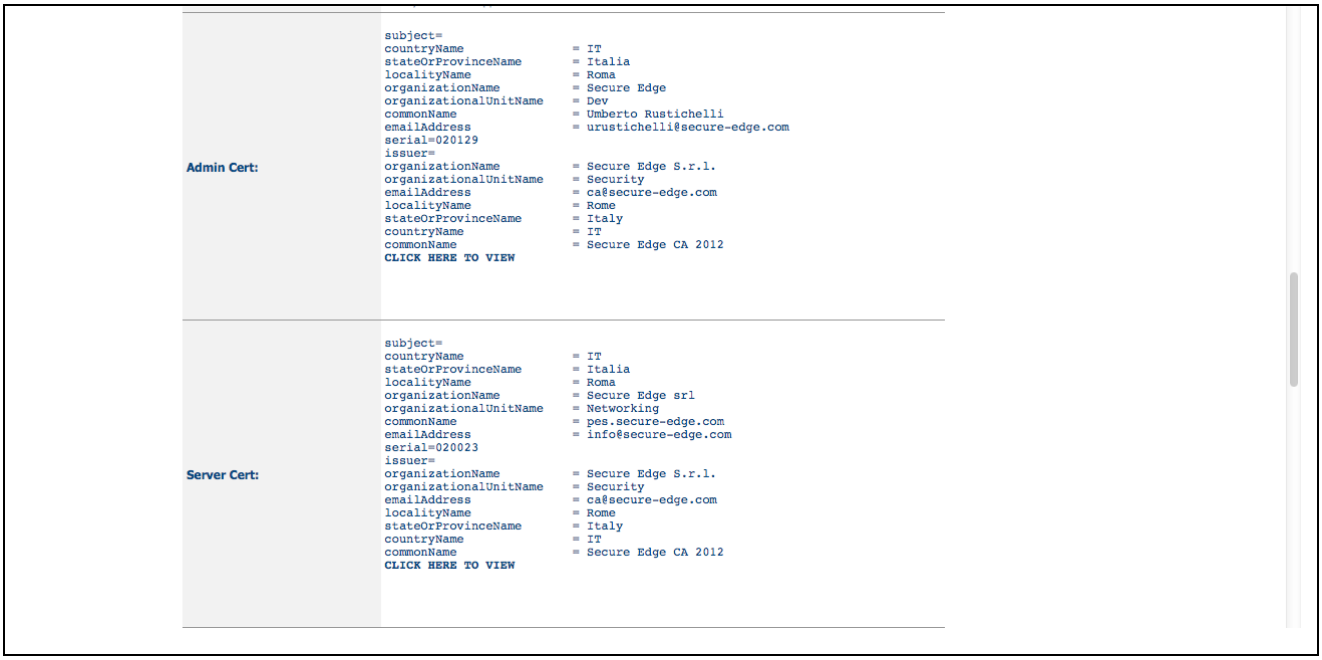
Infine, come illustrato nella seguente figura, vi è la possibilità di accedere ad alcune funzioni utili in caso di debug / troubleshooting, ovvero :

- *Download status pack*: consente di scaricare, sul proprio computer locale, un file in formato "*Ubi-StatusLogPack.[annomesegiornoora].PeS_info_pack*" contenente tutte le configurazioni (sia di sistema operativo, che di firma) attualmente presenti sull'appliance αPeS. Questo file rappresenta un valido backup della configurazione oltre ad essere uno strumenti di diagnostica che potrà essere richiesto dal supporto tecnico di Secure Edge srl.
- *Download rich status pack*: come il precedente, tuttavia vengono esportate tutte le impostazioni, nonché tutti i log in un intervallo temporale maggiore; da utilizzare in caso di troubleshooting avanzato.

Di seguito presentiamo un esempio di System Info.

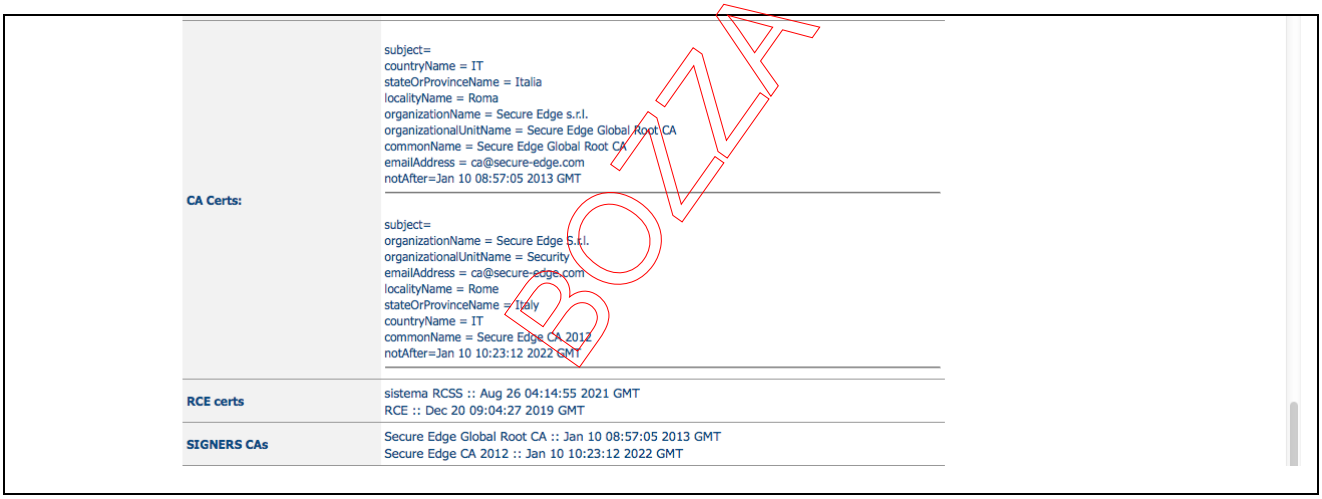
La sezione Log permette di visualizzare le ultime n righe del log selezionato da minimo 100 fino ad un massimo di 1000 righe.

La sezione Crypto riporta l'elenco dei driver di Smart Card presenti nel sistema e quelli attivati. I driver per i quali lo stato di ***Allowed*** è uguale ad ***N*** sono driver che per essere attivati richiedono il supporto di Secure Edge. Va ricordato che, a causa dei possibili conflitti fra driver differenti, è desiderabile attivare i soli driver necessari.

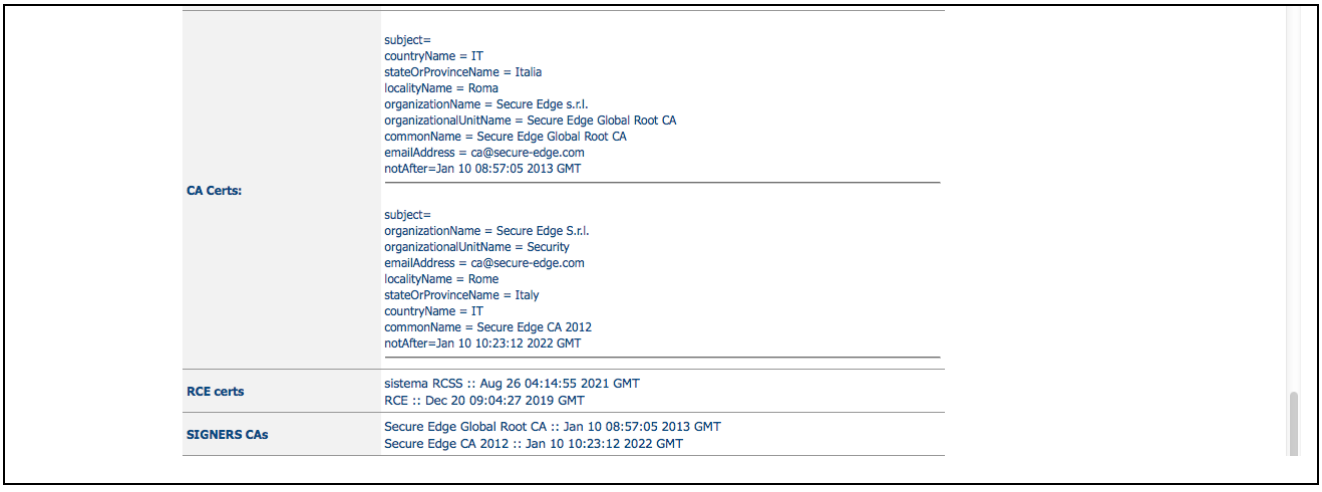


Admin Cert:	subject= countryName = IT stateOrProvinceName = Italia localityName = Roma organizationName = Secure Edge organizationalUnitName = Dev commonName = Umberto Rustichelli emailAddress = urustichelli@secure-edge.com serial=020129 issuer= organizationName = Secure Edge S.r.l. organizationalUnitName = Security emailAddress = ca@secure-edge.com localityName = Rome stateOrProvinceName = Italy countryName = IT commonName = Secure Edge CA 2012 **CLICK HERE TO VIEW**
Server Cert:	subject= countryName = IT stateOrProvinceName = Italia localityName = Roma organizationName = Secure Edge srl organizationalUnitName = Networking commonName = pes.secure-edge.com emailAddress = info@secure-edge.com serial=020023 issuer= organizationName = Secure Edge S.r.l. organizationalUnitName = Security emailAddress = ca@secure-edge.com localityName = Rome stateOrProvinceName = Italy countryName = IT commonName = Secure Edge CA 2012 **CLICK HERE TO VIEW**

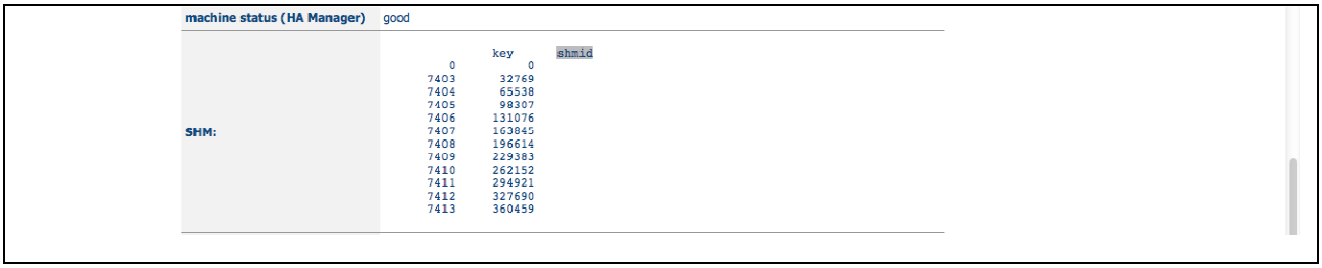
Le sezioni Admin Cert, Server Cert e CA Cert presentano le informazioni relative ai rispettivi certificati.



CA Certs:	subject= countryName = IT stateOrProvinceName = Italia localityName = Roma organizationName = Secure Edge s.r.l. organizationalUnitName = Secure Edge Global Root CA commonName = Secure Edge Global Root CA emailAddress = ca@secure-edge.com notAfter=Jan 10 08:57:05 2013 GMT --- subject= organizationName = Secure Edge S.r.l. organizationalUnitName = Security emailAddress = ca@secure-edge.com localityName = Rome stateOrProvinceName = Italy countryName = IT commonName = Secure Edge CA 2012 notAfter=Jan 10 10:23:12 2022 GMT ---
RCE certs	sistema RCSS :: Aug 26 04:14:55 2021 GMT RCE :: Dec 20 09:04:27 2019 GMT
SIGNERS CAs	Secure Edge Global Root CA :: Jan 10 08:57:05 2013 GMT Secure Edge CA 2012 :: Jan 10 10:23:12 2022 GMT



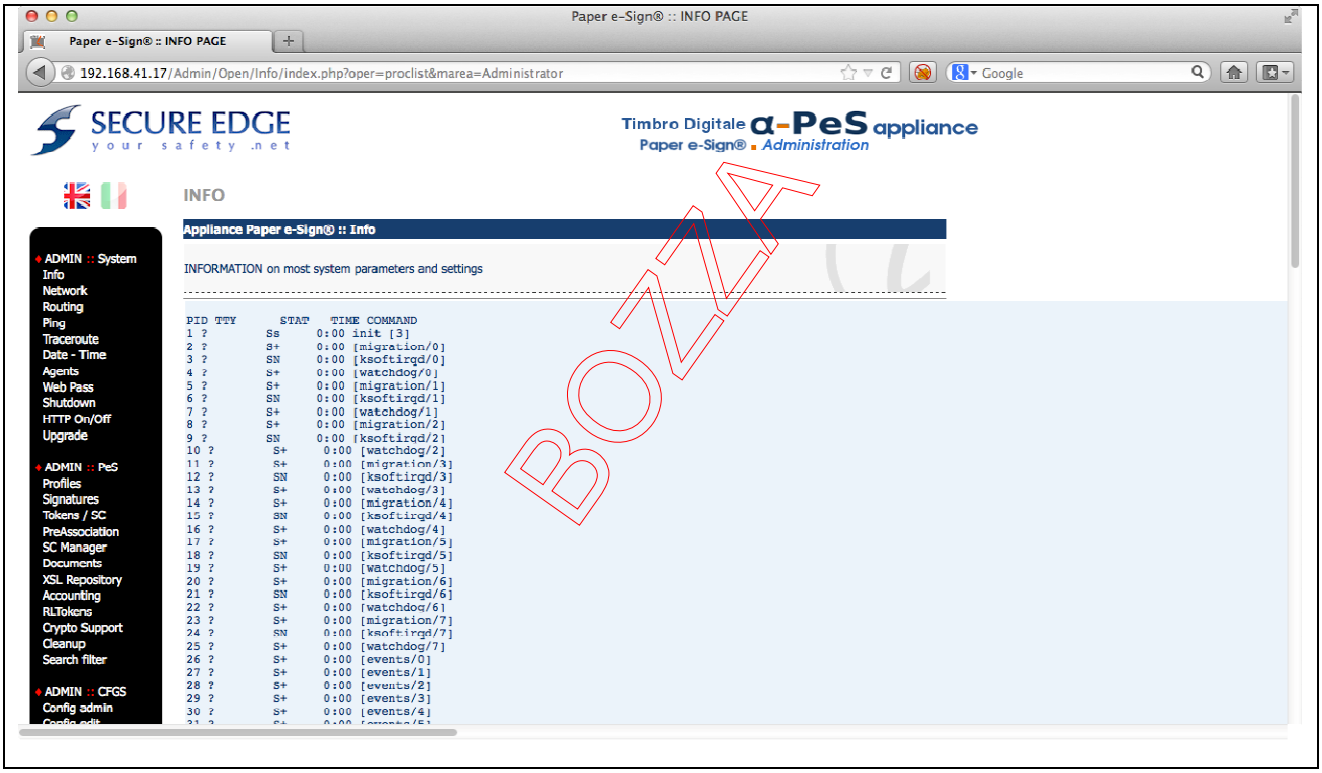
CA Certs:	subject= countryName = IT stateOrProvinceName = Italia localityName = Roma organizationName = Secure Edge s.r.l. organizationalUnitName = Secure Edge Global Root CA commonName = Secure Edge Global Root CA emailAddress = ca@secure-edge.com notAfter=Jan 10 08:57:05 2013 GMT --- subject= organizationName = Secure Edge S.r.l. organizationalUnitName = Security emailAddress = ca@secure-edge.com localityName = Rome stateOrProvinceName = Italy countryName = IT commonName = Secure Edge CA 2012 notAfter=Jan 10 10:23:12 2022 GMT ---
RCE certs	sistema RCSS :: Aug 26 04:14:55 2021 GMT RCE :: Dec 20 09:04:27 2019 GMT
SIGNERS CAs	Secure Edge Global Root CA :: Jan 10 08:57:05 2013 GMT Secure Edge CA 2012 :: Jan 10 10:23:12 2022 GMT



La sezione Machine status permette di vedere lo stato di funzionamento del servizio di HA (High Availability, Alta Affidabilità) in una configurazione in cluster di due appliance, ove previsto.

La sezione SHM permette di vedere le aree di memoria condivisa (shared memory) per ciascuna card di firma attiva sull'appliance.

La sezione Process List permette di richiedere la visualizzazione dei processi attivi sull'appliance:



Network: Configurazione della rete

Questo menù permette di modificare i parametri di rete del sistema.

L'aspetto della pagina è mostrato in figura:

Administrator – NETWORK

- ADMIN :: System
  - Info
  - Network
  - Routing
  - Ping
  - Traceroute
  - Date - Time
  - Agents
  - Web Pass
  - Shutdown
  - HTTP On/Off
  - Upgrade
- ADMIN :: PeS
  - Profiles
  - Signatures
  - Tokens / SC
  - PreAssociation
  - SC Manager
  - Documents
  - XSL Repository
  - Accounting
  - RLTokens
  - Crypto Support
  - Cleanup
  - Search filter
- ADMIN :: CFGS
  - Config admin
  - Config edit
  - XSL for PDF
  - XSL upload
- ADMIN :: Special
  - Authentication
- SIGNER
- OPEN AREA

v. 2013.03.04-14:10
>> ONLINE SUPPORT

Appliance Paper e-Sign® :: network configuration management

This page allows to configure the network parameters of the appliance.

NOTICE FOR APPLIANCES IN HOT-STANDBY MODE
If this is an appliance in hot-standby configuration, the heartbeat facilities will be updated accordingly.
Also, you can use this page to set the peer address and the virtual IP address.
Notice that if you change the address of this appliance or the IP virtual address, **you must update the configuration on the peer**: the heartbeat process on the peer needs to know about any change of this kind.

Network settings (eth0)

IP address	Netmask	Gateway	
192.168.41.17	255.255.255.0	192.168.41.1	Change IP eth0 / Reset

Network settings (eth1)

IP address	Netmask
10.200.200.201	255.255.255.248

Network settings (eth2)

IP address	Netmask	Gateway	
172.20.100.100	255.255.255.0	192.168.41.1	Change IP eth2 / Reset

Network settings (eth3)

IP address	Netmask	Gateway	
not assigned	255.255.255.0	192.168.41.1	Change IP eth3 / Reset

DNS settings

Primary DNS	Secondary DNS		
		Change DNS servers	Reset

Current DNS settings:

```
# Ubi aka Umberto Rustichelli
# set_dns generated file
nameserver 8.8.8.8
nameserver 0.0.0.0
```

Peer settings

Peer IP address (change takes a bit)		
192.168.41.232	Change Peer	Reset

HA service settings

HA service address (change takes a bit)			
192.168.3.131	21	Change HA service IP	Reset

If this Paper e-Sign® appliance is connected to another one, the heartbeat (HA) program takes care of "moving" the "service" IP address from one peer to the other.
If you need to make sure that this appliance DOES NOT OWN the service IP (for instance, because a signature facility is malfunctioning), switch off the HA program and the other peer will take charge of the IP.
If you want to switch off HA indefinetely, for instance for maintainance reasons, you also must turn off the HA Manager because the latter periodically checks for heartbeat: if your machine is in good health, the Manager will re-run the heartbeat (but the service IP will not be taken back, anyway, unless the peer is in bad shape).

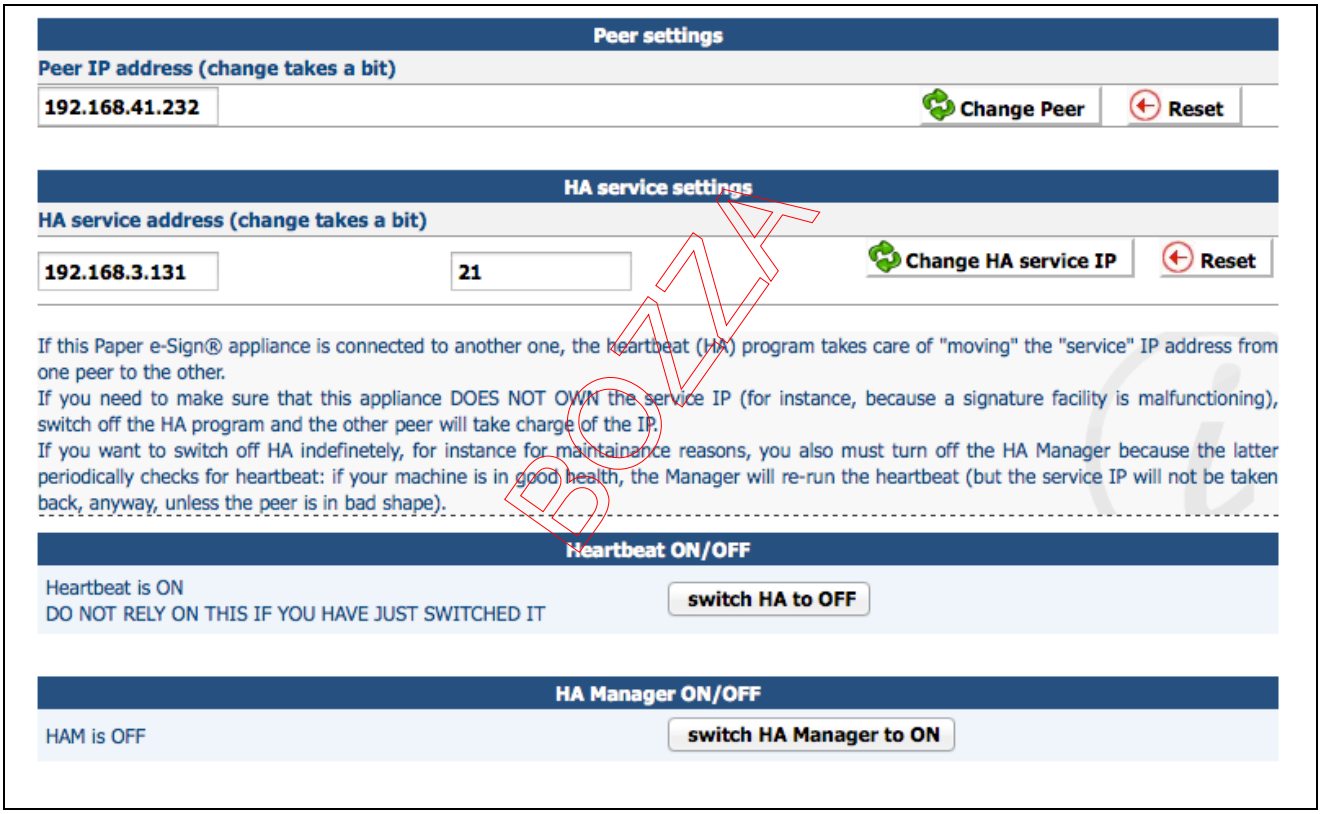
Heartbeat ON/OFF

Heartbeat is ON
DO NOT RELY ON THIS IF YOU HAVE JUST SWITCHED IT — switch HA to OFF

HA Manager ON/OFF

HAM is OFF — switch HA Manager to ON

Tramite le varie righe della tabella è possibile modificare i parametri di rete delle interfacce “eth0”, “eth2” e “eth3”. L’interfaccia “eth1” non è parametrizzabile in quanto è riservata alla sincronizzazione del servizio di Alta Disponibilità, con un valore prefissato (sottorete *10.200.200.200/29*). Si consiglia di utilizzare l’interfaccia “eth0” per le attività legate alla produzione dei timbri (interconnessione con gli applicativi). Le interfacce “eth2” e “eth3” possono essere utilizzate per interconnessione con altre reti, quali management appliance o altri segmenti di produzione. Qualora non sia presente alcun indirizzo sulle interfacce, comparirà il valore “*not assigned*”. La pagina si completa con le informazioni relative ai server DNS (può essere inserito anche un solo valore o non inserirne alcuno), l’indirizzo IP dell’appliance secondario, ovvero “*Peer IP*” di una configurazione in Altà Disponibilità, e la gestione del servizio di Alta Disponibilità, come illustrato nella figura seguente:



In particolare il campo “*HA service address*” è riservato per l’indicazione dell’indirizzo Virtuale (Virtual IP) che verrà condiviso fra le due macchine. La subnet mask, in questo caso, andrà indicata con la notazione CIDR (ad esempio “/24” per 255.255.255.0 “/16” per 255.255.0.0). Per la configurazione del servizio di Alta Disponibilità, si consiglia di utilizzare un indirizzo valido sulla rete associata all’interfaccia “eth0” (sia per il campo “*Peer IP*”, sia per il campo “*HA service address*”). L’indirizzo VIP viene associato, di volta in volta, all’appliance “attivo”, quindi un solo appliance avrà sulla propria configurazione tale indirizzo. In caso di disservizio per guasti o per interventi manuali, è bene ricordate che l’indirizzo VIP impiega circa 1-2 secondi per passare da una appliance all’altra.

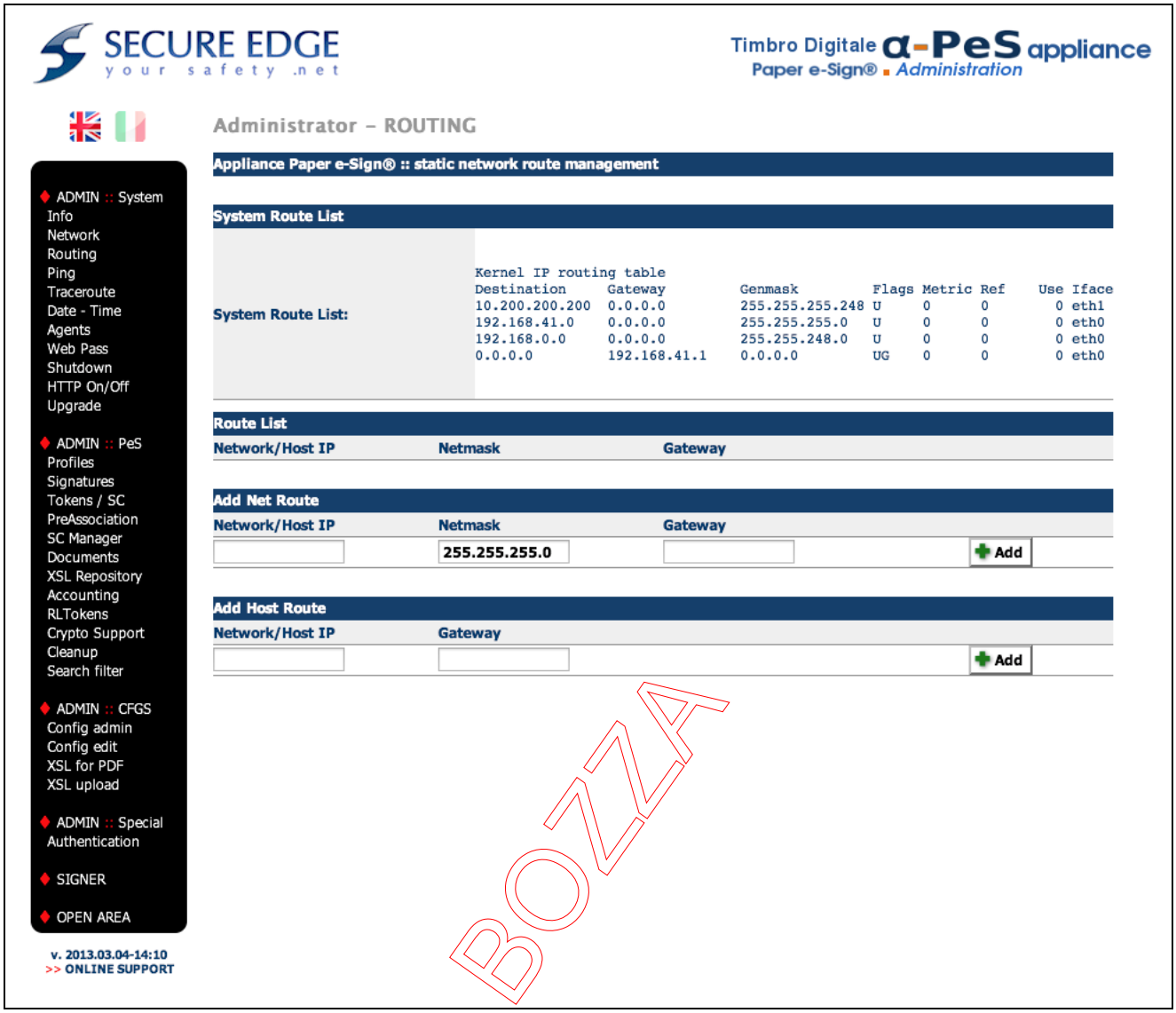
Tramite la pressione del tasto "***switch HA to OFF***" si interrompe momentaneamente il servizio di Alta Disponibilità (*Heartbeat*), forzando, manualmente, il passaggio dell'indirizzo VIP. Questa procedura può essere utile nel caso si siano verificati dei malfunzionamenti sull'appliance e si decida di passare in esercizio l'appliance "secondaria". Il servizio di Alta Disponibilità è configurato per ripartire automaticamente ogni 120 secondi, a meno di eseguire la completa disattivazione del servizio medesimo tramite la pressione del tasto "***switch HA Manager to OFF***" . In questo caso il servizio di Alta Disponibilità verrà mantenuto disattivato sul'appliance per tutto il tempo che l'Amministratore riterrà opportuno (ad esempio per gestire manutenzioni/aggiornamenti a livello software o la modifica ai meccanismi di firma su più Smart Card). Nel caso l'Amministratore decidesse di riattivare il servizio, potrà ripremere il pulsante "***switch HA Manager to ON***". Attenzione: l'aggiornamento della pagina richiede qualche secondo. Lo stato di funzionamento, tanto del servizio di Alta Disponibilità (*Heartbeat*), quanto del Manager dell'Alta Disponibilità (*HA Manager*) compare nella relativa riga all'interno della tabella, come illustrato nella figura precedente.

L'attivazione o lo spegnimento dei servizi di Alta Disponibilità e Manager dell'Alta Disponibilità vengono confermati da una finestra di pop-up.

Nella configurazione dei parametri di rete sull'appliance "secondaria", il valore "Peer IP" si riferisce all'indirizzo IP sulla rete di produzione dei timbri (in genere "eth0") dell'appliance "primaria".

Routing: Configurazione delle rotte

A seconda della tipologia di rete in cui l'appliance viene installato, potrebbe essere necessario configurare delle eventuali "rotte statiche", sia a livello di singolo sistema (host) che di intera sottorete. A tale scopo è possibile utilizzare il menù "*Routing*" dell'area "*System*". In questo modo si indicherà al sistema operativo di utilizzare un differente indirizzo IP per raggiungere una particolare sottorete o un particolare sistema, altrimenti non raggiungibili attraverso il gateway predefinito. Verrà quindi visualizzata la tabella illustrata nella figura seguente:



Qualora non fosse presente alcuna “rotta statica” e alcun default gatway, il campo “Route List” si presenterà vuoto. Il campo “Route List” potrà essere, successivamente, utilizzato anche per la cancellazione delle suddette rotte. Per l’inserimento di una rotta statica a livello di intera sotto-rete, è necessario utilizzare la riga “Add Net Route”, avendo cura di insidiare anche la relativa maschera di sottorete; per l’inserimento di una rotta a livello di singolo sistema, è necessario utilizzare la riga “Add Host Route” (in quest’ultima condizione, la maschera di sottorete sarà automaticamente impostata sul valore di /32 ovvero 255.255.255.255). Qualora la rotta sia stata scritta correttamente apparirà il seguente messaggio: “**Route Added**”. In caso la rotta fosse stata scritta in modo incorretto apparirà il seguente messaggio: “**ERROR: route cannot be added**”

Aggiunte correttamente eventuali rotte statiche, a livello di singolo host o di intera sottorete, le rotte verranno visualizzate nella sezione Route List con la possibilità di eliminare ciascuna rotta.

Nel caso di una rotta per singolo host non viene menzionata, come indicato in precedenza, la maschera di sottorete. Per la cancellazione di una rotta statica, è sufficiente ciccare sul tasto “Del”

Ping

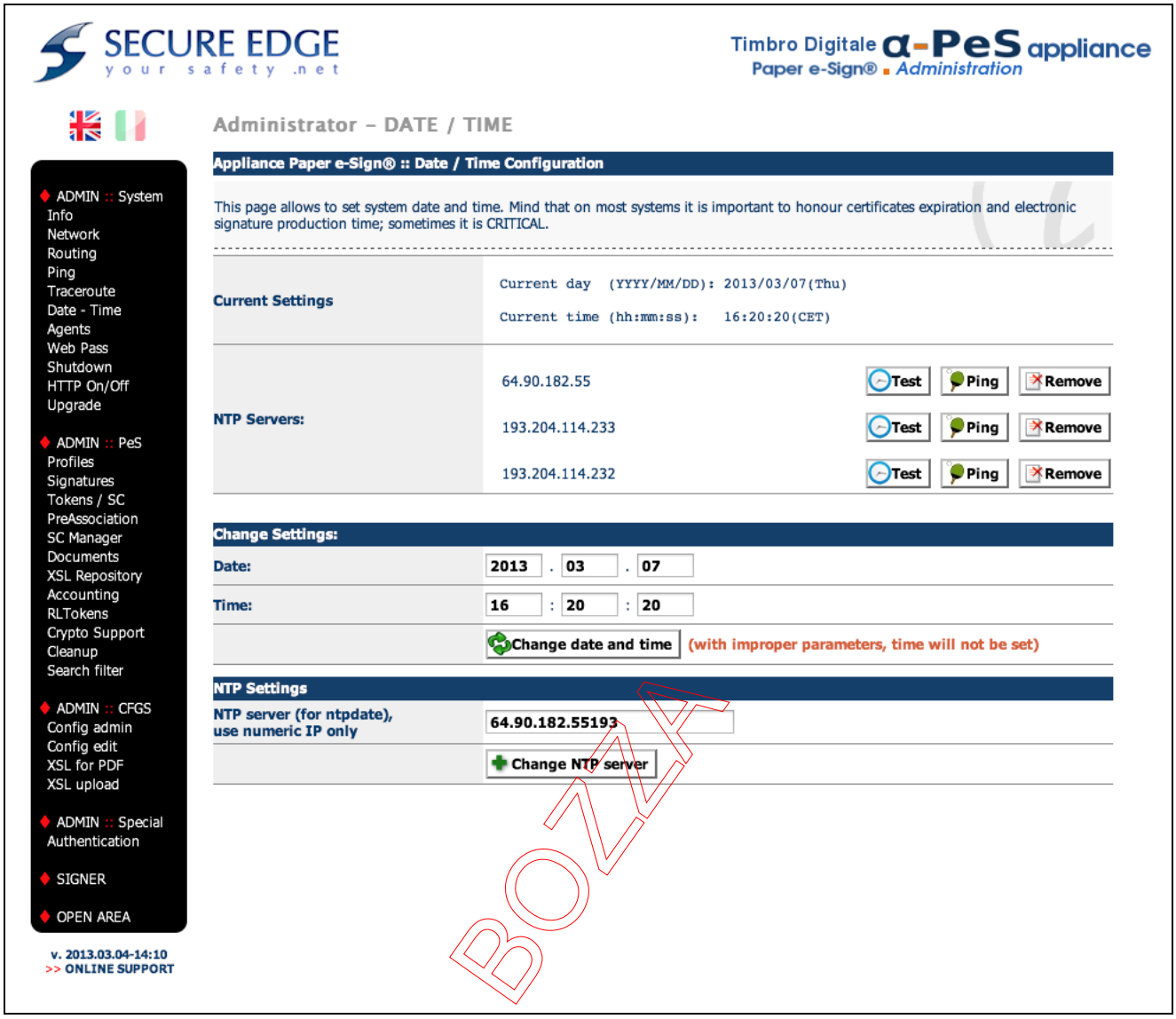
Questa funzione è descritta nel relativo paragrafo nel Open Area. Per la descrizione del comando, si rimanda al paragrafo "*Ping: Operazioni di troubleshooting*" a pagina 92.

Traceroute

Questa funzione è descritta nel relativo paragrafo nel Open Area. Per la descrizione del comando vedere "*Traceroute: Operazioni di troubleshooting*" a pagina 94.

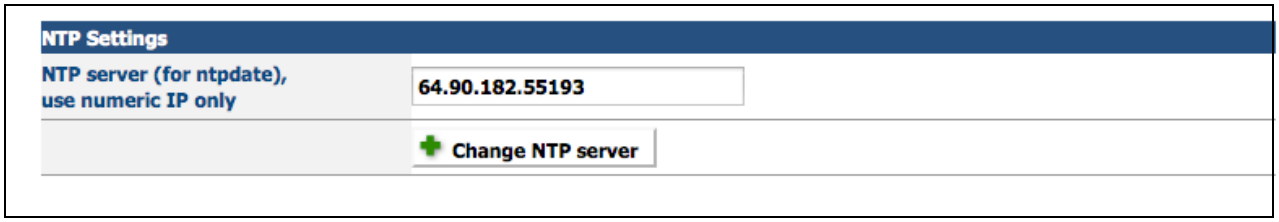
Date – Time: Configurazione della data e dell'ora

E' necessario che l'appliance αPeS possa gestire in modo coerente i certificati e tutti i parametri relativi alle scadenze dei meccanismi di firma. E' quindi è necessario impostare la data e l'orario di sistema, attraverso il menu "***Date / time***". In questo menu, è possibile impostare differenti configurazioni, ovvero scegliere di utilizzare un settaggio orario locale, altrimenti imporre una sincronizzazione da un server NTP esterno (sia su rete locale che pubblico). La figura seguente illustra la pagina di configurazione della data e dell'orario:



Senza alcun server NTP configurato, l'appliance αPeS utilizzerà il proprio orologio di sistema, che può, comunque, essere aggiornato manualmente attraverso la tabella "*Change Settings*" e confermando con il tasto "*Change date and time*". L'impostazione manuale della data e dell'orario viene verificata formalmente in modo da evitare l'inserimento di valori errati. (ad esempio verrà scartato un parametro quale, ad esempio, la data del 30 febbraio come impostazione mensile e giornaliera).

Per impostare un server NTP (di rete locale o pubblico) è sufficiente utilizzare la tabella "NTP Settings" ed inserire il relativo indirizzo, quindi ciccare sul tasto "Change NTP server". L'impostazione del server NTP, qualora effettuata correttamente, comparirà nella sovrastante tabella, come illustrato nella figura seguente:



Con il tasto "*Test*" si eseguirà una verifica di connettività verso l'indirizzo del server NTP associato: verrà eseguito un controllo "icmp echo-request" (ping) per verificare che l'indirizzo sia attivo e raggiungibile. Per cancellare l'indirizzo di un server (eventualemte dimesso o non più raggiungile) è sufficiente ciccare sul tast "*Del*"

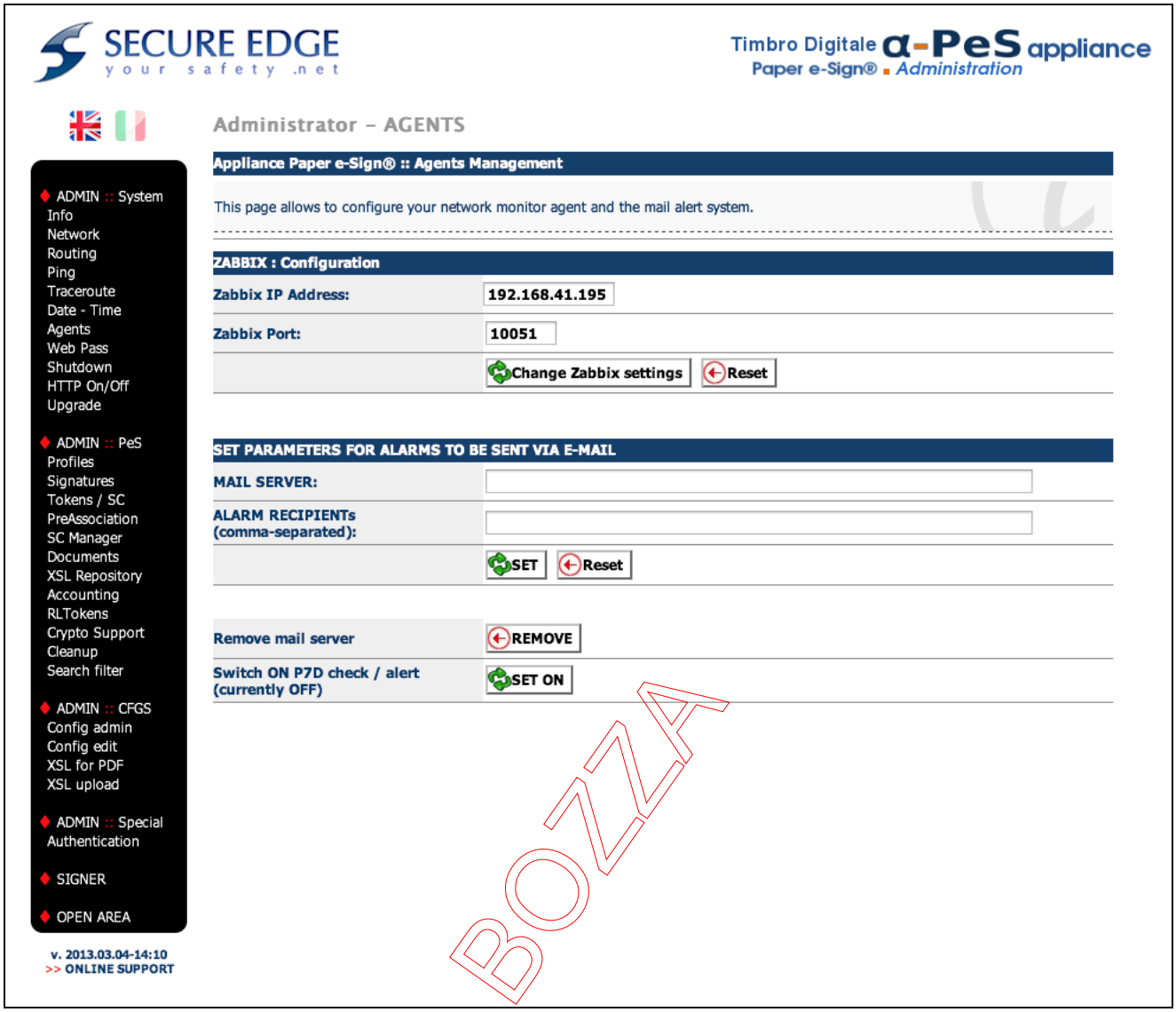
Il server NTP può essere impostato esclusivamente utilizzando il relativo indirizzo IP. Possono essere aggiunti "n" server NTP a piacimento. In caso sia presenti più server, l'aggiornamento dell'orario verrà eseguito con il primo presente in lista; qualora non fosse disponibile (timeout di connessione) si procederà con il successivo.

Agents: Configurazione agent di system monitoring

Se l'infrastruttura dispone di un sistema di "system monitoring", che utilizzi il software Zabbix, è possibile configurare, attraverso il sottomenù ***Agents***, il colloquio con l'appliance αPeS, in modo che possano essere monitorate, in modo centralizzato le principali caratteristiche di sistema. Come illustrato nella seguente figura, andrà impostato l'indirizzo IP del relativo server, nonché la porta di comunicazione (il valore predefinito è 10051). Sempre attraverso la stessa pagina, è possibile configurare un sistema di allarme automatico tramite email che avvisi in caso di demoni di firma non funzionanti o scaduti, indicando l'IP del server SMTP o l'account o gli account di posta elettronica dell'amministratore.

La funzione di allarme via mail è disponibile solo sulle interfacce di amministrazione successive al 4 marzo 2013. Per verificare la data di aggiornamento della propria interfaccia di amministrazione leggere il valore del parametro "*Admin itf version*" presente nel menu Info.

Per attivare la funzione di allarme relativa alla scadenza dei certificati, impostare su "On" il parametro "*Switch ON P7D check / alert*". Il valore predefinito di tale parametro è "Off"



Per facilitare il monitoraggio software, è utile sapere che l'appliance αPeS è fornita di un'unica partizione "root"

La connessione per l'invio di email di allarme avviene sulla porta TCP 25 senza autenticazione.

Crypto Support: Attivazione / Disattivazione del supporto per Smart Card

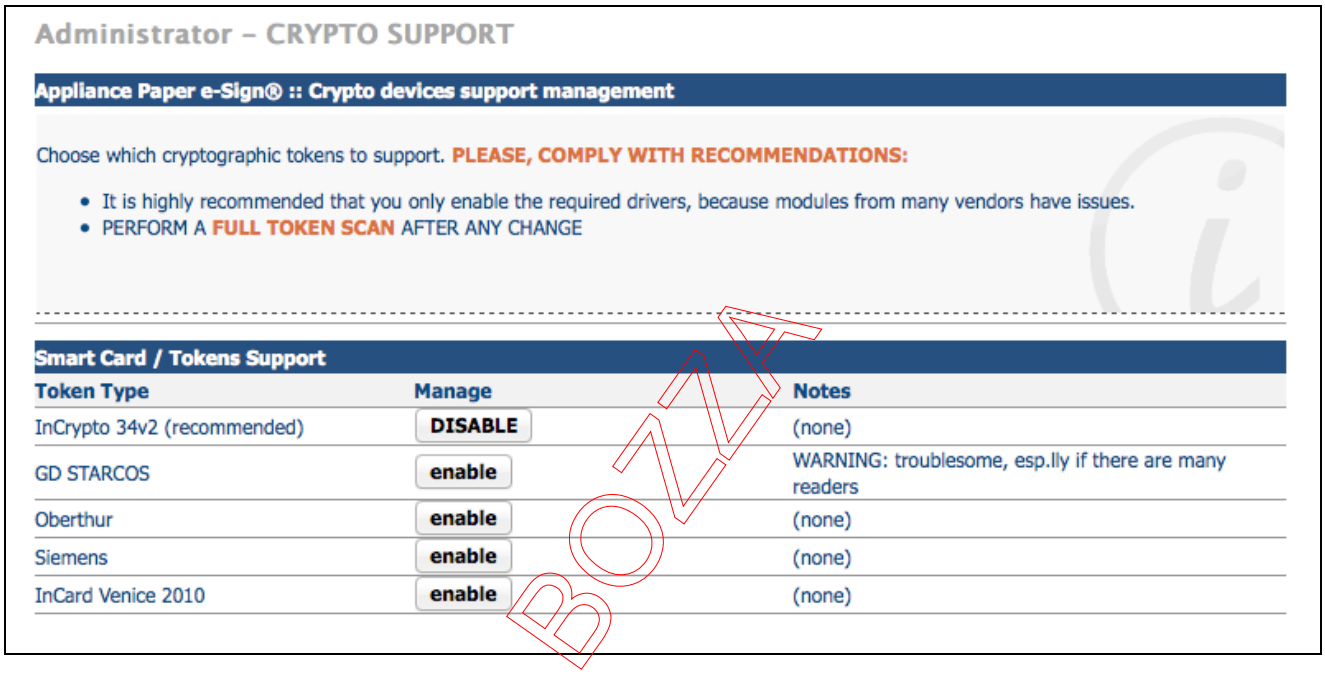
L'appliance αPeS è in grado di comunicare con i seguenti supporti di Smart Card:

- Incrypto 34v2
- Incrypto 2010 Venice
- GD StarCOs

- Oberthur
- Siemens

Si raccomanda di utilizzare esclusivamente smart card di tipo InCard e di attivare esclusivamente tale supporto. E' desiderabile attivare il supporto per le sole Smart Card utilizzate. La presenza di più driver di Card contemporaneamente può, in particolari condizioni, essere causa di malfunzionamenti.

Per abilitare o disabilitare i driver ad uno dei suddetti supporti crittografici, è sufficiente utilizzare il menu "***Crypto Support***" dalla barra laterale sinistra. Verrà visualizzata la pagina illustrata nella figura seguente:



La pagina presenta l'elenco delle Smart Card supportate con a fianco un tasto che riporta la funzione svolta se premuto. Le smart Card per le quali il driver è attivato presentano il tasto con la scritta "*disable*" le altre con la scritta "*enable*".

Per abilitare il supporto ad una smart card, cliccare sul tasto "*enable*" nella riga relativa alla tipologia di supporto crittografico. L'operazione viene confermata dalla comparsa della scritta "**OK, support for class of crypto Tokens added**". Viceversa, per disattivare il supporto il supporto ad una smart card, cliccare sul tasto "*disable*" nella riga relativa alla tipologia di supporto crittografico. L'operazione viene confermata dalla comparsa della scritta "**OK, support for class of crypto Tokens removed**".

L'appliance viene fornito con l'abilitazione unicamente delle smart card di tipo "Incrypto 34v2"

Si sconsiglia di utilizzare, in sede di esercizio, smart card del tipo "GD StarcOs" in quanto il relativo driver non è affidabile. Si sconsiglia inoltre, per la produzione, di utilizzare smart card di tipo "Oberthur" in quanto presentano prestazioni inferiori e

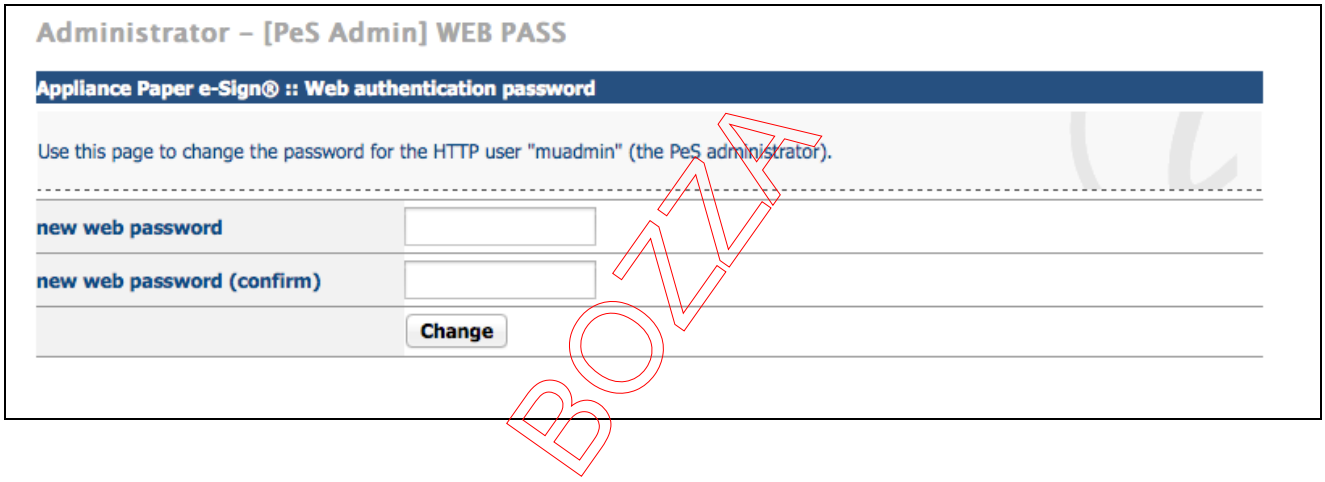
questo provoca un rallentamento nell'emissione di timbri.

