Attivazione servizio timbro digitale: procedure operative

(Piattaforma PeS® 2D Plus™)

Release	Data	Modifiche effettuate	Redatto (acronimo)	Approvato (acr. Pm)
1.0	03/12/2008	Emissione...	SFN	
1.1	12/02/2009	Gestione certificati, revoche firme e credenziali autenticazione	SFN	
1.2	09/04/2009	Interfaccia Web, Documentazione di riferimento	SFN	
1.3	14/04/2009	Inserimento immagine form, riorganizzazione testo, modifiche alla documentazione di riferimento, capitolo “Operazioni sul campo”	FCR	SFN
1.5	07/07/2007	Alcune modifiche apportate secondo suggerimenti personale Sysdata in aggiornamento presso nostra sede	ESP	

© GT50 s.r.l - Sede Legale: via Filippo Corridoni 19 - 00195 Roma (Italy)- R.I. 10707081005 Codice Fiscale e P. IVA 10707081005
REA di Roma 1251264 - GT50_PEC@legalmail.it - Cap. Sociale 10.000€ i.v. - fax 06.66016812 Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

SOMMARIO

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

1 DEFINIZIONI E ACRONIMI

Termine/Sigla	Descrizione
ADS	Firma digitale automatica
CAD	Codice dell'Amministrazione Digitale
Certificatore Accreditati	Una Certification Authority; che fornisce le Smart Card e le coppie di chiavi di firma digitale; deve risultare nell'elenco certificatori accreditati dal CNIPA
DRT (Dichiarazione per Richiesta Timbro)	Documento preparato dal RAp; contiene le informazioni necessarie affinchè il TSC abbia consapevolezza (legale) di ciò che la sua Smart Card firmerà
DT	Documento da firmare in modo automatico per generare il Timbro Digitale; identificato da IDD
ICP (Identificativo Configurazione PeS)	Identificativo di un gruppo di informazioni e parametri necessari per generare un timbro digitale per un DT, in modo coerente con quanto indicato
IDA (identificativo applicazione)	Identificativo della applicazione che genera documenti DT e richiede per questi timbri digitali; comprende una breve descrizione
IDD (identificativo documento)	Identificativo del singolo DT; comprende una breve descrizione
PAdm (PeS Administrator)	amministratore del Software Core Appliance αPeS 2D-Plus®
RAp (Responsabile Applicazione)	persona fisica/ufficio che fornisce le informazioni al Titolare relativamente al contenuto dei documenti che quest'ultimo autorizzerà a firmare in modo automatico, con la smart card di cui risulta intestatario.
TCP (Tabella Configurazioni PeS)	Contiene una entri per ogni univoco ICP/IDT/XAA
TD	Timbro Digitale
TSC (Titolare Smart card):	persona fisica, che fà la richiesta ed a cui è assegnata una Smart Card di firma digitale, di cui quindi risulta intestatario e responsabile;
XAT	Certificato di autenticazione X.509 del titolare (TSC)
XSG	Certificato di firma presente nella Smart Card di un TSC
XAA	Certificato di autenticazione X.509 dell'appliance che crea i DT e per questi documenti richiede la generazione del timbro digitale

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

2 DOCUMENTAZIONE DI RIFERIMENTO

Codice dell'Amministrazione Digitale Testo integrato e correttivo del DLGS 7/3/05 n. 82 e DLGS 4/4/06 n. 159
PAdm Manual Manuale dell'amministratore (PeS Administrator) del Software Core Appliance αPeS 2D-Plus® [SE_T-07-0049] T I DST PeS Admin Manual [u.v].doc
Smart Card Owner Guide Manuale dell'interfaccia web per il titolare di una Smart Card di firma digitale automatica [SE_T-07-0049] T I MAN Smart Card Owner Guide [u.v].doc
Procedure Operative Piattaforma PeS 2D-Plus® Guida alle procedure operative ed alle policy di sicurezza, nell'integrazione di una piattaforma 2D-Plus® [SE_T-07-0049] T I DST proc operative aPeS [u.v].doc
DRT- Form di richiesta TD Dichiarazione di Richiesta di un Timbro Digitale per uno specifico documento (Policy) [SE_T-07-0049] T E ALL DRT - Form richiesta TD [u.v].doc
Decoder Plus® - User Guide Manuale utente del software Decoder 2D-Plus® [SE_T-07-0053] T I MAN User Guide [u.v].doc
Code Examples Esempi di programmazione in vari linguaggi [SE_T-07-0053] T I ALL CodeExamples [u.v].doc
Making a XML/XSL Specifiche per la costruzione di file XSL-CSS di formattazione dei dati XML [SE_T-07-0053] T I ALL Making XML-XSL [u.v].doc
TextGraph Syntax Sintassi del file dati XML di input al programma TextGraph [SE_T-07-0053] T I ALL TextGraph Syntax [u.v].doc
SCBox 1U e 3U Brochure [SE_T-08-0054] T I BRC SCBox [u.v].doc