Web Pass: Modifica password di accesso.

L'accesso alla console di Amministrazione dell'appliance αPeS, sia da parte dell'Amministratore, sia da parte del Titolare del Certificato, deve sempre avvenire tramite certificati (quindi connessione cifrata, SSL). Tuttavia, in casi del tutto eccezionali, l'amministratore deve utilizzare una coppia (username / password).

E' possibile, ovviamente, modificare a proprio piacimento la password all'utenza di Amministratore (username "*muadmin*").

Questa operazione può essere svolta dall'Amministratore utilizzando il menu "***Web Pass***" dell'area "System" della barra laterale sinistra ed accedendo alla pagina descritta nella figura seguente:



L'amministratore dovrà quindi inserire nei due campi a disposizione (il secondo è il campo di verifica) la nuova password e lasciare il segno di spunta su "*super-administrator*" e cliccare sul tasto "*Change password*". Eseguita l'operazione di aggiornamento correttamente, comparirà il seguente messaggi:

"**Password changed.**"

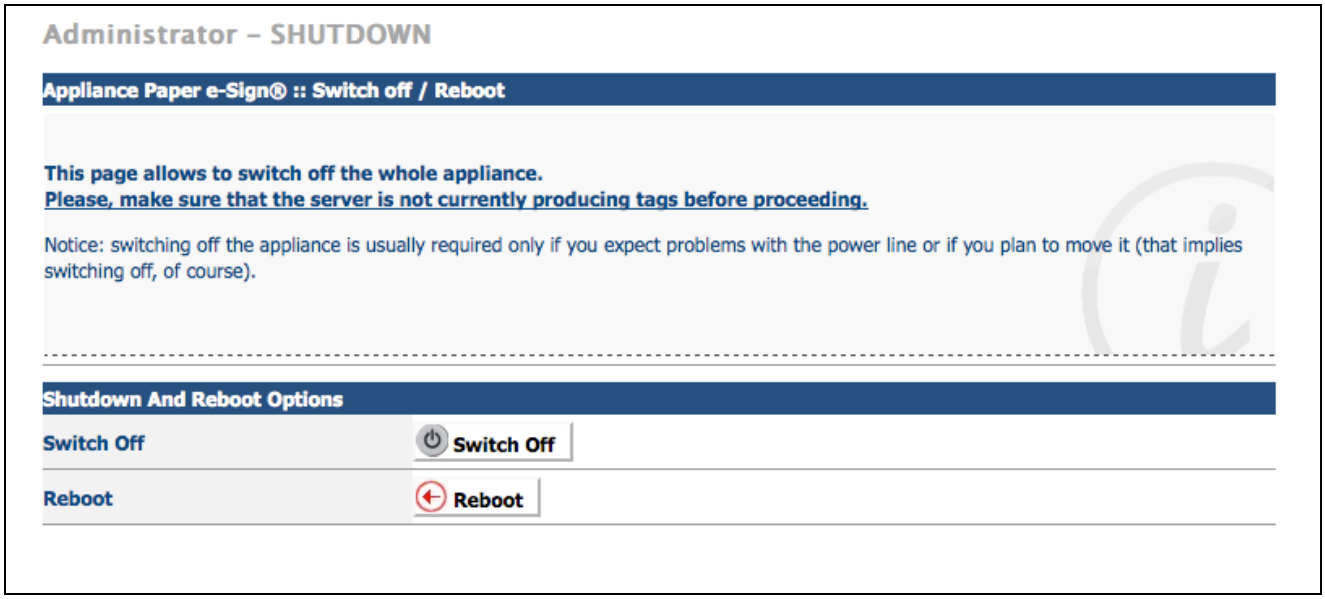
La password predefinita per l'utente di Amministratore in modalità non protetta è le seguente:

username: **muadmin**

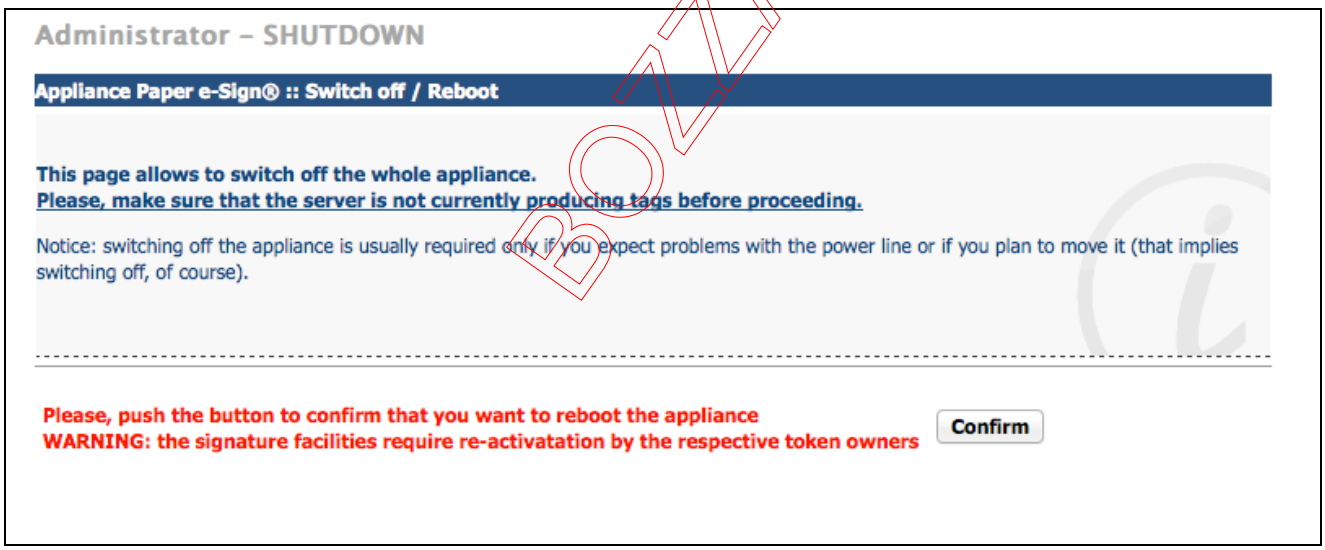
password: **timbrodigitale**

Shutdown: Spegnimento e riavvio del sistema

In caso di necessità, è possibile riavviare o spegnere in modo "controllato" l'appliance, attraverso il menu "***Shutdown***", selezionando gli opportuni comandi, come illustrato in figura:



Prima di procedere al reboot o allo spegnimento dell'appliance αPeS verrà sempre una ulteriore conferma all'Amministratore, come illustrato nella figura seguente:



Lo spegnimento o il reboot del sistema operativo comporta:

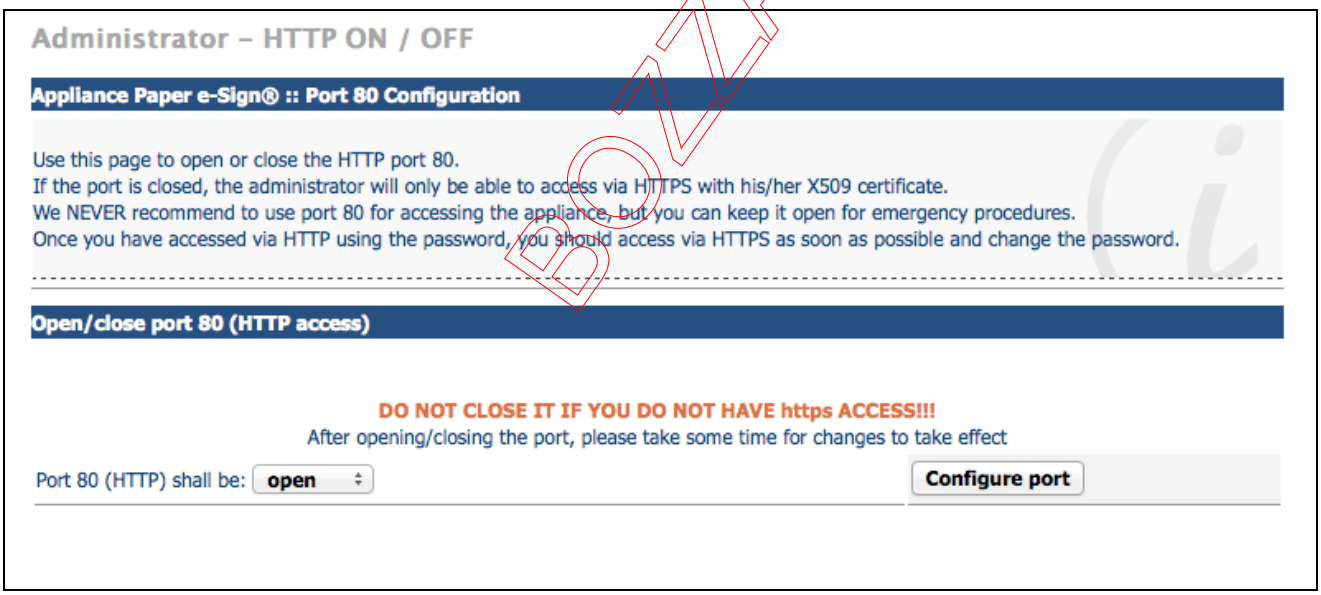
l'arresto del servizio di firma!

Effettuare questa operazione solamente nei casi in cui l'appliance αPeS non stia producendo timbri. Al successivo riavvio sarà comunque necessario ripristinare ciascun servizio di firma inserendo nuovamente PIN e passphrase da parte del titolare.

http On/Off: Disattivazione / attivazione comunicazioni "in chiaro" (http)

Questa funzione è deprecata e presente solo per permettere l'esecuzione di test applicativi prima che il sistema venga messo in esercizio o in caso di troubleshooting.

Le linee guida raccomandate da Secure Edge sull'utilizzo dell'appliance impongono di utilizzare la console di Amministrazione in modalità di mutua autenticazione forte, tramite i relativi certificati. digitali. Tuttavia, in casi eccezionali e del tutto temporanei, è possibile attivare il colloquio http. Per eseguire questa operazione, è disponibile il menu "***HTTP on / off***" dalla barra laterale sinistra. Tramite questo menu si include o si esclude completamente il web server dall'accettare connessioni sulla porta TCP 80. Come illustrato nella seguente figura, è sufficiente selezionare, dal menu a tendina, l'opzione "*closed*" e confermare con il tasto "*configure port*":

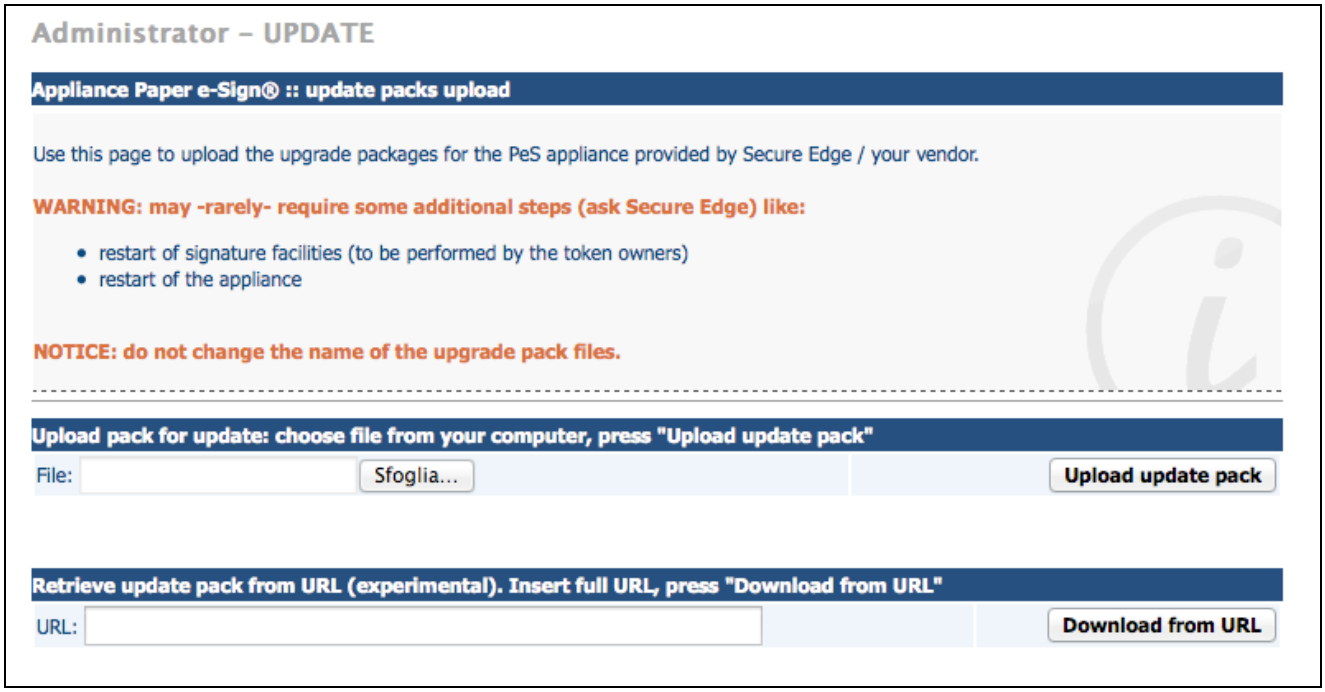


Come chiaramente indicato nella pagina, è necessario attendere circa 2 minuti affinché il sistema completi l'attivazione o lo spegnimento del servizio HTTP.

Update: Installazione pacchetti di aggiornamento

Secure Edge srl rilascia dei pacchetti di aggiornamento del sistema sia per correggere funzionalità sia per aggiungerne di nuove. Per operare l'installazione di questi pacchetti, è necessario utilizzare il meu "Update" dalla barra laterite sinistra.

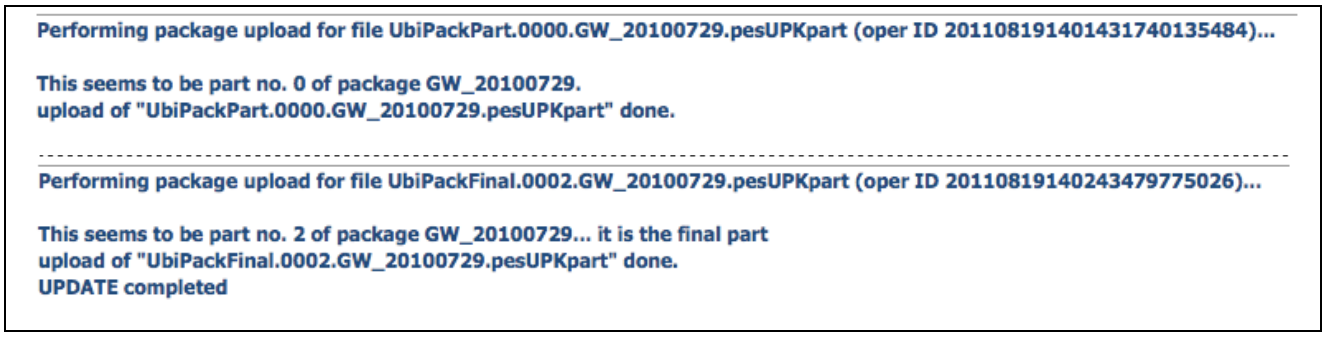
Verrà visualizzata la pagina illustrata come segue:



Sono possibili due modalità di installazione dei pacchetti di aggiornamento:

1. invio dei file dal computer dell'Amministratore
2. download dei file da un web server (su rete locale o pubblica)

Nel caso si scelga di utilizzare l'opzione 1, ovvero l'invio dei pacchetti presenti all'interno di una directory sul computer dell'Amministratore, utilizzare la tabella "*Upload pack for update: choose file from your computer*". E' bene ricordare che al momento è presente una limitazione sulla dimensione massima dei file che possono essere inviati all'appliance attraverso questa modalità ed è pari a **512 kbyte**. Per questa ragione, in caso di aggiornamenti di grandi dimensioni vengono forniti più file separati (con estensione "*.PeSUPKpart*"). Tali file devono essere installati seguendo la sequenza riportata direttamente sul nome stesso del file, a partire da "0000", fino all'ultimo, che riporta la dicitura "Final". Durante l'aggiornamento il nome dell'ultimo file caricato apparirà nella pagina, come illustrato nella figura seguente:



Al termine della procedura di aggiornamento, il nome del pacchetto comparirà anche in basso nella stessa finestra, come illustrato di seguito:

Read report for update UPK.GW_20100729

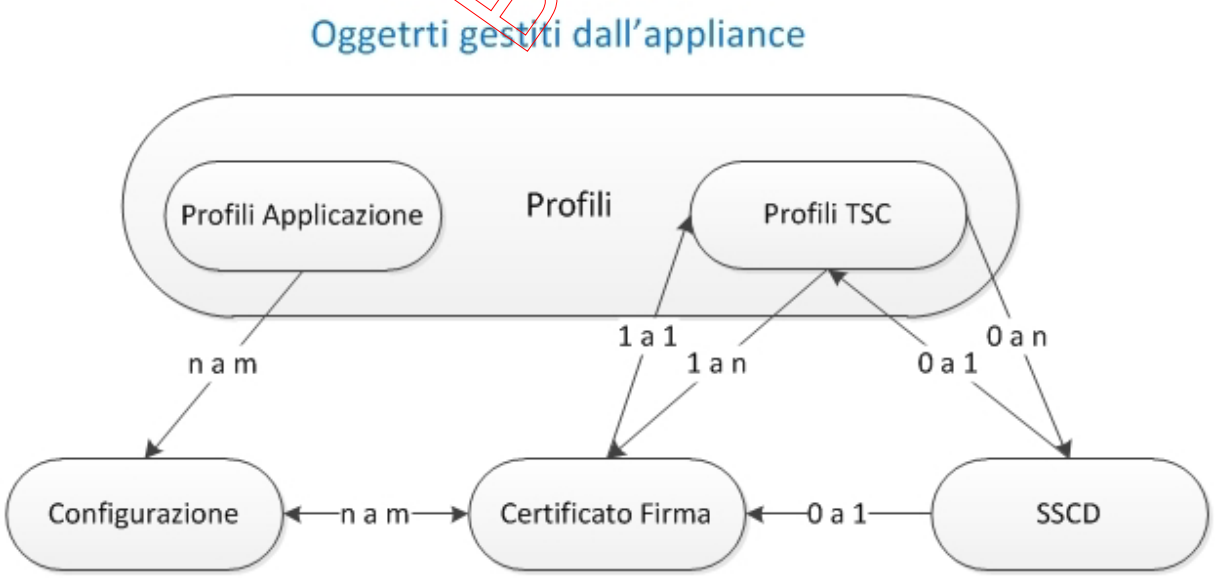
Cliccando sull'aggiornamento, è possibile leggere, all'interno di una nuova pagina, il report dell'attività, utile soprattutto in caso di troubleshooting.

Qualora l'Amministratore scelga di utilizzare il metodo nr.2 ovvero il download del pacchetto di aggiornamento da un webserver, dovrà esclusivamente prestare attenzione a digitare correttamente l'indirizzo URL assoluto, utilizzando la tabella "*Retrieve update pack from URL*". In questa modalità non esistono limiti di dimesione del file, quindi può essere utile utilizzare questa metodologia in caso di aggiornamenti particolarmente voluminosi, che altrimenti richiederebbero molteplici file separati. Sulla pagina apparirà la medesima scritta informativa relativa all'esecuzione dell'aggiornamento, come illustrato in precedenza e, quindi la conferma delle operazioni svolte.

Per particolari aggiornamenti potrebbe essere necessario riavviare il meccanismo di firma o l'intera appliance αPeS (reboot). In tal caso fare riferimento alle istruzioni che verranno allegate con l'aggiornamento da parte di Secure Edge srl.

PeS Area

Questa sezione dell'interfaccia di amministrazione opera sugli oggetti che permettono di generare i Timbri Digitali. Lo schema seguente illustra gli oggetti utilizzati dall'appliance nella produzione di Timbri Digitali.



- I profili rappresentano le entità autorizzate a colloquiare con l'appliance, utilizzando ciascuna il proprio certificato di autenticazione. I profili si riferiscono a TSC oppure ad applicazioni che richiedono i Timbri Digitali.
- I certificati di firma sono i certificati contenuti su Smart Card o HSM che firmano i documenti. Un TSC può essere titolare di più certificati di firma (relazione 1 a n).
- Le configurazioni sono la descrizione delle funzioni richieste all'appliance, tipicamente la produzione di un Timbro Digitale. Le configurazioni sono in relazione con i certificati di firma. Una configurazione può utilizzare uno o più certificati di firma e un certificato di firma può essere associato a più configurazioni (relazione n a m). Le configurazioni sono anche in relazione con i profili di applicazione per cui una configurazione è in relazione con uno o più profili di applicazione che a loro volta possono essere in relazione con uno o più configurazioni (relazione n a m).
- Gli SSCD sono gli apparati per effettuare firme digitali conforme alla direttiva Europea sulla firma elettronica 1999/93/UE utilizzati con l'MSBox. Nello schema precedente rappresentano le Smart Card prive di certificato perché, nello schema precedente, quando viene caricato il certificato trattiamo la Smart Card + certificato come un elemento unico denominato certificato di firma

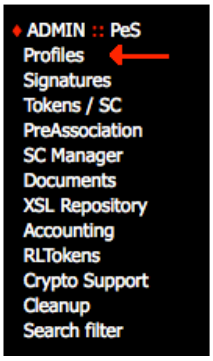
Esistono fasi intermedie durante la predisposizione dell'appliance in cui possono esistere Profili, Certificati di firma e Configurazioni non relazione tra loro. Tuttavia questa situazione rappresenta solo uno stadio intermedio della predisposizione dell'appliance. In tale situazione gli oggetti in questione non sono operativi.

Per tutto quello che riguarda le attività di amministrazione, ovvero la creazione di Profili (sia dei Titolari dei Certificato che delle Applicazioni), la gestione dei documenti ecc, si può fare riferimento alla sezione "***Pes Area***" . Questa sezione consente di accedere alla gestione delle seguenti funzioni (descritte nei paragrafi seguenti):

- *Profiles*: consente di gestire (creare/rimuovere) i Profili legati sia ai Titolari dei Certificato, sia alle Applicazioni e di visualizzare i Certificato associati a tali Profili, evidenziandone il loro stato.
- *Signatures*: consente di visualizzare i servizi di firma configurati e di cancellarli in caso siano scaduti, oppure sia necessario revocarli sia necessario ripetere la procedura di inizializzazione (Cerimonia)
- *Tokens*: consente di effettuare la scansione degli apparati di firma (smart card, HSM...) collegati all'appliance PeS e di effettuare l'assegnazione dei Certificati di firma trovati ai Profili dei rispettivi Titolari, nonché la pre-associazione alle Configurazioni
- *PreAssociation*: consente di impostare e di rimuovere le pre-associazioni esistenti fra Certificato di firma e Configurazioni
- *SCManager*: consente di inizializzare un SSCD "vuoto", inserendo al suo interno il certificato di firma ed eseguendo, successivamente, l'aggiornamento del PIN di protezione del Certificato medesimo

- *Documents*: elenca le configurazioni presenti e le firme ad esse associate
- *XSL Repository*: consente di visualizzare i template XLS/XML presenti nell'appliance ed eventualmente associati a delle Configurazioni, di cancellare quelli inutilizzati e di eseguirne il download
- *Accounting*: consente di visualizzare il numero complessivo di timbri a disposizione e di assegnare alle Configurazioni la licenza (denominata anche "facility") opportuna
- *RLTokens*: consente di stabilire un collegamento fra l'appliance αPeS e un apposito dispositivo di crittografia HSM all'interno del quale sono contenuti i Certificato di firma.

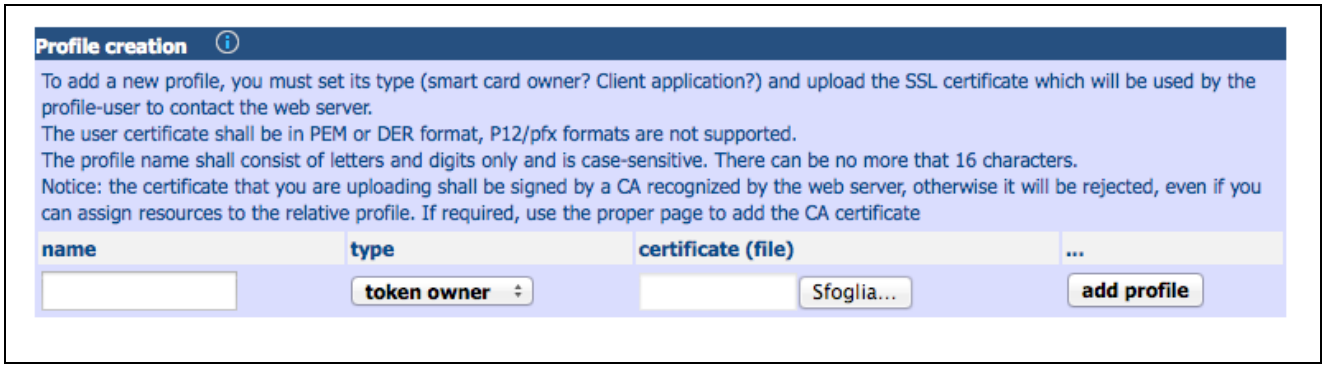
Profiles: aggiunta/rimozione di un Profilo Titolare o di Applicazione



Questa funzione permette di creare o rimuovere un profilo per un TSC o una applicazione, è possibile selezionare l'opzione "***Profiles***" dall'area "***PeS***" utilizzando il menu sulla sinistra.

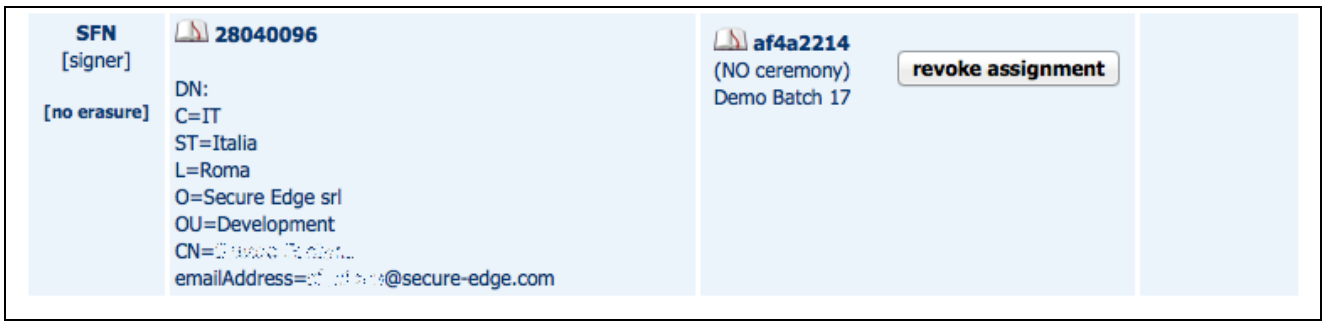
Utilizzando il riquadro "*Profile Creation*" è possibile inserire un "nome breve" (massimo 16 caratteri) per identificare il profilo e quindi indicare il certificato di autenticazione da associare al profilo (file .crt).

Dal menu a tendina selezionare "Token Owner", nel caso si tratti di un Profilo per un TSC, oppure "Application", nel caso si tratti di un Profilo per una applicazione di firma, quindi confermare con "*Add profile*", come illustrato nella seguente figura:



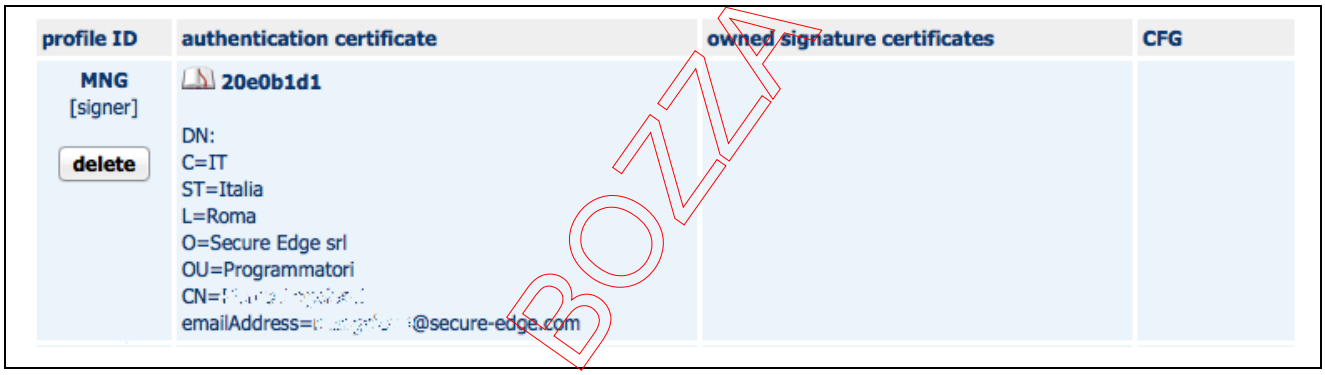
Per questa operazione è possibile utilizzare uno dei certificati presenti nel CD-Rom allegato. In alternativa è possibile utilizzare un qualunque certificato "crt"generato da un'altra Certification Authority. Il caricamento del certificato è sempre una operazione contestuale alla creazione del Profilo.

Quando il Profilo (sia per il Titolare del Certificato, sia per l'Applicazione) risulta correttamente caricato, questo compare nella successiva tabella denominata "*Manage existing certificates assignments*", come illustrato nella successiva figura:



Come si può notare, qualora il Profilo sia assegnato ad un Certificato di firma (presente all'interno di una Smart Card) o ad una Configurazione, non è possibile la cancellazione. In caso contrario, è presente il tasto "*Delete profile*".

Nell'immagine seguente si riporta un Profilo non associato ad alcun certificato di firma o Configurazione, per cui è possibile la cancellazione:



Per revocare l'assegnazione fra Profilo di un TSC e un Certificato di firma, l'Amministratore può cliccare sul tasto "*Revoke Assignment*" che compare sotto ciascun certificato.

Qualora un Certificato, assegnato ad un Profilo di TSC, sia stato correttamente inizializzato, è presente l'indicazione "*ceremony done*"; in caso contrario sarà presente l'indicazione "*NO ceremony*".

L'associazione fra Titolare del Certificato e Certificato di firma viene descritta nel dettaglio nel capitolo "*Procedure Operative: Quick Start*" al **Passo 6**, mentre l'inizializzazione del Certificato (operazione a cura del Titolare e non dell'Amministratore) viene descritta nel capitolo "*Procedure Operative: Quick Start*" al successivo **Passo 7**.

Ricordiamo che la creazione del Profilo per l'Applicazione è necessaria in un quanto le applicazioni si devono autenticare con il certificato del Profilo per poter comunicare con il gateway di firma dell'appliance, attraverso il consueto canale cifrato (SSL).

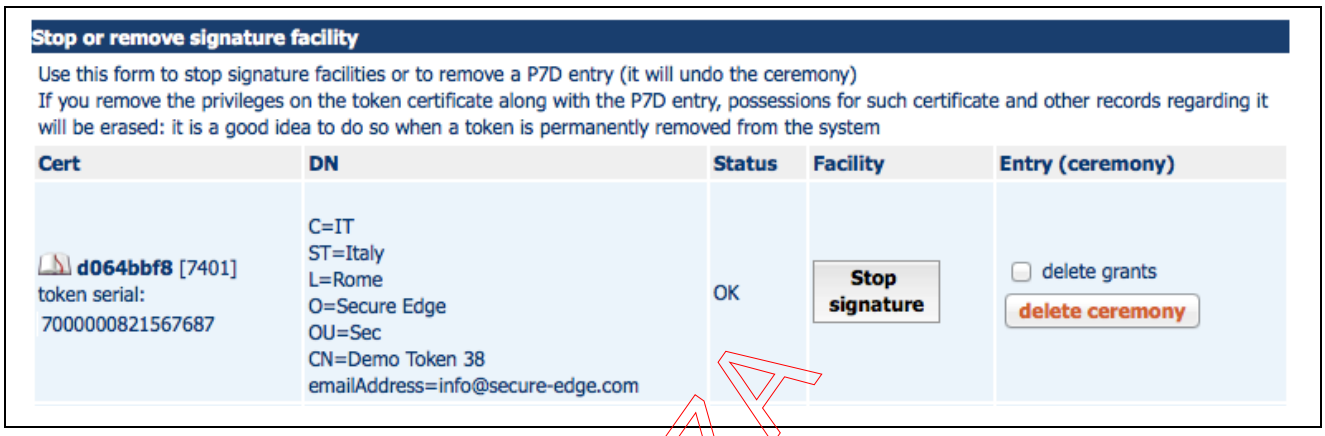
Signature: interruzione della firma / funzioni accessorie sul certificato di firma

Questo menu permette di:

- interrompere un servizio di firma

- cancellare la cerimonia (cioè la configurazione del servizio di firma) cancellando eventualmente anche l'assegnazione al TSC

Viene presentata la maschera seguente nella quale sono visualizzati tutti i certificati di firma presenti sull'appliance per i quali è stata fatta la cerimonia.



INTERRUZIONE FIRMA

Qualora sia necessario interrompere il meccanismo di firma e non sia presente il Titolare del certificato di firma, l'Amministratore può provvedere a questa operazione in totale autonomia. Per effettuare questa operazione, l'Amministratore deve identificare il certificato per cui deve interrompere il meccanismo di firma che avrà lo "*Status*" su "*OK*" che indica che il Certificato è stato correttamente inizializzato dal Titolare attraverso la relativa "Cerimonia" (come descritto nel capitolo "Procedure Operative: Quick Start" al Passo 7). L'amministratore deve quindi selezionare il tasto "*Stop Signature*" per interrompere il meccanismo di firma: dopo alcuni secondi l'indicazione "*Status*" risulterà "*Off*". In questa condizione, il Certificato potrà essere riattivato esclusivamente dal titolare.

CANCELLAZIONE CERIMONIA

Qualora il Titolare non sia più in possesso di una sua Pass-phrase oppure si modificare il PIN della smart card sia, è necessario eseguire nuovamente l'inizializzazione del relativo servizio di firma. L'amministratore può quindi provvedere ad eseguire la cancellazione della relativa "Cerimonia". Per eseguire questa operazione, è sufficiente cliccare sul tasto "Delete ceremony" presente sulla riga relativa al Certificato di firma su cui si intende operazione. Questa operazione mantiene inalterate le assegnazioni fra il Certificato di firma e il TSC e fra il Certificato di firma e la/le Configurazione/i.

Attenzione: questa operazione comporta l'interruzione delle operazioni di firma, poiché sarà necessario interrompere, temporaneamente, il funzionamento della smart card (o del dispositivo crittografico). L'operazione di cancellazione della cermonia è irreversibile! Prima di procedere controllare tutti i parametri relativi al Certificato che si intende resettare (in particolare l'ID del certificato)

CANCELLAZIONE ASSOCIAZIONE TSC CERTIFICATO

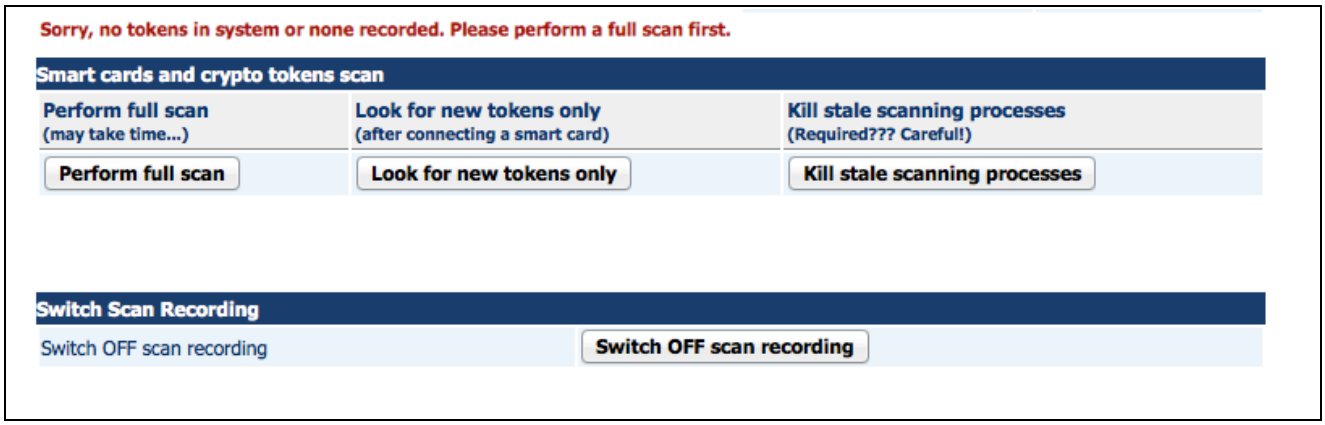
Per eseguire l'operazione di "cancellazione" del Certificato, l'Amministratore deve inserire il segno di spunta su "*delete grants*" e cliccare sul tasto "*Delete Ceremony*". L'operazione sarà confermata definitivamente dalla comparsa del seguente messaggio: "**Entry [*Certificate_ID*] successfully removed**"

L'Amministratore potrà nuovamente associare il Certificato al Profilo del Titolare.

Tokens: scansione dei Certificato di firma e associazione ai Profili e alle Configurazioni

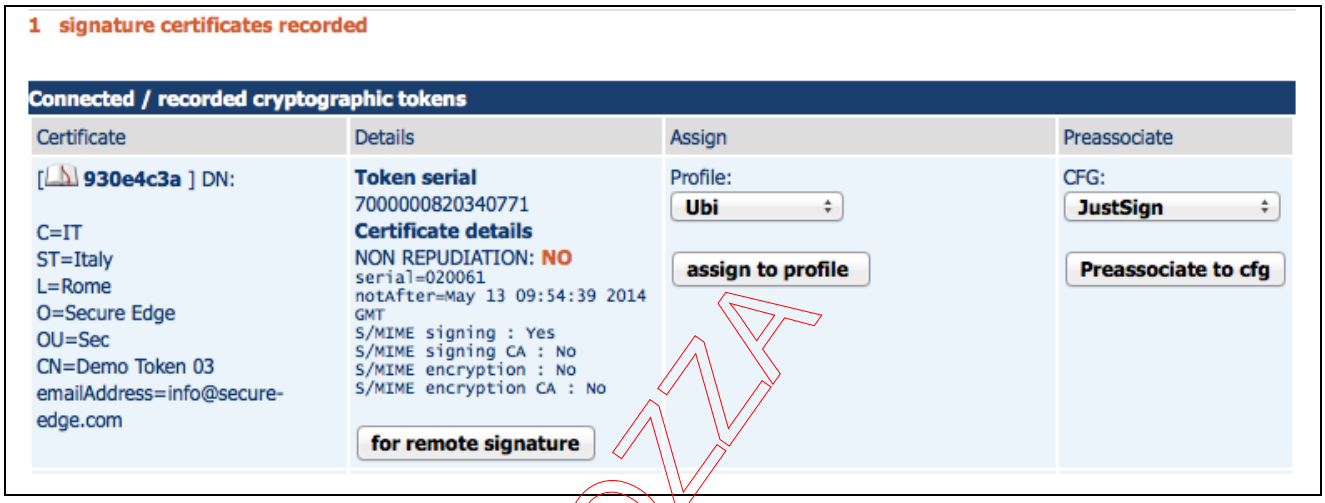
Prima di procedere a questa operazione assicurarsi di aver correttamente inserito le smart card all'interno dei relativi lettori nel dispositivo SCBox. Generalmente il corretto inserimento provoca un breve lampeggio del lettore, nel momento in cui la smart card viene inserita. Si ricorda che, in una configurazione in High Availability (Alta Affidabilità) solo una fila di lettori viene collegata all'appliance αPeS, tramite il relativo cavo USB, fornito in dotazione. L'altra fila di lettori andrà collegata all'appliance αPeS secondaria. In questa configurazione, il TSC dovrà disporre di una coppia di smart card con il medesimo scopo di firma.

Affinché i certificati (smart card) per la firma possano essere utilizzati, l'Amministratore deve operare la loro scansione. Questa operazione va ripetuta ogni volta che un nuovo certificato/Smart Card viene aggiunto all'interno dei lettori nel dispositivo SCBox. Per operare questa scansione, l'Amministratore deve utilizzare il menu "***Tokens***" nell'area "***PeS***". Qualora si tratti della prima scansione assoluta, la finestra non mostrerà ancora alcun Certificato in lista, come illustrato nella figura seguente:



L'Amministratore deve quindi premere il tasto "*Perform full scan*" per procedere alla prima scansione dei lettori collegati all'appliance αPeS. Per abbreviare i tempi di attesa, durante le scansioni successive, l'Amministratore potrà utilizzare il tasto "*Look for new Tokens only*" in modo da effettuare una scansione mirata a cercare variazioni rispetto al numero di smart card presenti (aggiunta o rimozione).

Durante la scansione compare il seguente messaggio: "**Scan in progress, may take time... please wait 2 minutes then go on with administration**". Attendere quindi 2 minuti. Se le smart card sono state inserite e correttamente rilevate appariranno nella tabella "*Connected / recorded cryptographic Tokens*", sopra la quale è anche presente un'indicazione numerica sul numero complessivo di certificati di firma rilevati (utile in presenza di molti tokens), come illustrato di seguito:



E' anche possibile configurare un token di firma per eseguire una "firma remota". Per utilizzare la firma remota, il titolare carica personalmente il file che intende firmare attraverso un form dedicato e inserisce PIN e passphrase. In sostanza, si tratta di una firma di tipo classico con l'unica differenza che il titolare, invece di avere la smart card con sé, la tiene collegata all'appliance. Per accedere a questa funzione, è sufficiente cliccare sul tasto "*for remote signature*". In caso non vi siano errori comparirà il messaggio "***OK, certificate [Certificate_ID] now reserved for remote signature***" e la tabella si presenterà come illustrato di seguito:

Per ritornare ad una situazione precedente, ovvero di "firma automatica", è sufficiente cliccare sul tasto "*no remote signature*". Comparirà il messaggio ***"OK, certificate [Certificate_ID] NO MORE for remote signature"***.

La firma remota non deve essere impostata per i certificati di firma automatica (che sono invece a disposizione delle applicazioni) in quanto non prevede l'attivazione di un demone di firma.

Nel caso in cui si desideri effettuare una scansione per rilevare esclusivamente i tokens inseriti successivamente, dopo aver cliccato il tasto "*Look for new Tokens*", apparirà la schermata come illustrato nella seguente immagine:

Records updated, found 1 new certificates

slot	ID	subject
01	b7d3ff9b	/C=IT/ST=Italy/L=Rome/O=Secure Edge/OU=Sec/CN=Demo Batch 02/emailAddress=info@secure-edge.com

(nel caso di specie è stato rilevato unicamente un nuovo Certificato)

Per consentire ad un Titolare di poter gestire direttamente il proprio Certificato di firma, l'Amministratore dell'appliance deve eseguire l'associazione fra il Profilo del Titolare (indicato nella colonna "*Assign*" – "*Profile*") all'interno della finestra a tendina ed il relativo Certificato. Dopo aver rilevato il Profilo opportuno, è necessario confermare questa operazione, cliccando sul tasto "*Assign crt to Profile*".

Per consentire al gateway di apporre la firma al documento, è necessario eseguire la sua "preassociazione" con la configurazione relativa al documento. Questa "preassociazione" dovrà poi essere confermata, successivamente, dal TSC con la Cerimoia; una volta eseguita la Cerimonia è possibile attivare la firma.

L'operazione di preassociazione può essere svolta:

1. immediatamente al termine della scansione (qualora la Configurazione sia già presente)
2. successivamente (qualora la Configurazione non sia ancora presente o dovesse essere modificata, in tal caso vedere il successivo paragrafo "PreAssociate")

Nel caso la Configurazione sia già presente e pronta ad essere utilizzata, è possibile utilizzare la colonna "Preassociate" "CGF" della tabella menzionata nell'immagine precedente e scegliere l'opportuna Configurazione dal menu a tendina; quindi confermare cliccando sul tasto "Preassociate to cfg" .

Prestare sempre attenzione al valore di identificazione (ID) del certificato di firma, prima di procedere con questa operazione. Il valore di identificazione è presente nella prima prima riga di dettaglio delle informazioni relative al certificato stesso.

Qualora si cerchi di preassociare lo stesso Certificato alla medesima Configurazione per più di una volta, comparirà il seguente messaggio di avviso; "**WARNING: pre-association already exists, skipping...**"

Una stessa Configurazione può avere associati più certificati di firma. Questa opzione è consentita per ottenere i seguenti vantaggi:

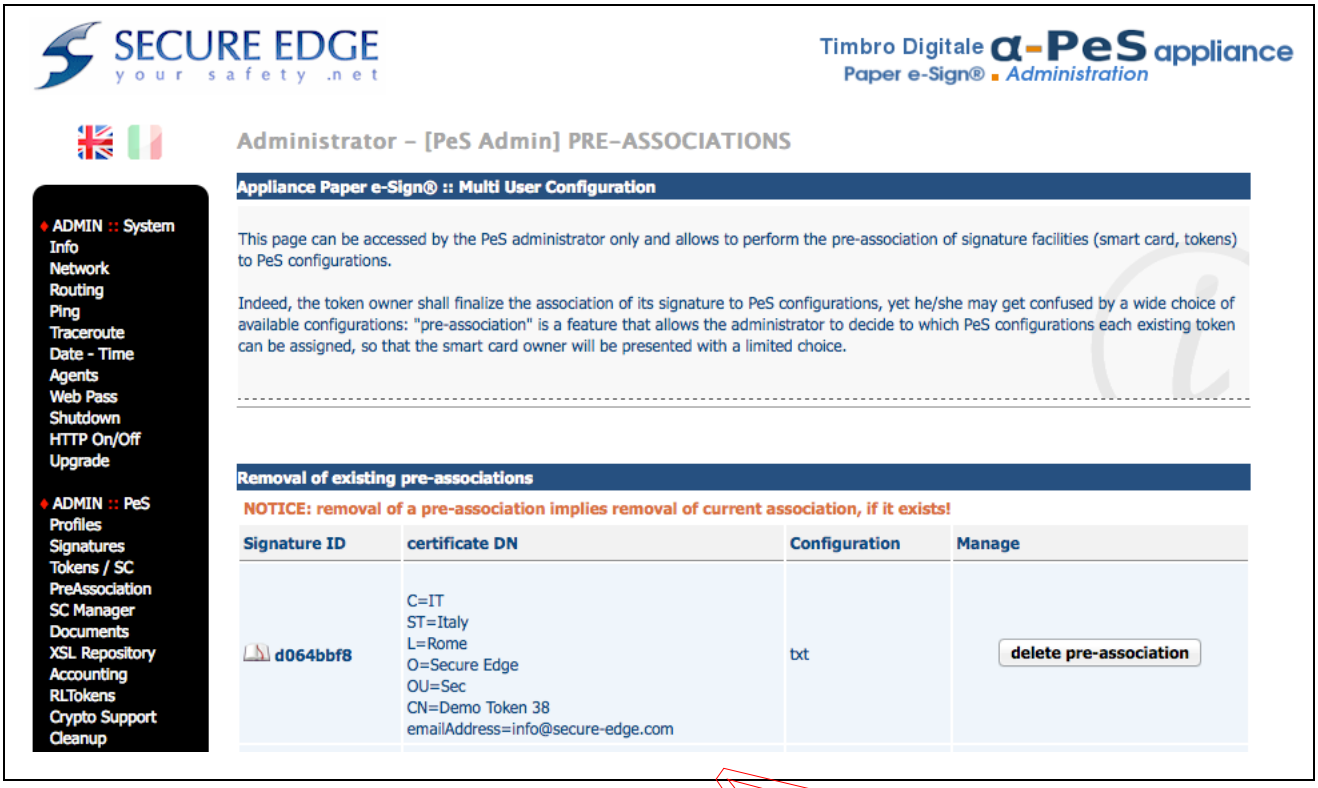
1. aumentare le prestazioni in quanto due certificati firmano il doppio dei documenti a parità di tempo.
2. Sopperire alla indisponibilità di un titolare in caso di riavvio del sistema e necessità di autorizzare la firma.

Nel primo caso, più certificati sono assegnati allo stesso TSC. Nel secondo più caso più TSC sono assegnati allo stesso certificato (si tratta di una condizione particolare).

In mancanza di una pre-associazione fra Certificato e Configurazione, il Titolare del Certificato non potrà procedere alla definiva assegnazione per proprio certificato di firma alla Configurazione. E' quindi assolutamente necessario che l'Amministratore ottemperi questa operazione prima che il Certificato venga inizializzato (Cerimonia) dal Titolare.

PreAssociation: impostazione / rimozione di una preassociazione tra un Certificato di firma ad una Configurazione

Come indicato nel precedente paragrafo "Tokens", per consentire al TSC di associare il certificato di firma ad una configurazione, è necessario che l'Amministratore abbia eseguito la preassociazione. Nel caso la configurazione non sia ancora disponibile al momento della scansione dei Certificato (o comunque si intenda posticipare questa operazione) è possibile utilizzare anche l'apposito menu "***PreAssociation***" dell'are "***PeS***". In tal modo si giunge alla pagina illustrata nella figura seguente:

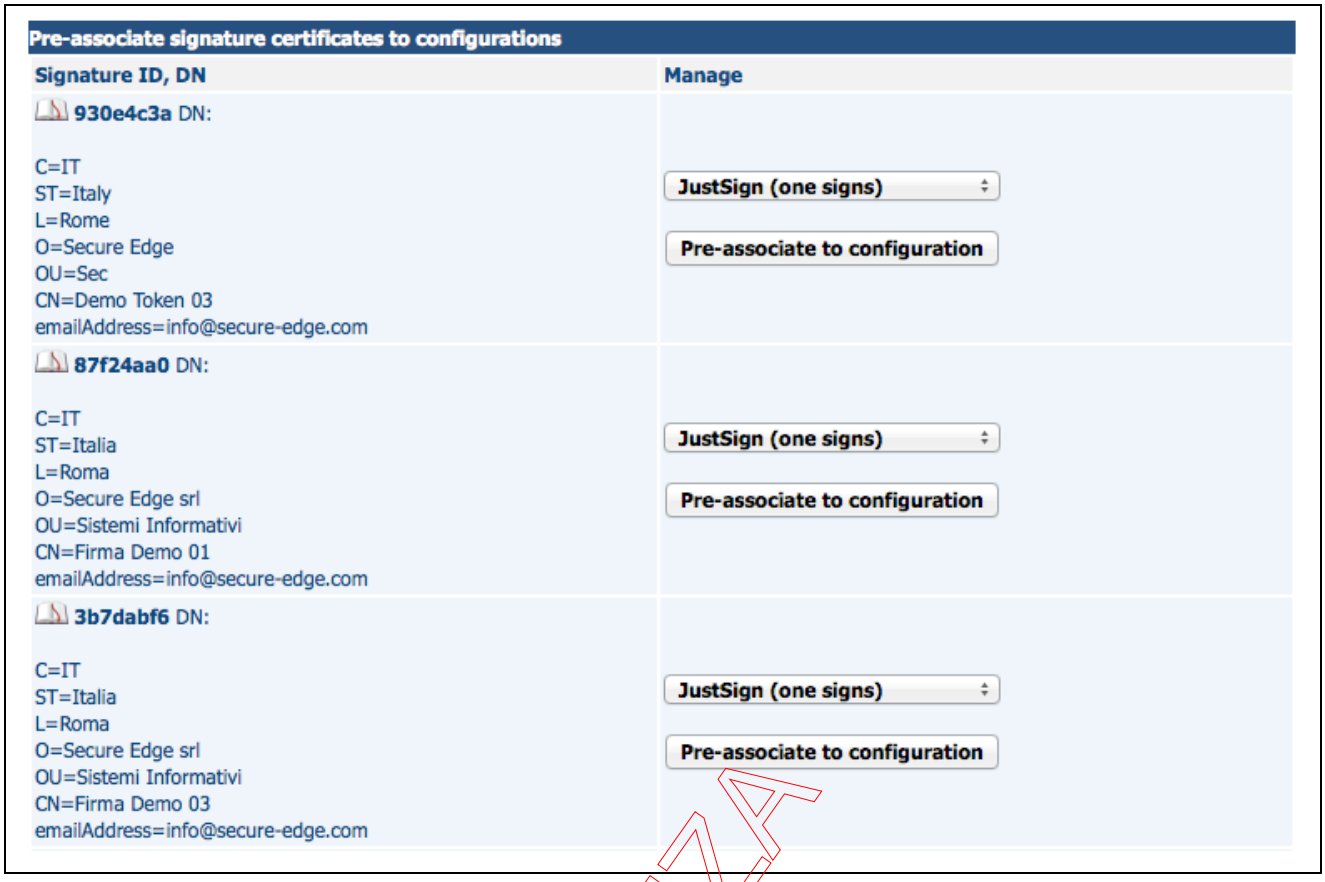


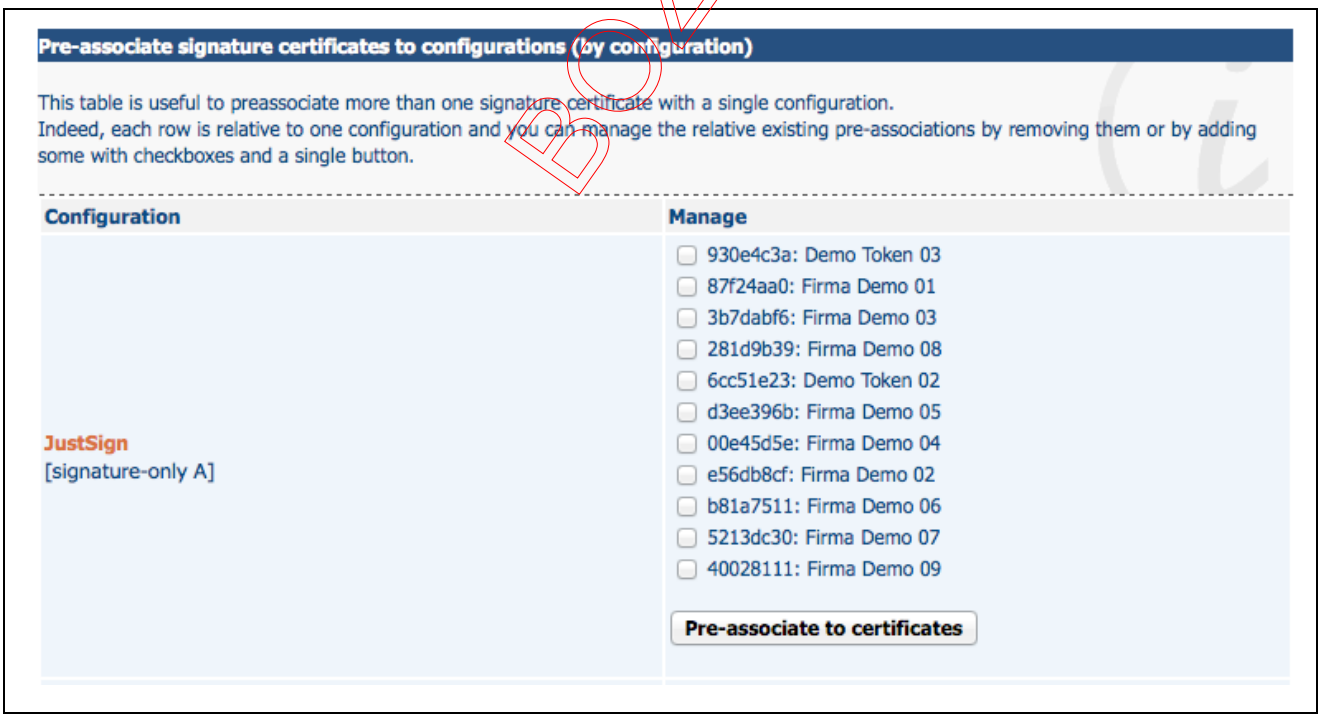
In questa prima tabella si prevede la possibilità di rimuovere le pre-associazioni esistenti (solo fino al momento in cui il Certificato non è stato inizializzato dal Titolare). Nel caso in cui nessuna pre-associazione sia stata effettuata, chiaramente la tabella si presenterà vuota. Questa funzione è utile nel caso in cui l'Amministratore abbia commesso un errore o comunque sia necessario eseguire la rimozione di una pre-associazione fra Certificato e Configurazione. Per eseguire questa operazione, è sufficiente che l'Amministratore individui, all'interno della tabella "*Removal of existing pre-associations*" la Configurazione per la quale deve essere effettuata la rimozione della pre-associazione dal relativo Certificato di firma e clicchi sul pulsante "*Delete preassociation*". La rimozione verrà confermata dal messaggio "**Removed certificate [Certificate_ID] preassociation with configuration [Configuration_Name]**".

La stessa pagina consente, inoltre, di eseguire due ulteriori e utili operazioni:

- pre-associare ogni singolo Token ad una Configurazione;
- pre-associare ogni singola Configurazione ad uno o più Token (funzione utile quando siano presenti multipli Token da pre-associare ad una Configurazione)

Le due operazioni sono illustrate nelle figure seguenti:





Per poter effettuare la pre-associazione fra il Certificato e la Configurazione è, quindi, sufficiente utilizzare la tabella denominata "*Pre-associate signature certificates to configurations*", selezionando per ciascun certificato di firma la relativa Configurazione dalla finestra a tendina verticale e confermando la scelta cliccando sul pulsante "*Pre-associate Certificato to Configuration*". La preassociazione verrà quindi

confermata dalla presenza del messaggio "**Pre-association of certificate [*ID_Certificate*] to configuration [*Configuration_Name*] performed successfully**". Tale pre-associazione sarà quindi successivamente inserita nella tabella "*Removal of existing pre-associations*".

Per eseguire, invece, una pre-associazione fra una Configurazione ed il relativo Token di firma, è necessario utilizzare la tabella denominata "*Pre-associate signature certificates to configurations (by configuration)*" e inserire il segno di spunta su ogni singolo Token che si desidera pre-associare, quindi confermare cliccando sul tasto "*Pre-associate to certificates*".

E' utile ricordare che un Certificato di firma può essere associato a più Configurazioni. Questo può accadere nel caso in cui lo stesso certificato firma deve essere utilizzato per firmare più documenti di differente tipologia.

Prestare sempre attenzione al valore di identificazione (ID) del certificato di firma, prima di procedere con questa operazione. Il valore di identificazione è presente nella prima prima riga di dettaglio delle informazioni relative al certificato stesso. Qualora si cerchi di preassociare lo stesso Certificato alla medesima Configurazion, comparirà il seguente messaggio di avviso: "**WARNING: pre-association already exists, skipping...**"

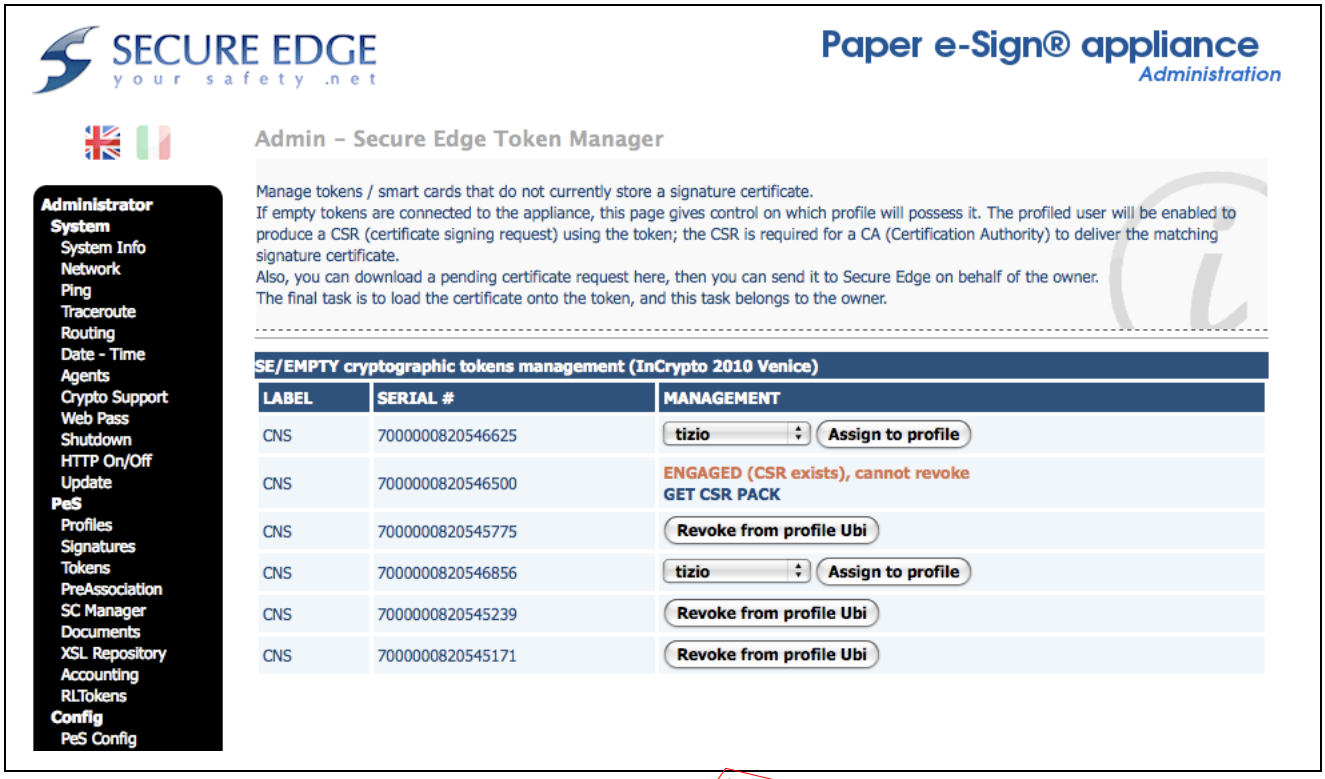
In mancanza di una pre-associazione fra Certificato e Configurazione, il Titolare del Certificato non potrà procedere alla definiva assegnazione per proprio certificato di firma alla Configurazione. E' quindi assolutamente necessario che l'Amministratore ottemperi questa operazione prima che il Certificato venga inizializzato (Cerimonia) dal Titolare.

SC Manager: assegnazione di un token SSCD ad un titolare

Questa funzione permette al PAdm di assegnare una Smart Card vuota ad un titolare; quest'ultimo potrà richiedere un certificato di firma da caricare sulla smart card.

Dopo aver effettuato la scansione dei device crittografici dal menu Tokens, gli SSCD non inizializzati vengono elencati in questa pagina di cui diamo un esempio nel seguito.

Questa funzione è orientata alla gestione dei Certificato di firma in particolare tramite il dispositivo "Multi SSCD Box"



In particolare nella tabella si individuano le seguenti colonne:

- *Label*: denominazione del dispositivo crittografico (nota: spesso appare "CNS", ovvero "Carta Nazionale dei Servizi, ma la smart card non è effettivamente di questo tipo)
- *Serial*: indica il numero di serie del dispositivo crittografico (univoco)
- *Management*: indica il Profilo del Titolare che potrà gestire il processo di inserimento del certificato di firma all'interno del Certificato e la successiva modifica del PIN, oppure consente di assegnare un (solo) titolare o, se la procedura non è stata avviata, di revocare l'assegnazione

Qualora un Certificato venga visualizzato nello stato di "Engaged", ciò indica che il Titolare ne ha effettato la CSR e quindi non può più essere revocato dall'Amministratore attraverso questo Menù.

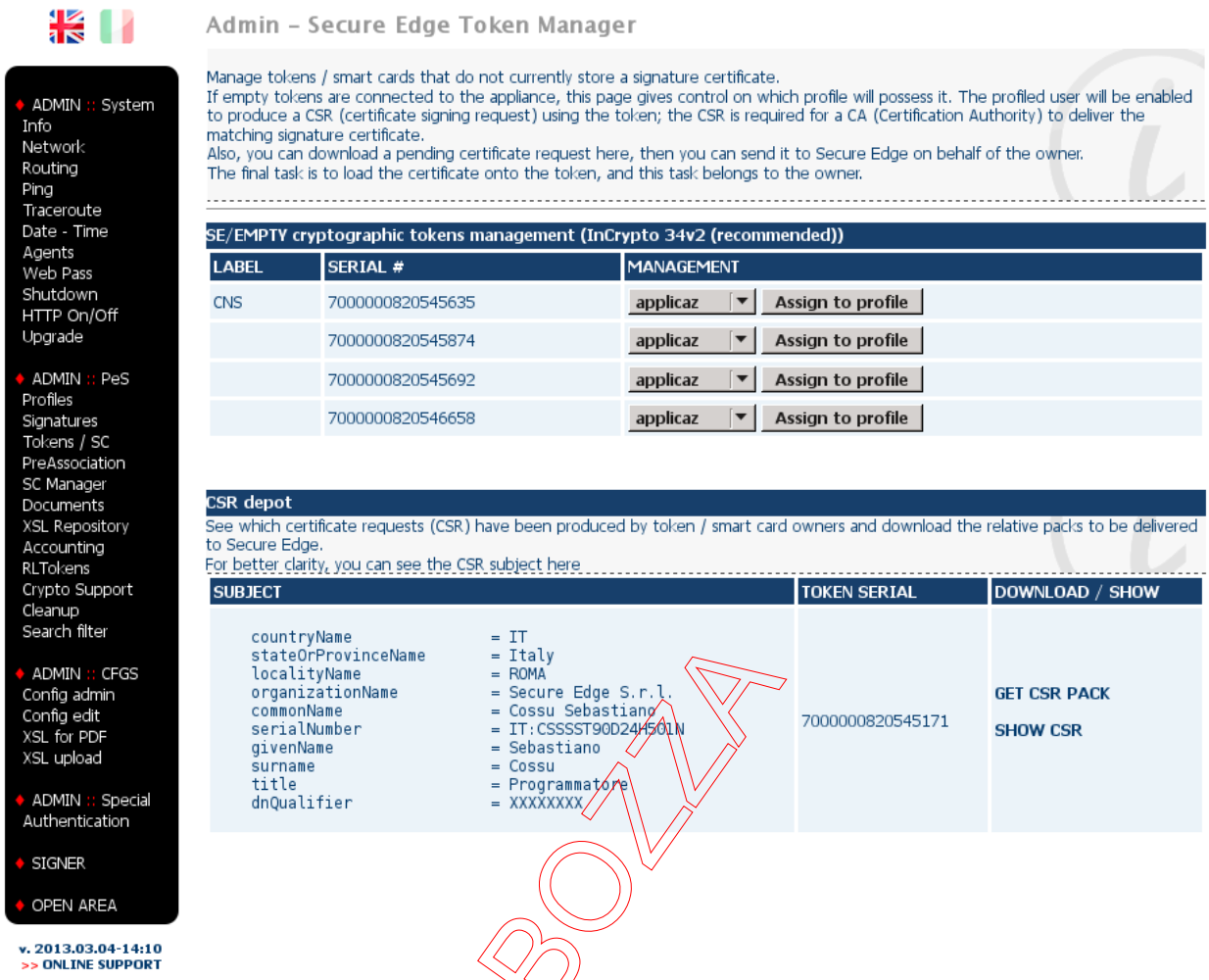
La procedura si articola nei seguenti passi:

1. Il titolare deve avere ottenuto da Secure Edge, tramite il sistema CRSS, un "pre-CSR pack" (è un singolo file) che lo abilita ad avviare la procedura di popolazione della smart card
2. l'Amministratore associa una smart card vuota ad un profilo (utilizzando l'apposita finestra a tendina nella colonna "Management") cliccando sul taso "*Assign to Profile*"
3. il Titolare entra nella console di amministrazione con il proprio Profilo, attraverso la pagina "***SCM Keys/Request***";
4. il Titolare carica il pre-CSR pack ed ottiene indietro un CSR (Certificate Signing Request) pack da inviare a Secure Edge srl

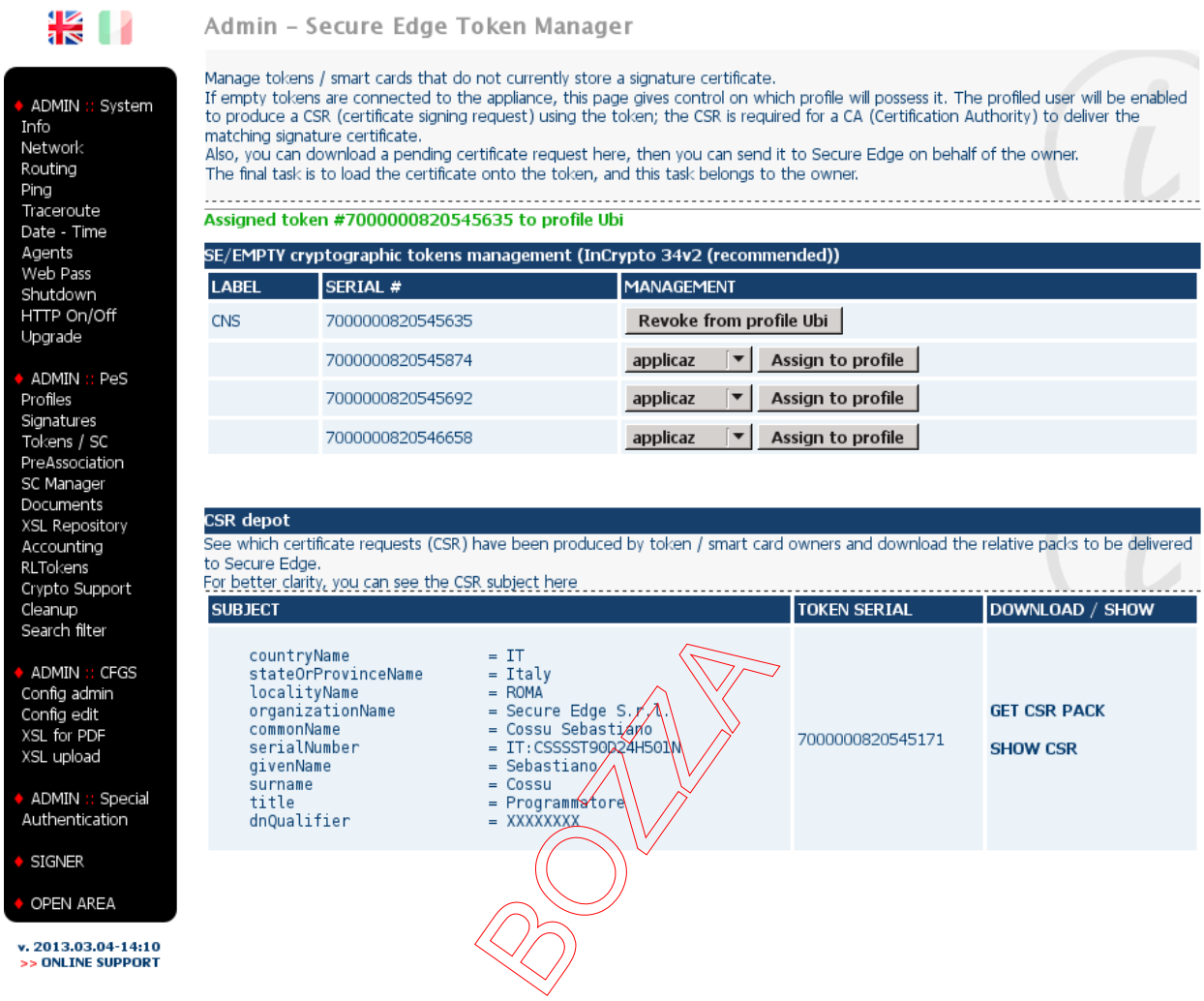
5. Secure Edge, ricevuto il CSR (pack), emette il certificato per il titolare, nonché il relativo “Certificate Pack”
6. Il Titolare utilizza il “Certificate Pack” per caricare il certificato all’interno della smart card

Alla fine, la smart card è del tutto identica alle altre (non vuote) presenti sugli appliance; il titolare può avviare il relativo servizio di firma. Un esempio è illustrato dalle immagini:

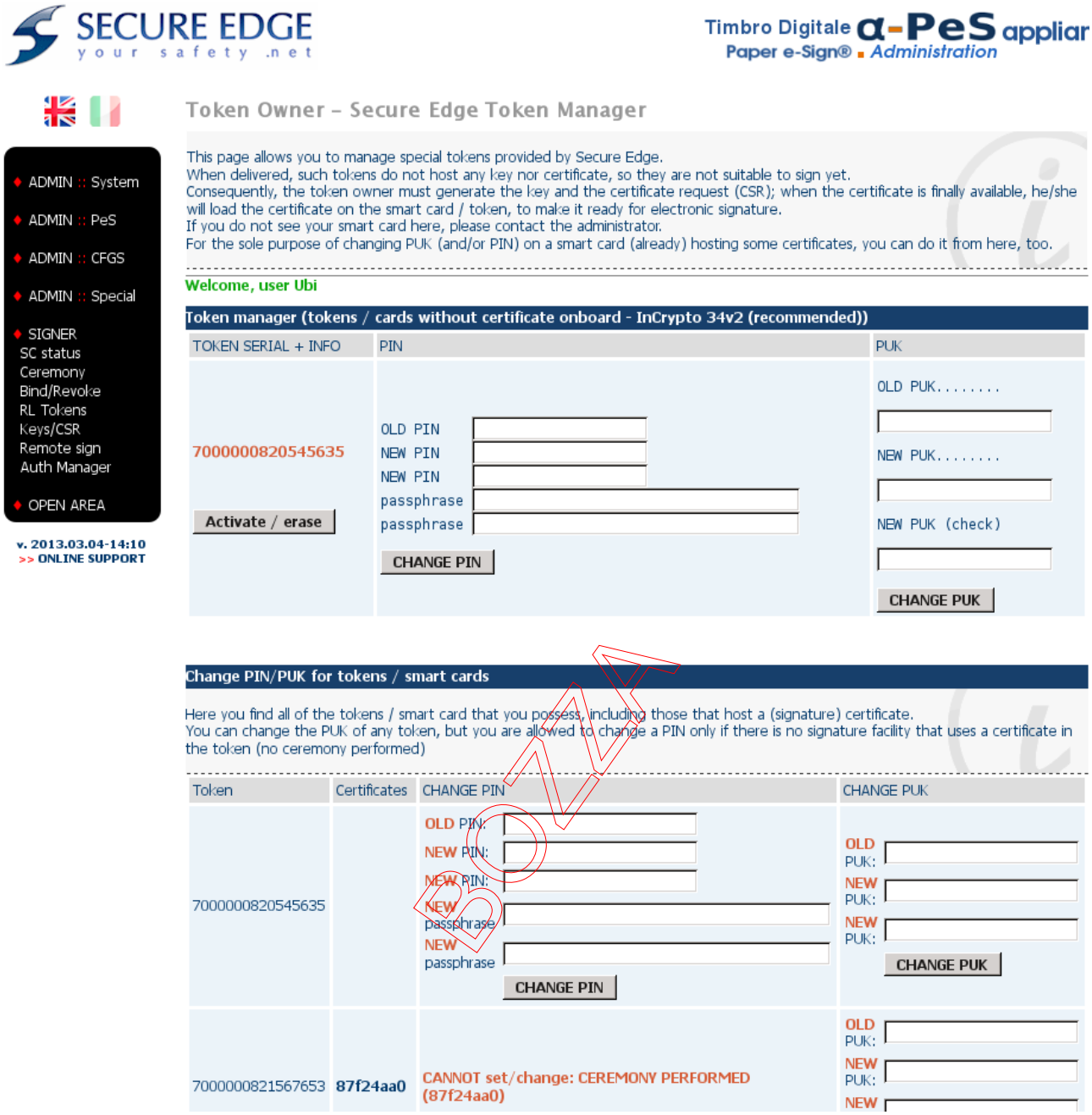
L'amministratore ha eseguito la scansione dei token dopo aver collegato dei nuovi token crittografici vuoti. Se questi erano già presenti (per esempio in un MSBox) non serve eseguire la scansione.



Dopo aver atteso il tempo necessario al completamento della scansione dei token, l'amministratore accede alla pagina "SC manager", dove vede una lista di (in questo caso) 4 token vuoti.

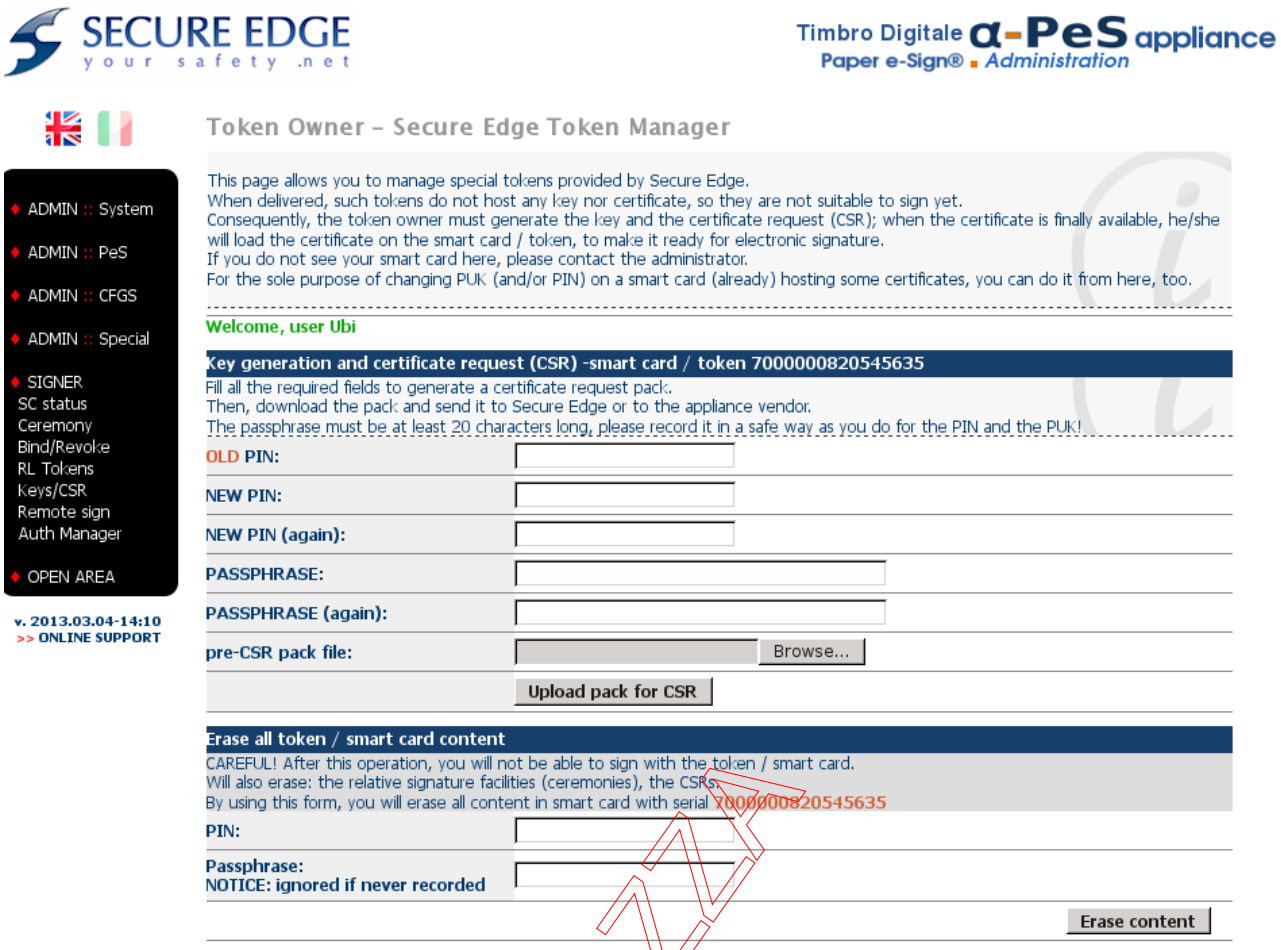


L'amministratore ha scelto di assegnare al profilo "Ubi" il primo token della lista.



Il titolare della firma, corrispondente al profilo Ubi, accede alla pagina Keys/CSR dove vede i token che gli sono stati assegnati.

Deve premere il tasto “Activate / erase” per accedere alla pagina che consente il caricamento del pre-CSR pack.



Il token owner ha premuto “Activate / erase”, ha quindi davanti il form dove immette il PIN corrente, il nuovo PIN, la passphrase e carica il pre-CSR pack ricevuto per e-mail dal sistema CRSS di Secure Edge.

Poiché il PIN originale della smart card è quello di default, noto anche all’amministratore dell’appliance, è responsabilità del titolare cambiarlo e registrarlo in modo da avere accesso egli solo a questa informazione.

Si suggerisce di registrare la passphrase assieme al PIN.

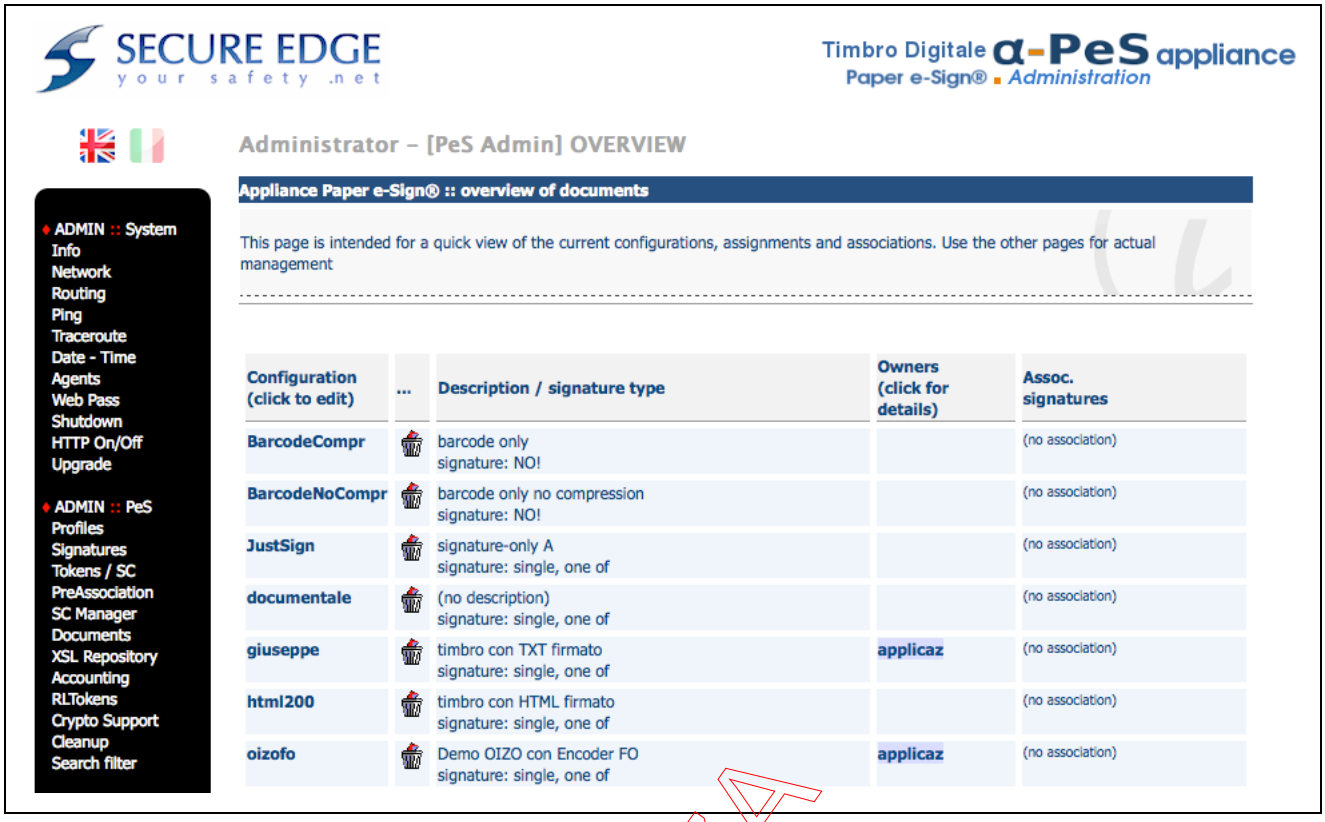
Dopo aver caricato il pre-CSR, ottiene alcuni messaggi di conferma e un link (in fondo) per scaricare il CSR pack, che deve essere fornito a Secure Edge / caricato sul sistema CRSS (vedi il relativo manuale).

Nota: nella schermata, compare la scritta “to upload...”; trattasi di un refuso corretto nella successiva versione dell’interfaccia. Dovrebbe apparire “to download...”

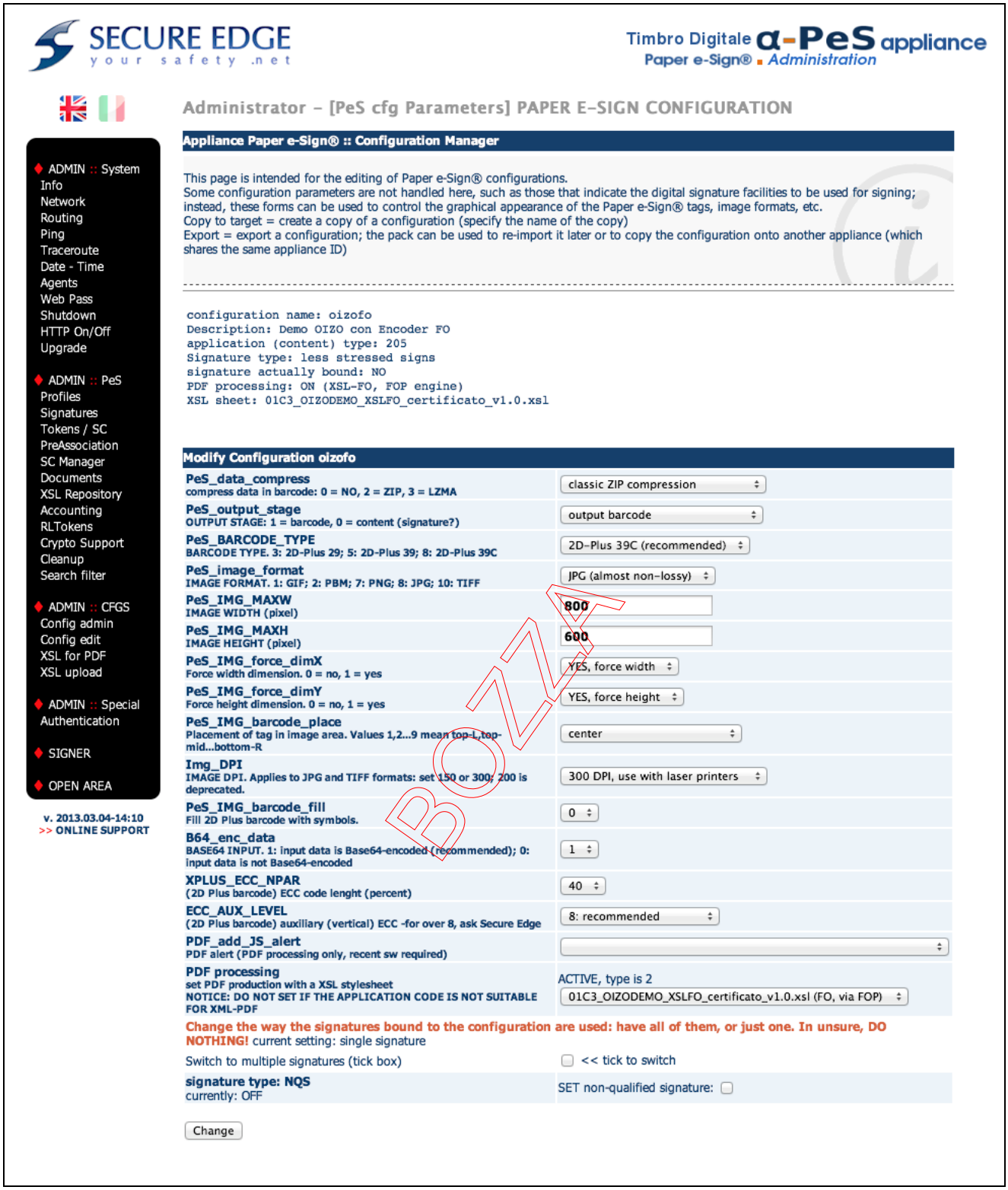
Avendo il CRT pack a disposizione, il titolare deve accedere ancora alla pagina “Keys/CSR”, premere il tasto “Activate / erase” per accedere al form che gli consentirà di caricare quest’ultimo pack.

Documents: modifica dei parametri di una Configurazione

In tutti quei casi in cui sia necessario modificare alcuni parametri particolari di una Configurazioni (quali, ad esempio, l’altezza e/o larghezza dell’area in cui verrà applicato il Timbro, oppure la densità in pollici del Timbro ecc…) l’Amministratore può fare riferimento al Menù “**Documents**” dell’area “**PeS**”. Cliccando su questo menu viene visualizzata la finestra illustrata nell’immagine seguente:



Per poter modificare i parametri di dettaglio di una Configurazione, l'Amministratore deve cliccare sul nome della stessa dalla colonna "*Configuration*" della tabella "*Overview of documents*". Si accederà quindi alla pagina seguente, illustrata di seguito:



In particolare è bene che l'Amministratore verifichi che il valore del parametro "Application type" corrisponda effettivamente a quello previsto per la Configurazione. Come è possibile osservare dall'immagine sopra-riportata, è possibile variare il dettaglio di molti parametri attraverso le relative finestre a tendina. I valori che possono essere impostati per ogni parametro sono sintetizzati nella relativa riga di dettaglio, tuttavia per una trattazione più esauriente si rimanda la lettura del documento ***[SE_T-07-0049] T I DST Usage from applications [3.9].pdf***. Per confermare le modifiche apportate e tornare alla pagina

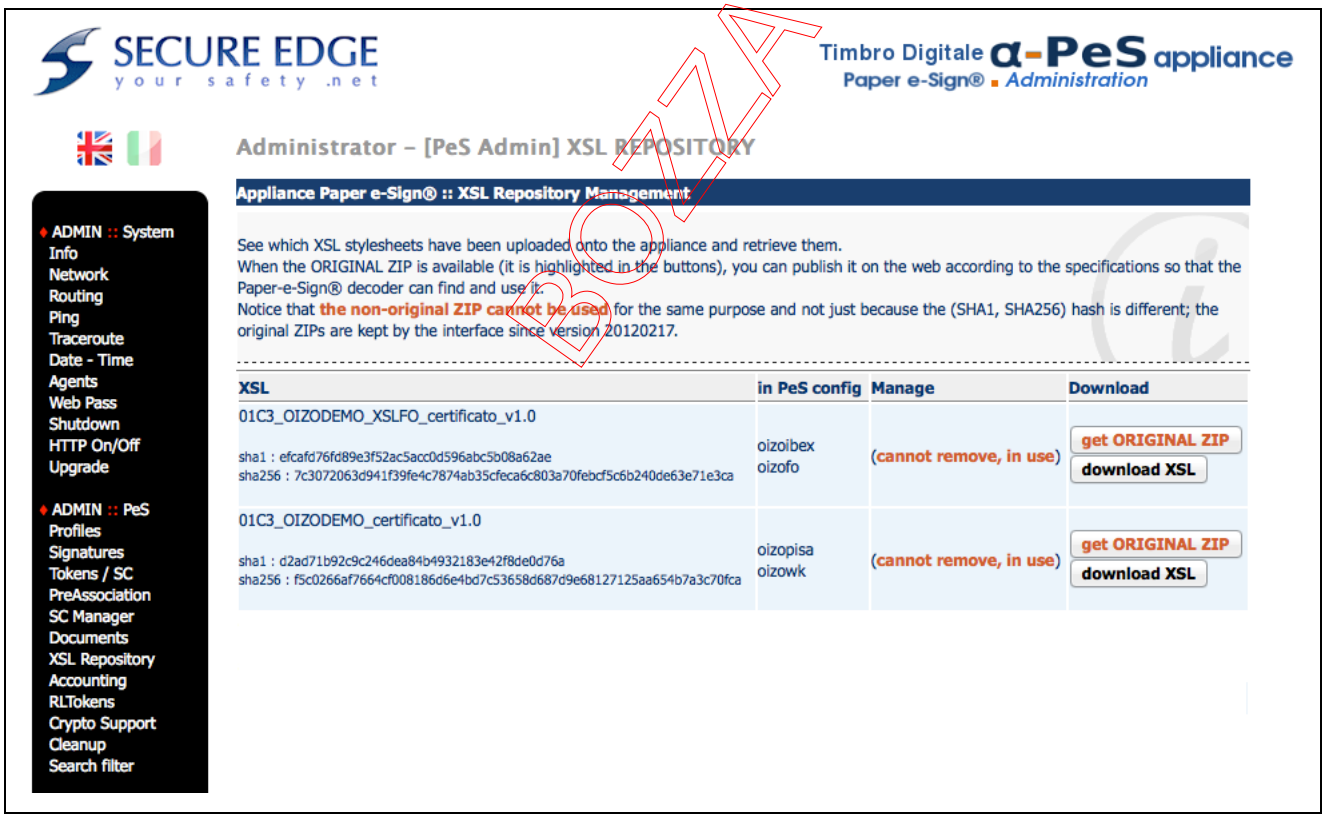
precedente, è necessario cliccare sul tasto "Change": apparirà la conferma "***The configuration "[Configuration_Name]" has been modified!***"

XSL Repository: visualizzazione dei template XSL importati, download e cancellazione dei template XSL

Tramite il Menù "XSL Repository" dell'area "PeS" l'Amministratore può eseguire le seguenti attività:

1. Visualizzare i template precedentemente caricati e verificare a quale o quali Configurazioni tali template siano già associati
2. Effettuare il download dei template
3. Effettuare la cancellazione dei template

Qualora non vi siano tamplate XSL già importati la pagina si presenterà la scritta "***Sorry there are no XSL in this appliance***". Chiaramente, non sarà possibile, per l'Amministratore, eseguire alcuna operazione. Altrimenti la lista dei template XSL comparirà come illustrato nella figura seguente:



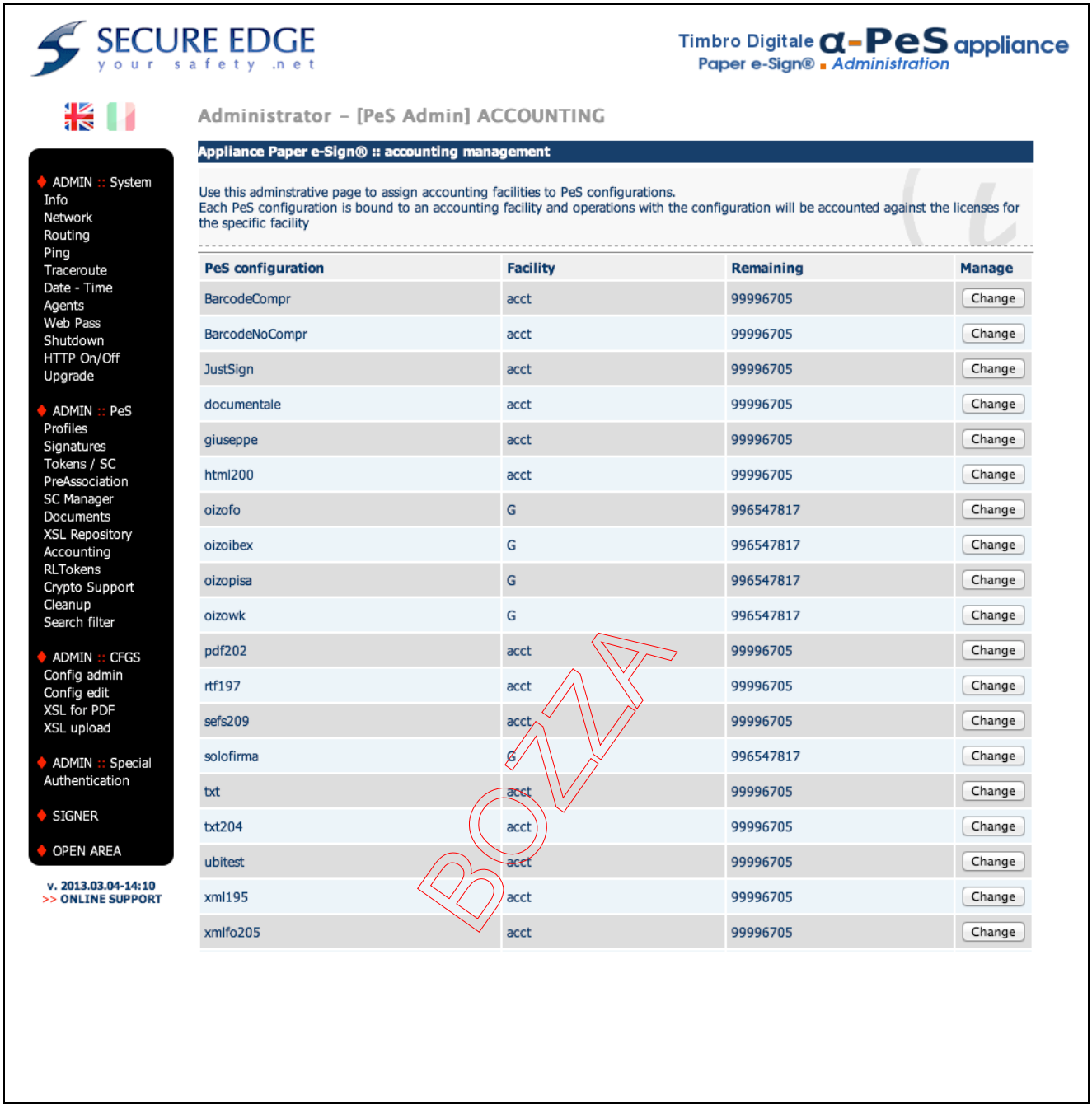
Come si può notare dall'immagine, un template può essere associato ad "n" Configurazioni". Per cancellare il template sarà sufficiente che l'Amministratore clicchi sul tasto "*Delete XSL*" nella riga relativa al nome del file che si andrà a rimuovere dall'archivio. Similarmente, per effettuare il download del template, come originariamente importato, è possibile cliccare sul bottone "*get ORIGINAL ZIP*". Se si desidera avere lo stesso template con il formato di compressione TGZ, è sufficiente che l'Amministratore clicchi sul tasto

"*Download XSL*" nella riga relativa al nome del file che si andrà a scaricare sul computer locale. In entrambi i casi sarà eseguito il download del file XSL e di tutti i file accessori (foglio di stile, immagini ecc…)

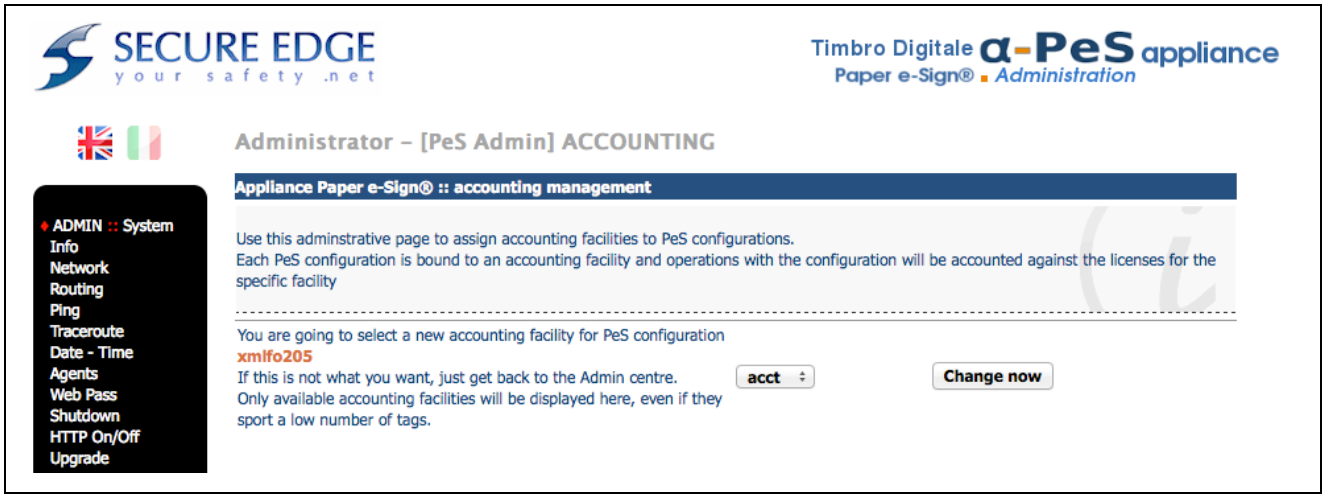
Qualora un Template sia già stato associato ad una Configurazione non sarà possibile cancellarlo dall'archivio e comparirà l'indicazione "***Cannot remove, in use***". Per rimuovere l'associazione fra un Template ed una configurazione, si rimanda al paragrafo "***XSL for PDF***"

Accounting: visualizzazione del numero dei tmbri a disposizione e assegnazione delle licenze per le Configurazioni

Questa funzione permette di visualizzare il numero di timbri da emettere per ciascuna configurazione. L'indicazione potrebbe trarre in inganno in quanto il numero di timbri ancora emettibile è associato al parametro Facility che può essere condiviso tra più configurazioni portando, di fatto, ad indicare un numero di timbri totali disponibili falsato. Nell'esempio sottostante il numero totale di timbri è 15200 e non 11x15200 in quanto tutte le configurazioni fanno riferimento alla stessa facility.



Qualora si disponesse di differenti tipologie di licenze (“facility”) l’Amministratore ha facoltà di associare ad una specifica Configurazione una relativa licenza cliccando sul tasto “*Change*” sulla riga relativa. Verrà visualizzata la finestra illustrata di seguito:

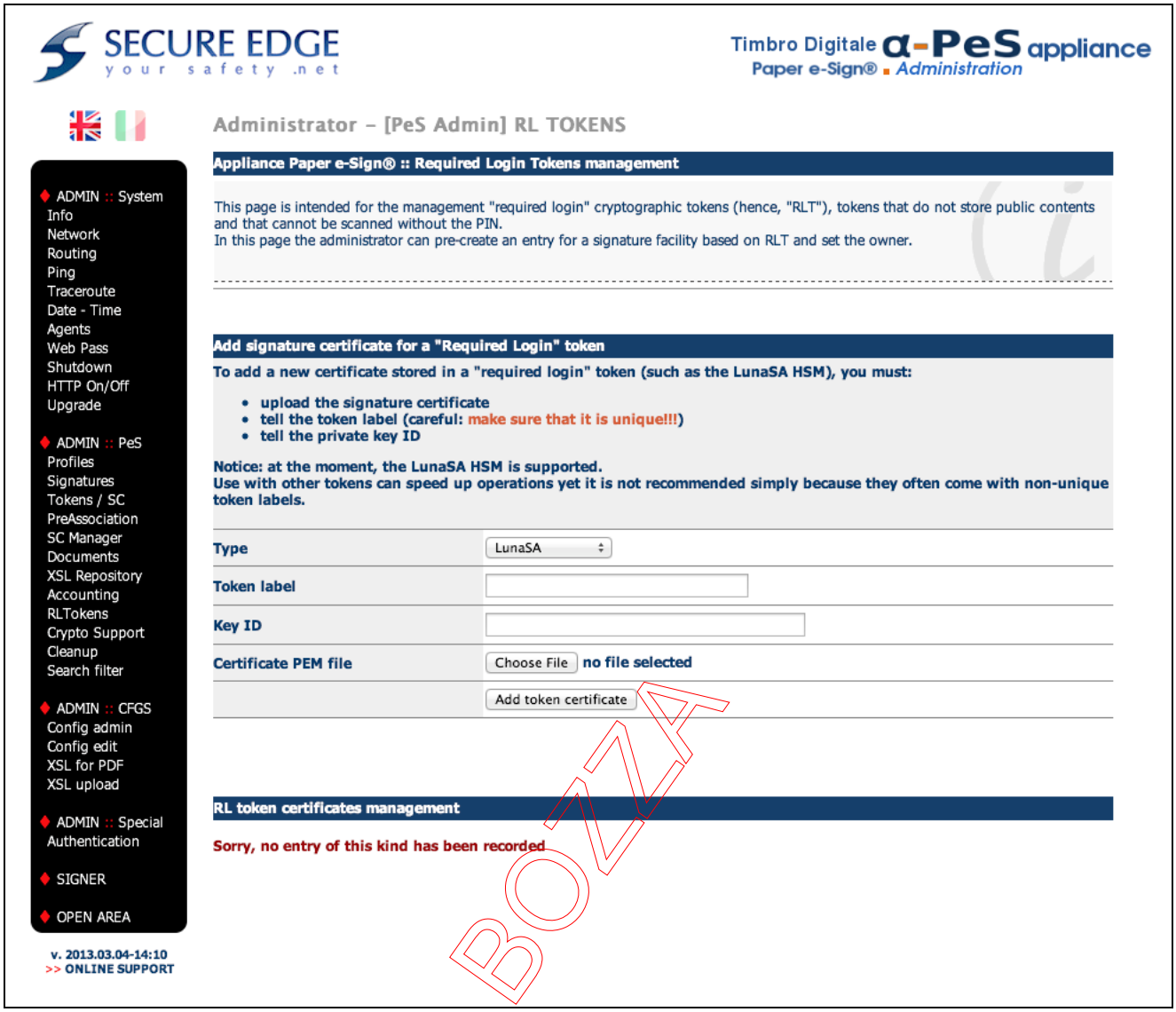


Nel caso illustrato in figura la Configurazione "xmlfo205" può essere impostata con la licenza "***acct***" avente, a sua volta, un certo numero di timbri a disposizione.

Qualora il valore del parametro "facility" sia impostato a "G" ciò indica una licenza illimitata per la configurazione a cui è assegnata. La licenza illimitata visualizza un numero di timbri rimanenti molto grande.

RLTokens: collegamento ad un dispositivo "HSM" - LunaSA

Qualora l'appliance αPeS venga collegata, anziché ad un SCBox o an MultiSSCD Box, ad un apparato crittografico HSM del tipo "Luna SA" di Safenet, è necessario che venga stabilita l'inter-comunicazione fra i due dispositivi. Difatti il dispositivo HSM sarà visto dall'appliance come un repository di certificati di firma, alla stregua di un Certificato (ma, potenzialmente, con un numero molto elevato di certificati al suo interno). Per stabilire quessta intercomunicazione, l'Amministratore può usare il Menù "***RLTokens***" dell'area "***PeS***", come illustrato nella figura seguente:



L'Amministratore dovrà inserire i parametri relativi a:

- tipologia di HSM
- denominazione ("label") del Certificato a cui si intende accedere, avendo cura di specificarlo in modo univoco
- ID della chiave di accesso al Certificato
- Caricare la chiave privata per la mutua autenticazione con il dispositivo HSM (è fornita dall'Amministratore del dispositivo HSM).

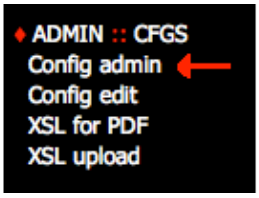
Quindi confermare i parametri inseriti cliccando sul tasto "*Add token certificate*" e attendere che l'appliance αPeS abbia importato il Certificato dal dispositivo HSM.

Admin : CFGS Area

L'area "***Admin :Cfgs***" consente di operare direttamente sulle Configurazioni, nonché su eventuali template XSL da associare (per il processamento XSL-PDF, e quindi la generazione direttamente sull'appliance di documenti PDF contenenti il timbro digitale). L'area si suddivide nei seguenti Menu:

- *Config Admin*: consente di creare nuove Configurazioni, nonché di importare precedenti configurazioni esportate
- *Config edit*: consente di modificare i parametri di una configurazione o di eseguirne la duplicazione, con altra denominazione
- *Configurations*: consente di modificare, duplicare, cancellare ed esportare le Configurazioni presenti
- *XSL for PDF*: consente di associare alle Configurazioni il template XSL, a seconda della tipologia di Timbro da produrre (XSL-CSS o XSL-FO)
- *XSL Upload*: consente di importare nell'appliance αPeS i file di archivio (.zip) relativi ai template XSL

Config Admin: Creazione / Importazione di una Configurazione – Assegnazione di una Configurazione ad un Profilo di Applicazione

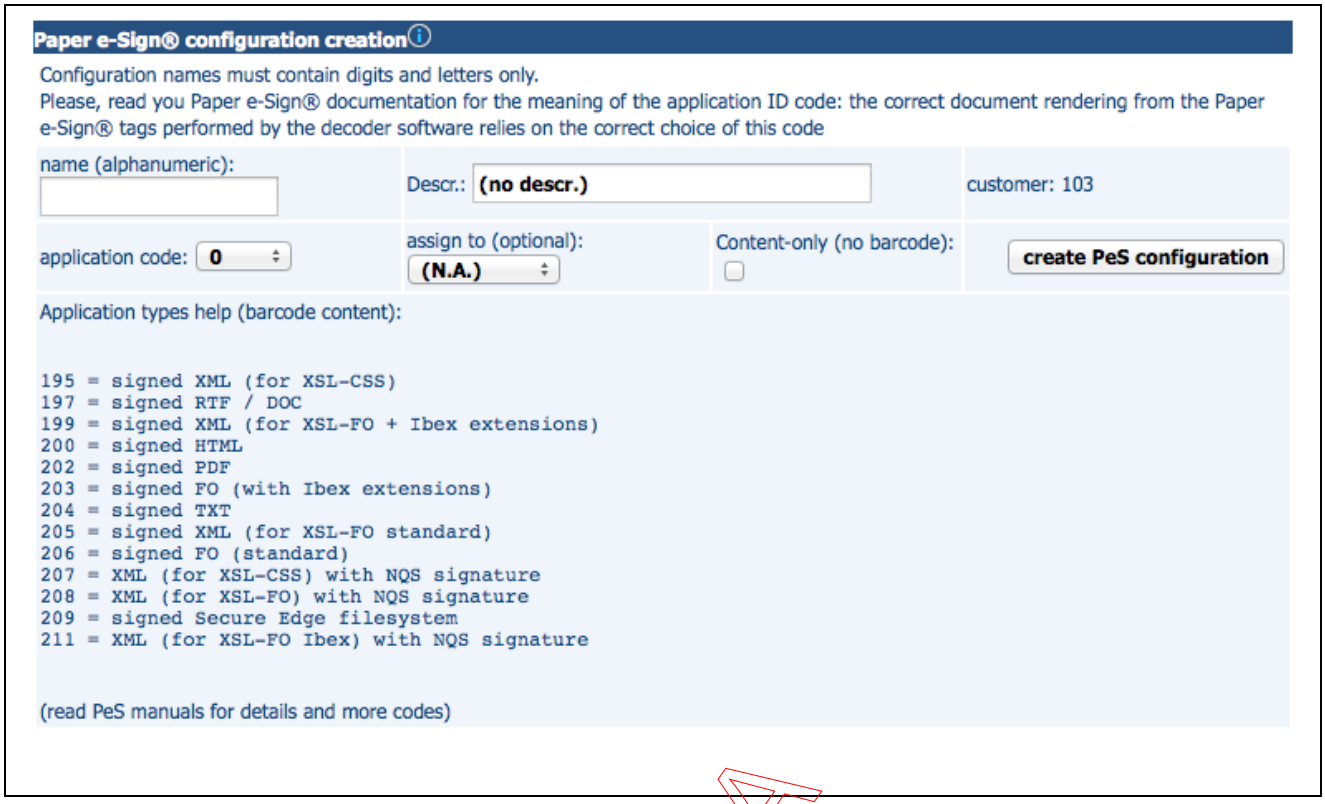


Per consentire il funzionamento dell'infrastruttura di firma automatica, è necessario che l'appliance αPeS "conosca" la tipologia di documento che verrà ricevuto dall'applicazione, nonché il certificato SSL con cui l'applicazione comunicherà con il gateway di firma dell'appliance (in modo che la comunicazione avvenga sempre in modo "sicuro" e con mutua autenticazione forte). Per creare nuove Configurazioni, è necessario utilizzare l'opzione "***Config Admin***" dall'area "***Admin : Cfgs***" del menu a sinistra. e quindi la tabella "*Paper e-Sign® configuration creation*".

E' innanzitutto necessario indicare un nome per la Configurazione (in questo caso si consiglia un nome auto-esplicativo). Quindi è necessario impostare il codice numerico che consente al gateway di firma, di riconoscere la tipologia di documento che andrà a firmare (detto codice numerico può variare da 0 a 255, tuttavia i più frequenti e comuni sono riportati all'interno della medesima tabella. Si consiglia vivamente di aggiungere una descrizione esplicava della configurazione.

Per avere una descrizione di dettaglio su tutti i codici di Configurazioni, si rimanda al documento "***Useful Data Structures***" ("*[SE_T-07-0053] T I DST useful data structures [1.13].pdf*") capitolo 4.3.

Di seguito si riporta la tabella per la creazione di Configurazioni:



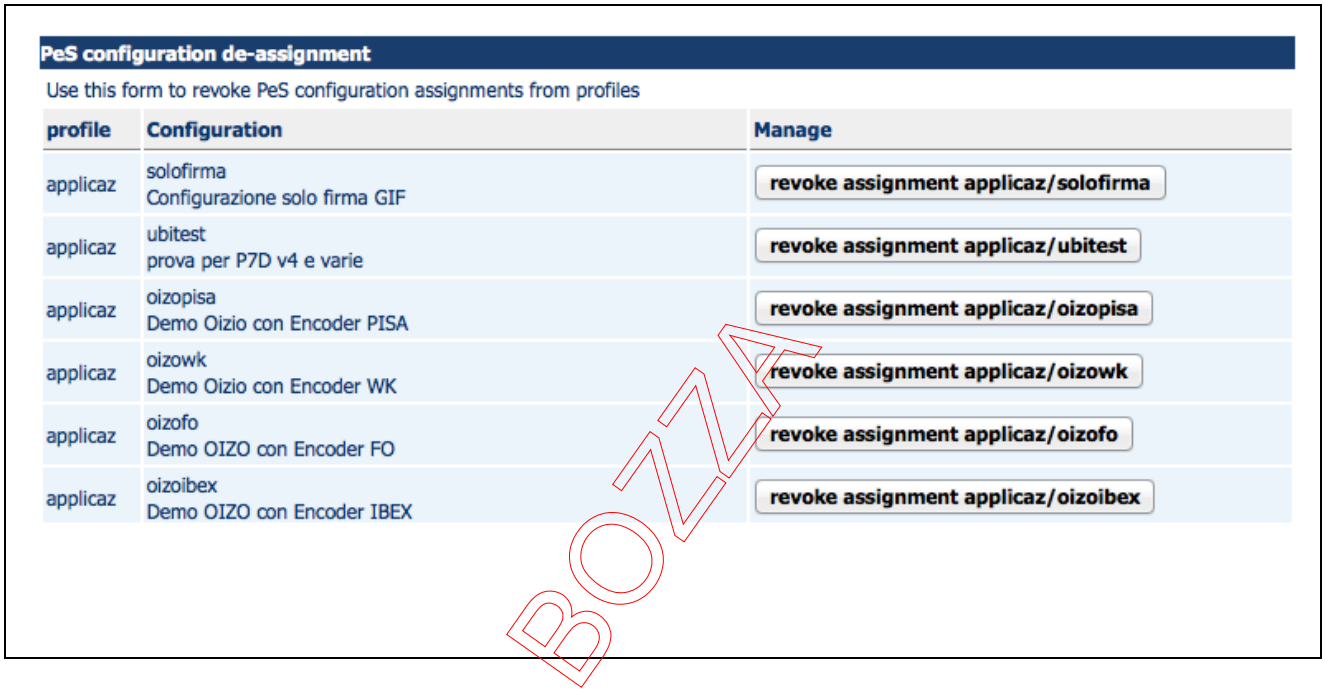
Qualora sia necessario che il gateway restituisca solamente il file *.p7m* relativamente alla firma digitale aggiungere il segno di spunta all'opzione "*Content-only (no barcode)*". In condizioni standard il gateway di firma restituisce il documento firmato (ovvero il documento con il timbro digitale).

E' utile ricordare che un Profilo dell'Applicazione può essere associato ad "n" Configurazioni. Questo può accadere nel caso in cui lo stesso certificato di comunicazione dell'Applicazione sia necessario per apporre il Timbro su più documenti di differente tipologia.

L'associazione fra il Profilo dell'Applicazione e la Configurazione prescinde dalla presenza di Certificato già inizializzati dal Titolare. Questa operazione tuttavia è assolutamente necessaria per poter consentire al Titolare del Certificato di poter poi associare il Certificato alla Configurazione.

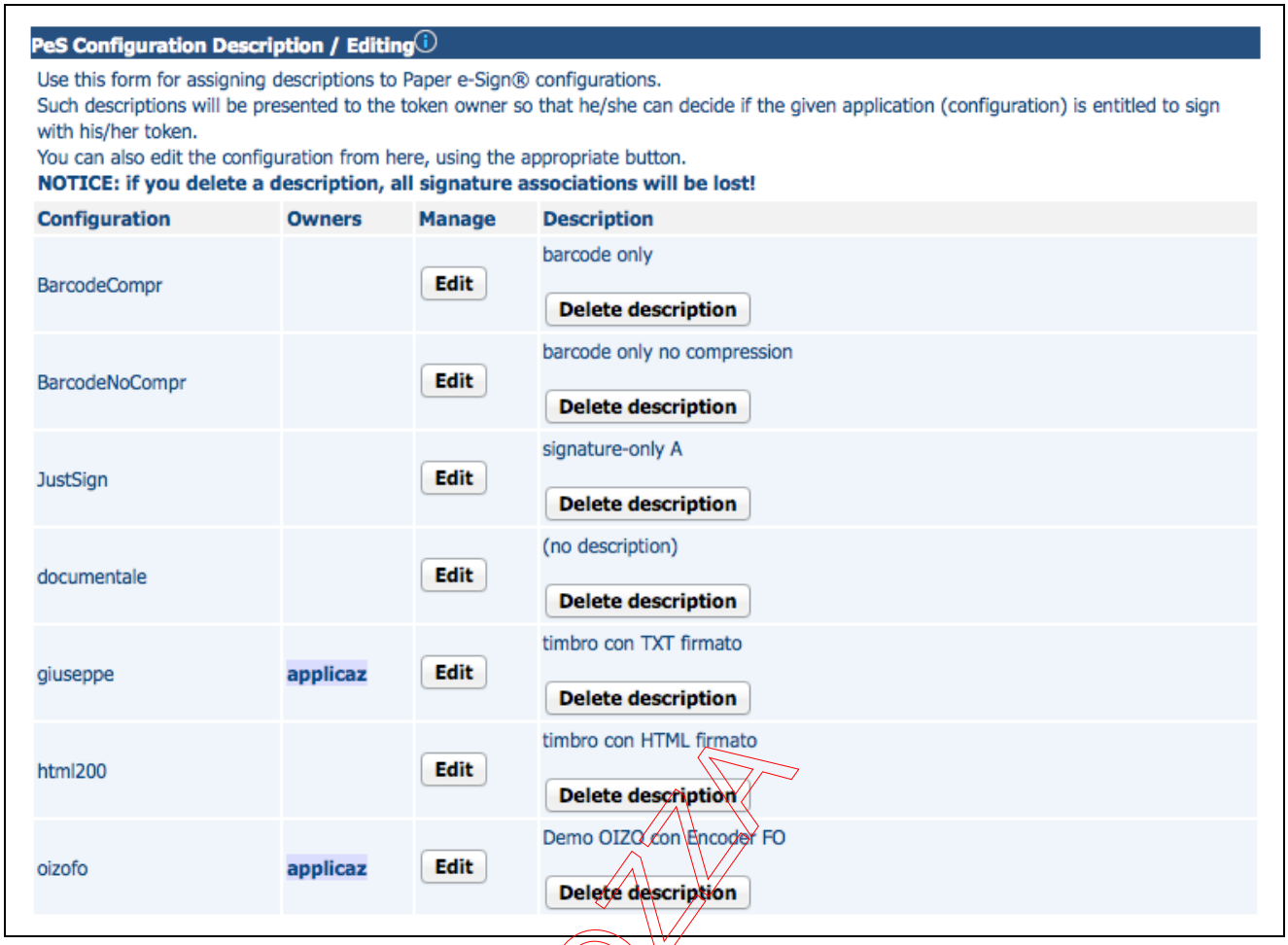
In linea generale, l'associazione fra il Profilo dell'Applicazione e la relativa configurazione dovrebbe essere effettuata congiuntamente alla creazione della configurazione medesima. Tuttavia è possibile effettuare questa associazione anche in un secondo momento, utilizzando il box "*Assign configuration to profil*", del menu "***Config Admin***" dell'area "***Admin : Cfgs***", come illustrato nella figura seguente e confermare con il tasto "*Assign PeS Configuration*".

Effettuata l'assegnazione fra Configurazione e Profilo dell'applicazione, questa apparirà nella tabella così come illustrato nella seguente immagine:



Tramite il pulsante "*Revoke assignment*" è possibile eliminare l'associazione fra Configurazione e il Profilo dell'applicazione client (ad esempio nel caso il certificato del Profilo dell'applicazione sia scaduto di validità)

Per verificare la corrispondenza fra la Configurazione e il Profilo dell'applicazione, fare riferimento alla tabella "*PeS Configuration Description / Editing*" come illustrato nella figura seguente, in particolare il valore della colonna "*Owners*" il quale riporta il nome del Profilo per ciascuna configurazione:

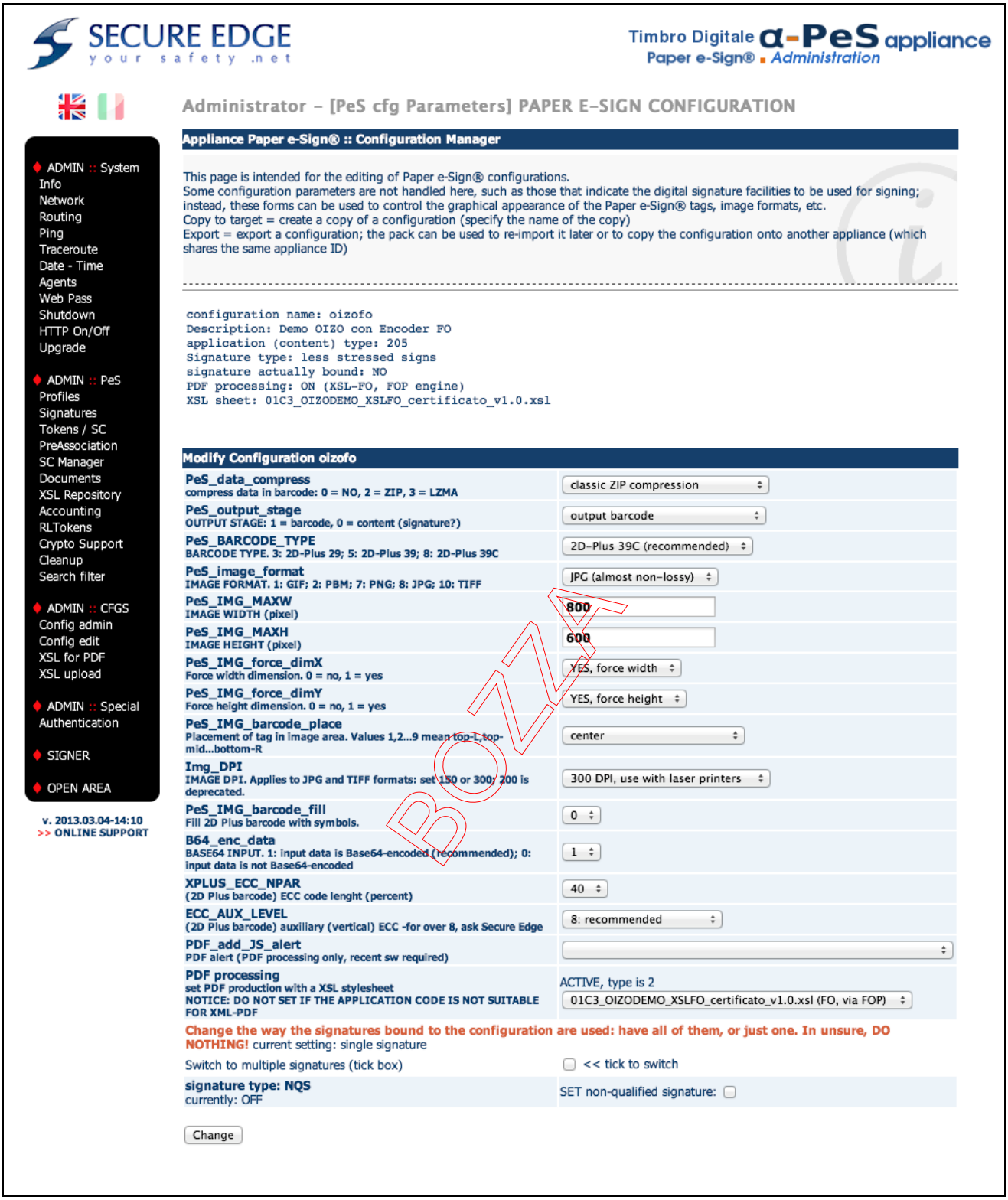


PeS Configuration Description / Editing

Use this form for assigning descriptions to Paper e-Sign® configurations.
Such descriptions will be presented to the token owner so that he/she can decide if the given application (configuration) is entitled to sign with his/her token.
You can also edit the configuration from here, using the appropriate button.
NOTICE: if you delete a description, all signature associations will be lost!

Configuration	Owners	Manage	Description
BarcodeCompr		Edit	barcode only Delete description
BarcodeNoCompr		Edit	barcode only no compression Delete description
JustSign		Edit	signature-only A Delete description
documentale		Edit	(no description) Delete description
giuseppe	applicaz	Edit	timbro con TXT firmato Delete description
html200		Edit	timbro con HTML firmato Delete description
oizofo	applicaz	Edit	Demo OIZO con Encoder FO Delete description

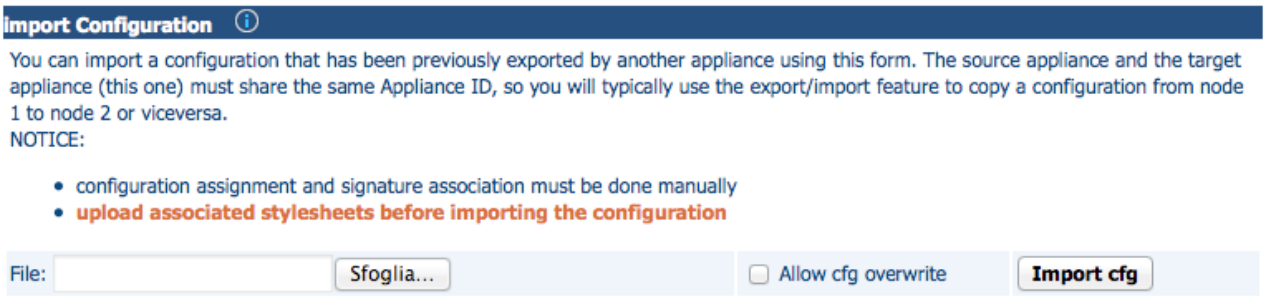
Cliccando sul bottone "*Edit*" si accede alla finestra per la modifica di tutti i principali parametri di realizzazione del timbro, come illustrato di seguito:



Il dettaglio per meglio comprendere il significato di ogni parametro è descritto nel documento: ***[SE_T-07-0049] T I DST Usage from applications [3.9].pdf***

L'Amministratore può giungere alla medesima pagina utilizzando il menù "***Config Edit***" dell'area "***Admin : Cfgs***".

Qualora si disponga già di un file di configurazione (ad esempio un backup da una seconda appliance in configurazione di hot-standby o dalla medesima appliance) è possibile importarlo utilizzando il box sottostante, come illustrato nella seguente immagine:



Qualora il nome del profilo sia già esistente, spuntare l'opzione "*Allow cfg overwite*" per consentire la sovrascrittura, altrimenti l'importazione restituirà un messaggio di errore ("**ERROR: at least one configuration ([*application_name*]) already exists in appliance**").

Il file da importare deve avere estensione "*.PeS_cfg_export*"

E' possibile importare esclusivamente Configurazioni provenienti da appliance con il medesimo "appliance ID" (lo si legge nella pagina "Info")

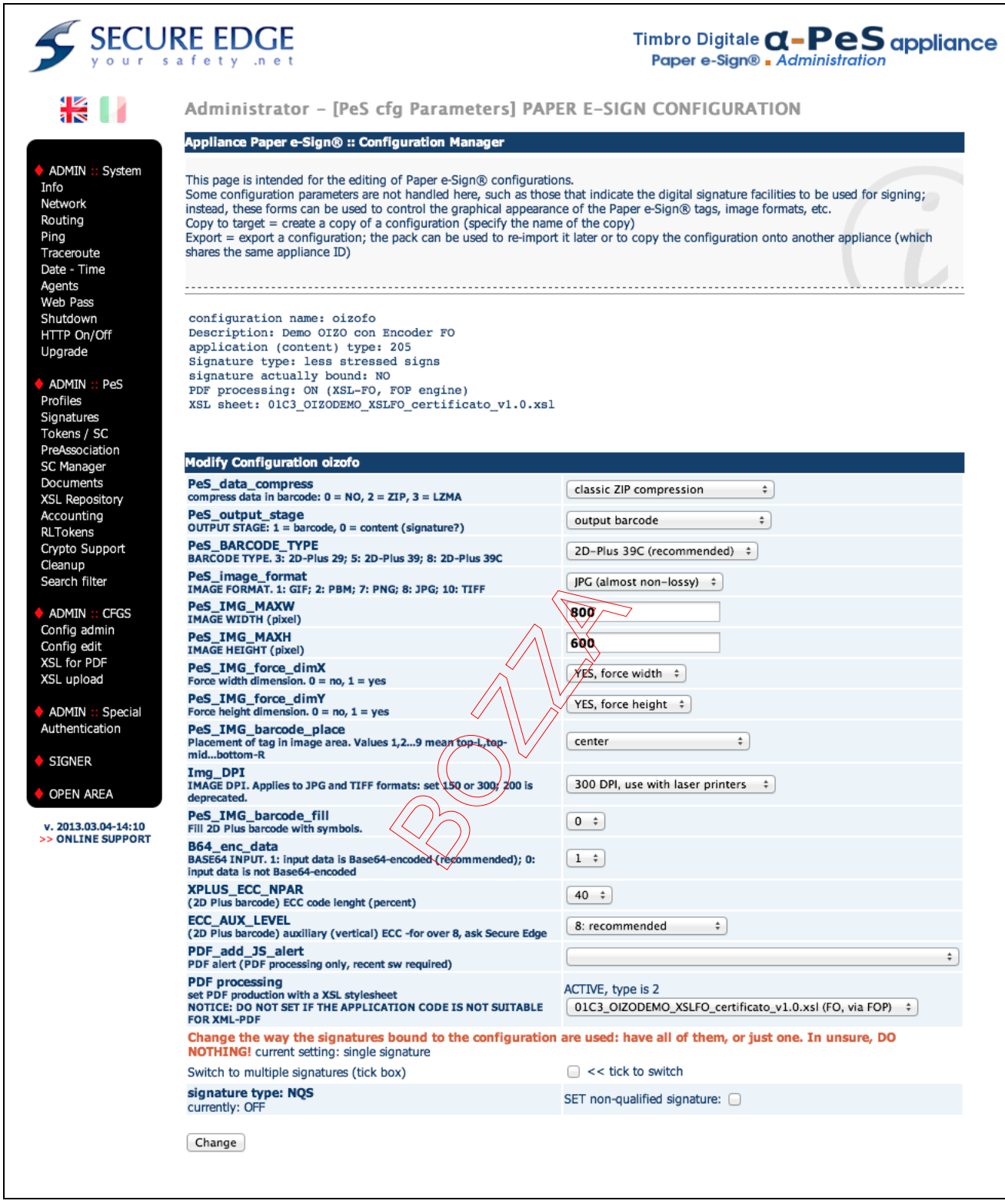
Configuration: Modifica / Cancellazione / Duplicazione / Esportazione di una Configurazione

In alcune condizioni, l'Amministratore potrebbe avere la necessità di operare alcune operazioni sulle configurazioni presenti all'interno dell'appliance αPeS, ovvero:

- La modifica dei parametri di generazione del Timbro associati ad una Configurazione
- La duplicazione di una Configurazione (con un nome differente)
- La cancellazione di una Configurazione
- L'esportazione su file di una Configurazione

Per operare queste operazioni, è a disposizione dell'Amministratore il menu "*Config Edit*" dell'area "*Admin : Cfgs*" dalla barra laterale sinistra. Verrà visualizzata la pagina illustrata nella figura seguente:

Per poter accedere ai parametri di generazione del Timbro, cliccare sul simbolo della matita nella colonna "edit", presente alla destra di ciascuna Configurazione. Verrà quindi presentata la pagina illustrata nella figura seguente:



Il dettaglio per meglio comprendere il significato di ogni parametro è descritto nel documento *[SE_T-07-0049] T I DST Usage from applications [3.9].pdf*

Per effettuare la cancellazione di una Configurazione (ad esempio non più in uso o errata), utilizzare il simbolo del cestino  presente nella colonna "*delete*". Qualora l'operazione venisse completata con successo verrà visualizzato il messaggio "***Deleting configuration [Configuration_name]... Configuration deleted!***"

E' possibile eseguire la cancellazione anche di una configurazione associata da un Titolare ad un Certificato.

Per effettuare la duplicazione di una Configurazione, utilizzare il tasto "*Copy*" dalla colonna "*copy*". Prima di cliccare su questo tasto, l'Amministratore deve inserire nel campo "*Copy target name*" un nome da assegnare alla nuova configurazione (chiaramente differente dall'originale). L'operazione verrà confermata dal seguente messaggio: "***Configuration copied successfully NOTICE: pre-associations and assignment to profiles must be manually performed***". La nuova Configurazione duplicata chiaramente avrà tutti i parametri relativi alla generazione del Timbro identici alla Configurazione originale. Tuttavia, come indica il messaggio di conferma, l'Amministratore dovrà ricreare, per la Configurazione duplicata, sia la preassociazione al Certificato di firma (vedi Passo 6) sia l'associazione al Profilo dell'Applicazione opportuno (passo 4).

Per effettuare l'esportazione di una Configurazione è necessario cliccare sul relativo tasto "*Export*": verrà generato automaticamente un link, come illustrato nella figura seguente:

Export pack created. Click on this link to retrieve.

Cliccando su "this link" si accede al download del file relativo alla Configurazione.

Il file esportato è in formato "*.PeS_cfg_export*". E' utile sapere che il file può essere importato solo su un appliance αPeS con il medesimo "appliance ID" (in genere lo stesso appliance oppure l'appliance secondario in una configurazione in Alta Affidabilità).

XSL for PDF: Associazione dei Template XSL alle Configurazioni - Attivazione dei Template XSL

Seguire questa procedura solamente nel caso in cui si desideri che l'appliance αPeS produca direttamente un file .PDF contenente il timbro digitale, utilizzando un opportuno template XSL.

Qualora l'Amministratore disponga già di uno o più template XSL all'interno dell'appliance αPeS, ne può eseguire l'associazione alle opportune Configurazioni. Per effettuare questa operazione, può utilizzare il Menù "***XSL for PDF***", sempre nell'area "***Config***", come illustrato nella figura seguente:

Per eseguire l'associazione è sufficiente selezionare il file .xsl da menu a tendina all'interno della colonna

centrale “*Assign*” (utilizzando la riga in cui è presente il nome della Configurazione) e confermare con il tasto “*Assign*”. Successivamente il nome del file .xsl compare nella tabella, all’interno della colonna “*Status*”; per completare l’associazione, è necessario cliccare sul tasto “Activate”, come illustrato nelle figure seguenti:

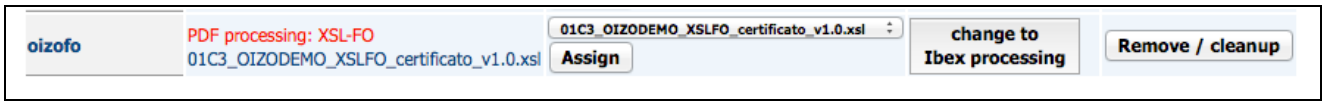
(prima della pressione del tasto “Activate”)

(dopo la pressione del tasto “Activate”)

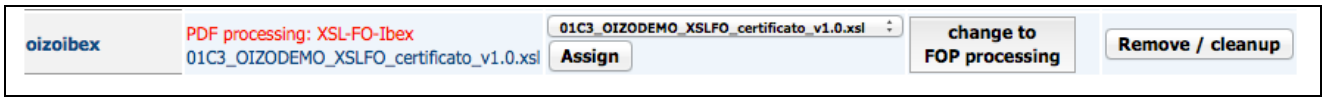
Non è possibile associare un file XLS ad una Configurazione che risulta avere già associato un certificato (certificato) di firma inizializzato (ovvero il cui Titolare ne abbia già eseguita la Cerimonia)

In caso di necessità, è sempre possibile rimuovere l’associazione fra file PDF e Configurazione, attraverso il tasto “*Remove / Cleanup*” che riporta ad una condizione di origine.

Nel caso sia necessario produrre un documento PDF attraverso la libreria “FOP” di Apache, dopo la pressione del tasto “Activate” comparirà un ulteriore tasto denominato “Ibex Processing” , come illustrato nella seguente immagine :

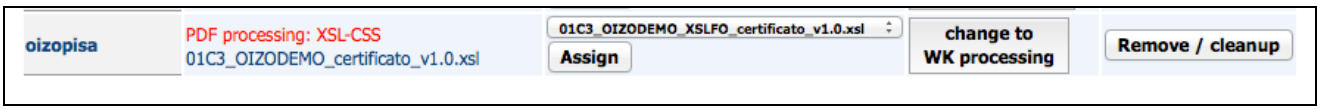


Questo tasto consente di attivare l’uso della libreria “FO-Ibex”, il quale genera un timbro lievemente differente nella struttura, ma pienamente compatibile con l’attuale implementazione del software di Decoder. E’ comunque possibile ripristinare l’uso della libreria “FOP” di Apache, cliccando sul tasto “FOP Processing” che comparirà successivamente, come illustrato nella seguente immagine:

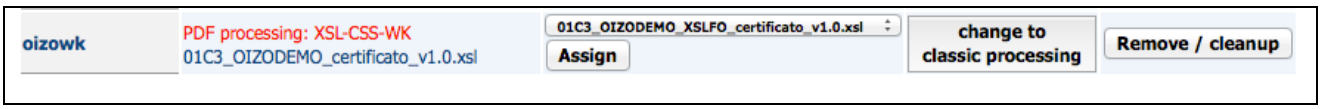


E’ infine possibile utilizzare l’engine WK per i template CSS. L’engine WK ciò consente di generare dei timbri più velocemente sebbene abbiano una struttura lievemente differente dal CSS “standard” tramite engine con PISA. Per utilizzare l’engine WK cliccare sul tasto “*Change to WK processing*” come illustrato

nella figura seguente:



Per tornare all'utilizzo dell'engine PISA cliccare sul tasto "Change to classical processing", come illustrato nella figura seguente:



Si ricorda che uno stesso template XSL tecnicamente può essere associato a più Configurazioni contemporaneamente. Questo può essere utile soprattutto in fase di test di pre-esercizio.

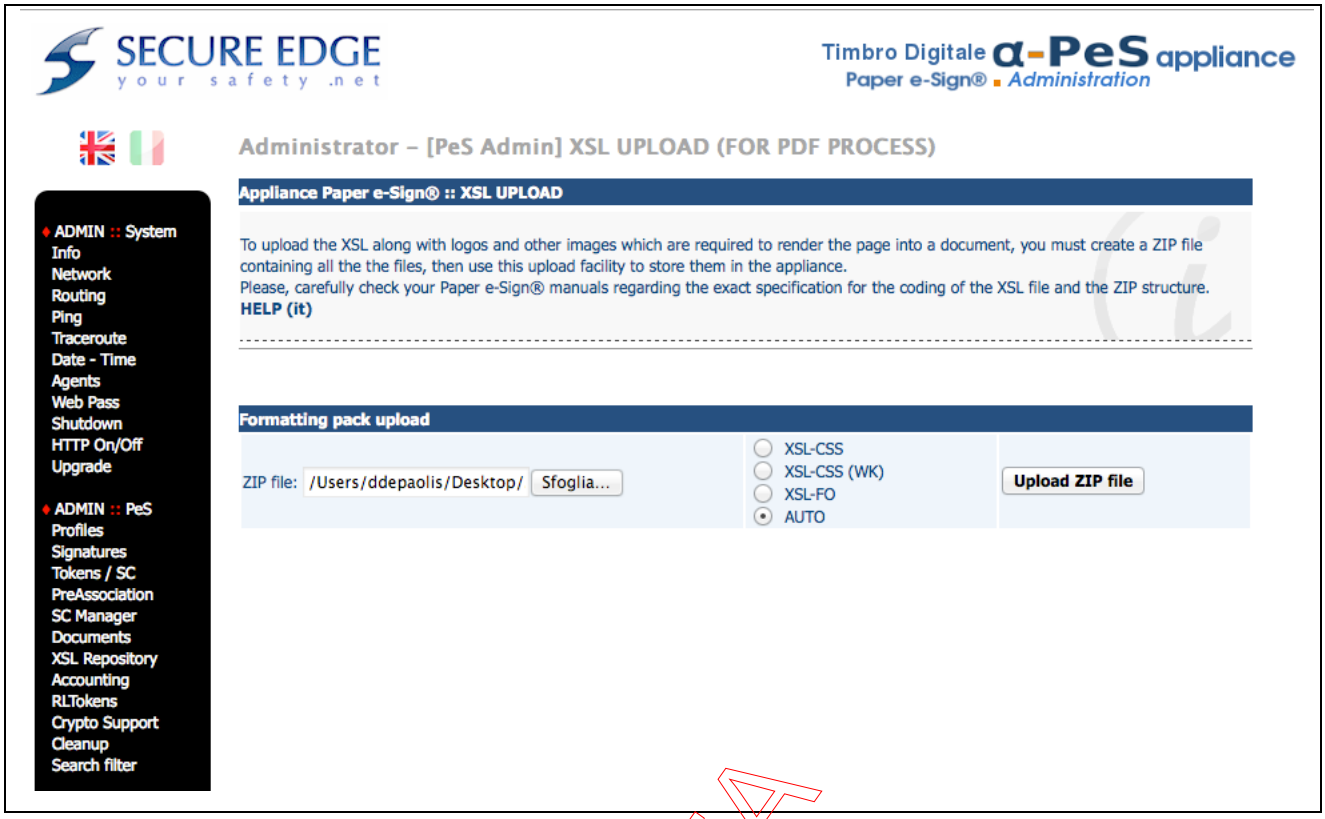
XSL Upload: importazione dei file relativi ai Template XSL

Seguire questa procedura solamente nel caso in cui si desideri che l'appliance αPeS produca direttamente un file .PDF contenente il timbro digitale, utilizzando un opportuno template XSL.

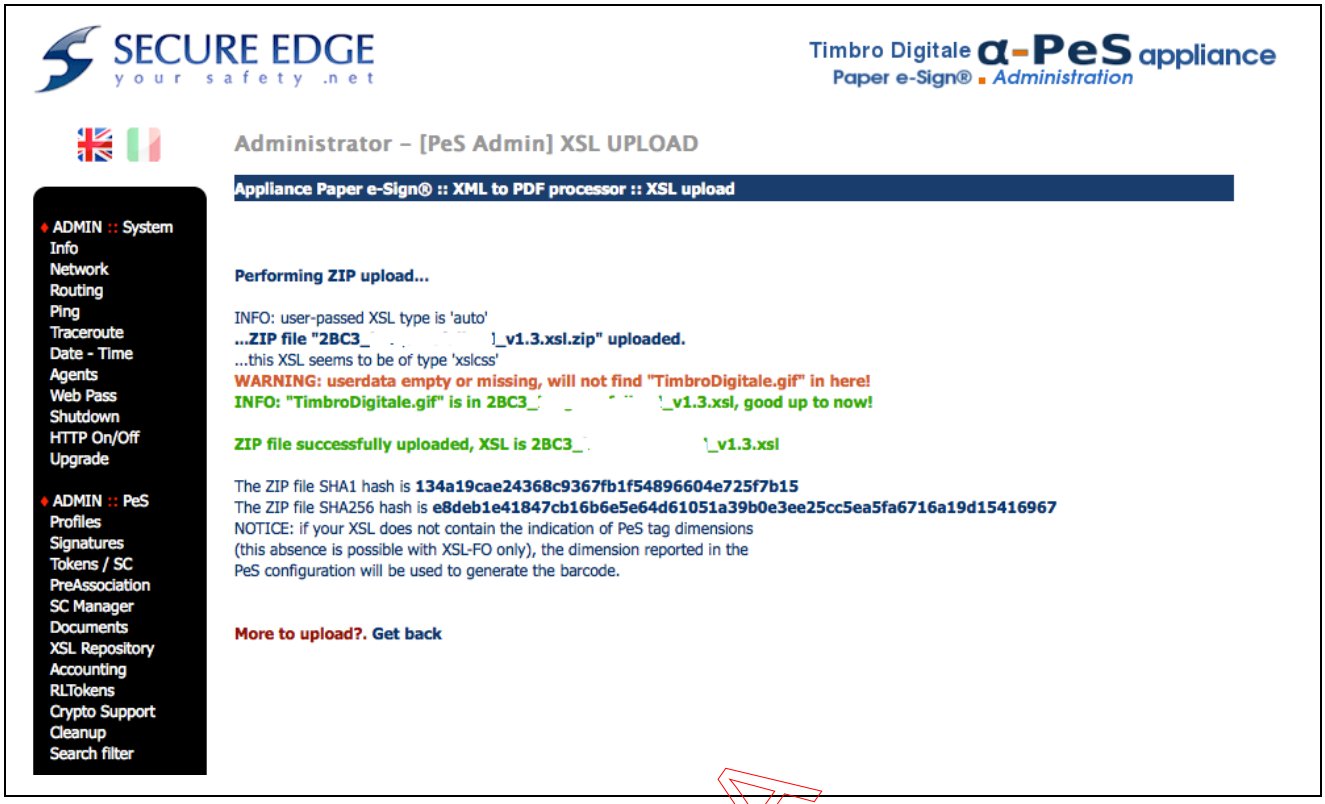
Eseguita la creazione di una Configurazione, qualora l'infrastruttura preveda che l'appliance αPeS produca direttamente un file .PDF firmato, è possibile caricare un file di "template" XSL da associare alla Configurazione medesima.

Per operare questa attività è necessario, innanzitutto, disporre di un file di archivio (.zip) al cui interno devono essere inseriti il file XSL e gli eventuali allegati "grafici" in formato .jpg; tali allegati grafici devono, a loro volta, essere contenuti all'interno della sottodirectory "img".

Per caricare tale file di archivio, l'Amministratore deve utilizzare il menu "XSL Upload" nell'area "Config", come illustrato nella figura seguente:



Cliccando sul tasto “Sfoglia”, si seleziona il percorso locale all’interno del quale è presente il file di archivio da importare sull’appliance. Il box per l’importazione del file di archivio consente di specificare anche la tipologia di formattazione del file XLS, ovvero “FO” (Formatting Objects”), “CSS” (Cascade Style Sheet) oppure “CSS” con engine WK. Normalmente, per specificare il tipo di XSL, si deve utilizzare l’opzione “Auto”. Nel caso in cui l’appliance non riesca a riconoscere, autonomamente, la tipologia di file, è possibile specificarne la tipologia manualmente. Ciò rappresenta, comunque, un’eccezione. Difatti, il verificarsi di questa situazione indica, probabilmente, un errore al momento della creazione del file .zip o .xsl. Qualora l’importazione si avvenuta correttamente, verrà visualizzata una pagina simile alla seguente illustrazione:



Il template XSL è ora pronto per essere utilizzato dall'Amministratore e quindi associato alle opportune Configurazioni.

Special Area

Quest'area serve a svolgere attività speciali ed in particolare a gestire i certificati di autenticazione all'appliance. Per accedere a quest'area non è necessario un certificato; si accede con utente e password.

La login e password di default dell'appliance αPeS sono:
Login: **muadmin**
Password: **timbrodigitale**

In quest'area è possibile svolgere le seguenti funzioni:

- **CA certificates**: visualizza le informazioni del certificato di CA caricato uno o più.

- **CA certificate upload**: permette di caricare un certificato di CA
- **Admin certificate upload**: permette di caricare il certificato di autenticazione dell'amministratore.
- **Certificate test**: permette di verificare un certificato.
- **Toggle legacy insecure renegotiation**: permette di attivare o deattivare la rinegoziazione insicura con i browser

Tutte le funzioni indicate vengono svolte direttamente dalla pagina Special Area.

Il PAdm può caricare il certificato di CA e il proprio certificato di autenticazione accedendo a questo servizio e fornendo la login e password.

E' compito dell'PAdm cambiare la password di default con una nuova password.
La funzione per cambiare la password si trova sotto:
Aministrator => System => Web Password

Per accedere alla Special Area è possibile utilizzare il menu "*Special*" ⇒ "*Authentication*" o la seguente URL:

https://<appliance IP>/Admin/Special/SSLAuth/index.php

La Special Area permette di effettuale le seguenti attività:

- caricamento di un nuovo certificato (.crt) di Certification Authority.
- caricamento di un nuovo certificato (.crt) per l'amministratore.
- effettuazione di un test di verifica di un certificato X509
- caricamento del certificato (.crt) di un profilo. Per una serie di ragioni, l'appliance potrebbe "conoscere" un profilo ma non avere registrato il suo certificato di autenticazione. Questo non costituisce un problema per l'operatività ma un fastidio perché alcuni dati non potranno essere mostrati dall'interfaccia
- abilitare la rinegoziazione "insicura" SSL (in caso di problemi di compatibilità con alcuni browser)

CA CETIFICATE UPLOAD.

L'appliance αPeS è in grado di gestire di Certification Authority di terze parti (ad esempio una propria CA aziendale interna). Si può quindi scegliere se ricorrere a certificati di terze parti oppure utilizzare i certificati forniti da Secure Edge srl, attraverso la relativa CA. Nel caso sia necessario caricare un ulteriore certificato di CA di terze parti è necessario selezionare l'opzione ***Authentication*** dalla barra dei menu di sinistra (Area

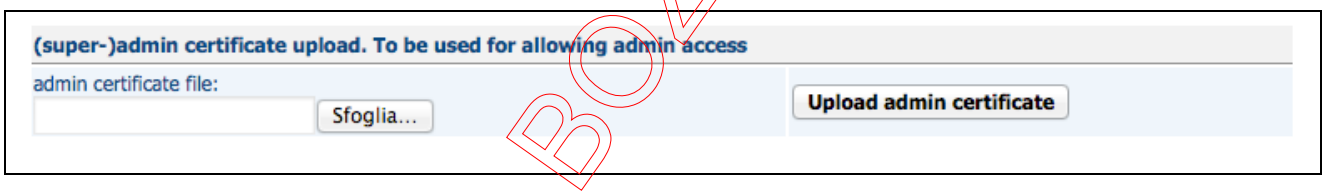
"Special"). Nella relativa pagina, è possibile visualizzare i dati relativi alla CA attualmente in uso ed eseguire il caricamento di un nuovo certificato pubblico di CA, come illustrato nell'immagine seguente:

Selezionare l'opportuno file .crt della CA che si intende importare, all'interno del riquadro "Upload CA *Certificate*"

Ogni nuovo certificato caricato comparirà nella lista sul box superiore.

ADMIN UPLOAD.

Tramite questo menu è inoltre possibile aggiornare il certificato dell'Amministratore dell'appliance, in caso di revoca o di scadenza. Ricordiamo che l'Amministratore è sempre un'unica persona. Non possono essere quindi caricati due certificati contemporaneamente. In questo caso, è sufficiente utilizzare il riquadro "Upload *admin certificate*", indicando, anche in questo caso, il percorso del file locale .crt relativo al nuovo Amministratore, come illustrato nella figura seguente:

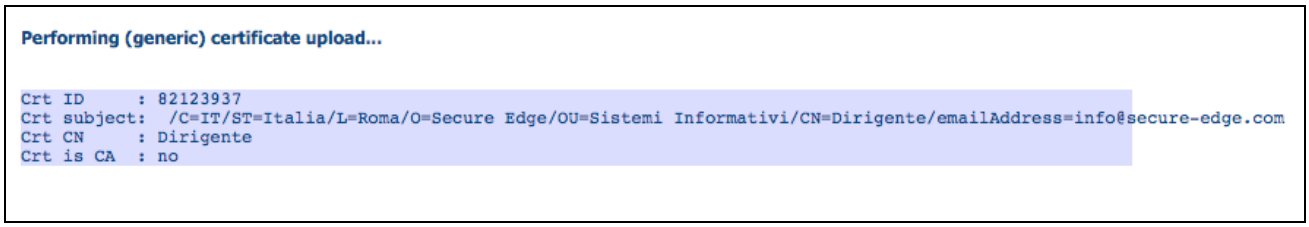


Le operazioni di caricamento di nuovi certificati (CA o Amministratore) comportano una momentanea interruzione, di 3-4 secondi, del servizio HTTPS.
L'ultimo certificato di Amministratore caricato sovrascrive sempre i precedenti.

CERTIFICATE TEST.

In alcuni casi, può risultare utile effettuare una verifica di funzionamento e visualizzare il contenuto di un certificato X509. Per operare questa verificare caricare un certificato (in formato "pem"). Per operare questo test, utilizzare il box denominato "*Certificate Test*", come illustrato nella figura seguente:

In caso di test effettuato con successo, verrà visualizzato il suo contenuto, come illustrato nella figura seguente:



I file relativi ai Certificati dei Profili devono essere in formato “pem”.

TOGGLE LEGACY INSECURE RENEGOTIATION

Questo bottone permette di abilitare o disabilitare la funzione **legacy insecure renegotiation** per consentire la rinegoziazione insicura SSL e risolvere alcuni problemi di compatibilità con i browser e con le librerie di colloquio SSL delle applicazioni. Qualora si presentassero problemi di accesso all’appliance da parte dei browser o delle applicazioni, si può provare ad abilitare la rinegoziazione insicura (portando tale valore su “On”) per verificare se il problema fosse legato agli strumenti in uso. Questa funzione è descritta nell’immagine seguente:

Il valore predefinito della rinegoziazione insicura è su “Off”

Signer Area

L’area “Signer” è dedicata esclusivamente all’accesso da parte dei Titolari dei Certificato, con apposito certificato SSL, così come definito dall’Amministratore nel relativo Profilo. Quest’area consente ai Titolari di svolgere le seguenti attività:

- *SC Status*: consente al Certificate Owner di verificare lo stato di funzionamento dei Certificato di firma a lui assegnati e di eseguirle l'attivazione o la disattivazione, nonché di verificare quali configurazioni siano associate ad ogni Certificato
- *Ceremony*: consente al Certificate Owner di inizializzare il proprio Certificato di firma, associando ad esso una Passphrase univoca
- *Assign / Revoke*: consente al Certificate Owner di assegnare o revoca l'associazione fra i Certificato di firma a lui assegnati e le relative Configurazioni
- *RL Tokens*: consente al Certificate Owner di gestire i Certificato a lui assegnati attraverso un dispositivo HSM
- *SCM Keys / Request*: consente al Certificate Owner di gestire le richieste di nuovi certificati da inserire direttamente sul Certificato assegnato dall'Amministratore, nonché consente al titolare della firma di modificare il PIN e il PUK associati al Certificato di firma
- *Auth Manager*: consente al Certificate Owner di aggiornare il proprio Certificato di accesso SSL, ovvero il Certificato assegnato al suo Profilo di Titolare.

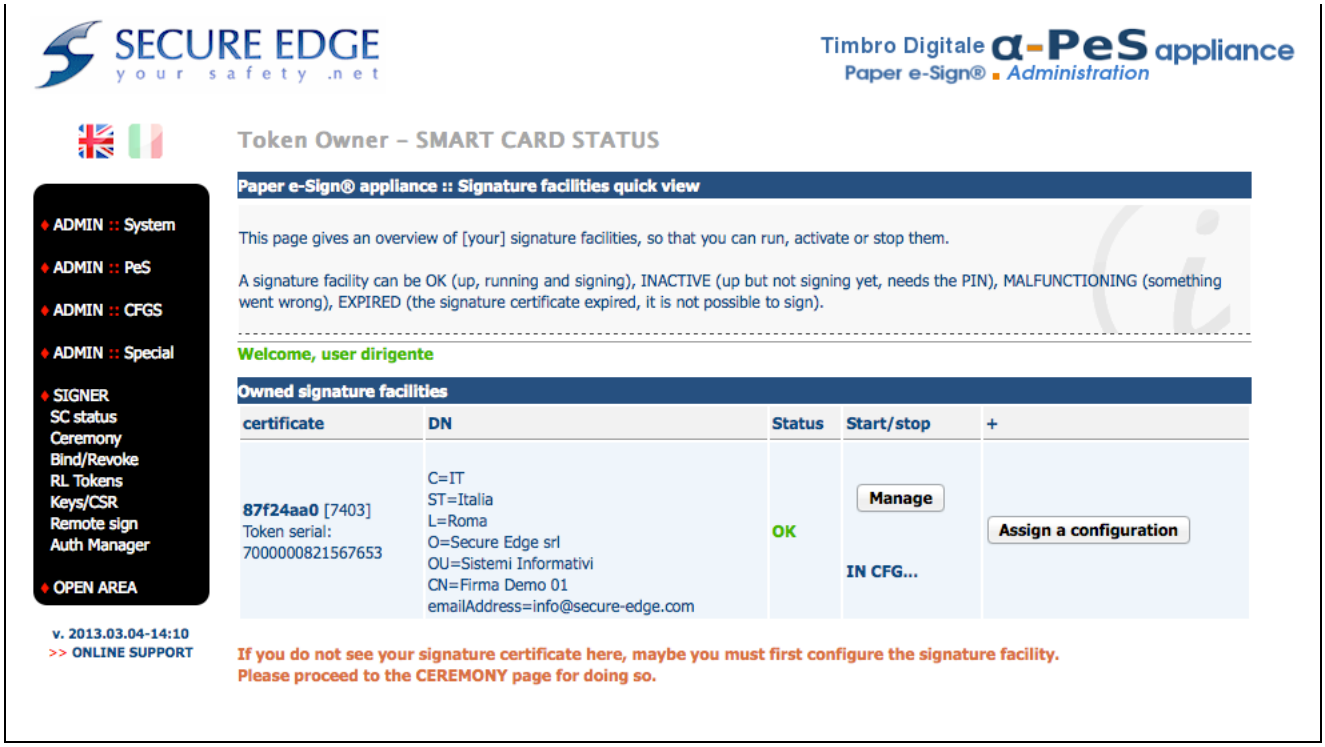
SC Status: Visualizzazione dello Stato dei Certificato assegnati al Titolare / attivazione della firma sul Certificato

Il Titolare del Certificato deve accedere dalla home page, all'area "*Smart Card Owner*", disponibile anche attraverso il seguente indirizzo URL:

https://<appliance IP>/ Admin/Profiles/SCInfo/quickview.php

Nel caso in cui non sia ancora stata eseguita alcuna Cerimonia (inizializzazione) di alcun Certificato, il Titolare visualizzerà la schermata illustrata nella figura seguente:

Qualora, invece, sia stata già eseguita correttamente una o più Cerimonie, il Titolare visualizzerà la schermata illustrata nella figura seguente:



Come illustrato nella pagina stessa, la pagina illustra lo stato di funzionamento del Certificato, che può assumere i seguenti valori:

- OK: certificato regolarmente attivo e in grado di firmare
- OFF: certificato regolarmente attivo, ma il cui demone di firma è "spento": è necessario che il Titolare del Certificato inserisca PIN e Passphrase per riattivare il demone di firma
- INACTIVE: certificato non ancora correttamente inizializzato: ripetere o procedere con la Cerimonia di inizializzazione
- MALFUNCTING: certificato che presenta un possibile problema, a livello elettrico, nella lettura; si consiglia, se possibile, di re-inserire il certificato nel lettore o, se il problema persistesse, di spostare il certificato in un lettore differente
- EXPIRED: certificato la cui validità è stata superata: non può essere utilizzato per firmare, necessita di essere sostituito

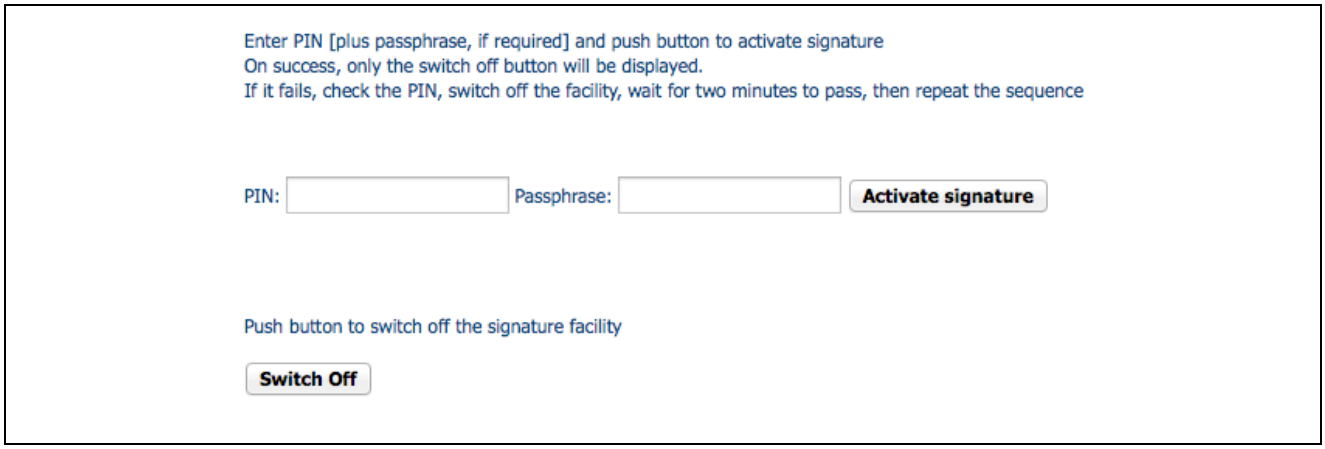
Per rendere operativo il certificato di firma, dopo averne effettuata la Cerimonia (inizializzazione) come descritto al paragrafo "Cermony", è necessario che il Titolare del Certificato ("Certificato Owner") ne esegua la successiva attivazione. In assenza di tale operazione il certificato di firma non potrà essere utilizzato dall'appliance αPeS per la generazione di Timbri.

Per eseguire questa operazione, il Titolare del Certificato deve accedere al menu "***SC Status***" . Cliccare quindi, all'interno della tabella "*Owned signature facilities*"sul tasto "*Manage*" relativo al Certificato (certificato di firma) che si desidera attivare, dallo stato iniziale di "Off", come illustrato nella figura seguente:

Verrà quindi visualizzata la seguente pagina, come illustrato di seguito:

Come sempre, nella parte superiore della pagina, vengono riportate nuovamente, per ulteriore controllo/garanzia le informazioni relative al certificato di firma, prima di eseguirne l'attivazione. Qualora tutto coincida, il Titolare può proseguire con l'attivazione, cliccando sul tasto "*Switch On*".

Verrà chiesto di inserire nuovamente il PIN di sblocco della Smart Card (o del dispositivo crittografico), nonché la pass-phrase inserita durante la procedura di Cerimonia (inizializzazione), come illustrato nella figura seguente:



Il titolare del Certificato, dopo aver inserito questi due parametri, deve cliccare sul tasto "*Activate Signature*".

Qualora l'operazione venga conclusa con successo, apparirà la scritta "***Activating signature... O:3.0.6:OK Checking facility status... THE FACILITY IS RUNNING AND THE SIGNATURE IS ACTIVE***" e il certificato verrà visualizzato in stato di "*Ok*" nella tabella della pagina "*Smart Card Status*", come illustrato nell'immagine seguente:

Nel caso in cui, per un errore di digitazione, il PIN o la pass-phrase non coincidessero a quanto inserito al momento della procedura di Cerimonia, comparirà il seguente messaggio di errore: "***ERROR: PIN (or passphrase) is not the same you entered the last time. Try again***". Questo errore non comporta la possibilità di un eventuale blocco di funzionamento della smart card (o del dispositivo crittografico).Il Titolare dovrà quindi ripetere l'operazione.

A questo punto il certificato di firma è pronto e funzionante e necessita, unicamente, di essere associato all'opportuna Configurazione.

Infine per conoscere le Configurazioni associate al Certificato, è sufficiente che il Titolare clicchi sul link "*used by*": la lista delle Configurazioni associate verrà visualizzata in una nuova finestra.

Ceremony: inizializzazione del Certificato di firma

Per rendere operativa la firma presente all'interno della Smart Card, è necessario che il Titolare del Certificato ("Certificato Owner") acceda alla propria area di amministrazione ed effettui l'inizializzazione o "cerimonia", in modo da associare al PIN una propria pass-phrase univoca, di almeno 20 caratteri, che andrà poi re-inserita successivamente, per confermare ogni ulteriore operazione.

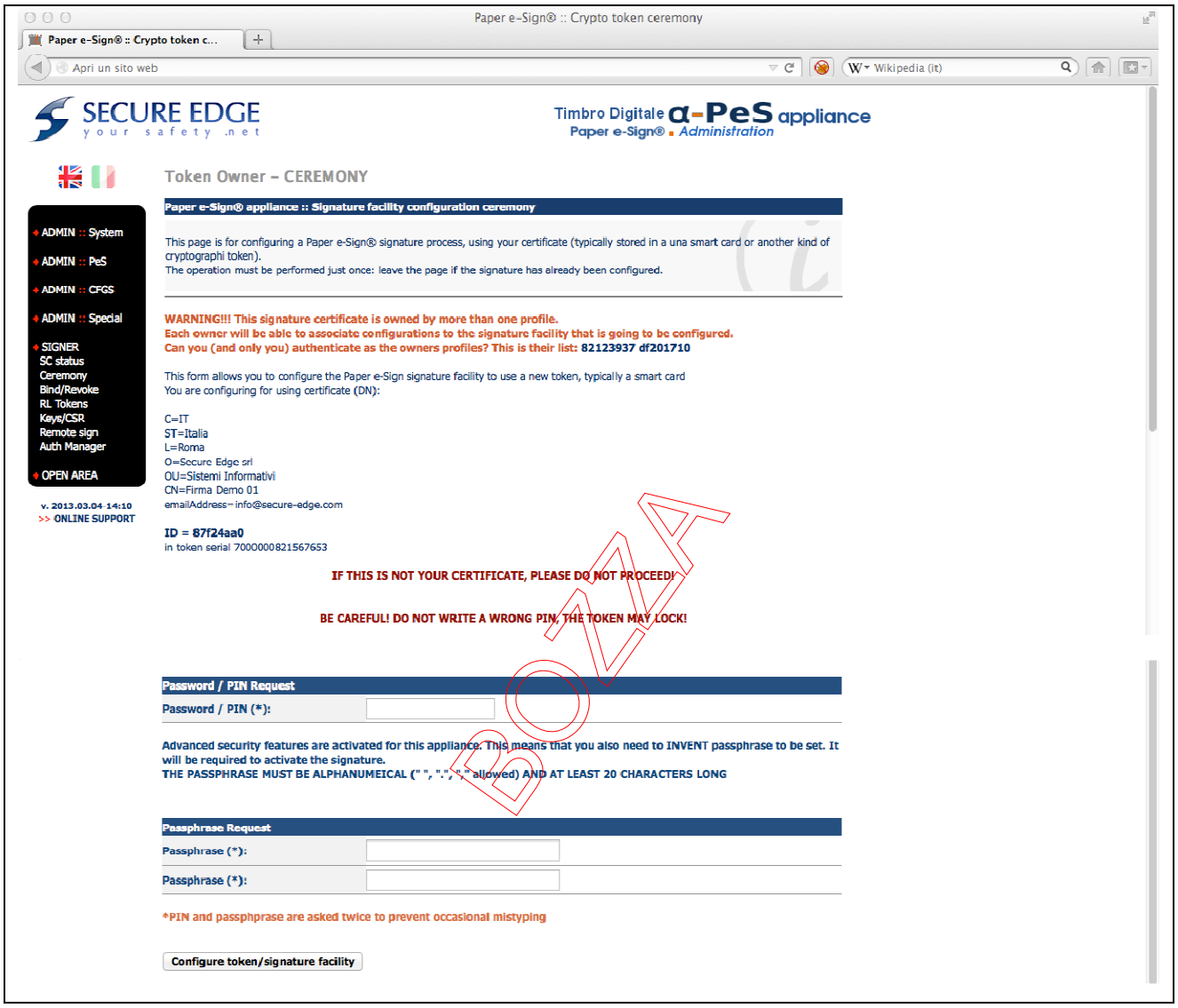
Le operazioni che seguono devono essere svolte unicamente dal titolare del certificato di firma, che dovrà accedere con un proprio browser web, utilizzando il profilo di "Certificate Owner" e quindi il relativo certificato, precedentemente caricato dall'amministratore. Tale certificato può essere importato all'interno del browser oppure inserito all'interno di un apposito dispositivo crittografico USB (scelta consigliata)

Attraverso il menu "Ceremony" è anche possibile modificare il PIN associato alla smart card / token crittografico; la modifica del PIN deve essere eseguita prima dell'esecuzione della Cerimonia

Per effettuare la Cerimonia, il Titolare del Certificato deve selezionare il menu "**Ceremony**" dell'area "***Signer***". Verrà quindi visualizzata la pagina illustrata nella seguente figura:

In questa pagina vengono presentati tutti i Certificato di firma che l'Amministratore ha assegnato al Titolare. In questa tabella non vengono effettuate distinzioni sulla tipologia di Certificato (ad esempio Oberthur,

Incrypto 34v2 ecc…): tutti i Certificato assegnati vengono visualizzati. Il Titolare deve cliccare sul tasto "*Configure this token (ceremony)*" relativo al Certificato di cui intende effettuare la Cerimonia, per poter procedere alla sua inizializzazione. Si accedere quindi alla pagina di esecuzione della Cerimonia vera e propria illustrata nella figura seguente:



Nella parte superiore della pagina vengono riportate nuovamente, per ulteriore controllo/garanzia le informazioni relative al certificato di firma per il quale sta per essere eseguita la cerimonia. Qualora tutto coincida, il Titolare può proseguire con la Cerimonia e quindi può inserire, al riparo da sguardi indiscreti, il PIN di sblocco della Smart Card (o dispositivo di crittografia in cui è contenuto il certificato), comunicato dal fornitore della medesima (ad esempio "Actalis" o "Aruba") all'interno della tabella "Password / PIN request".

Qualora si inserisca un PIN errato per più di 3 volte consecutive, la Smart Card verrà automaticamente bloccata e risulterà impossibile proseguire questa operazione! In questa situazione sarà necessario effettuare lo sblocco della smart card attraverso apposito software di amministrazione, disponibile in genere sul sito

web del fornitore della smart card medesima, utilizzando il relativo codice PUK. Tale procedura è descritta più avanti in questo paragrafo. Qualora venga ulteriormente inserito in modo errato il codice PUK per più di 10 volte, la smart card risulterà definitivamente bloccata e sarà necessario procedere alla richiesta di una nuova smart card.

Quindi il Titolare del Certificato deve inserire una pass-phrase di sua fiducia di almeno 20 caratteri, all'interno della tabella "*Passphrase Request*". Infine premere il tasto "*Configure token / signature facility*" per completare il processo di inizializzazione.

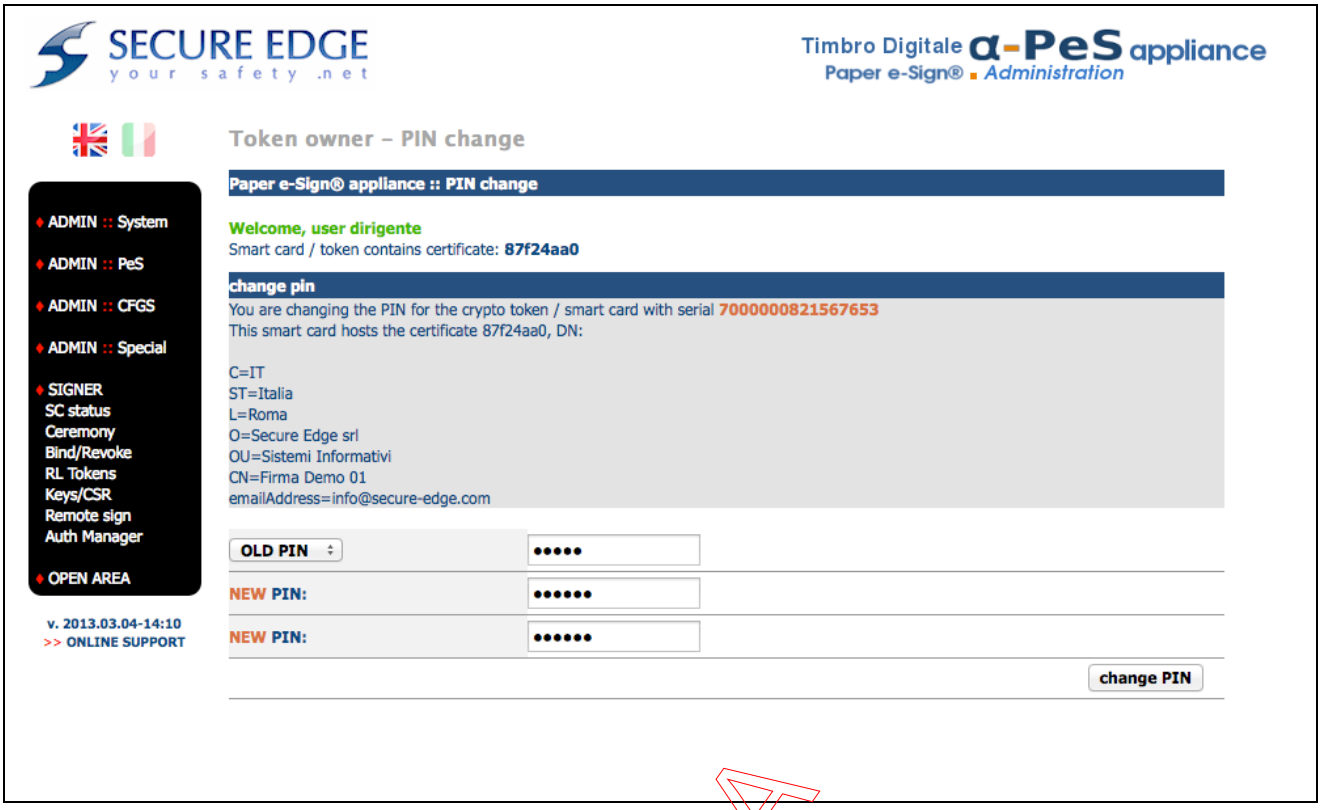
Nella scelta della pass-phrase si consiglia di inserire caratteri maiuscoli, minuscoli e numeri.

Qualora l'operazione di inizializzazione sia completata con successo, ovvero sia stato correttamente inserito il PIN, e sia stata confermata una pass-phrase valida, comparirà il seguente messaggio di conferma: "***checking PIN...OK OK, the system is configured for the new certificate".***

In caso non coincedesse il PIN inserito con quello assegnato alla smart card (o dispositivo crittografico), comparirà il seguente messaggio di errore: "***SORRY, the PIN check failed, cannot accept this configuration. BE CAREFUL! You may lock your certificato if you mistake the PIN too many times!***". La procedura di Cerimonia andrà ripetuta, e il Titolare del Certificato dovrà cliccare nuovamente sul menù "***Ceremony***" dalla barra laterale sinistra.

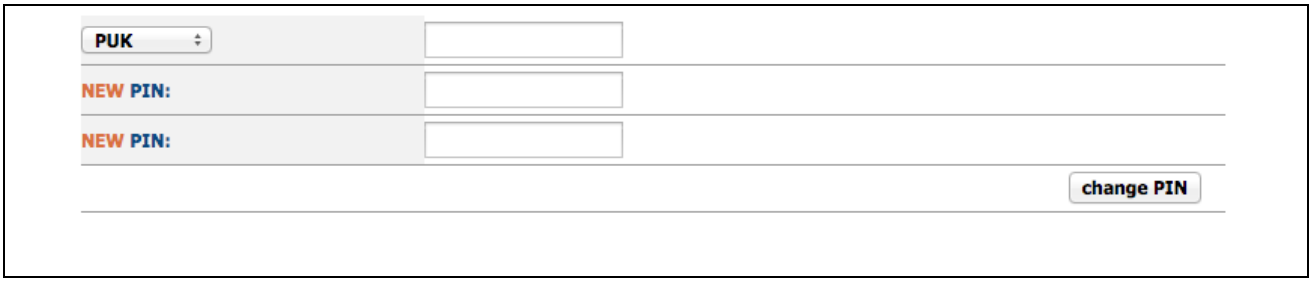
In caso non coincidesse la Passphrase inserita (ovvero la Passphrase inserita nel campo superiore fosse differente da quella inseita nel campo inferiore della tabella "*Passphrase Request*") comparirà il seguente messaggio di errore: "***ERROR: entered passphrases do not match***". La procedura di Cerimonia andrà ripetuta, e il Titolare del Certificato dovrà cliccare nuovamente sul menù "Ceremony" dalla barra laterale sinistra. Questo errore non comporta la possibilità di un eventuale blocco di funzionamento della smart card (o del dispositivo crittografico).

Nel caso il titolare, per maggiore sicurezza, desideri eseguire la modifica/aggiornamento del PIN, può eseguire questa operazione cliccando sul tasto "change PIN" nella pagina principale, come illustrato in precedenza. Comparirà quindi la pagina illustrata di seguito:



Come illustrato nell'immagine deve essere inserito il PIN precedente e deve essere inserito il nuovo PIN, confermando tale inserimento una seconda volta; quindi cliccare sul tasto "Change PIN". In caso tutti i valori coincidano, comparirà il messaggio "***PIN successfully changed, record the new one!...***"

Qualora sia necessario procedere allo sblocco di una Smart card, a causa di un errato inserimento del PIN per più di tre volte nell'operazione di Cerimonia, selezionare dal menu a tendina di questa pagina il parametro "PUK", come illustrato di seguito:



Inserire quindi il PUK e quindi inserire due volte un nuovo PIN e confermare l'operazione con il tasto "*Change PIN*". Questa operazione consente di avere un nuovo PIN e quindi di poter utilizzare nuovamente la Smart card.

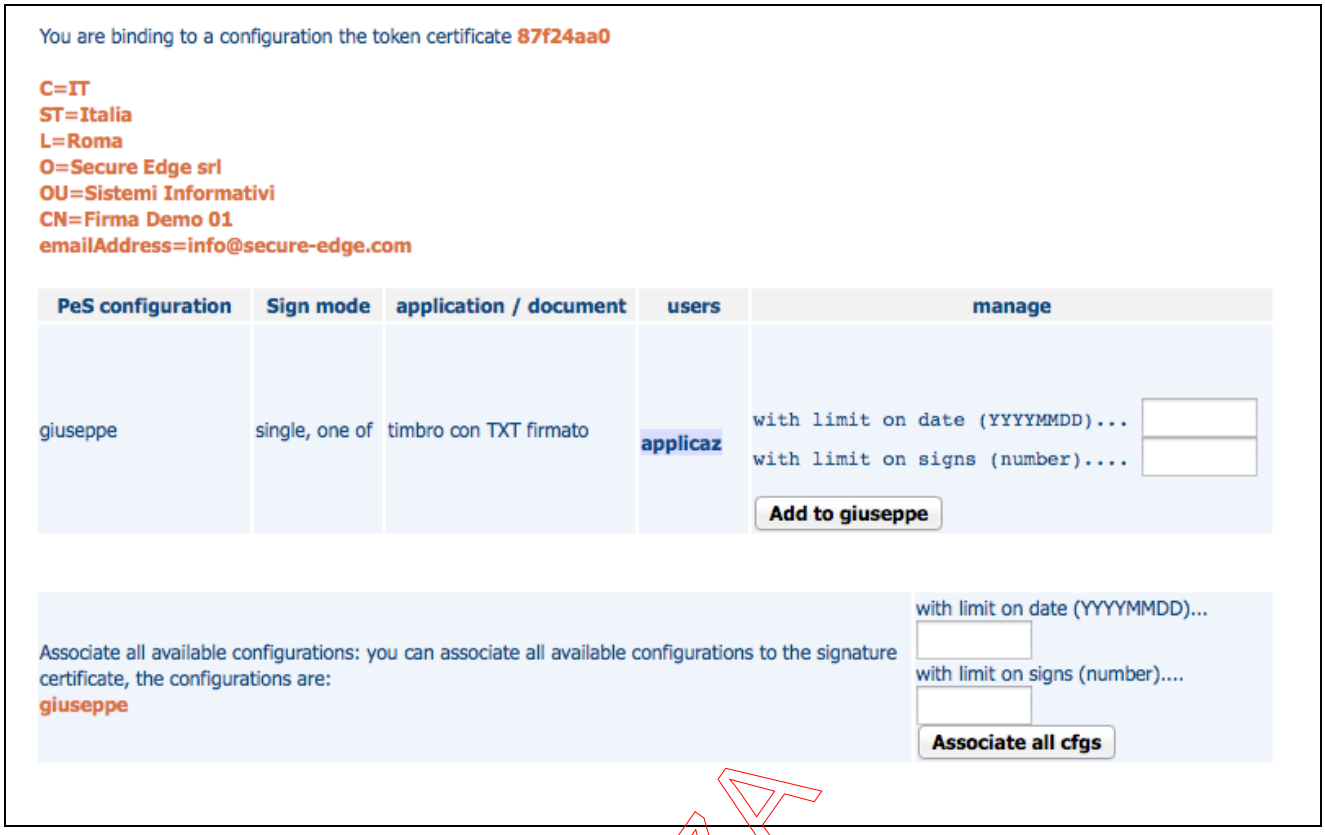
Assign/Revoke: assegnazione – revoca di un Certificato ad una o più Configurazioni

Per completare la configurazione del gateway di firma è necessario associare la firma, all'interno della Smart Card (o del dispositivo crittografico) alla relativa Configurazione, secondo la preassociazione effettuata dall'Amministratore. Questa operazione deve essere svolta dal Titolare del Certificato. Accedere quindi al

menu “***Bind / Revoke***” e selezionare, dalla seguente tabella “*Signature facilities management*”, la riga contenente il certificato abilitato al precedente Passo 8 (verificare sempre la corrispondenza dell’ID del certificato ed il relativo Distinguished Name) come illustrato nella seguente figura:

(nel caso illustrato in questa figura non sono presenti Certificati già associati dal Titolare, i quali comparirebbero nella tabella “Assignment of certificato to Paper e-Sign configurations”)

Cliccare quindi sul tasto “*Bind to PeS config…*” nella riga della tabella relativa al certificato per il quale si deve completare la procedura di associazione alla Configurazione. Verrà visualizzata la finestra illustrata nella seguente illustrazione:



In quest'ultima pagina, vengono sempre visualizzate (per ulteriore controllo) le informazioni relative all'ID del certificato di firma che si sta associando alla configurazione, con i principali dati dati relativi agli scopi del certificato medesimo. La tabella sottostante riepiloga il nome della configurazione a cui si sta associando il certificato di firma, la sua descrizione sintetica inserita dall'Amministratore, nonché il nome del Profilo dell'Applicazione associata alla configurazione (sempre a cura dell'Amministratore). Il Titolare del Certificato dovrà cliccare sul tasto "*Add to [configuration_name]*" per procedere al completamento dell'associazione. Qualora il Titolare del Certificato desiderasse, per motivi di gestione, limitare la validità di questa associazione potrà inserire una limitazione temporale per la validità del processo di firma (campo "*with limit on sings*") e/o una limitazione al numero di firme che possono essere effettuate (campo "*with limit on date*"). Questi parametri sono del tutto indipendenti dal numero di firme previste dalla licenza d'uso globale oppure dalla validità temporale del certificato presente all'interno della Smart Card (o infrastruttura di crittografia). Qualora il Titolare del Certificato non specifichi alcun parametro, resteranno validi il numero di firme previste dalla licenza e la scadenza temporale del certificato, secondo quanto previsto al momento del rilascio da parte della relativa Certification Authority.

L'operazione viene confermata dal seguente messaggio:

"***performed binding of signature certificate [Certificate_ID] to configuration [Configuration_name]***

OK: signature [Certificate_ID] now associated with configuration [Configuration_name]"

Non è possibile procedere all'associazione fra Configurazione e Certificato da parte del Titolare qualora la Configurazione non abbia già assegnato un Profilo dell'Applicazione,. Accettarsi quindi che l'Amministrazione abbia già eseguito questo passaggio; in caso contrario comparirà il messaggio di avviso

"***CFG has no OWNERS.CANNOT associate signature***".

Qualora siano presenti due o più Configurazioni che il Titolare di Firma dovesse associare al Certificato, per sua comodità d'uso può utilizzare la tabella illustrata nella figura seguente, la quale si trova in fondo alla pagina:

Cliccando sul pulsate "*Associate to all cfgs*" il Certificato di firma viene automaticamente associato a tutte le configurazioni indicate in colore arancio. Similarmente a quanto previsto per la singola configurazione, anche in questo caso è possibile applicare le stesse limitazioni numeriche e/o temporali a questa associazione multipla. Gli stessi parametri di limitazione saranno automaticamente applicati a tutte le Configurazioni. E' quindi evidente che, in caso si desiderasse applicare delle limitazioni differenti per ogni singola Configurazione, il Titolare del Certificato dovrà procedere singolarmente ad indicare questi parametri e quindi ad operare singolarmente le associazioni una alla volta.

Terminata questa procedura, l'appliance αPeS è pronto per ricevere i documenti da sottoporre al processo di firma digitale; ciò è confermato dall'inserimento della Configurazione all'interno della tabella "*Assignment of certificato to Paper e-Sign configurations*" come illustrato nella figura seguente:

Existing assignments of signatures to Paper e-Sign configurations

PeS config	Signature crt ID	Signature Certificate	Limits	Manage
giuseppe timbro con TXT firmato signature type: single, one of	**87f24aa0**	C=IT ST=Italia L=Roma O=Secure Edge srl OU=Sistemi Informativi CN=Firma Demo 01 emailAddress=info@secure-edge.com	max 15000 signatures remaining: 15000 till date 2014-09-01	**Revoke assignment**

(nel caso specifico è presente anche l'indicazione di una limitazione temporanea a 15000 timbri ed una scadenza della validità di questa associazione dal 1/09/2014)

Come si può notare, il titolare del Certificato può, in ogni momento lo ritenesse opportuno, bloccare il meccanismo di firma, cliccando sul tasto "*Revoke assignment.*". In questo modo viene revocata l'associazione fra il Certificato di firma e la Configurazione. Tuttavia il Certificato mantiene il completo stato di validità e il Titolare non ha necessità di reinseirire alcun PIN e Pass-phrase. L'operarazione di revoca dell'assegnazione viene confermata dalla presenza del seguente messaggio:

Proceeding with deassignment...

Completed deassignment of signature facility from [Configuration_name]

RL Tokens: attivazione Certificato all'interno di un HSM

Qualora il certificato di firma sia contenuto all'interno di un dispositivo crittografico HSM "Luna SA", il Titolare del Certificato deve utilizzare il Menù "*RL Tokens*" all'interno dell'area "*Certificato Owner*".

Keys / CSR: caricamento del certificato di firma all'interno del Certificato e modifica dei pametri di PIN e PUK del Certificato

Questa funzione è orientata alla gestione dei Certificato di firma in particolare tramite il dispositivo "Multi SSCD Box"

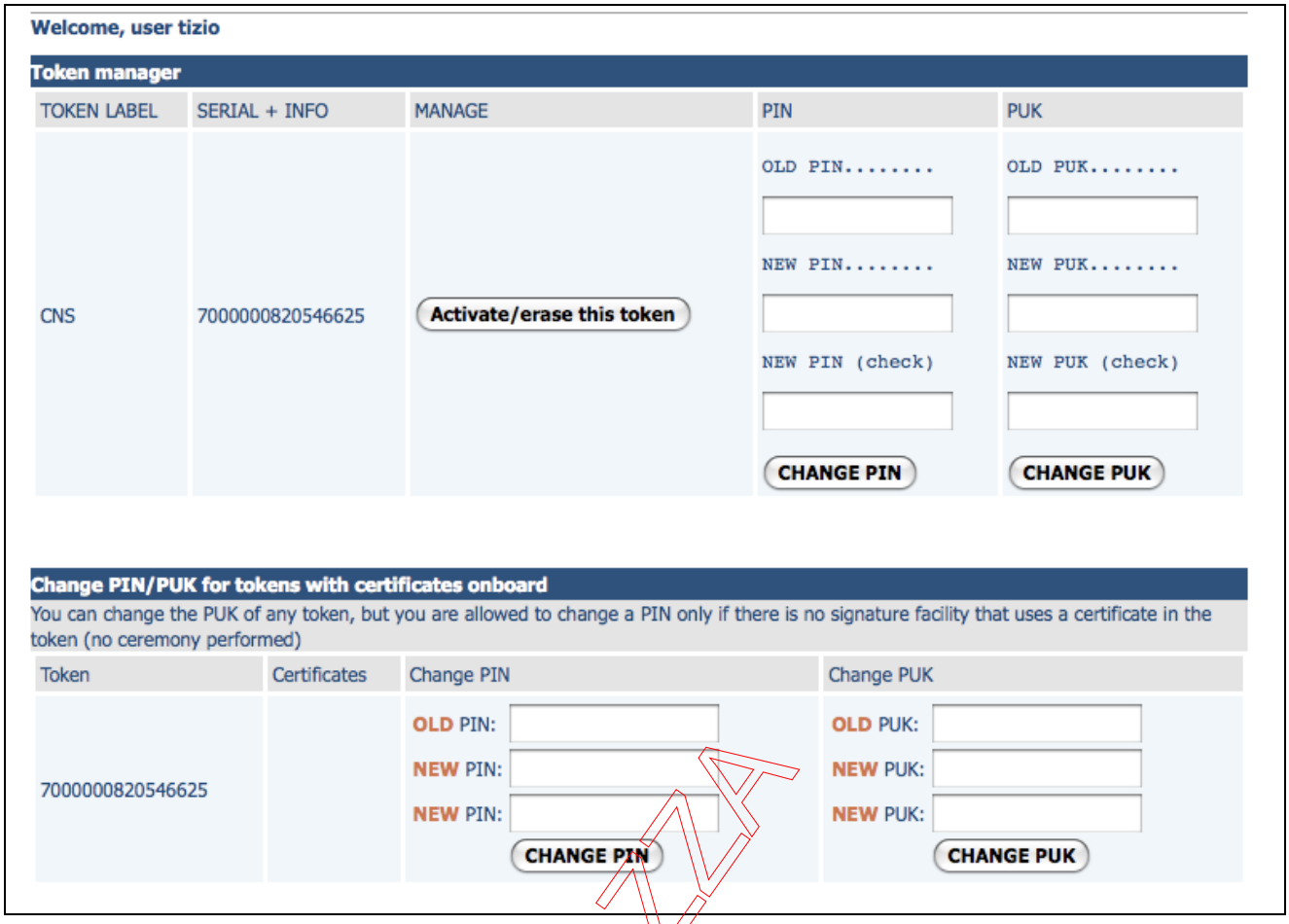
Questa funzione è accessibile unicamente nel caso in cui l'Amministratore abbia già, preventivamente, assegnato un Certificato "vuoto" al relativo Titolare, attraverso la funzione "***SC Manager***"

Quando è necessario che il Titolare gestisca direttamente un Certificato di firma, è necessario che egli effettui le seguenti operazioni preliminari:

- Aggiornamento dei parametri del PIN e del PUK per il Certificato
- Richiesta di certificato (da caricare successivamente nela Smart Card / token)

Al termine di queste operazioni preliminari il Titolare potrà attivare il certificato di firma all'interno del Certificato e poter quindi gestire tale certificato per la successiva inizializzazione ("Cerimomnia") e assegnazione alle relative Configurazioni.

Per effettuare queste operazioni, è a disposizione il Menù "***SCM Keys / Request***" dell'area "***Certificato Owner***". Quando il titolare vi accede, visualizzerà una pagina illustrata come segue:

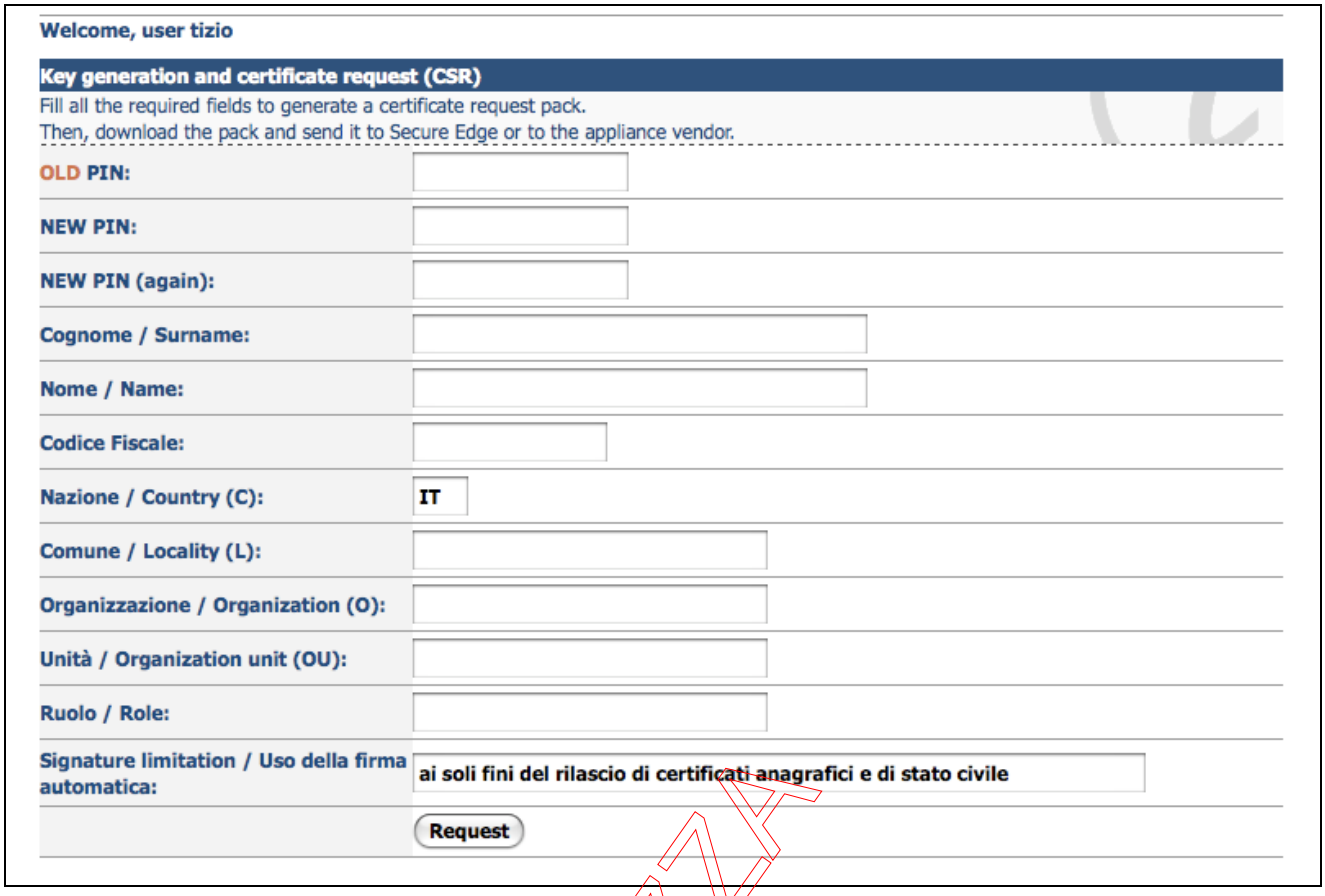


Tramite la tabella "*Token Manager*" il Titolare potrà effettuare, innanzitutto, l'aggiornamento dei parametric di PIN e PUK (uno alla volta) confermando la richiesta di modifica tramite i relativi tasti "*Change PIN*" e "*Change PUK*".

I valori di PIN e PUK possono anche coincidere, ma non possono essere coincidenti ai valori pregressi (ovvero presenti nei campi "Old PIN" e "Old PUK").

Si ricorda al Titolare che, in genere, sono ammissimibili massimo 3 tentativi nel cambio del PIN e 10 tentativi nel cambio del PUK, superati i quali il Certificato si bloccherà e non potrà più essere utilizzato!

Effettuato l'aggiornamento del PIN e del PUK, il Titolare deve cliccare sul tasto "*Activate / erase this certificato*" e accederà alla pagina per la compilazione del modulo di richiesta del certificato, illustrata nella figura seguente:



Ovviamente il Titolare dovrà compilare tutti i campi presenti nel form. All'interno del campo "*Old PIN*" dovrà inserire il PIN aggiornato al precedente passaggio: tramite questa procedura si otterrà un terzo cambiamento del PIN. Al termine della compilazione il Titolare deve cliccare sul tasto "*Request*" e attendere alcuni secondi affinché l'appliance αPeS completi la creazione del pacchetto di richiesta del Certificato (CSR). Il titolare dovrà quindi scaricare il pacchetto e inviarlo tramite posta elettronica a Secure Edge srl per poter, successivamente, ottenere il pacchetto definitivo di attivazione del Certificato.

Auth Manager: aggiornamento di un Certificato assegnato ad un Profilo di Titolare

Qualora il Titolare si trovi ad avere un certificato prossimo alla scadenza o già scaduto, può direttamente eseguire l'aggiornamento utilizzando il menù "*Auth Manager*" dall'area "*Signer*". Come illustrato nella figura seguente, il Titolare dovrà caricare, attraverso il form nella tabella "*Set new Certificate*", il file relativo al nuovo certificato (in formato "pem") e confermare con il tasto "*Change Certificate*":

L'operazione viene confermata con il messaggio: "***OK, change performed. This page does not require authentication, this is why you can see it. Now set your browser to use the new certificate***"

Open Area: Stato del sistema

All'interno dei menu di amministrazione, l'area "***Open***" consente di accedere alla visualizzazione rapida di alcune informazioni riepilogative e poter eseguire alcuni controlli sui meccanismi di funzionamento.

Le informazioni visualizzate sono:

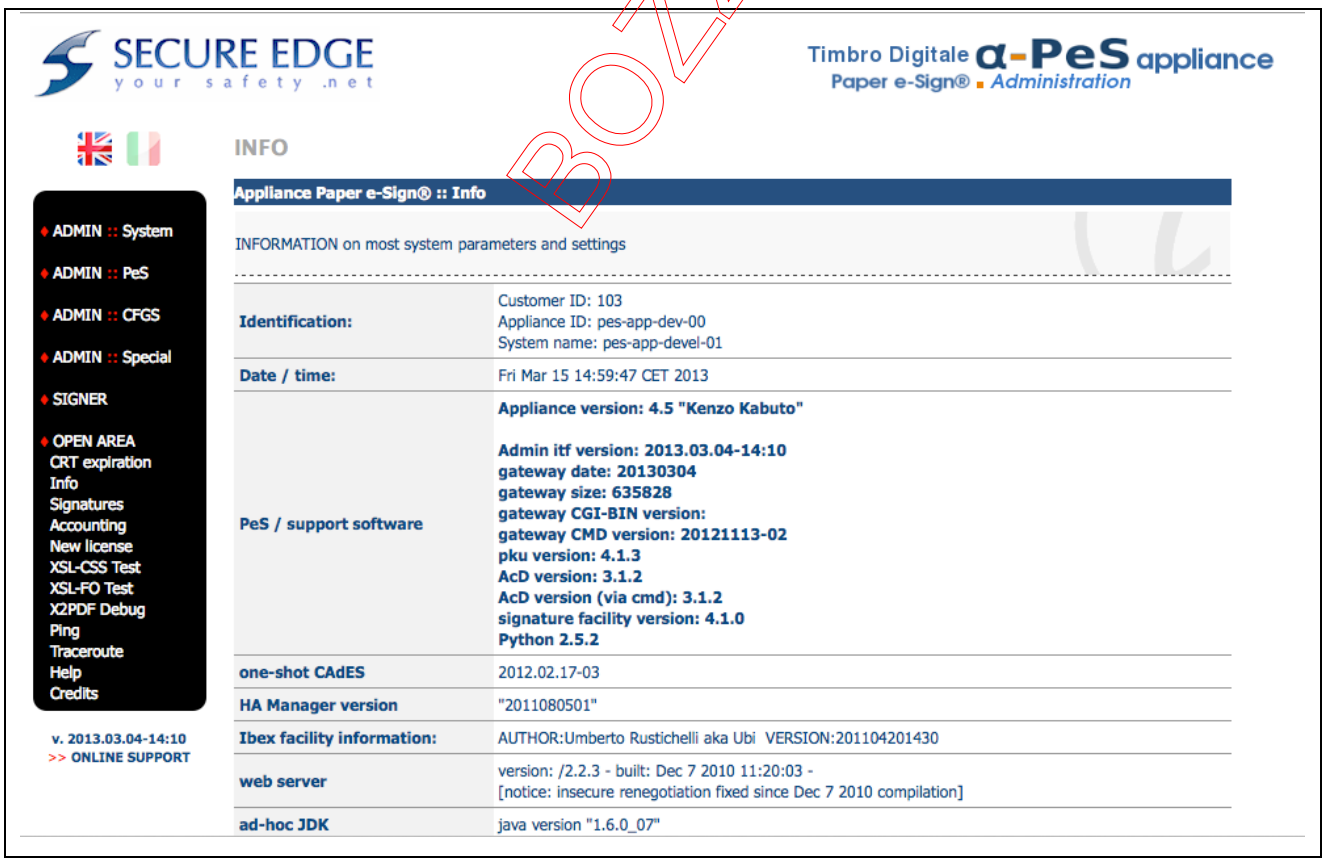
- **CRT expiration:** la visualizzazione dei certificati di comunicazione SSL (utile per visualizzare la loro scadenza);
- **Info:** Informazioni sul sistema
- **Signature:** indica le caratteristiche dei certificati di firma all'interno dei Certificato (solo i certificati inizializzati dai rispettivi Titolari)
- **Accounting:** il numero di firme a disposizione,
- **New license:** l'aggiornamento dei file di licenza;
- **XSL-CSS Test:** test di funzionamento del timbro (in caso sia necessario generare un PDF a partire da un template XML-CSS)
- **XSL-FO Test:** test di funzionamento del timbro (in caso sia necessario generare un PDF a partire da un template XML con engine FO)
- **X2PDFDebug:** log delle ultime transazioni per la generazione di un PDF
- **Ping:** l'esecuzione di semplici test di funzionamenti, quali "ping"
- **Traceroute:** l'esecuzione di semplici test di funzionamenti, quali "traceroute"
- **Help:** l'accesso alla pagina sintetica di aiuto on-line

Info: Informazioni sullo stato del sistema

Cliccando sul tasto "**Info**" dal menu laterale, si possono ottenere una serie di informazioni circa:

- identificazione della macchina (Customer ID / Appliance ID)
- versione del software αPeS
- dati identificativi del certificato dell'amministratore (Admin Cert)
- dati identificativi del certificato della Certification Authority interna
- data e orario di sistema
- indirizzi IP delle interfacce di rete;
- visualizzazione della tabella di routing;
- visualizzazione delle tabelle dei server DNS impostati

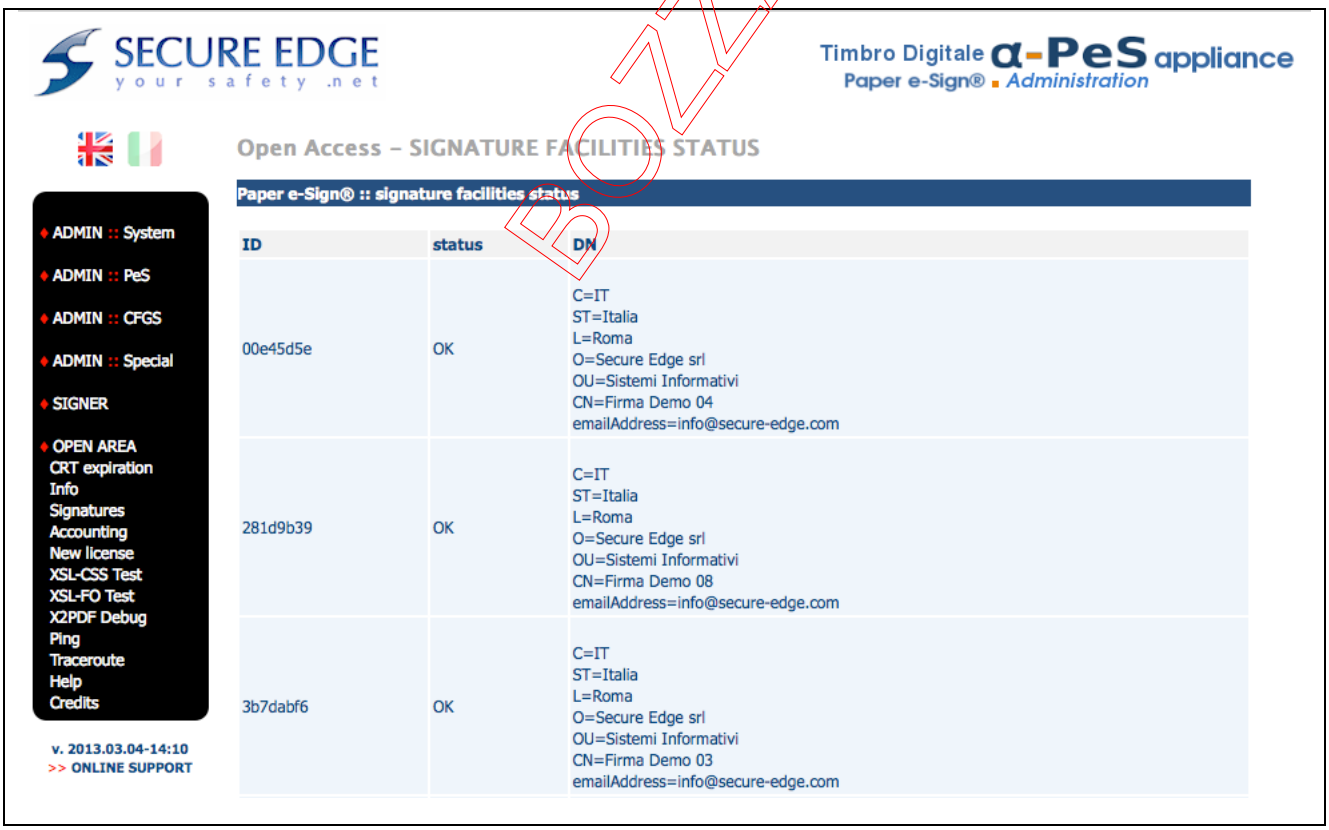
Di seguito si riporta un estratto del contenuto della pagina di riepilogo informativo:



Signature: Informazioni sullo stato dei Certificato di firma

Per visualizzare lo stato di funzionamento di un Certificato (certificato) di firma automatica all'interno di una smart card oppure di un altro dispositivo crittografico, è possibile utilizzare la funzione "***Signature***". Attraverso questa funzione, vengono visualizzate tutti ti Certificato di firma collegati all'appliance, i quali possono avere uno tra i seguenti cinque stati:

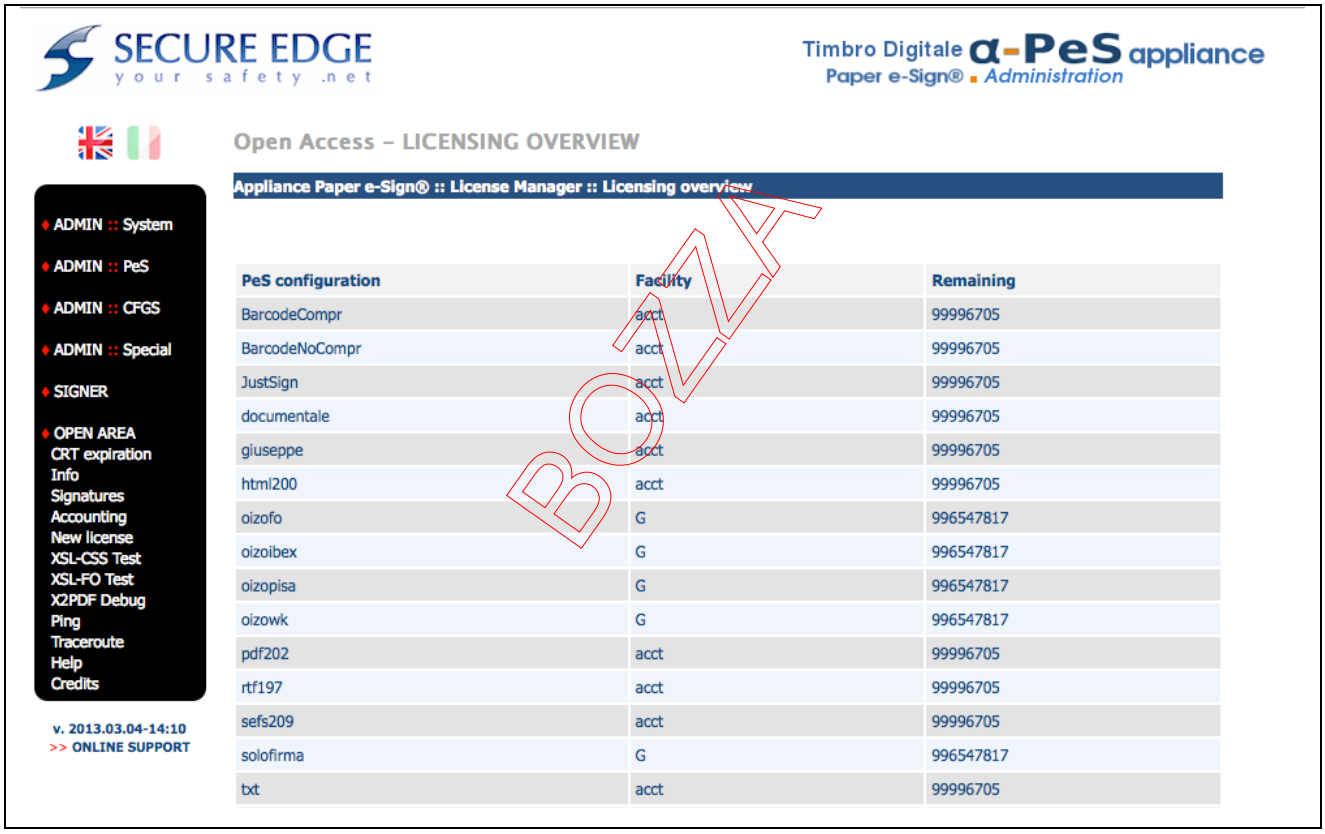
- OK: certificato regolarmente attivo e in grado di firmare
- OFF: certificato regolarmente attivo, ma il cui demone di firma è "spento": è necessario che il Titolare del Certificato inserisca PIN e Passphrase per riattivare il demone di firma
- INACTIVE: certificato non ancora correttamente inizializzato: ripetere o procedere con la Cerimonia di inizializzazione
- MALFUNCTING: certificato che presenta un possibile problema, a livello elettrico, nella lettura; si consiglia, se possibile, di re-inserire il certificato nel lettore o, se il problema persistesse, di spostare il certificato in un lettore differente
- EXPIRED: certificato la cui validità è stata superata: non può essere utilizzato per firmare, necessita di essere sostituito)



In caso si riscontri un problema sui lettori, darne immediata comunicazione a Secure Edge srl per la pianificazione delle successive attività di manutenzione

Accaunting: Timbri disponibili

Questa funzione permette di visualizzare il numero di timbri da emettere per ciascuna configurazione. L'indicazione potrebbe trarre in inganno in quanto il numero di timbri ancora emettibile è associato al parametro Facility che può essere condiviso tra più configurazioni portando, di fatto, ad indicare un numero di timbri totali disponibili falsato. Nell'esempio sottostante il numero totale di timbri è 99996705 per la Facility "*acct*" (condivisa da 11 Configurazioni), mentre è di 996547817 per la Facility "*G*" (condivisa da 5 Configurazioni)



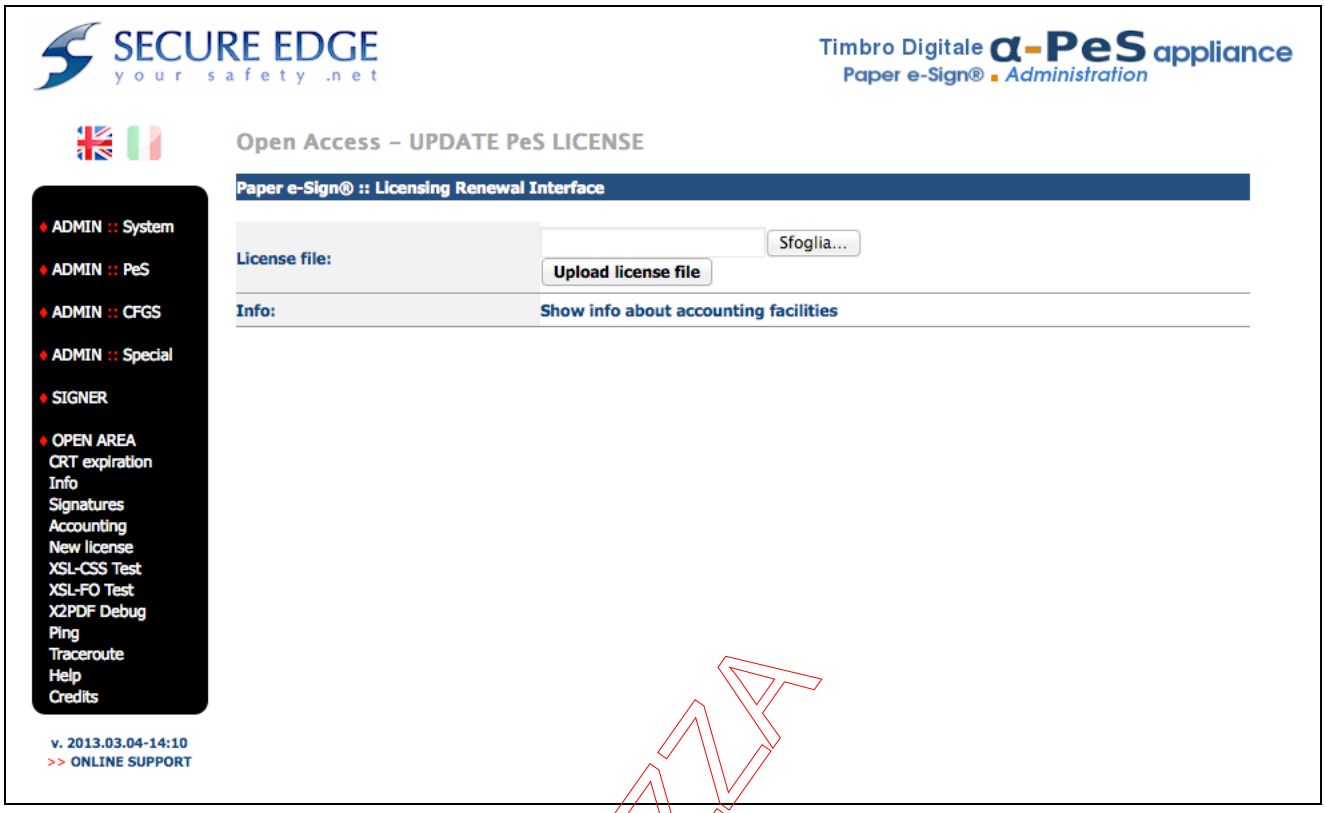
PeS configuration	Facility	Remaining
BarcodeCompr	acct	99996705
BarcodeNoCompr	acct	99996705
JustSign	acct	99996705
documentale	acct	99996705
giuseppe	acct	99996705
html200	acct	99996705
oizofo	G	996547817
oizoibex	G	996547817
oizopisa	G	996547817
oizowk	G	996547817
pdf202	acct	99996705
rtf197	acct	99996705
sefs209	acct	99996705
solofirma	G	996547817
txt	acct	99996705

Qualora il valore del parametro "facility" sia impostato a "G" ciò indica una licenza illimitata per la configurazione a cui è assegnata. La licenza illimitata visualizza un numero di timbri rimanenti molto grande

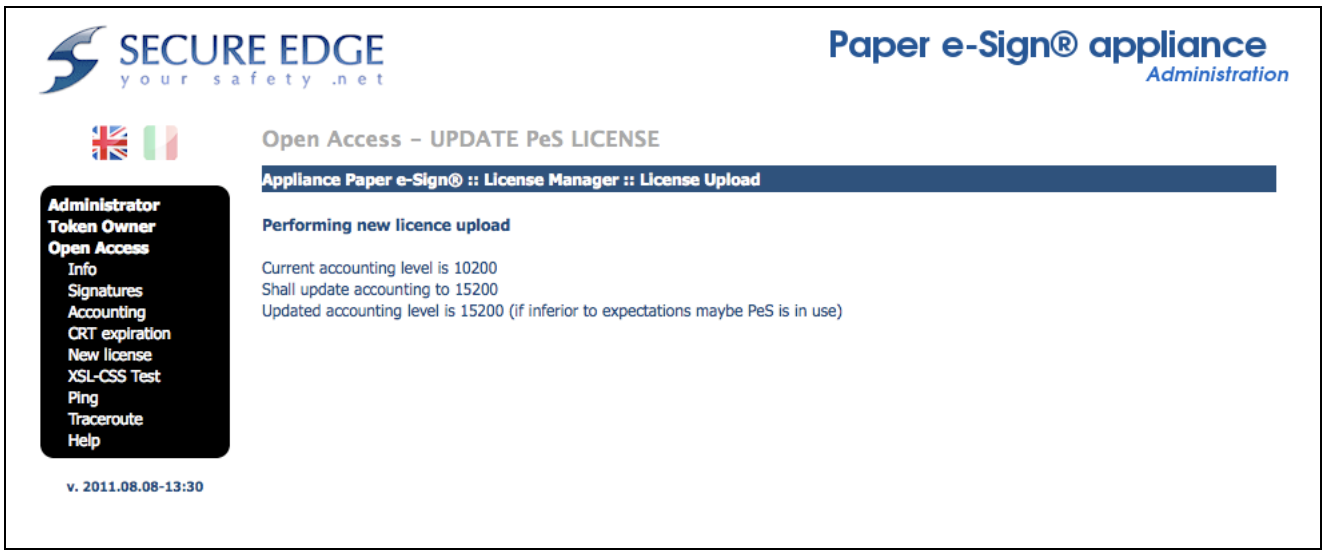
New license: Aggiornamento e gestione licenze

Qualora il numero di timbri sia in fase di esaurimento, è possibile richiedere a Secure Edge srl il rilascio di una nuova licenza per l'estensione del servizio. Il file di licenza è in genere fornito in formato ".dat" e può essere separato su due file. Ricevuti i file è necessario importarli sull'appiliance: questa operazione,

attraverso il menu "***New License***" presente sulla barra laterale destra. Viene quindi visualizzata la pagina, come illustrato nella seguente figura:



Al termine del caricamento della nuova licenza, viene visualizzato il nuovo numero di timbri consentito, come illustrato nella seguente figura (in particolare è presente il messaggio di conferma "*Performing new license upload*"):



Per conoscere il numero di timbri utilizzati per ciascuna configurazione è possibile utilizzare, dal menu a sinistra, l'opzione "***Accounting***".

Ogni file di licenza (o coppia di file di licenza) può essere caricato una volta soltanto. In caso si tenti usare lo stesso file di licenza più volte comparirà il messaggio "***Sorry, this license has already been used***"

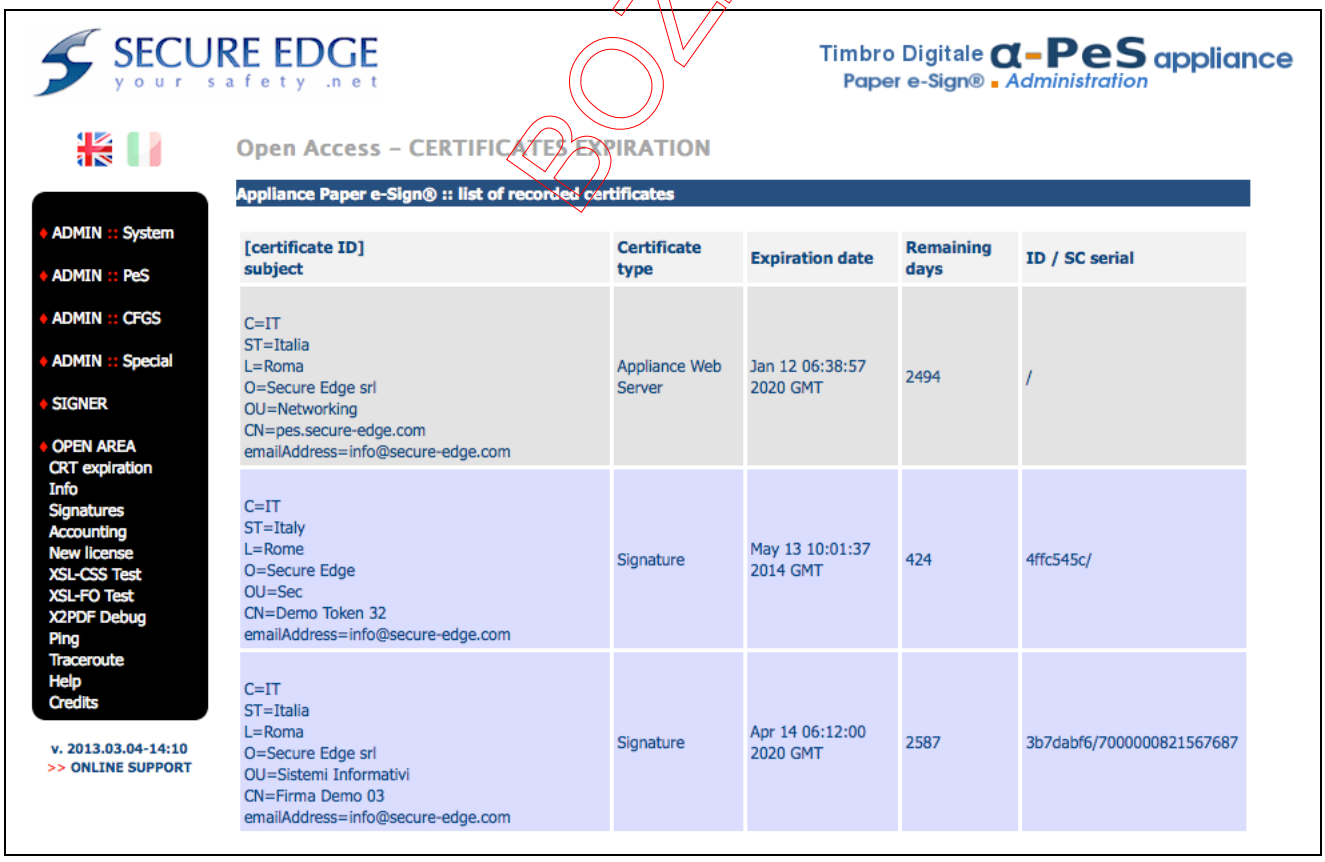
CRT expiration: Informazioni sul la scadenza dei certificati SSL

Questa funzione permette di visualizzare i certificati presenti sull'appliance suddivisi per gruppi ed ordinati secondo il numero di giorni mancanti alla scadenza con quelli in scadenza per primi.

I gruppi di certificati sono:

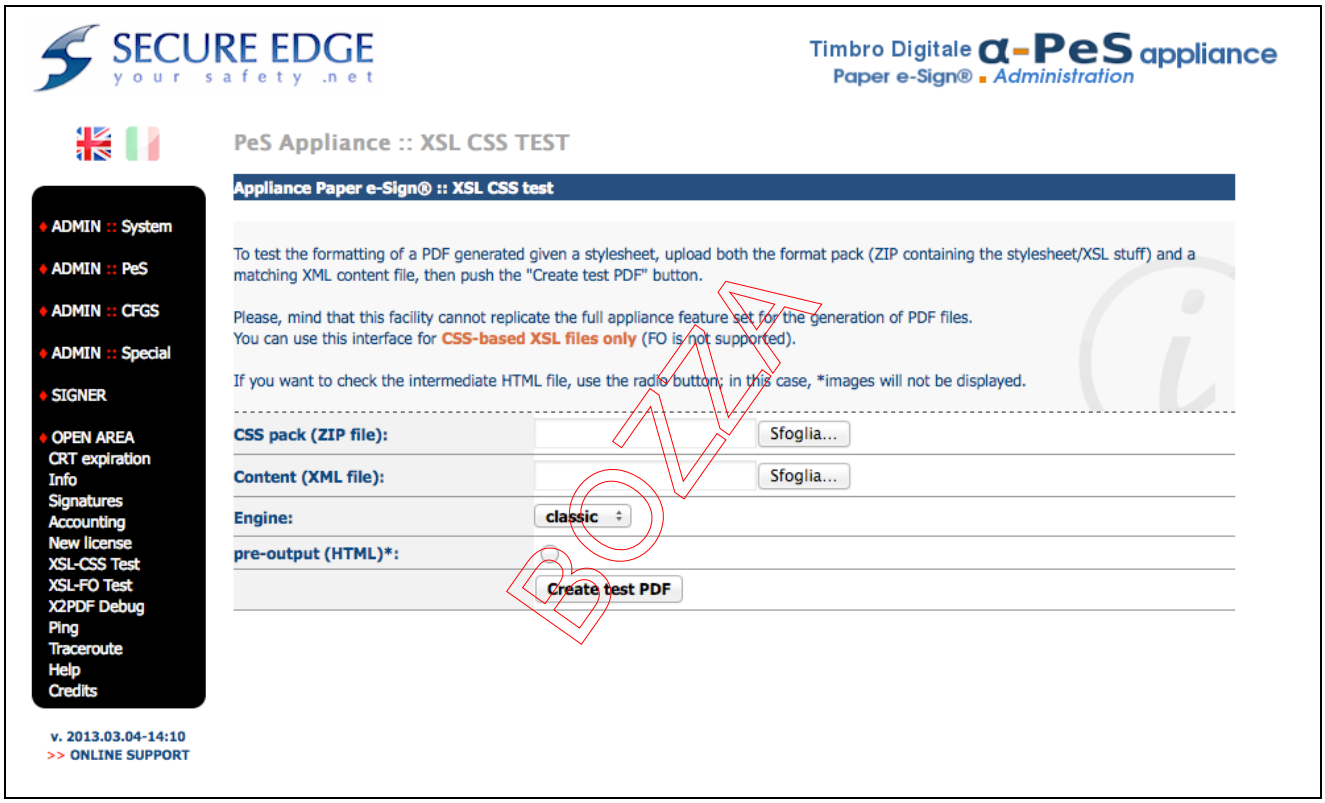
1. Certificato dell'interfaccia WEB dell'appliance
2. Certificato di CA
3. Certificati di Firma su Smart Card o HSM
4. Certificati di autenticazione utenti e applicazioni.

La visualizzazione delle informazioni è auto esplicativa. Va solo notato che del certificato vengono presentati i dati salienti.



XSL-CSS Test: Test sulla funzionalità di timbro "XSL-CSS"

In alcune circostanze, può essere utile effettuare una prova di generazione di un documento PDF partendo da un template "XLS_CSS" per verificare che il pacchetto che poi si andrà a caricare sull'appliance sia realizzato correttamente. Per effettuare questa operazione, cliccare sul menu "***XSL-CSS Test***". Come illustrato nella figura seguente, caricare dal proprio sistema operativo il file relativo all'archivio del pacchetto (in formato "*.xsl.zip*") e il file "template" (in formato "XML"). Viene restituito un file PDF contenente il template e un riferimento per visualizzare le dimensioni e la posizione del timbro che verrà apposto sulla pagina (il timbro è "vuoto"). Qualora si selezioni la funzione "pre-output", la pagina verrà visualizzata in formato HTML all'interno del browser.

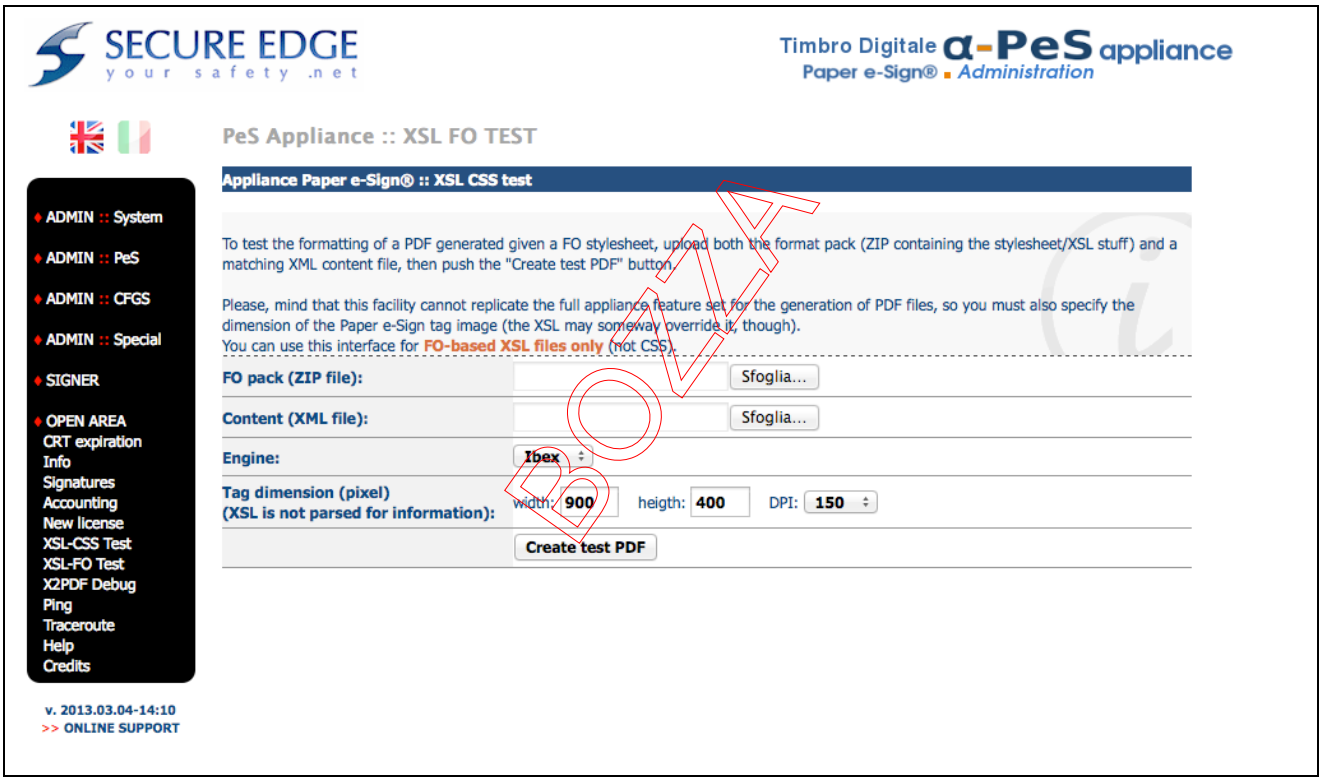


Per un miglior apprezzamento del test, si consiglia di utilizzare la generazione del file .PDF, mantenendo de-selezionata l'opzione "*pre-output*"

E' possibile selezionare la simulazione dell'engine "WK", anziché il classico CSS con PISA

XSL-FO Test: Test sulla funzionalità di timbro "XSL-FOP"

Quanto riportato nel precedente paragrafo "XSL-CSS" è valido anche nel caso si scelga di utilizzare gli engone FOP oppure Ibex. Anche in questa situazione, l'utente effettuare una prova di generazione di un documento PDF partendo da un template "XLS_FO" per verificare che il pacchetto che poi si andrà a caricare sull'appliance sia realizzato correttamente. Per effettuare questa operazione, cliccare sul menu "***XSL-FO Test***". Come illustrato nella figura seguente, caricare dal proprio sistema operativo il file relativo all'archivio del pacchetto (in formato "*.xsl.zip*") e il file "template" (in formato "XML"). Viene restituito un file PDF contenente il template e un riferimento per visualizzare le dimensioni e la posizione del timbro che verrà apposto sulla pagina (il timbro è "vuoto"). Rispetto alla versione per template CSS, in questo test è possibile specificare le dimensioni del timbro relative alla larghezza ("width"), all'altezza ("height") ed alla densità (150, 200, 300 DPI).

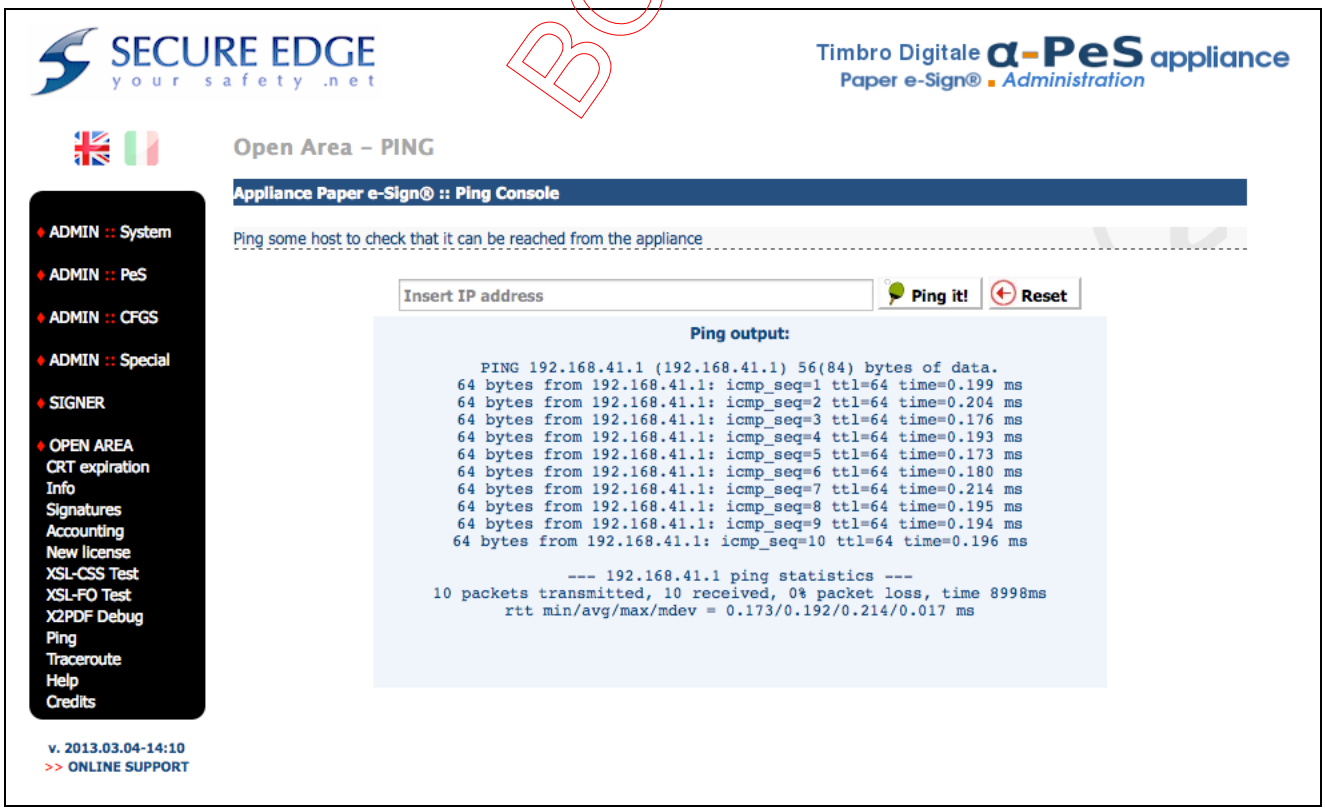


E' possibile selezionare la simulazione dell'engine "Ibex", anziché il classico FOP.

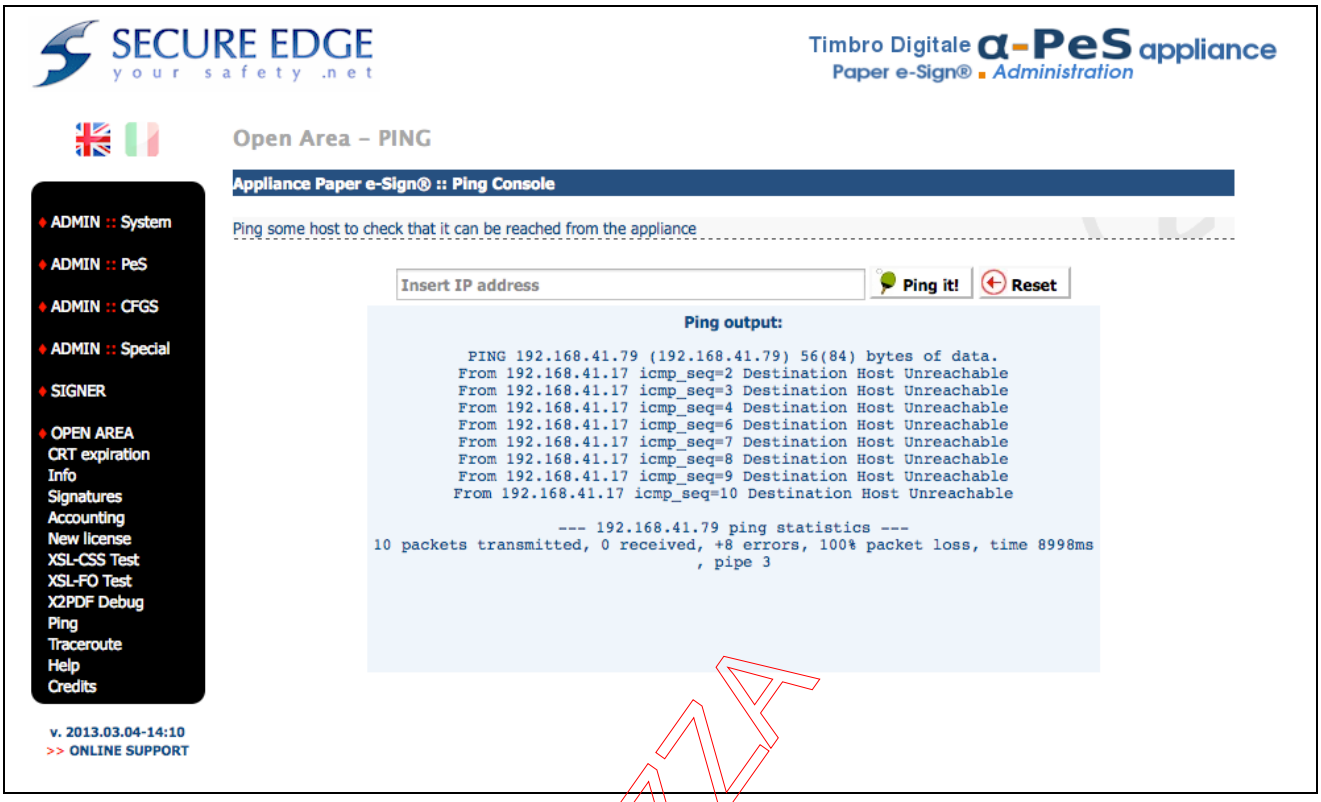
Ping: Operazioni di troubleshooting

Qualora sia necessaria verificare la comunicazione fra l'appliance αPeS e altri sistemi/apparati necessari al completo funzionamento dell'infrastruttura, è possibile utilizzare le due funzioni di "***Ping***" e "***Traceroute***", tramite il relativo menu sulla sinistra.

La pagina di “ping” consente l’invio di 10 pacchetti ICMP del tipo “*echo-request*” verso qualunque indirizzo (pubblico o privato), come illustrato nelle figure seguenti:



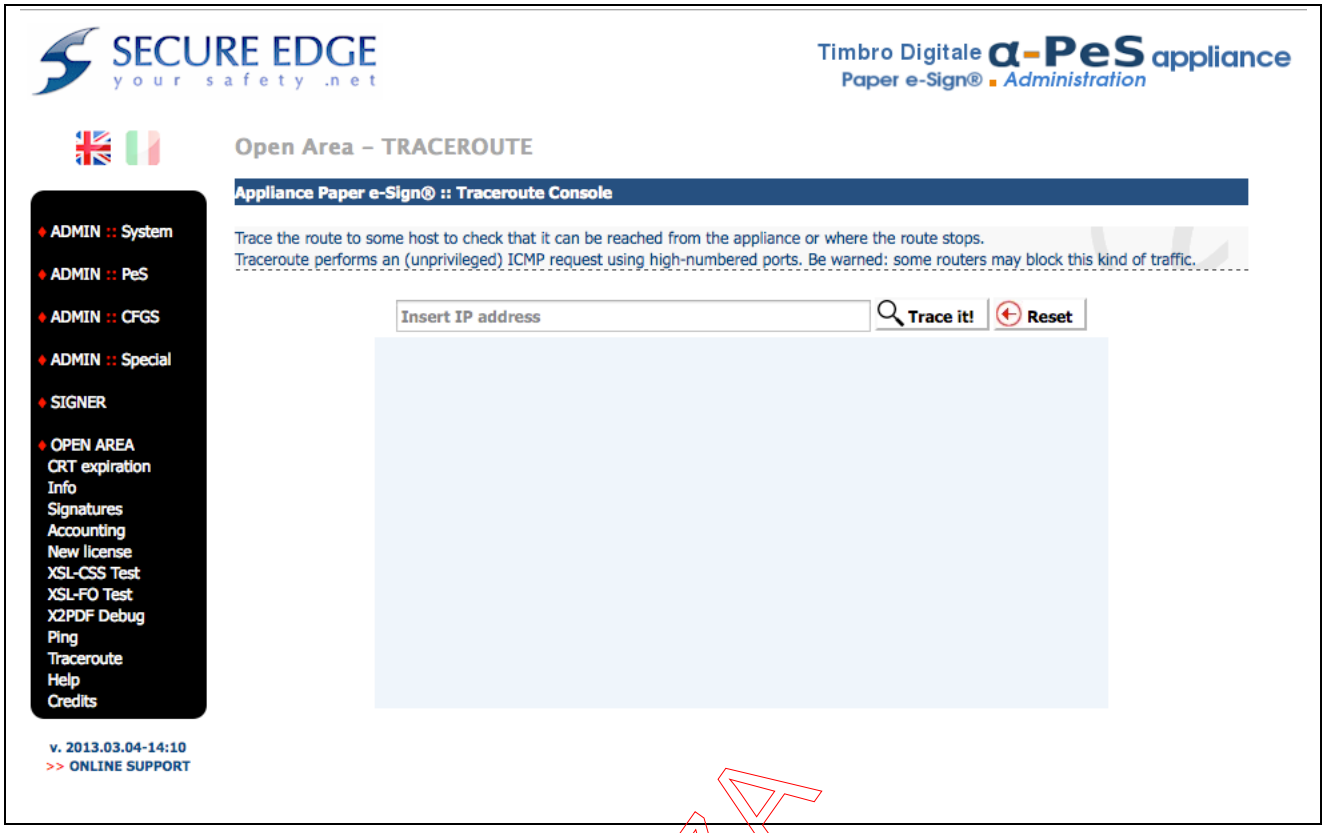
Nel caso in cui non si ricevessero risposte "*echo-reply*", si otterrà il seguente output, illustrato nella figura seguente, al termine di un periodo di attesa di circa 10 secondi:



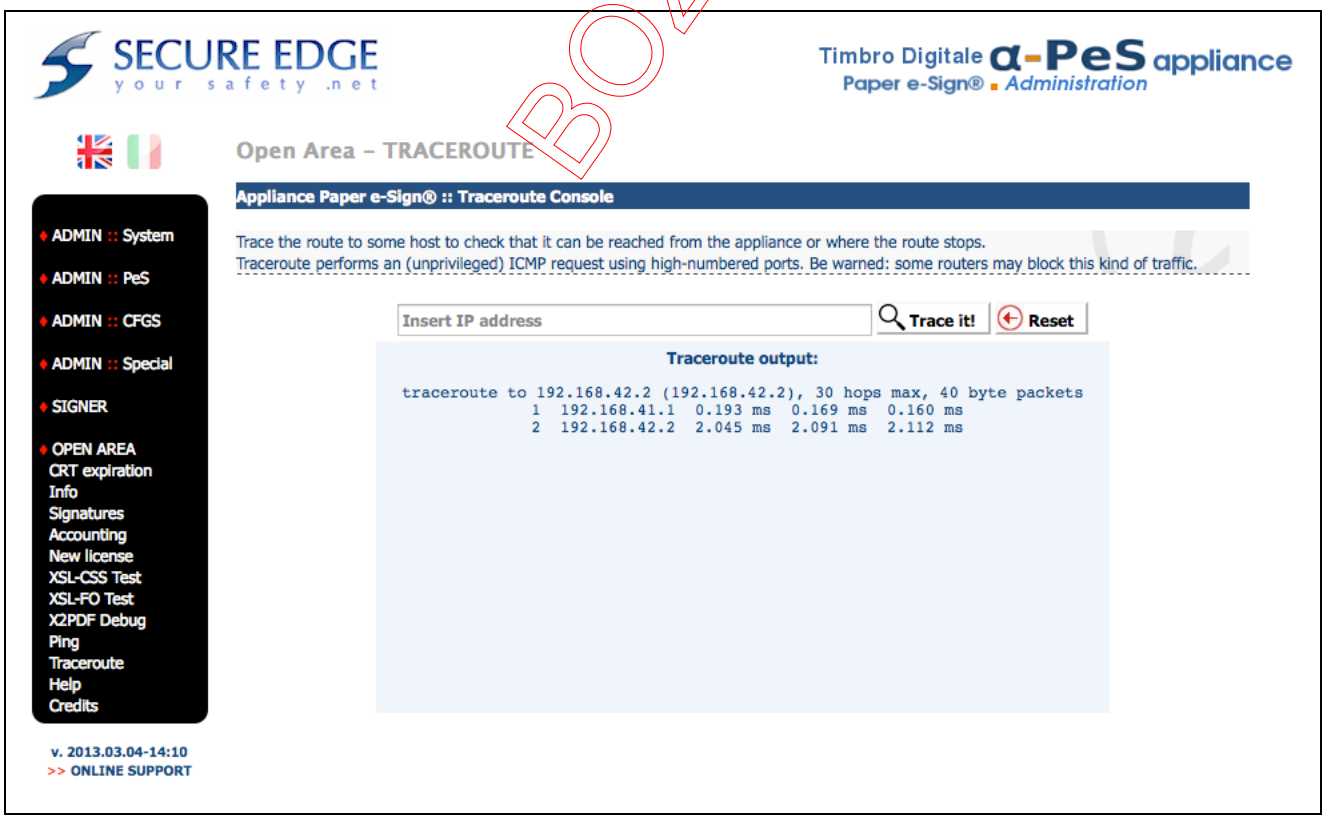
Inserire unicamente un indirizzo IP numerico; non sono accettati hostname

Traceroute: Operazioni di troubleshooting

La funzione "traceroute" consente, invece, di tracciare tutti gli apparati che vengono "attraversati" fino a raggiungere l'indirizzo IP desiderato. Questo può essere molto utile per verificare sia il numero/tipologia di apparati necessari alla comunicazione fra l'appliance αPeS e un altro dispositivo remoto, sia per verificare, in caso di problematiche legate alla configurazione di rete (per la presenza di regole di routine o politiche di firewalling) quale possa essere l'ultimo dispositivo con cui l'appliance riesce a comunicare nel tentativo di raggiungere un determinato indirizzo IP. La finestra a disposizione è similare a quella illustrata per la funzione di "ping":

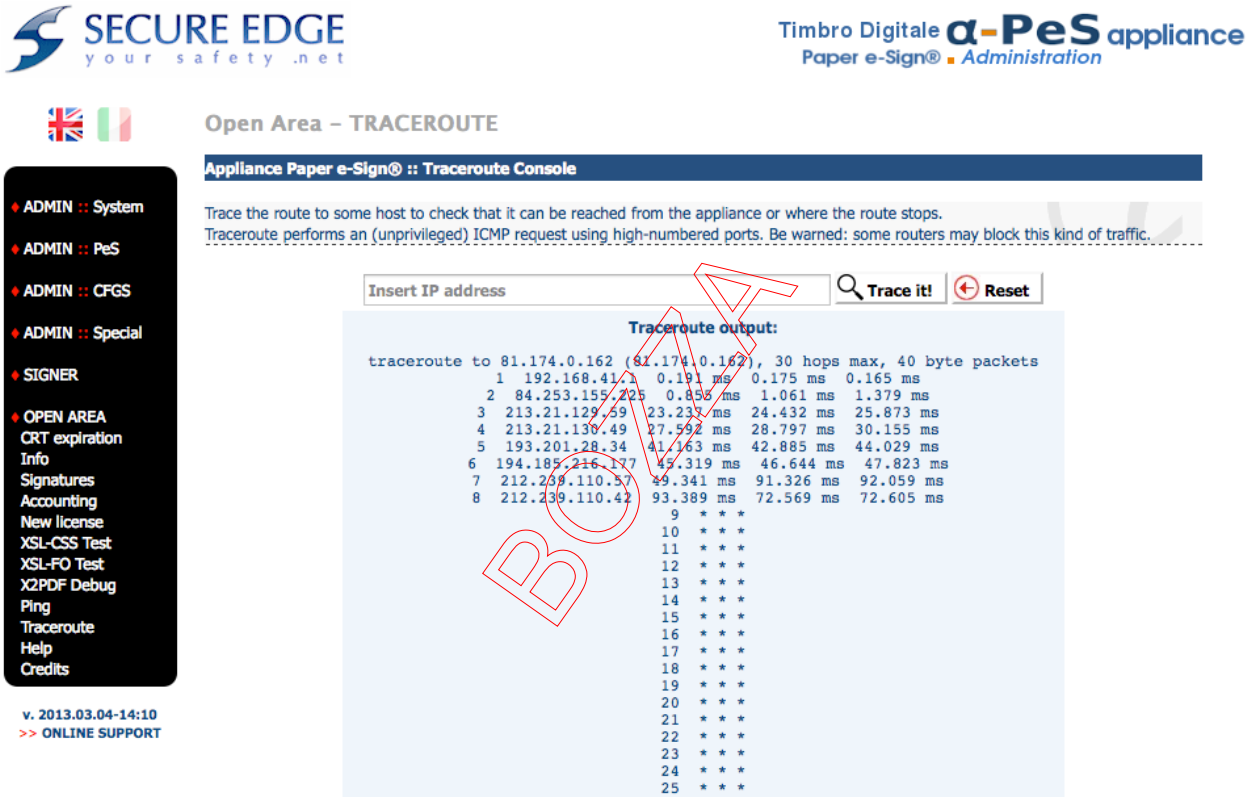


Nell'immagine seguente, ecco quanto il risultato dell'operazione:



Inserire unicamente un indirizzo IP numerico; non sono accettati hostname

Prestare particolare attenzione nel caso si usi questa funzione con indirizzi IP pubblici o con segmenti di rete protetti da firewall. Difatti la funzione “traceroute” presente sull’appliance αPeS utilizza il protocollo UDP e invia una serie di pacchetti utilizzando delle porte dinamiche comprese fra la 33434 e la 33434 + il numero massimo di “hop” (apparati) -1. Di conseguenza, in alcune circostanze si potrebbe avere un risultato “falsato” da questo particolare meccanismo di funzionamento del protocollo, in quanto potrebbero essere presenti dei router o dei firewall che bloccano tali comunicazioni, come illustrato nella figura seguente:



Nel caso illustrato in figura, i pacchetti UDP non vengono inoltrati successivamente all’hop nr. 8 con indirizzo 212.239.110.42

Procedure Operative: Quick Start

Di seguito vengono presentati i passi necessari a configurare l'appliance; non entreremo nel dettaglio della configurazione sistemistica del l'appliance αPeS perché assimilabile a qualsiasi altro apparato mentre presenteremo i passi necessari a configurare il sistema per la produzione di Timbri Digitali.

Gestione della configurazione dell'appliance αPeS

Prima di eseguire qualunque operazione di configurazione, si consiglia vivamente di inserire le Smart Card / Token all'interno dell'SCBox o Mini SCBox collegata alla porta USB dell'appliance αPeS. In caso di utilizzo del dispositivo SCBox rispettare il corretto orientamento del microchip durante l'operazione di inserimento; a questo proposito vedere il manuale dell'SCBox.

Di seguito si riportano i passaggi necessari a configurare l'appliance αPeS in modo che possa accettare le richiesta di generazione di timbri da parte di un'applicazione web.

Ogni passaggio verrà quindi illustrato nel dettaglio; per praticità si può seguire questo flusso di operazioni, partendo da una situazione in cui non sia presente alcuna Configurazione ed alcun Profilo (ad eccezione delle credenziali di Amministratore):

Se necessario, l'Amministratore carica sull'appliance i Certificati delle CA emittenti i certificati dei Profili (come già illustrato nel paragrafo "*Operazioni speciali: caricamento e aggiornamento Certificati*").

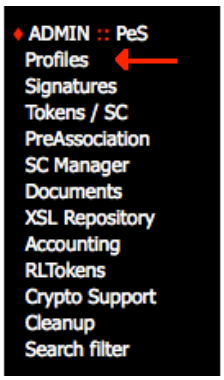
1. l'Amministratore crea il *Profilo* del Titolare del Certificato, indicando il relativo certificato;
2. l'Amministratore crea il *Profilo* dell'applicazione, indicando il relativo certificato;
3. l'Amministratore crea la *Configurazione*, indicando opportunamente il codice "*tipo applicazione*", specificando un commento descrittivo e possibilmente assegnandola al profilo applicativo;
4. in caso di generazione di PDF da parte dell'appliance, l'Amministratore carica il relativo file XSL associando tale XSL alla *Configurazione* e attiva il meccanismo opportuno di generazione del PDF (XSL-CSS oppure XSL-FO).
5. l'Amministratore esegue la scansione di tutte (o parte) delle smart card inserite all'interno dei lettori nel dispositivo SCBox, quindi ne effettua la pre-associazione con la relativa *Configurazione*;
6. l'Amministratore assegna il certificato all'interno di una Smart Card o di un HSM al Profilo del Titolare del Certificato (affinché quest'ultimo possa disporre del potere di amministrazione sulla firma contenuta nella Smart Card o di un HSM);
7. il Titolare del Certificato esegue la Cerimonia indicando il PIN della Smart Card ed una propria

Pass-phrase per il Certificato di firma, contenuto all'interno di una Smart Card o di un HSM

8. il Titolare del Certificato esegue l'attivazione del Certificato di firma e contestualmente esegue l'associazione vera e propria fra il Certificato di firma e la Configurazione, in base a quanto pre-associato dall'amministratore al punto 6;
9. il Titolare del certificato, a livello opzionale, può limitare il numero di timbri emessi per ciascuna Configurazione in base ad una data di scadenza (che non potrà comunque mai superare quella del Certificato di firma);

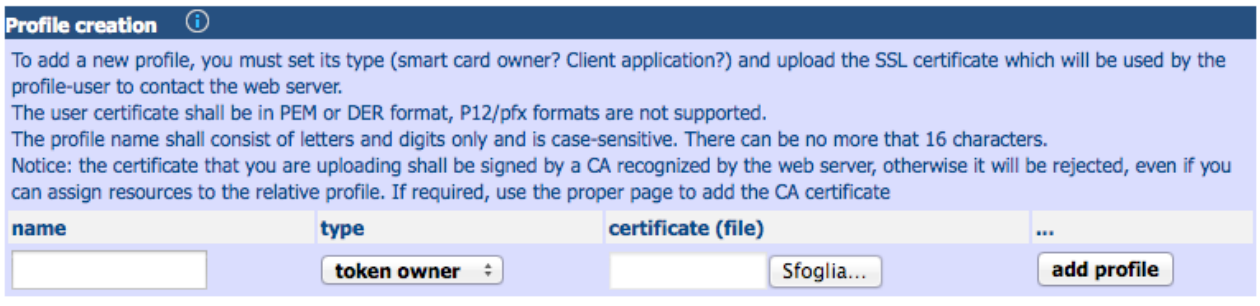
Passo 1: creazione dei Profili

Tutte le operazioni di "Gestione della configurazione" prevedono l'autenticazione dell'Amministratore attraverso il proprio Certificato, attraverso sessione SSL



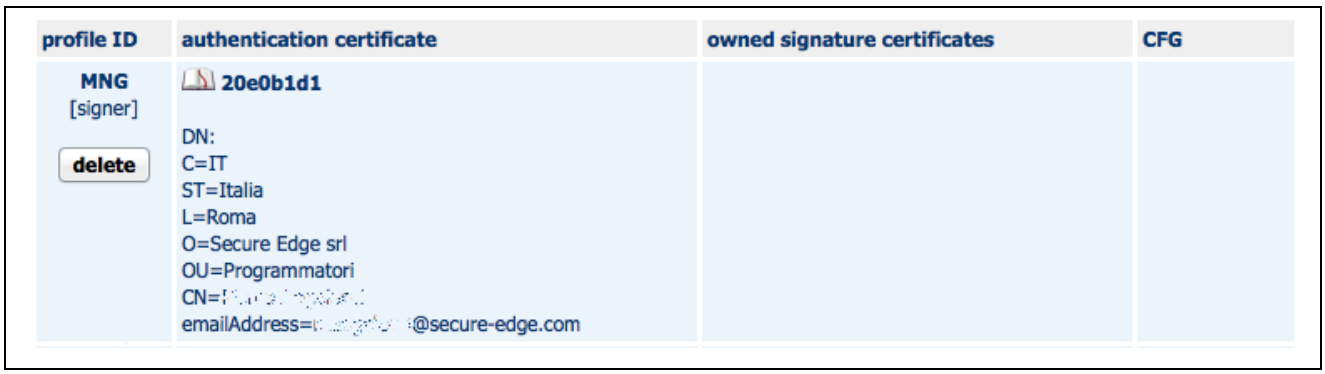
Qualora l'appliance non disponga di alcun profilo di Titolare del Certificato e/o di Applicazione o esso sia scaduto o sia necessario aggiungerne uno ex-novo, è possibile utilizzare l'opzione "***Profiles***" dall'area "***PeS***" utilizzando il menu sulla sinistra.

Utilizzando il riquadro "*Add new Profile*" è possibile inserire un "nome breve" (massimo 16 caratteri) per identificare il Titolare del Certificato (o dell'Applicazione). Si consiglia di caricare direttamente il file "*.crt*" dedicato al Profilo, tramite il riquadro "*Certificate (file)*" e quindi confermare con "*Add*", come illustrato nella seguente figura:



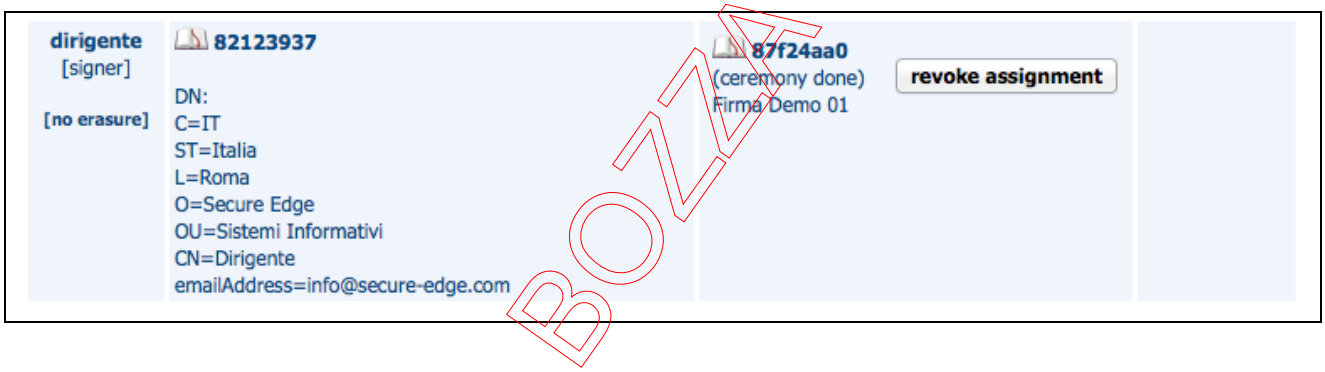
Per questa operazione è possibile utilizzare uno dei certificati presenti nel CD-Rom allegato. In alternativa è possibile utilizzare un qualunque certificato PKCS12 generato da un'altra Certification Authority; nel caso si deve caricare anche il certificato della CA. Il caricamento del certificato è sempre una operazione contestuale alla creazione del Profilo.

Quando il Profilo (sia per il Titolare del Certificato, sia per l'Applicazione) risulta correttamente caricato, questo compare nella successiva tabella denominata *"Manage existing certificato assignments"*, come illustrato nella successiva figura:



Come si può notare è presente il tasto "*Delete*" per eseguirne la cancellazione.

Nel caso in cui al Profilo sia associato un Certificato (ovvero un Certificato di firma, presente all'interno di una Smart Card o di un HSM), esso compare nella colonna destra, come illustrato nella figura seguente:



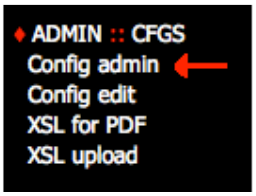
Come si può notare, compare anche il tasto "*Revoke Assignment*" nel caso in cui l'Amministratore decida di revocare l'assegnazione di un Certificato di firma ad un Titolare del Certificato.

Qualora un Certificato, assegnato ad un Profilo di Titolare di firma, sia stato correttamente inizializzato, è presente l'indicazione "*ceremony done*"; in caso contrario sarà presente l'indicazione "*NO ceremony*".

L'associazione fra Titolare del Certificato e Certificato di firma viene descritta nel dettaglio al **Passo 6**, mentre l'inizializzazione del Certificato (operazione a cura del Titolare e non dell'Amministratore) viene descritta al successivo **Passo 7**.

Ricordiamo che la creazione del Profilo per l'Applicazione è necessaria in un quanto le applicazioni si devono autenticare con il certificato del Profilo per poter comunicare con il gateway di firma dell'appliance, attraverso il consueto canale cifrato (SSL).

Passo 2: creazione / importazione della Configurazione (ripristino di un backup della Configurazione)

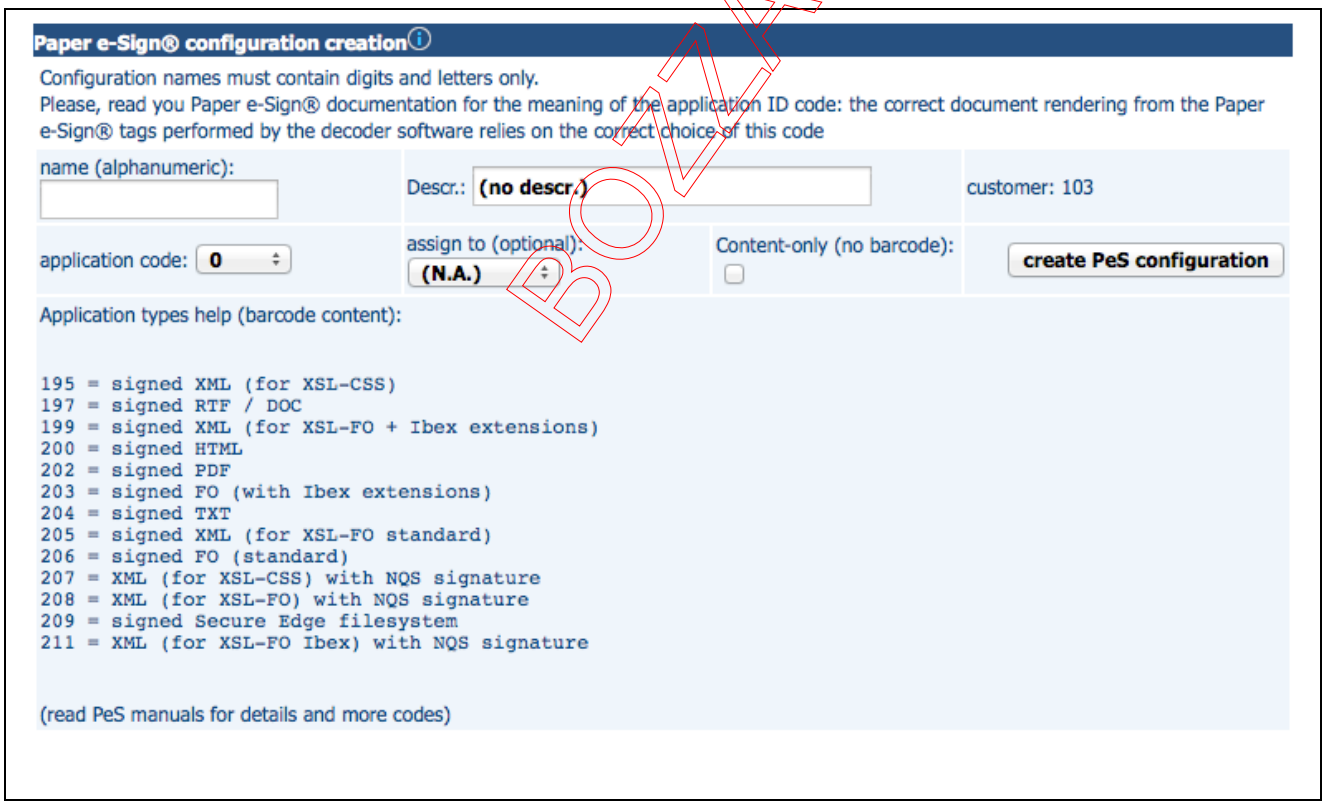


Eseguita la creazione dei Profili, è necessario creare la Configurazione del tipo di documento che il gateway andrà poi a firmare. In questo caso è necessario utilizzare l'opzione "***Config admin***" dall'area "***Admin : Cfgs***" del menu a sinistra. e quindi la tabella "*Paper e-Sign® configuration creation*".

E' innanzitutto necessario indicare un nome per la Configurazione (in questo caso si consiglia un nome auto-esplicativo), quindi è necessario impostare il codice numerico che consente al gateway di firma, di riconoscere la tipologia di documento che andrà a firmare (detto codice numerico può variare da 0 a 255, tuttavia i più frequenti e comuni sono riportati all'interno della medesima tabella.

Per avere una descrizione di dettaglio su tutti i codici di Configurazioni, si rimanda al documento "***Useful Data Structures***" ("*[SE_T-07-0053] T I DST useful data structures [1.13].pdf*") capitolo 4.3.

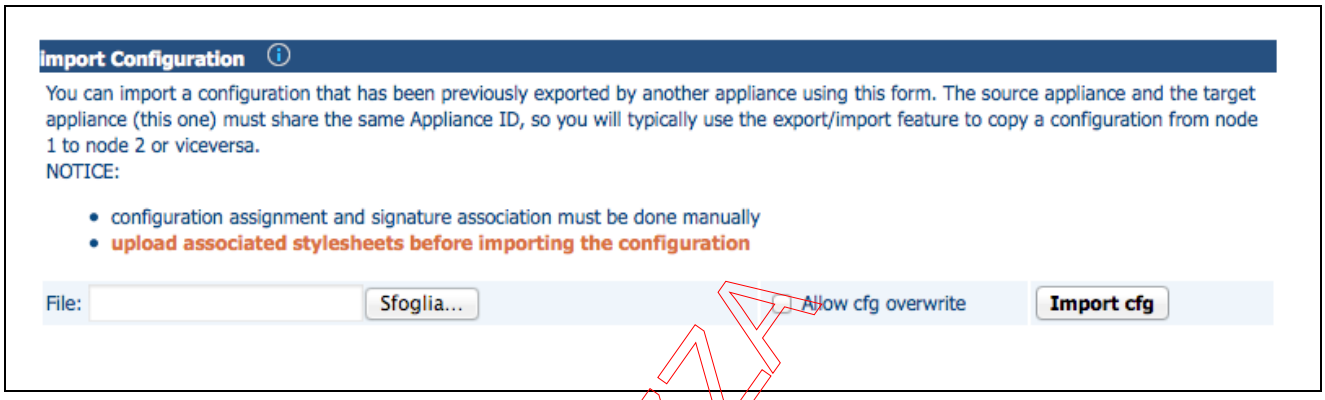
Di seguito si riporta la tabella per la creazione di Configurazioni:



Qualora sia necessario che il gateway restituisca solamente il file *.p7m* relativamente alla firma digitale aggiungere il segno di spunta all'opzione "*Content-only (no barcode)*". In condizioni standard il gateway di firma restituisce il documento firmato (ovvero il documento con il timbro digitale).

Si consiglia vivamente di aggiungere una descrizione esplicava della configurazione. Durante questa operazione è consigliato effettuare anche l'associazione fra la Configurazione e il Profilo dell'applicazione (client) per garantire il canale cifrato (SSL) fra i due oggetti (applicazione e appliance αPeS). Altrimenti sarà possibile effettuare tale applicazione anche in secondo momento: fare in tal caso riferimento al **Passo 4** della Gestione dell'Appliance.

Qualora si disponga già di un file di configurazione (ad esempio un backup da una seconda appliance in configurazione di hot-standby o dalla medesima appliance) è possibile importarlo utilizzando il box sottostante, come illustrato nella seguente immagine:



Qualora il nome del profilo sia già esistente, spuntare l'opzione "*Allow cfg overwite*" per consentire la sovrascrittura, altrimenti l'importazione restituirà un messaggio di errore ("**ERROR: at least one configuration ([*application_name*]) already exists in appliance**").

Il file da importare deve avere estensione "*.PeS_cfg_export*"

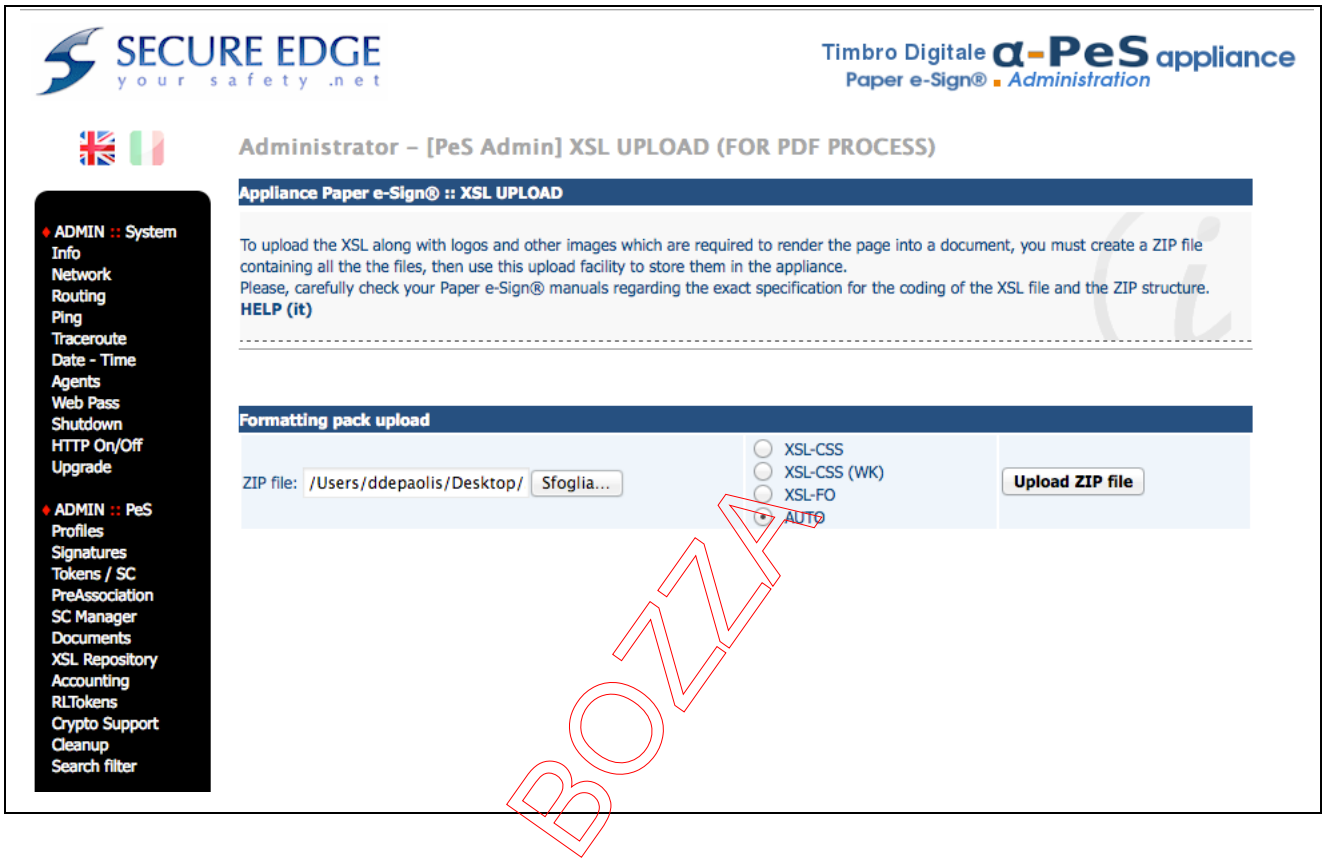
Passo 3: caricamento XSL e assegnazione alla Configurazione

Eseguire questa procedura solamente nel caso in cui si desideri che l'appliance αPeS produca direttamente un file .PDF contenente il timbro digitale, utilizzando un opportuno "template" XSL. In tutte le altre situazioni procedere immeditamente con il passo 4

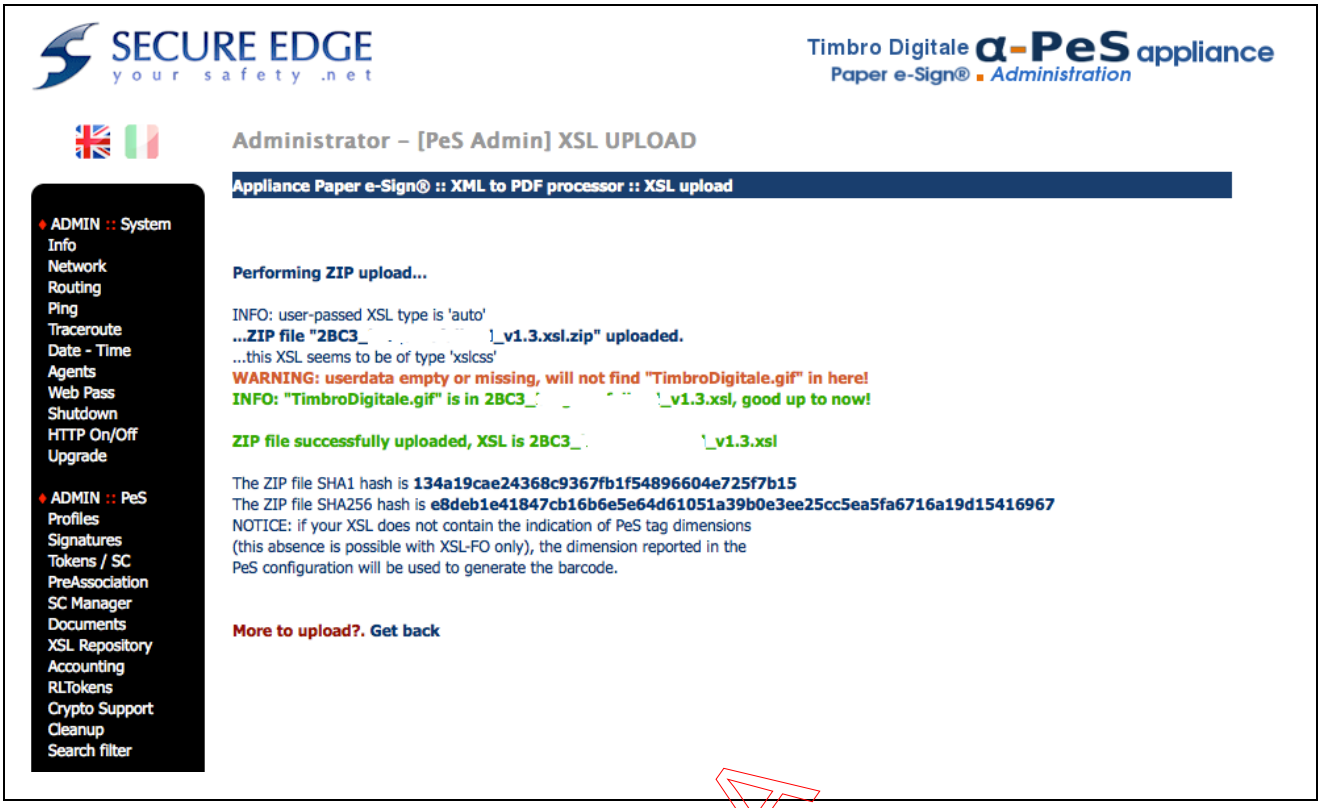
Eseguita la creazione di una Configurazione, è possibile caricare un file di "template" XSL da associare alla Configurazione medesima. Ciò è necessario qualora l'infrastruttura preveda che l'appliance αPeS produca direttamente un file .PDF firmato.

Per eseguire questa operazione è necessario, innanzitutto, disporre di un file di archivio (.zip) al cui interno devono essere inseriti il file XSL e gli eventuali allegati "grafici" in formato .jpg; tali allegati grafici devono, a loro volta, essere contenuti all'interno della sottodirectory "img".

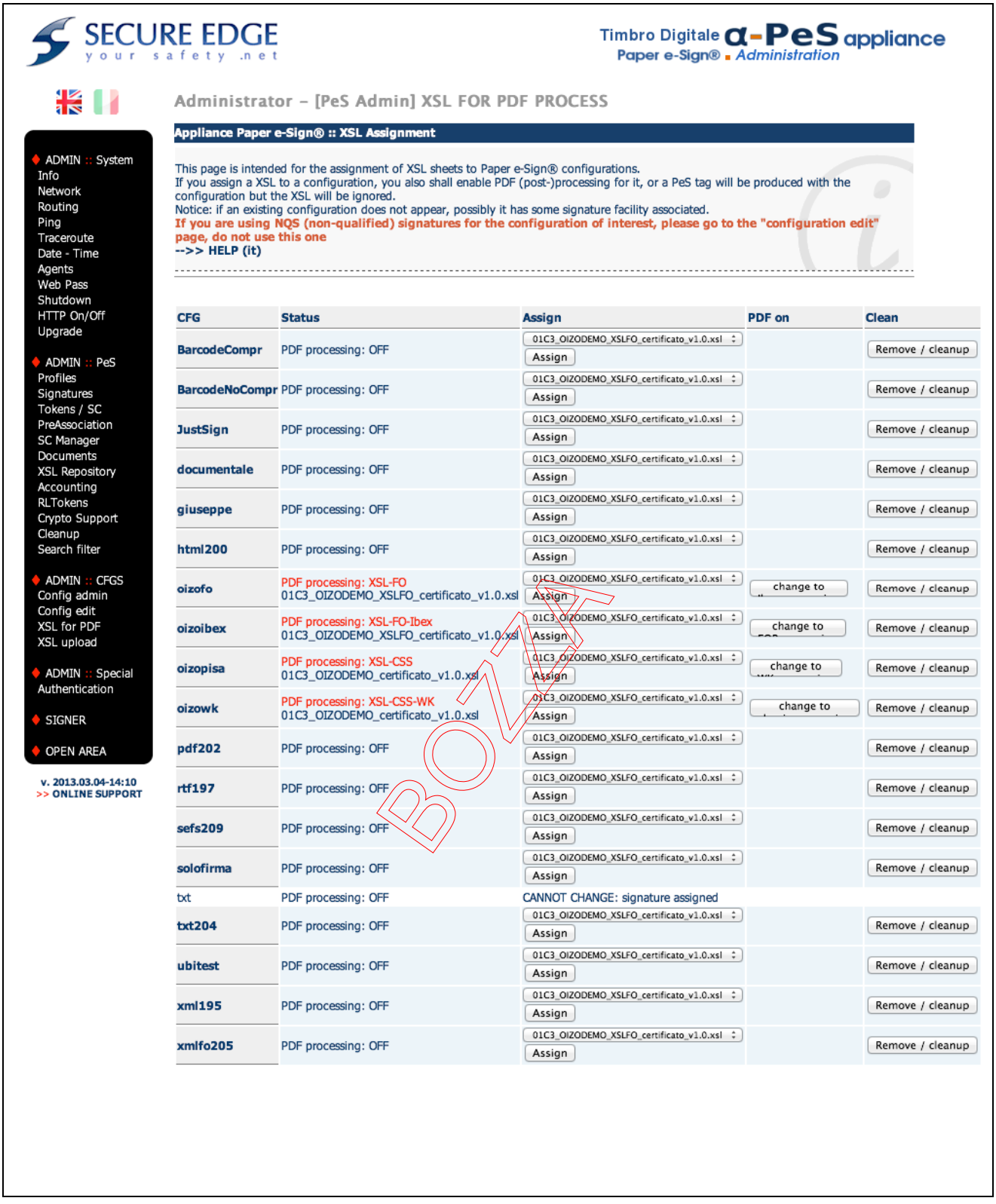
Per caricare tale file di archivio, l'Amministratore deve utilizzare il menu ***"XSL Upload"*** nell'area ***"Config"***, come illustrato nella figura seguente:



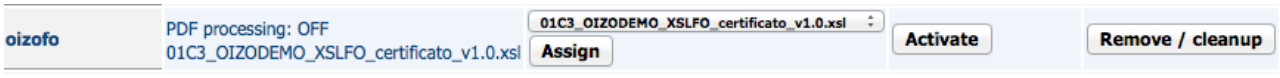
Cliccando sul tasto "Sfoglia" si seleziona il percorso locale all'interno del quale è presente il file di archivio da importare sull'appliance. Il box per l'importazione del file di archivio consente di specificare anche la tipologia di formattazione del file XLS, ovvero "FO" (Formatting Objects") oppure "CSS" (Cascade Style Sheet). E' anche possibile specificare di importare un XSL che prevede l'utilizzo dell'engine WK. Normalmente, per specificare il tipo di XSL, si deve utilizzare l'opzione "Auto". Nel caso in cui l'appliance non riesca a riconoscere, autonomamente, la tipologia di file, è possibile specificarne la tipologia manualmente. Ciò rappresenta, comunque, una eccezione in quanto il verificarsi di questa situazione indica, probabilmente, un errore al momento della creazione del file .zip o .xsl. Qualora l'importazione si avvenuta correttamente, verrà visualizzata una pagina simile alla seguente illustrazione:



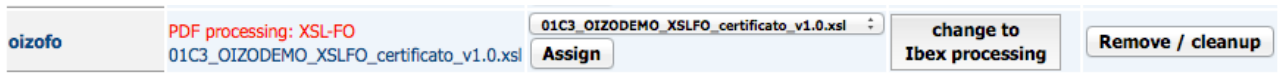
Effettuato il caricamento dei file relativi al layout del documento, l'Amministratore può effettuare l'associazione del file XSL alla relativa Configurazione utilizzando l'area "***XSL for PDF***", sempre nell'area "***Admin : Cfgs***", come illustrato nella figura seguente:



Per eseguire l'associazione è sufficiente selezionare il file .xsl da menu a tendina all'interno della colonna centrale "*Assign*" (utilizzando la riga in cui è presente il nome della Configurazione) e confermare con il tasto "*Assign*". Successivamente il nome del file .xsl compare nella tabella, all'interno della colonna "*Status*"; per completare l'associazione, è necessario cliccare sul tasto "Activate", come illustrato nelle figure seguenti:



(prima della pressione del tasto "Activate")



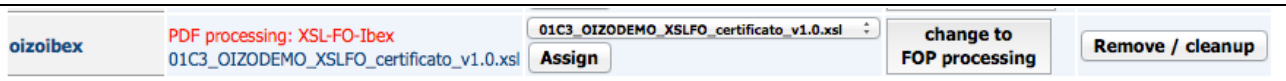
(dopo la pressione del tasto "Activate")

Non è possibile associare un file XLS ad una Configurazione che risulta avere già associato un certificato (certificato) di firma inizializzato (ovvero il cui Titolare ne abbia già eseguita la Cerimonia)

In caso di necessità, è sempre possibile rimuovere l'associazione fra file PDF e Configurazione, attraverso il tasto "*Remove / Cleanup*" che riporta ad una condizione di origine.

Nel caso sia necessario produrre un documento PDF attraverso la libreria "FOP" di Apache, dopo la pressione del tasto "*Ativate*" comparirà un ulteriore tasto denominato "*Ibex Processing*" , come illustrato nella nell'immagine precedente.

Questo tasto consente di attivare l'uso della libreria "FO-Ibex", il quale genera un timbro lievemente differente nella struttura, ma pienamente compatibile con l'attuale implementazione del software di Decoder. E' comunque possibile ripristinare l'uso della libreria "FOP" di Apache, cliccando sul tasto "*Change to FOP Processing*" che comparirà successivamente, come illustrato nella seguente immagine:



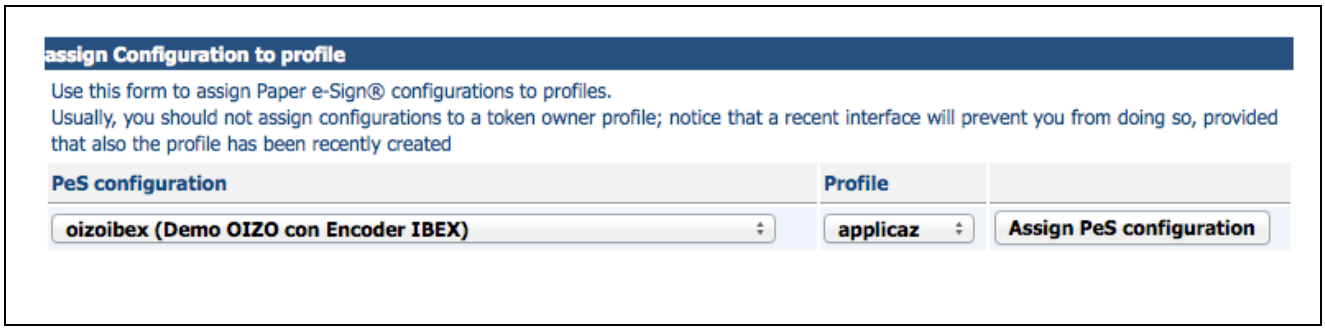
Passo 4: associazione / rimozione del Profilo dell'applicazione alla Configurazione

E' utile ricordare che un Profilo dell'Applicazione può essere associato ad "n" Configurazioni. Questo può accadere nel caso in cui lo stesso certificato di comunicazione dell'Applicazione sia necessario per apporre il Timbro su più documenti di differente tipologia.

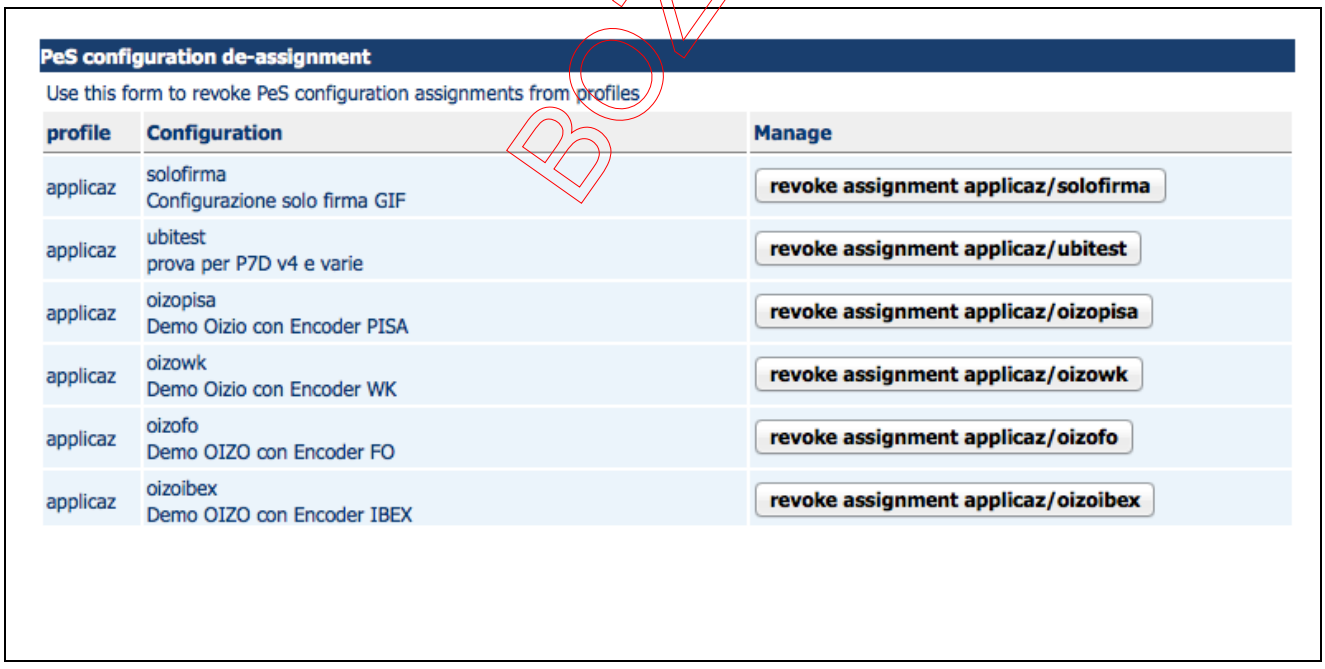
L'associazione fra il Profilo dell'Applicazione e la Configurazione prescinde dalla presenza di Certificato già inizializzati dal Titolare. Questa operazione tuttavia è assolutamente necessaria per poter consentire al Titolare del Certificato di poter poi associare il Certificato alla Configurazione.

Dopo aver creato la Configurazione, come descritto al Passo 2, è necessario associare questa Configurazione al relativo Profilo dell'applicazione, in modo che l'applicazione che comunicherà con il "gateway" dell'appliance αPeS, possa farlo correttamente attraverso un apposito canale SSL.

In linea generale l'assegnazione fra il Profilo dell'Applicazione e la relativa configurazione dovrebbe essere effettuata congiuntamente alla creazione della configurazione. Tuttavia è possibile effettuare questa associazione anche in un secondo momento, utilizzando il box "*PeS Configuration Assignment*", del menu "***Config Admin***" dell'area "***Admin : Cfgs***", come illustrato nella figura seguente e confermare con il tasto "*Assign PeS Configuration*".

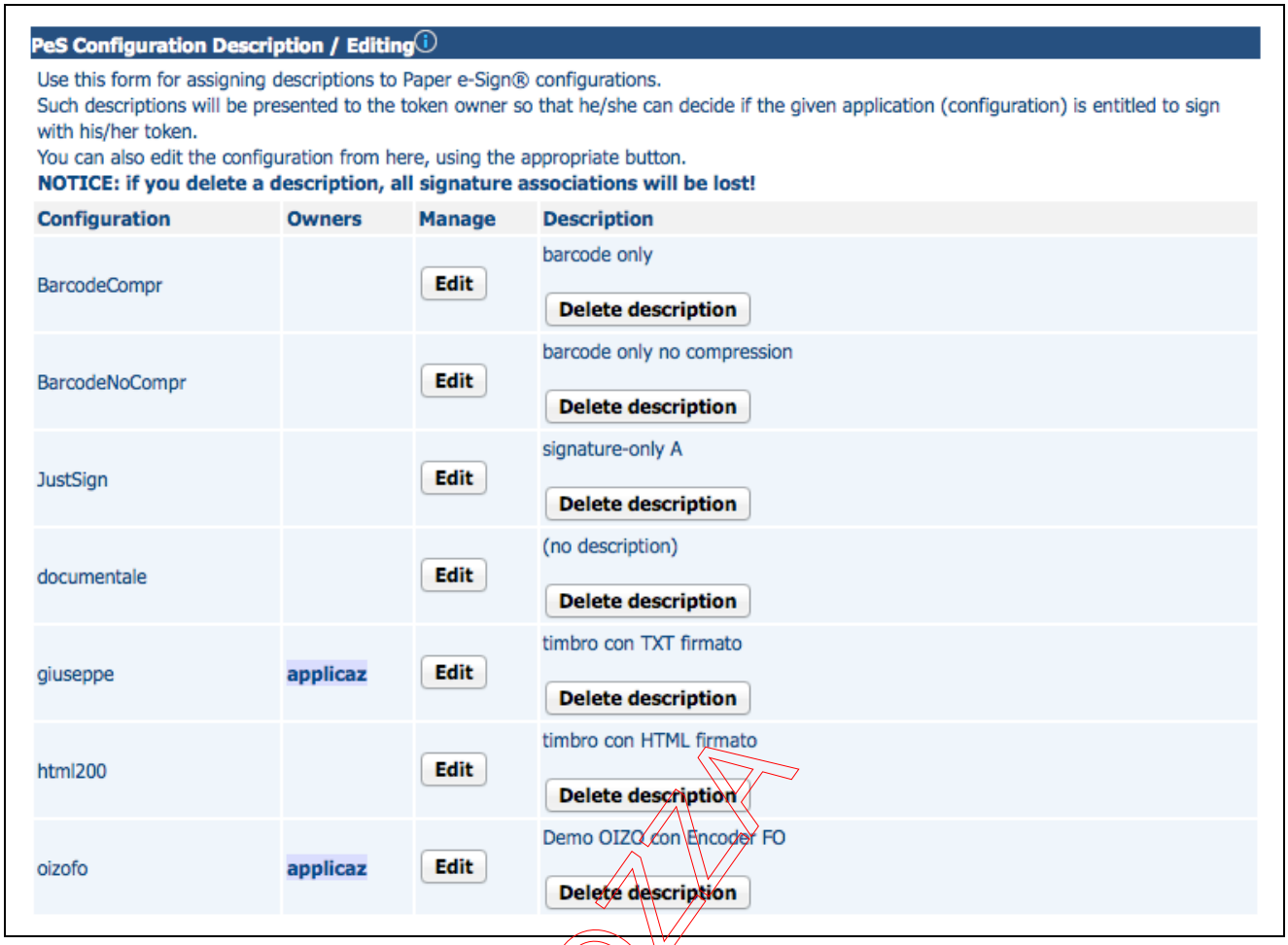


Effettuata l'assegnazione fra Configurazione e Profilo dell'applicazione, questa apparirà nella tabella così come illustrato nella seguente immagine:



Tramite il pulsante "*Revoke assignment*" è possibile eliminare l'assegnazione fra Configurazione e il Profilo dell'applicazione client (ad esempio nel caso il certificato del Profilo dell'applicazione sia scaduto di validità)

Per verificare la corrisponza fra la Configurazione e il Profilo dell'applicazione, fare riferimento alla tabella "*PeS Configuration Description / Editing*" come illustrato nella figura seguente, in particolare il valore della colonna "*Owners*" il quale riporta il nome del Profilo per ciascuna configurazione:

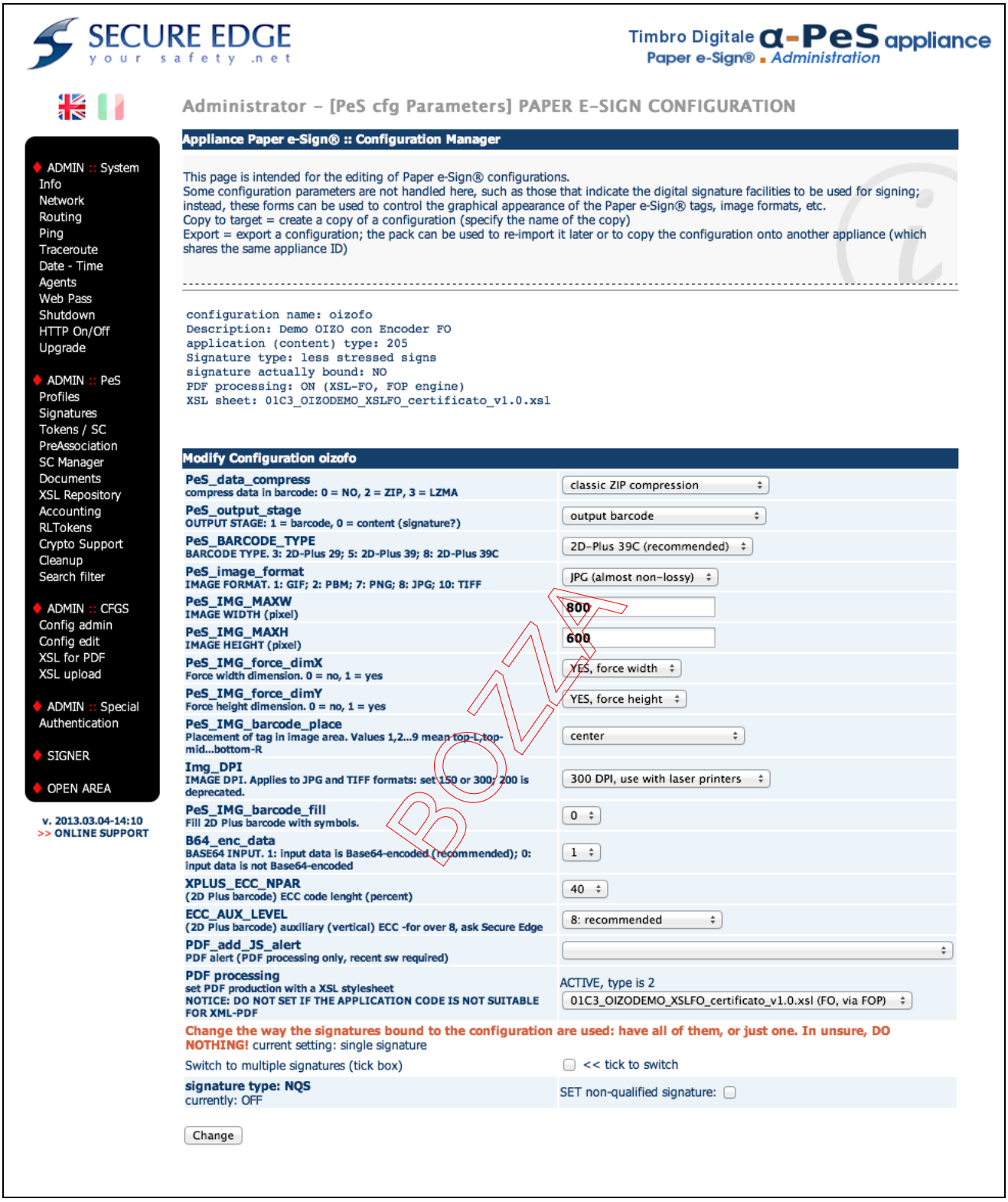


PeS Configuration Description / Editing

Use this form for assigning descriptions to Paper e-Sign® configurations.
Such descriptions will be presented to the token owner so that he/she can decide if the given application (configuration) is entitled to sign with his/her token.
You can also edit the configuration from here, using the appropriate button.
NOTICE: if you delete a description, all signature associations will be lost!

Configuration	Owners	Manage	Description
BarcodeCompr		Edit	barcode only Delete description
BarcodeNoCompr		Edit	barcode only no compression Delete description
JustSign		Edit	signature-only A Delete description
documentale		Edit	(no description) Delete description
giuseppe	applicaz	Edit	timbro con TXT firmato Delete description
html200		Edit	timbro con HTML firmato Delete description
oizofo	applicaz	Edit	Demo OIZO con Encoder FO Delete description

Cliccando sul bottone "*Edit*" si accede alla finstra per la modifica di tutti i principali parametri di realizzazione del timbro, come illustrato di seguito:



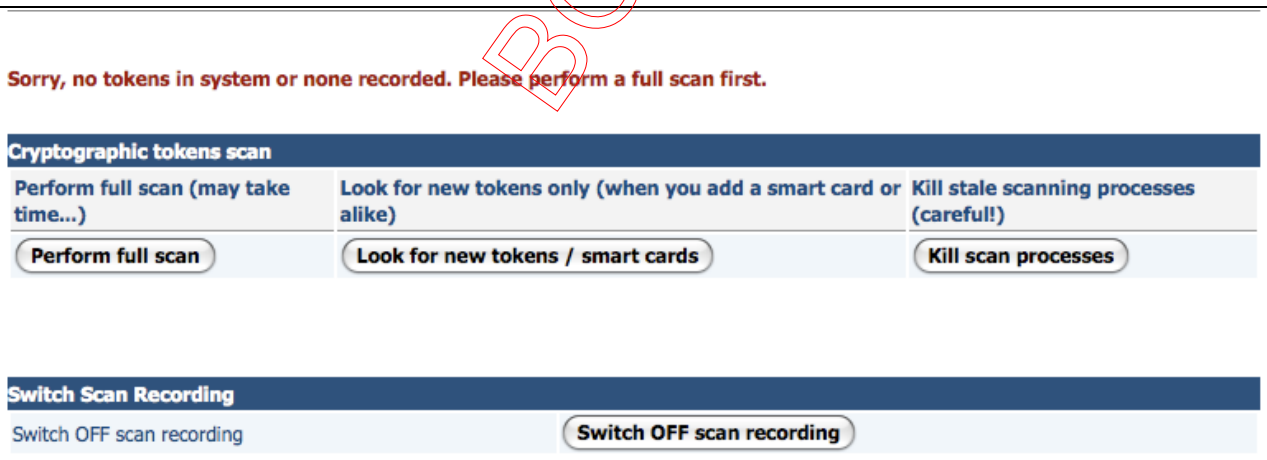
Il dettaglio per meglio comprendere il significato di ogni parametro è descritto nel documento: ***[SE_T-07-0049] T I DST Usage from applications [3.9].pdf***

L'Amministratore può giungere alla medesima pagina utilizzando il menù "***Configuration***s" dell'area "***Config***" come illustrato nel capitolo "*Troubleshooting: modifica / duplicazione / cancellazione / esportazione di una Configurazione*"

Passo 5: scansione dei Certificato di firma e preassociazione fra Certificato e la relativa Configurazione

Prima di procedere a questa operazione assicurarsi di aver correttamente inserito le smart card all'interno dei relativi lettori nel dispositivo SCBox. Generalmente il corretto inserimento provoca un breve lampeggio del lettore, nel momento in cui la smart card viene inserita. Si ricorda che, in una configurazione in High Availability (Alta Affidabilità) solo una fila di lettori viene collegata all'appliance αPeS, tramite il relativo cavo USB, fornito in dotazione. L'altra fila di lettori andrà collegata all'appliance αPeS secondaria. In questa configurazione, l'Amministratore dovrà disporre di una coppia di smart card con il medesimo scopo di firma.

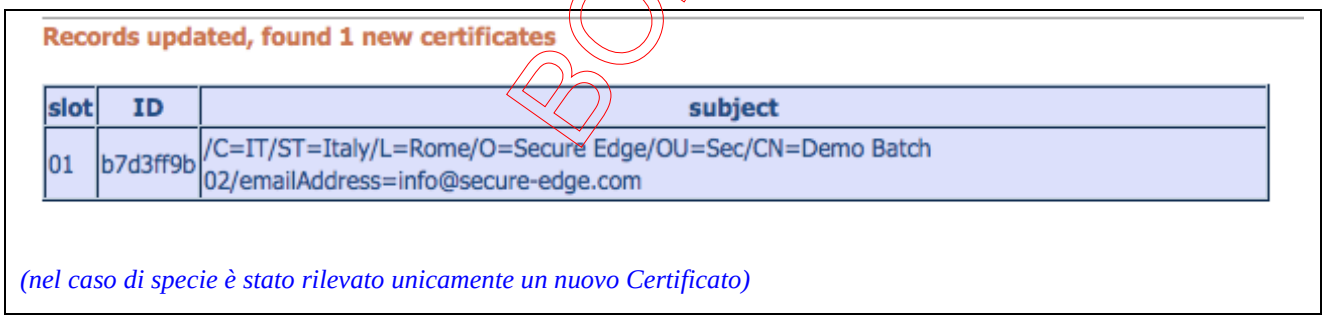
Affinché i Certificato (smart card / token) per la firma possano essere utilizzati, l'Amministratore deve operare la loro scansione. Questa operazione va ripetuta ogni volta che un nuovo Certificato viene aggiunto all'interno dei lettori nel dispositivo SCBox / Mini SCBox. Per operare questa scansione, l'Amministratore deve utilizzare il menu "Tokens" nell'area "PeS". Qualora si tratti della prima scansione assoluta, la finestra non mostrerà ancora alcun Certificato in lista, come illustrato nella figura seguente:



L'Amministratore deve quindi premere il tasto "*Perform full scan*" per procedere alla prima scansione dei lettori collegati all'appliance αPeS. Per abbreviare i tempi di attesa, durante le scansioni successive, l'Amministratore potrà utilizzare il tasto "*Look for new Tokens*" in modo da effettuare una scansione mirata a cercare variazioni rispetto al numero di smart card presenti (aggiunta o rimozione).

Durante la scansione compare il seguente messaggio: "**Scan in progress, may take time... please wait 2 minutes then go on with administration**". Attendere quindi 120 secondi. Se le smart card sono state inserite e correttamente rilevate appariranno nella tabella "*Connected / recorded cryptographic Tokens*", sopra la quale è anche presente una indicazione numerica sul numero complessivo di Certificato rilevati (utile in presenza di molti Certificato), come illustrato di seguito:

Nel caso in cui si desideri effettuare una scansione per rilevare esclusivamente i Certificato inseriti successivamente, dopo aver cliccato il tasto "*Look for new Tokens*", apparirà la schermata come illustrato nella seguente immagine:



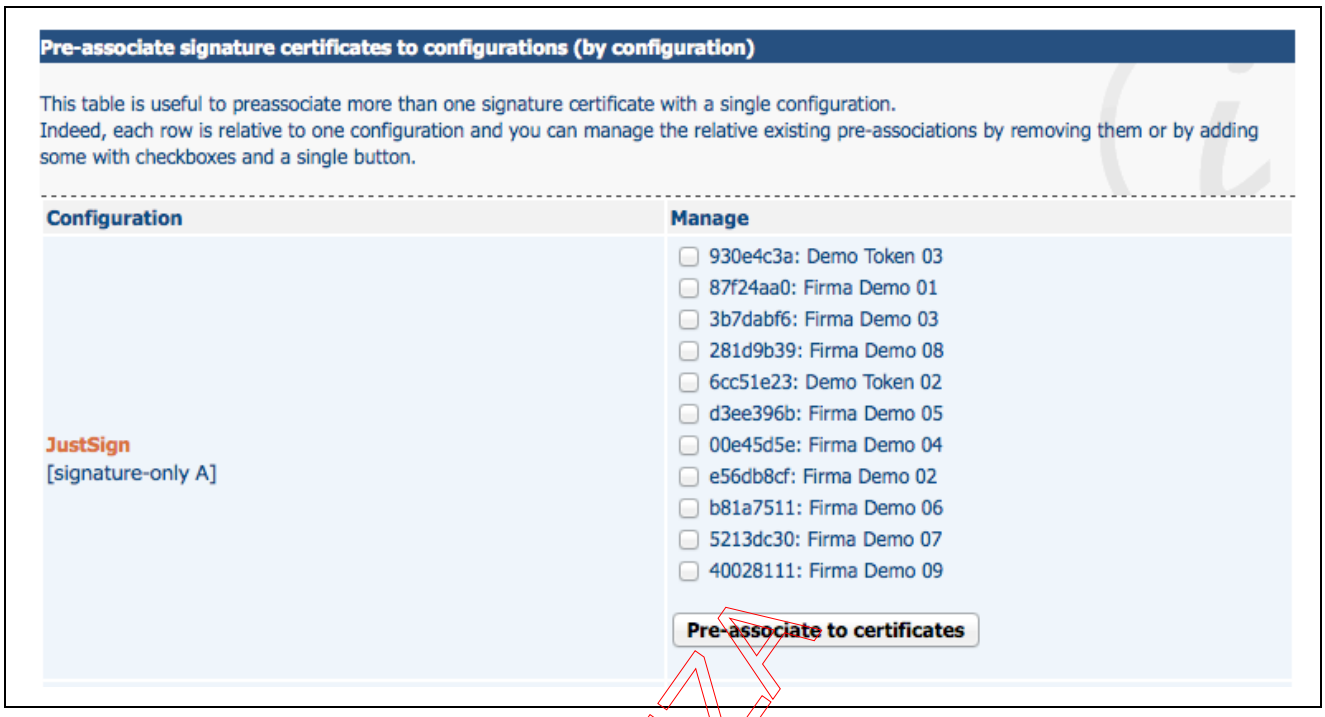
(nel caso di specie è stato rilevato unicamente un nuovo Certificato)

Per consentire al gateway di apporre la firma al documento, è necessario eseguire la sua "pre-associazione" con la Configurazione relativa al documento medesimo. Questa "pre-associazione" dovrà poi essere confermata, successivamente, dal Titolare del Certificato, una volta eseguita la Cerimonia e quindi l'attivazione del Certificato medesimo. L'operazione di preassociazione può essere svolta:

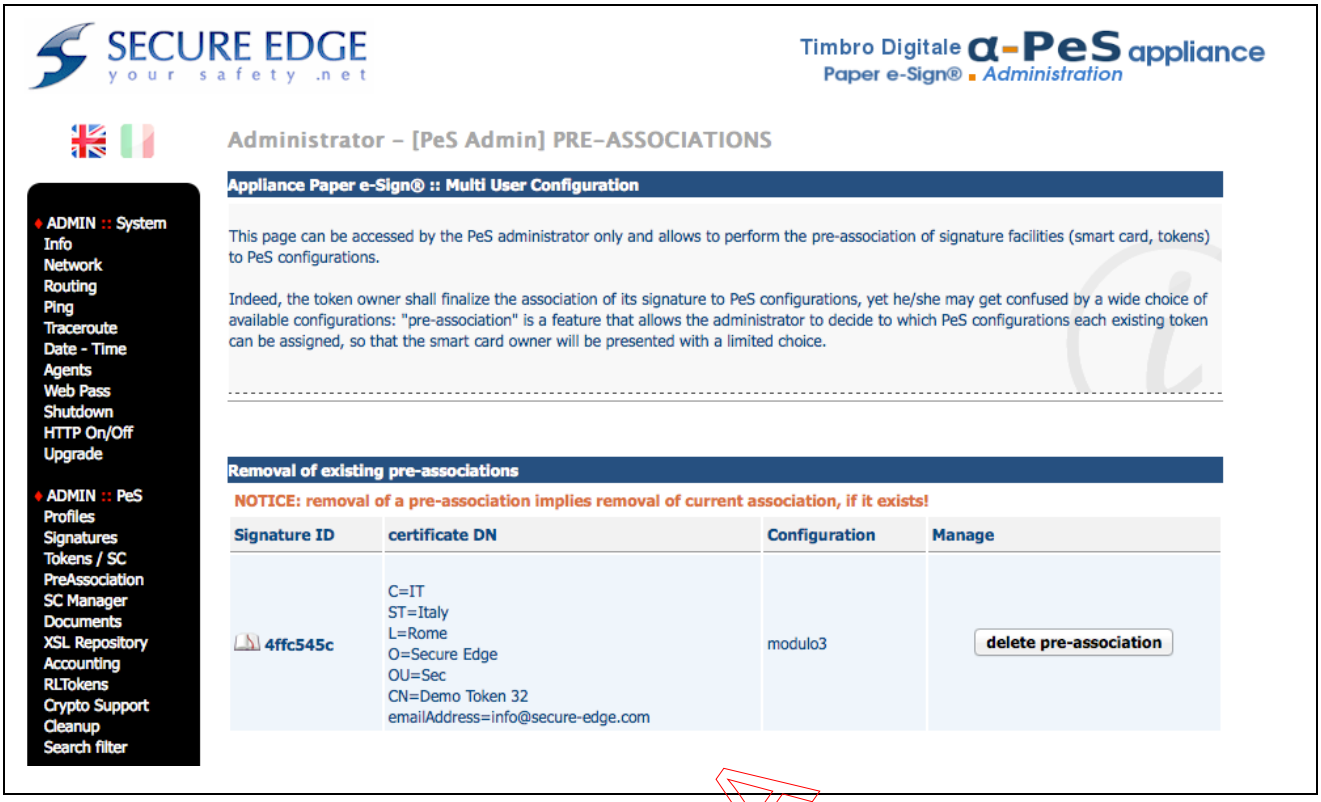
3. immediatamente al termine della scansione (qualora la Configurazione sia già presente)
4. successivamente (qualora la Configurazione non sia ancora presente o dovesse essere modificata)

Nel caso la Configurazione sia già presente e pronta ad essere utilizzata, è possibile utilizzare la colonna "*Preassociate*" della tabella menzionata nell'immagine precedente e scegliere l'opportuna Configurazione dal menu a tendina; quindi confermare cliccando sul tasto "*Preassociate to cfg*" .

Nel caso la configurazione non sia ancora disponibile (o comunque si intenda posticipare questa operazione, è possibile utilizzare anche l'apposito menu "***PreAssociation***" dell'area "***Admin : PeS***". In tal modo si giunge tabella "*Pre-associate signature certificate to configuration*", illustrata nella figura seguente:



La pagina prevede anche la possibilità di rimuovere le pre-associazioni esistenti (solo fino al momento in cui il Certificato non è stato inizializzato dal Titolare). Nel caso in cui nessuna pre-associazione sia stata effettuata, chiaramente la tabella "*Removal of existing pre-associations*" si presenterà vuota. Per poter effettuare la pre-associazione fra il Certificato e la Configurazione è sufficiente utilizzare la successiva tabella ("*Pre-association cryptographic Tokens*"), selezionando per ciascun certificato di firma la relativa Configurazione dalla finestra a tendina verticale e confermando la scelta cliccando sul pulsante "*Pre-associate Certificato to Configuration*". La pre-associazione verrà quindi confermata sia dalla presenza del messaggio "***Pre-association of certificate [ID_Certificate] to configuration [Configuration_Name] performed successfully***", sia dall'inserimento della pre-associazione nella tabella "*Removal of existing pre-associations*", come illustrato nella figura seguente:



Prestare sempre attenzione al valore di identificazione (ID) del certificato di firma, prima di procedere con questa operazione. Il valore di identificazione è presente nella prima prima riga di dettaglio delle informazioni relative al certificato stesso. Qualora si cerchi di pre-associare lo stesso Certificato alla medesima Configurazione per più di una volta, comparirà il seguente messaggio di avviso; "*WARNING: pre-association already exists, skipping...*"

Una stessa Configurazione può avere pre-associati "n" Certificato di firma. Questa operazione è consentita qualora più Titolari siano abilitati a firmare il medesimo documento previsto dalla Configurazione oppure per consentire ad uno stesso Titolare di firma di apporre il Timbro sulla stessa Configurazione sfruttando più certificato contemporaneamente, in caso si preveda un numero molto elevato di richieste di firma.

In mancanza di una preassociazione fra Certificato e Configurazione, il Titolare del Certificato non potrà procedere alla definiva assegnazione per proprio certificato di firma alla Configurazione. E' quindi assolutamente necessario che l'Amministratore ottemperi questa operazione prima che il Certificato venga inizializzato (Cerimonia) dal Titolare.

Passo 6: associazione del profilo titolare del Certificato al relativo Certificato di firma

Prima di procedere a questa operazione assicurarsi di aver correttamente inserito le smart card all'interno dei relativi lettori nel dispositivo SCBox. Generalmente il corretto inserimento provoca un breve lampeggio del lettore, nel momento in cui la smart card viene inserita. Si ricorda che, in una configurazione in High Availability (Alta Affidabilità) solo una fila di lettori viene collegata all'appliance αPeS, tramite il relativo cavo USB, fornito in dotazione. L'altra fila di lettori andrà collegata all'appliance αPeS secondaria. In questa configurazione, l'Amministratore dovrà disporre di una coppia di smart card con il medesimo scopo di firma.

Prima di eseguire l'inizializzazione del Certificato contenente il certificato di firma ("Cerimonia"), l'Amministratore deve associare univocamente il profilo di Titolare del Certificato al relativo certificato di firma. Tramite questa operazione, il titolare del Certificato potrà utilizzare unicamente il certificato di firma per il quale è autorizzato. Per eseguire questa operazione è a disposizione il Menu "***Tokens***" dell'area "***Admin*** : ***PeS***" della barra laterale sinistra. E' possibile eseguire l'associazione successivamente alla scansione dei Certificato presenti all'interno dei relativi lettori. All'interno della tabella "*Connected / recorded cryptographic Tokens*" selezionare dalla colonna "*Assign*" il nome del Profilo del Titolare, tramite l'apposita finestra a tendina, come illustrato nella figura seguente:

La corretta associazione fra il certificato di firma presente nel Certificato e il Profilo del titolare, viene confermata con il messaggio: "***assignment of certificato [ID_Certificate] to profile [Profile_name] performed***".

Prestare sempre attenzione al valore di identificazione (ID) del certificato di firma, prima di procedere con questa operazione. Il valore di identificazione è presente nella prima prima riga di dettaglio delle informazioni relative al certificato stesso. Qualora si cerchi di associare lo stesso Certificato al medesimo Profilo del titolare per più di una volta, comparirà il seguente messaggio di errore: "***ERROR: cannot perform assignment, this profile already owns the given certificate.***"

Per avere una ulteriore conferma circa la corretta associazione fra il Profilo del Titolare di firma ed il Certificato, l'Amministratore può fare riferimento al menu "***Profiles***" dell'area "***Admin : PeS***", verificando la tabella "*Manage existing certificato assignments*", in paticolare nella colonna Tokens. Come illustrato nella figura seguente, nella riga relativa al Profilo del Titolare compariranno tutti i Certificato a lui assegnati.

(nel caso di specie, il Profilo del Titolare "Dirigente" risulta ora avere associato un Certificato di firma inizializzato, in quanto presente la dicitura "Ceremony done"; qualora fosse stato associato ad un certificato non ancora inizializzato sarebbe comparsa la dicitura "NO ceremony)

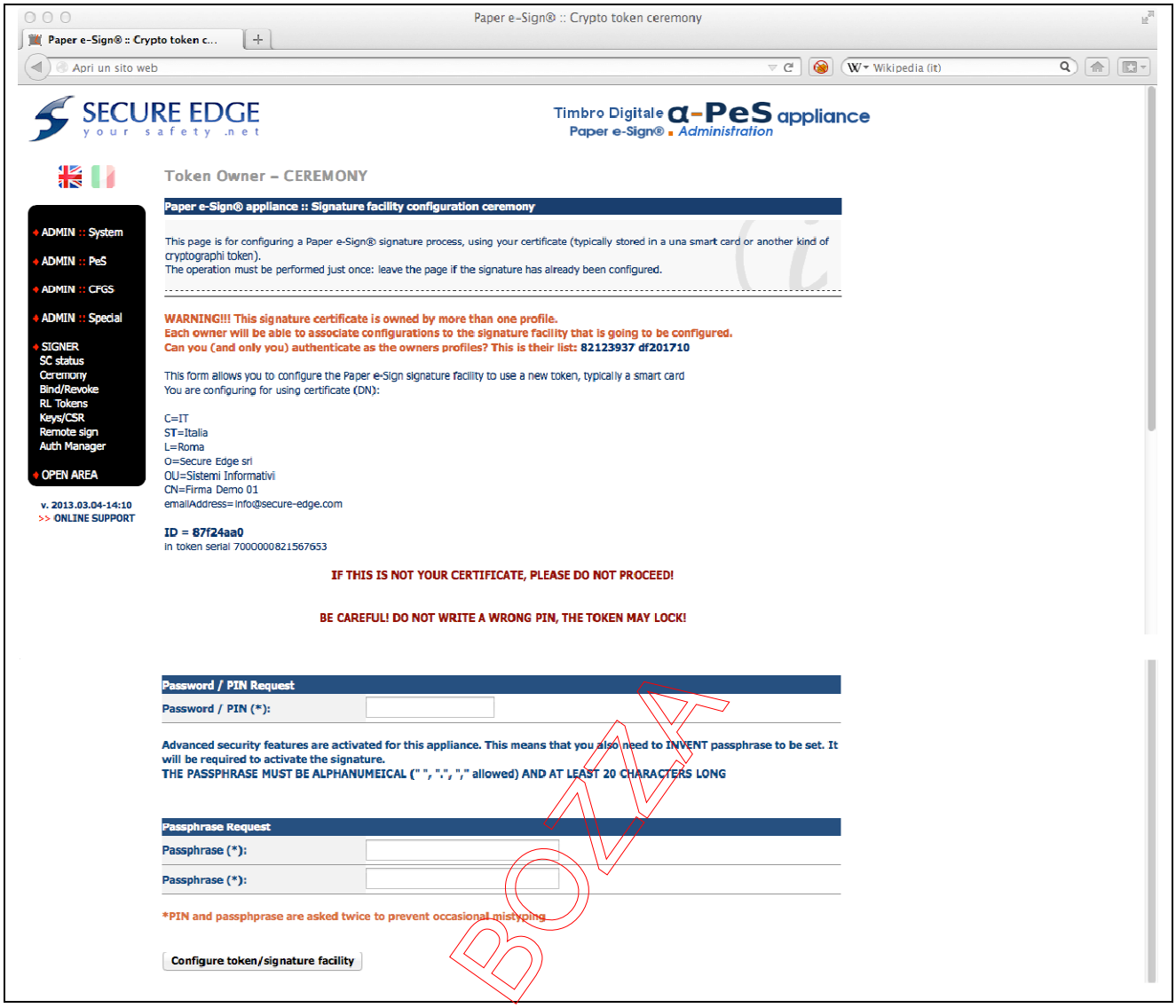
Passo 7: esecuzione della Cerimonia

Per rendere operativa la firma presente all'interno della Smart Card, è necessario che il Titolare del Certificato ("Certificato Owner") acceda alla propria area di amministrazione ed effettui l'inizializzazione o "cerimonia", in modo da associare al PIN una propria pass-phrase univoca, di almeno 20 caratteri, che andrà poi re-inserita successivamente, per confermare ogni ulteriore operazione.

Le operazioni che seguono devono essere svolte unicamente dal titolare del certificato di firma, che dovrà accedere con un proprio browser web, utilizzando il profilo di "Certificato Owner" e quindi il relativo certificato, precedentemente caricato dall'amministratore, come illustrato al precedente Passo 1. Tale certificato può essere importato all'interno del browser oppure inserito all'interno di un apposito dispositivo crittografico USB (scelta consigliata)

Per effettuare la Cerimonia, il Titolare del Certificato deve selezionare il menu "**Ceremony**". Verrà quindi visualizzata la pagina illustrata nella seguente figura:

In questa pagina vengono presentati tutti i Certificato di firma che l'Amministratore ha assegnato (tramite l'operazione di pre-associazione descritta al precedente Passo 6) al Titolare. In questa tabella non vengono effettuate distinzioni sulla tipologia di Certificato (ad esempio Oberthur, Incrypto 34v2 ecc…): tutti i Certificato assegnati vengono visualizzati. Il Titolare deve cliccare sul tasto "*Configure this token (ceremony)*" relativo al Certificato di cui intende effettuare la Cerimonia, per poter procedere alla sua inizializzazione. Si accedere quindi alla pagina di esecuzione della Cerimonia vera e propria illustrata nella figura seguente:



Nella parte superiore della pagina vengono riportate nuovamente, per ulteriore controllo/garanzia le informazioni relative al certificato di firma per il quale sta per essere eseguita la cerimonia. Qualora tutto coincida, il Titolare può proseguire con la Cerimonia e quindi può inserire, al riparo da sguardi indiscreti, il PIN di sblocco della Smart Card (o dispositivo di crittografia in cui è contenuto il certificato), comunicato dal fornitore della medesima (ad esempio “Actalis” o “Aruba”) all’interno della tabella “Password / PIN request”.

Qualora si inserisca un PIN errato per più di 3 volte consecutive, la Smart Card verrà automaticamente bloccata e risulterà impossibile proseguire questa operazione! In questa situazione sarà necessario effettuare lo sblocco della smart card attraverso apposito software di amministrazione, disponibile in genere sul sito web del fornitore della smart card medesima, utilizzando il relativo codice PUK. Qualora venga ulteriormente inserito in modo errato il codice PUK per più di 10 volte, la smart card risulterà definitivamente bloccata e sarà necessario procedere alla richiesta di una nuova smart card.

Quindi il Titolare del Certificato deve inserire una pass-phrase di sua fiducia di almeno 20 caratteri, all'interno della tabella "*Passphrase Request*". Infine premere il tasto "*Configure this token / signature facility*" per completare il processo di inizializzazione.

Nella scelta della pass-phrase si consiglia di inserire caratteri maiuscoli, minuscoli e numeri.

Qualora l'operazione di inizializzazione sia completata con successo, ovvero sia stato correttamente inserito il PIN, e sia stata confermata una pass-phrase valida, comparirà il seguente messaggio di conferma: "***checking PIN...OK OK, the system is configured for the new certificate".***

In caso non coincedesse il PIN inserito con quello assegnato alla smart card (o dispositivo crittografico), comparirà il seguente messaggio di errore: "***SORRY, the PIN check failed, cannot accept this configuration. BE CAREFUL! You may lock your certificato if you mistake the PIN too many times!***". La procedura di Cerimonia andrà ripetuta, e il Titolare del Certificato dovrà cliccare nuovamente sul menù "***Ceremony***" dalla barra laterale sinistra.

In caso non coincidesse la Passphrase inserita (ovvero la Passphrase inserita nel campo superiore fosse differente da quella inseita nel campo inferiore della tabella "*Passphrase Request*") comparirà il seguente messaggio di errore: "***ERROR: entered passphrases do not match***". La procedura di Cerimonia andrà ripetuta, e il Titolare del Certificato dovrà cliccare nuovamente sul menù "Ceremony" dalla barra laterale sinistra.

Passo 8: attivazione del certificato di firma

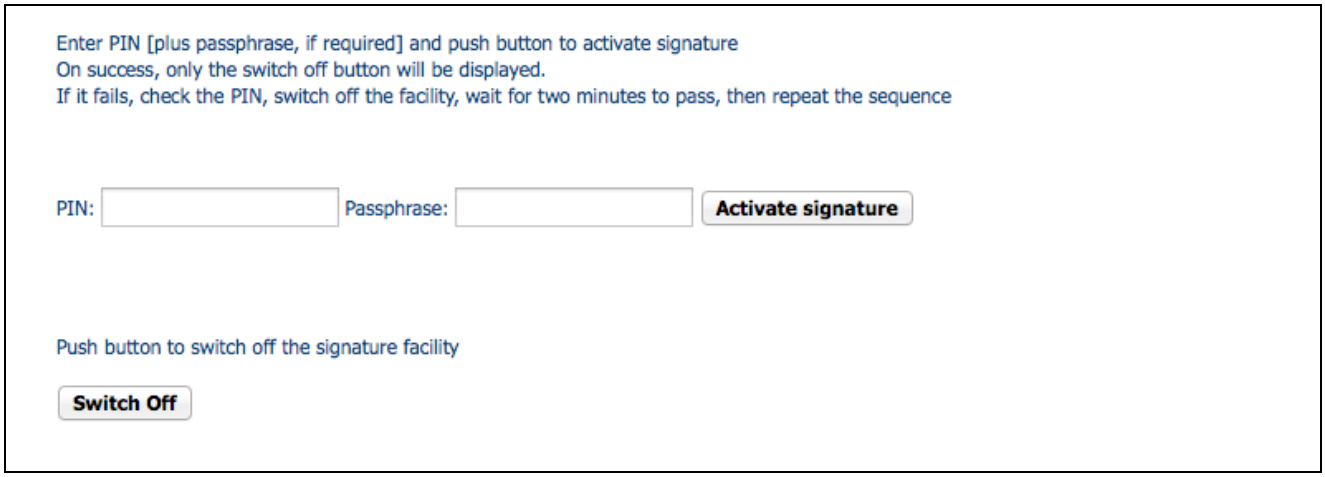
Per rendere operativo il certificato di firma, dopo averne effettuata la Cerimonia (inizializzazione) come descritto al precedente Passo 7, è necessario che il Titolare del Certificato ("Certificate Owner") ne esegua la successiva attivazione. In assenza di tale operazione il certificato di firma non potrà essere utilizzato dall'appliance αPeS per la generazione di Timbri.

Per eseguire questa operazione, il Titolare del Certificato deve accedere al menu "***SC Status***" . Cliccare quindi, all'interno della tabella "*Owned signature facilities*" sul tasto "*Manage*" relativo al Certificato (certificato di firma) che si desidera attivare, dallo stato iniziale di "Off", come illustrato nella figura seguente:

Verrà quindi visualizzata la seguente pagina, come illustrato di seguito:

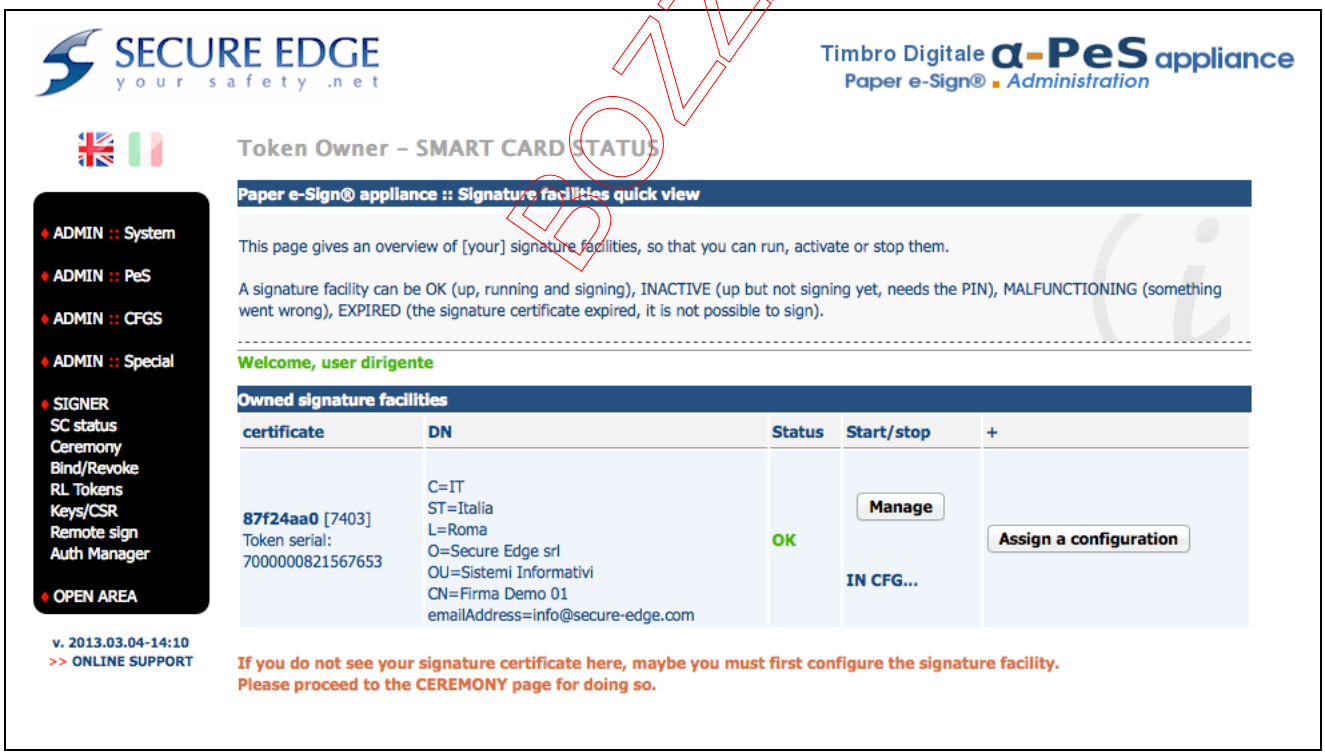
Come sempre, nella parte superiore della pagina, vengono riportate nuovamente, per ulteriore controllo/garanzia le informazioni relative al certificato di firma, prima di eseguirne l'attivazione. Qualora tutto coincida, il Titolare può proseguire con l'attivazione, cliccando sul tasto "*Switch On*".

Verrà chiesto di inserire nuovamente il PIN di sblocco della Smart Card (o del dispositivo crittografico), nonché la pass-phrase inserita durante la procedura di Cerimonia (inizializzazione), come illustrato nella figura seguente:



Il titolare del Certificato, dopo aver inserito questi due parametrri, deve cliccare sul tasto "*Activate Signature*".

Qualora l'operazione venga conclusa con successo, apparirà la scritta "***Activating signature... O:3.0.6:OK Checking facility status... THE FACILITY IS RUNNING AND THE SIGNATURE IS ACTIVE***" e il certificato verrà visualizzato in stato di "*Ok*" nella tabella della pagina "*Smart Card Status*", come illustrato nell'immagine seguente:



Nel caso in cui, per un errore di digitazione, il PIN o la pass-phrase non coincidessero a quanto inserito al momento della procedura di Cerimonia, comparirà il seguente messaggio di errore: "***ERROR: PIN (or passphrase) is not the same you entered the last time. Try again***". Questo errore non comporta la possibilità

di un eventuale blocco di funzionamento della smart card (o del dispositivo crittografico).Il Titolare dovrà quindi ripetere l'operazione.

A questo punto il certificato di firma è pronto e funzionante e necessita, unicamente, di essere associato all'opportuna Configurazione.

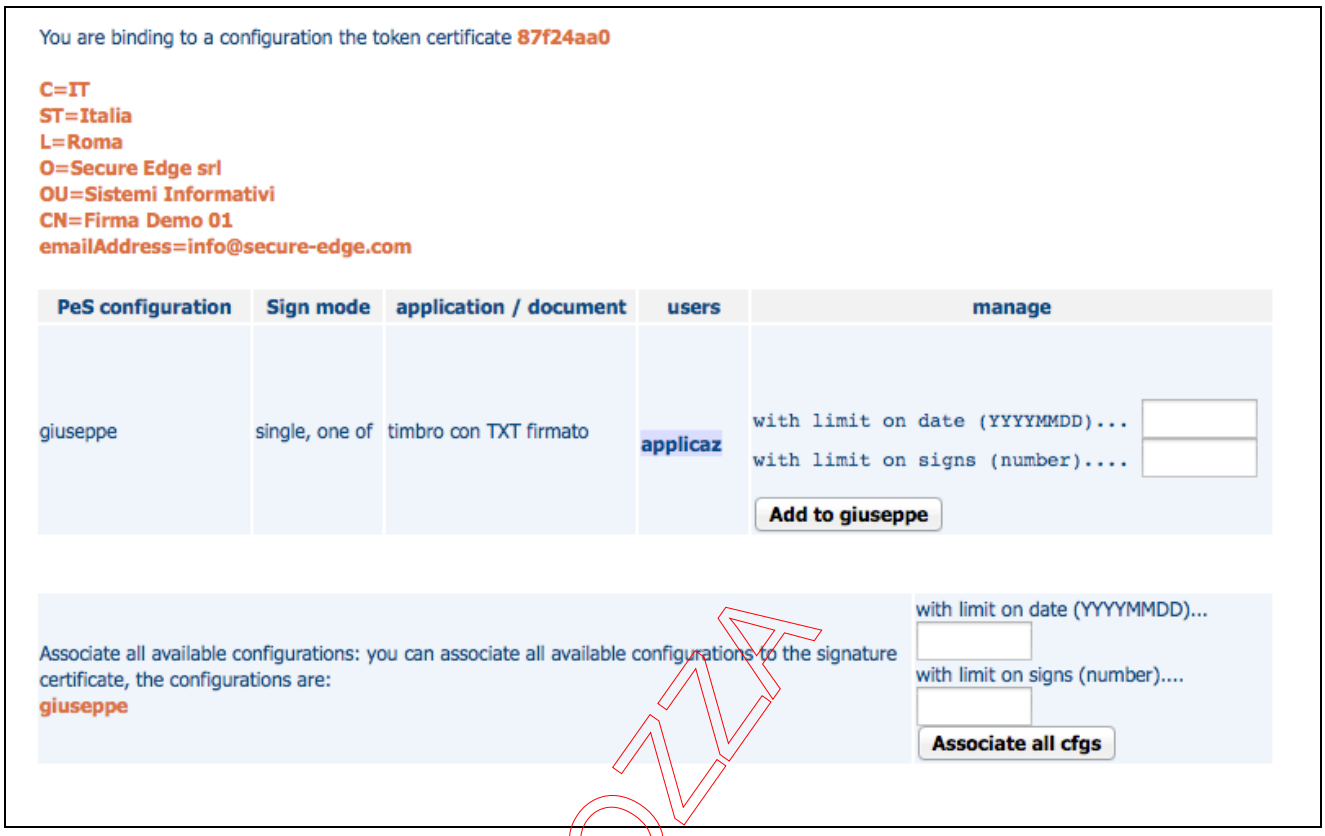
Infine per conoscere le Configurazioni associate al Certificato, è sufficiente che il Titolare clicchi sul link "*used by*": la lista delle Configurazioni associate verrà visualizzata in una nuova finestra.

Passo 9: associazione / revoca del certificato di firma alla Configurazione

L'ultimo passaggio per completare la configurazione del gateway di firma è quello di associare la firma, all'interno della Smart Card (o del dispositivo crittografico) alla relativa Configurazione, secondo la preassociazione effettuata dall'Amministratore al precedente Passo 5. Questa operazione deve essere svolta dal Titolare del Certificato. Accedere quindi al menu "***Assign / Revoke***" e selezionare, dalla seguente tabella "*Signature facilities management*", la riga contenente il certificato abilitato al precedente Passo 8 (verificare sempre la corrispondenza dell'ID del certificato ed il relativo Distinguished Name) come illustrato nella seguente figura:

(nel caso illustrato in questa figura non sono presenti Certificato già associati dal Titolare, i quali comparirebbero nella tabella "Existing assignments of signatures to Paper e-Sign configurations")

Cliccare quindi sul tasto "*Bind to PeS config…*" nella riga della tabella relativa al certificato per il quale si deve completare la procedura di associazione alla Configurazione. Verrà visualizzata la finestra illustrata nella seguente illustrazione:



In quest'ultima pagina, vengono sempre visualizzate (per ulteriore controllo) le informazioni relative all'ID del certificato di firma che si sta associando alla configurazione, con i principali dati dati relativi agli scopi del certificato medesimo. La tabella sottostante riepiloga il nome della configurazione a cui si sta associando il certificato di firma, la sua descrizione sintetica inserita dall'Amministratore, nonché il nome del Profilo dell'Applicazione associata alla configurazione (sempre a cura dell'Amministratore). Il Titolare del Certificato dovrà ciccare sul tasto "*Add to [configuration_name]*" per procedere al completamento dell'associazione. Qualora il Titolare del Certificato desiderasse, per motivi di gestione, limitare la validità di questa associazione potrà inserire una limitazione temporale per la validità del processo di firma (campo "*with limit on sings*") e/o una limitazione al numero di firme che possono essere effettuate (campo "*with limit on date*"). Questi parametri sono del tutto indipendenti dal numero di firme previste dalla licenza d'uso globale oppure dalla validità temporale del certificato presente all'interno della Smart Card (o infrastruttura di crittografia). Qualora il Titolare del Certificato non specifichi alcun parametro, resteranno validi il numero di firme previste dalla licenza e la scadenza temporale del certificato, secondo quanto previsto al momento del rilascio da parte della relativa Certification Authority.

L'operazione viene confermata dal seguente messaggio:

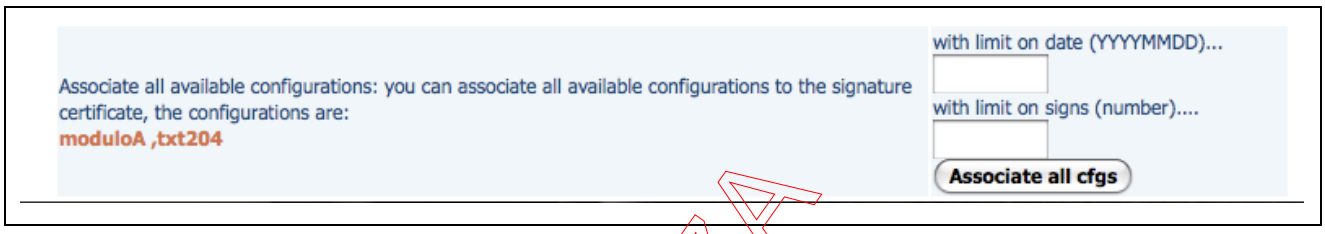
"***performed binding of signature certificate [Certificate_ID] to configuration [Configuration_name]***

OK: signature [Certificate_ID] now associated with configuration [Configuration_name]"

Non è possibile procedere all'associazione fra Configurazione e Certificato da parte del Titolare qualora la Configurazione non abbia già assegnato un Profilo dell'Applicazione, come illustrato nel precedente Passo nr. 4. Accettarsi quindi che l'Amministrazione abbia già eseguito questo passaggio; in caso contrario comparirà il messaggio di avviso

"***CFG has no OWNERS.CANNOT associate signature***".

Qualora siano presenti due o più Configurazioni che il Titolare di Firma dovesse associare al Certificato, per sua comodità d'uso può utilizzare la tabella illustrata nella figura seguente, la quale si trova in fondo alla pagina:



Cliccando sul pulsate "*Associate to all cfgs*" il Certificato di firma viene automaticamente associato a tutte le configurazioni indicate in colore arancio. Similarmente a quanto previsto per la singola configurazione, anche in questo caso è possibile applicare le stesse limitazioni numeriche e/o temporali a questa associazione multipla. Gli stessi parametri di limitazione saranno automaticamente applicati a tutte le Configurazioni. E' quindi evidente che, in caso si desiderasse applicare delle limitazioni differenti per ogni singola Configurazione, il Titolare del Certificato dovrà procedere singolarmente ad indicare questi parametri e quindi ad operare singolarmente le associazioni una alla volta.

Terminata questa procedura, l'appliance αPeS è pronto per ricevere i documenti da sottoporre al processo di firma digitale; ciò è confermato dall'inserimento della Configurazione all'interno della tabella "*Assignment of certificato to Paper e-Sign configurations*" come illustrato nella figura seguente:

Existing assignments of signatures to Paper e-Sign configurations

PeS config	Signature crt ID	Signature Certificate	Limits	Manage
giuseppe timbro con TXT firmato signature type: single, one of	87f24aa0	C=IT ST=Italia L=Roma O=Secure Edge srl OU=Sistemi Informativi CN=Firma Demo 01 emailAddress=info@secure-edge.com	max 15000 signatures remaining: 15000 till date 2014-09-01	Revoke assignment

(nel caso specifico è presente anche l'indicazione di una limitazione temporanea a 15000 timbri ed una scadenza della validità di questa associazione al 1/09/2014)

Come si può notare il titolare del Certificato può, in ogni momento lo ritenesse opportuno, bloccare il meccanismo di firma, cliccando sul tasto "*Revoke assignment.*". In questo modo viene revocata l'associazione fra il Certificato di firma e la Configurazione. Tuttavia il Certificato mantiene il completo stato di validità e il Titolare non ha necessità di reinseirire alcun PIN e Pass-phrase. L'operarazione di revoca dell'assegnazione viene confermata dalla presenza del seguente messaggio:

Proceeding with deassignment...

Completed deassignment of signature facility from [Configuration_name]

Per ripristinare nuovamente il l'associazione dovrà essere ripetuto quando descritto all'interno di questo questo Passo nr. 9.

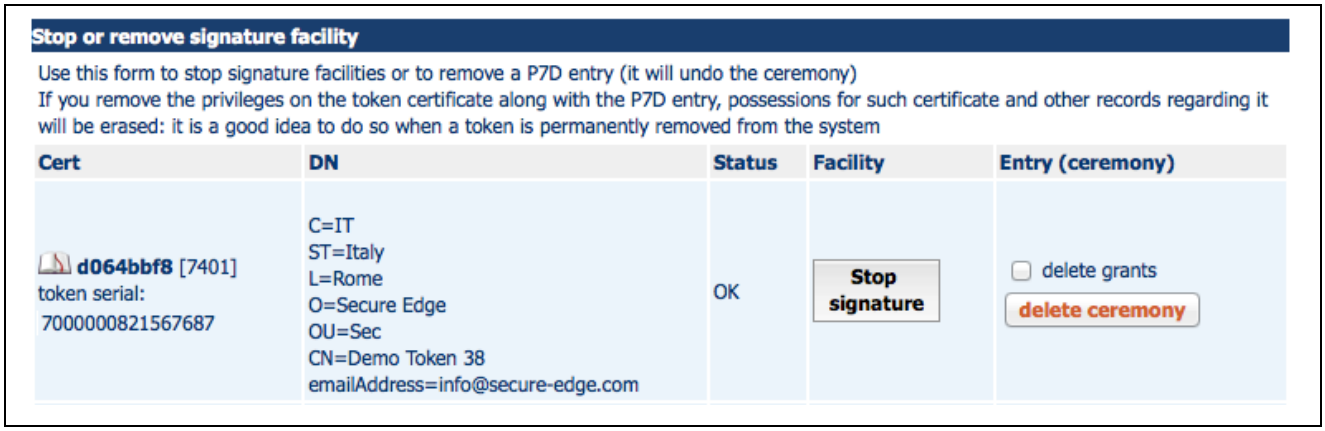
Troubleshooting sulla configurazione

Reset del Certificato associato ad un Titolare (smarrimento pass-phrase)

Qualora il Titolare smarrisca la pass-phrase associata al proprio Certificato, l'Amministratore ne può eseguire il reset.

Attenzione: questa operazione comporta l'interruzione delle operazioni di firma, poiché sarà necessario interrompere, temporaneamente, il funzionamento della smart card (o del dispositivo crittografico). L'operazione di reset del Certificato è irreversibile! Prima di procedere controllare tutti i parametri relativi al Certificato che si intende resettare (in particolare l'ID del certificato)

Per effettuare questa operazione, l'Amministratore deve utilizzare il menu "***Signatures***" dell'area "***Admin : PeS***" dalla barra laterale sinistra. Verrà quindi visualizzata la pagina descritta nella figura seguente:



L'indicazione dello "*Status*" su "*OK*" indica che il Certificato è stato correttamente inizializzato dal Titolare attraverso la relativa "Cerimonia". Qualora sia necessario eseguire un reset della Cerimonia (e quindi della pass-phrase associata al PIN), l'Amministratore deve semplicemente cliccare sul tasto "*Remove Entry*", associato al Certificato per il quale si desidera eseguire questa operazione di reset. L'operazione sarà confermata definitivamente dalla comparsa del seguente messaggio: "***Entry [Certificate_ID] successfully removed***". Il Certificato scomparirà dalla tabella "*Stop or remove signature facilities*".

L'Amministratore potrà nuovamente associare il Certificato al Profilo del Titolare, come illustrato al Punto 6.

Questa pagina può anche essere utilizzata dall'Amministratore per operare una semplice interruzione del meccanismo di firma associato al Certificato, nel caso in cui si rendesse necessario.

Funzioni Accessorie

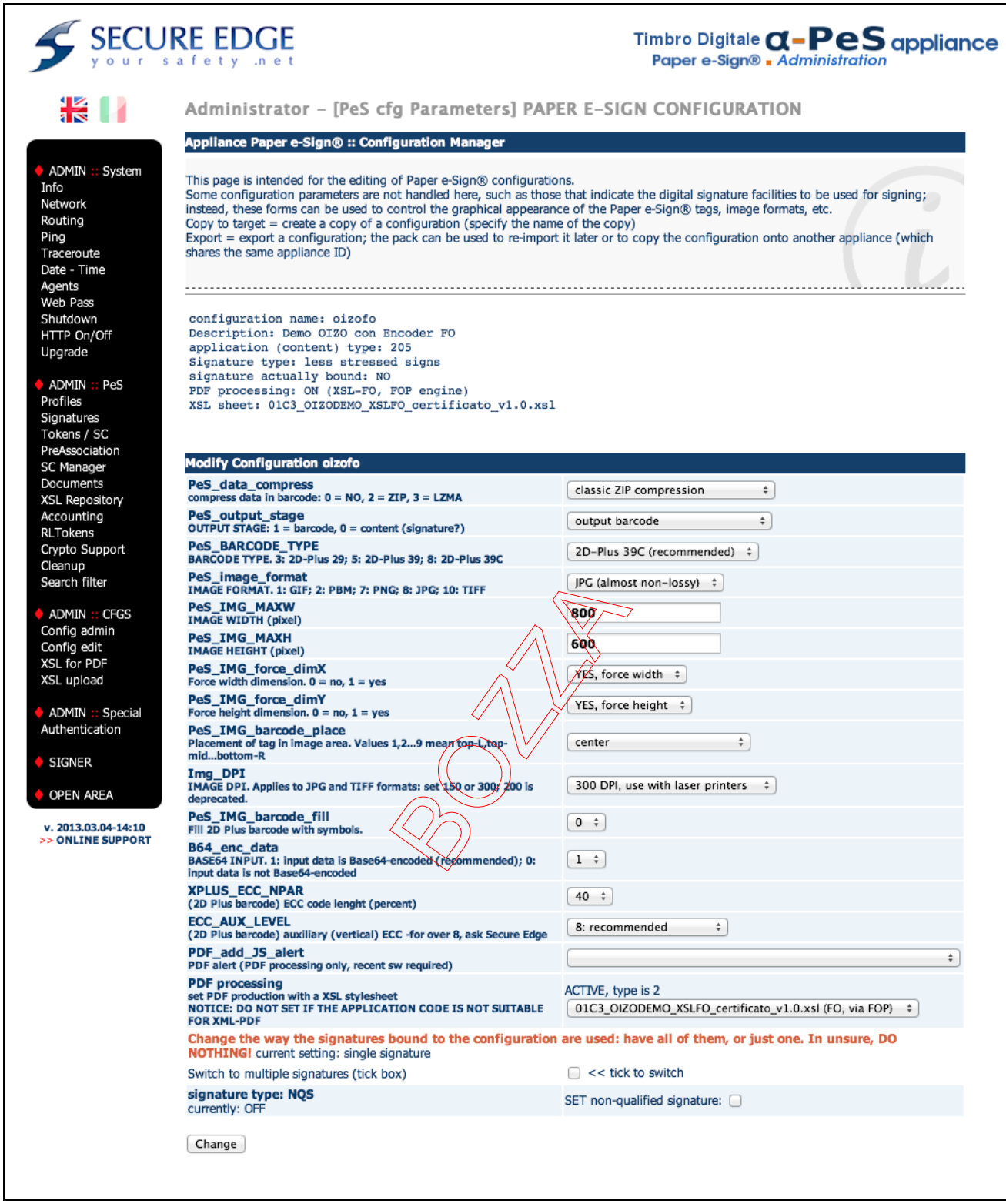
Modifica / Copia / Cancellazione / Esportazione di una Configurazione

In alcune condizioni, l'Amministratore potrebbe avere la necessità di operare alcune operazioni sulle configurazioni presenti all'interno dell'appliance αPeS, ovvero:

- La modifica dei parametri di generazione del Tibro associati ad una Configurazione
- La duplicazione di una Configurazione (con un nome differente)
- La cancellazione di una Configurazione
- L'esportazione su file di una Configurazione

Per operare queste operazioni, è a disposizione dell'Amministratore il menu "***Config Edit***" dell'area "***Admin : Cfgs***" dalla barra laterale sinistra. Verrà visualizzata la pagina illustrata nella figura seguente:

Per poter accedere ai parametri di generazione del Timbro, cliccare sul simbolo della matita all'interno della colonna "*Edit*". Verrà quindi presentata la pagina illustrata nella figura seguente:



Il dettaglio per meglio comprendere il significato di ogni parametro è descritto nel documento *[SE_T-07-0049] T I DST Usage from applications [3.9].pdf*

Per effettuare la cancellazione di una Configurazione (ad esempio non più in uso o errata), utilizzare il simbolo del cestino  dalla colonna "*Delete*". Qualora l'operazione venisse completata con successo verrà visualizzato il messaggio "***Deleting configuration [Configuration_name]... Configuration deleted!***

E' possibile eseguire la cancellazione anche di una configurazione associata da un Titolare ad un Certificato.

Per effettuare la duplicazione di una Configurazione, utilizzare il tasto "*Duplicate*" dalla colonna "*Make a copy*". Prima di cliccare su questo tasto l'Amministratore deve inserire nel campo "*target configuration name"* un nome da assegnare alla nuova configurazione (chiaramente differente dall'originale). L'operazione verrà confermata dal seguente messaggio: "***Configuration copied successfully NOTICE: pre-associations and assignment to profiles must be manually performed***". La nuova Configurazione duplicata chiaramente avrà tutti i parametri relativi alla generazione del Timbro identici alla Configurazione originale. Tuttavia, come indica il messaggio di conferma, l'Amministratore dovrà ricreare, per la Configurazione duplicata, sia la preassociazione al Certificato di firma (vedi Passo 6) sia l'associazione al Profilo dell'Applicazione opportuno (passo 4).

Per effettuare l'esportazione di una Configurazione è necessario cliccare sul relativo tasto "Export": verrà generato automaticamente un link, come illustrato nella figura seguente:

Export pack created. Click on this link to retrieve.

Cliccando su "*this link*" si accede al download del file relativo alla Configurazione.

Il file esportato è in formato "*.PeS_cfg_export*". E' utile sapere che il file può essere importato solo su un appliance αPeS con il medesimo "Client ID" (in genere lo stesso appliance oppure l'appliance secondario in una configurazione in Alta Affidabilità).

Indice