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

3 PREMESSA

Un processo automatico di firma digitale [ADS] viene tipicamente messo in atto quando c'è un consistente numero di documenti da firmare.

In questo caso, il processo di firma è governato da un computer, al quale è stata *assegnata* una smart card dedicata al processo.

Nel nostro caso, questo computer è un Appliance αPeS™ 2D-Plus®, un apparato dedicato alla ADS ed alla generazione di Timbri Digitali, pensato per gestire più smart card e più processi logicamente separati di ADS.

In questo documento, si dà per acquisita la competenza sui processi di ADS, così come sono presentati e consentiti dal Codice dell'Amministrazione Digitale [CAD], e da tutta la normativa che regola l'uso dei dispositivi sicuri di firma.

3.1 SCOPO DEL DOCUMENTO

Lo scopo di questo documento è quello di suggerire le procedure operative e le policy di sicurezza, associate all'utilizzo di un Appliance αPeS 2D-Plus®, in contesti dove esistano uno o più Titolari di Smart Card [TSC] ed uno o più documenti sui quali apporre un timbro digitale.

La capacità dell'Appliance αPeS 2D-Plus® di gestire più titolari abilitati a lavorare con questo sistema comporta una serie di adempimenti tecnici ed organizzativi.

Il documento descriverà:

- ✓ le motivazioni che rendono necessario l'uso di uno speciale hardware per la conservazione delle Smart Card dedicate alla ADS (SCBox);
- ✓ le apparecchiature hardware ed i software necessari;
- ✓ le procedure operative che si rendono necessarie per fornire ai Titolari delle firme digitali ed propietari delle Smart Card un livello adeguato di assicurazione relativamente all'utilizzo delle Smart Card stesse ed all'esercizio della ADS ad esse associata;

❖

3.2 RICHIAMO ALLA NORMA

Si ricorda che le applicazioni che contemplano l'uso della ADS necessitano di una coppia di chiavi dedicate a questo utilizzo e della richiesta ad un Certificatore accreditato di un certificato di firma (X.509) che dovrà riportare come destinazione d'uso: per Firma Digitale Automatica (ADS).

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

A discrezione del Certificatore, questo particolare utilizzo potrebbe risultare come un limite d'uso di questa coppia di chiavi, indicato all'interno del certificato X.509 rilasciato.

Si richiede che ogni dispositivo di firma utilizzato per procedure automatiche debba disporre di coppie di chiavi differenti, una per dispositivo, anche se il Titolare fosse lo stesso.

Altresì è richiesto che il titolare del certificato garantisca la custodia del dispositivo di firma e che lo utilizzi personalmente.

In ultimo si ricorda che, una volta che il dispositivo di firma contenente la coppia di chiavi fosse pronto all'uso, solo il Titolare deve avere la possibilità di attivarlo e disattivarlo.

Tutti questi obblighi sono dettati dalla normativa italiana in materia di Firma Digitale.

Nella trattazione che segue i "dispositivi sicuri di firma" sono delle Smart Card che possiedono le caratteristiche richieste dalla legge.

❖

3.3 OVERVIEW SULL'OPERATIVITA' DELLA PIATTAFORMA

A grandi linee, il processo di generazione di un timbro digitale prevede che un'applicazione software faccia, tramite una connessione in rete, una richiesta di timbro digitale all'appliance passando a quest'ultimo i dati da firmare ed alcune informazioni accessorie.

L'appliance a sua volta deve avere a disposizione una certo numero di informazioni e la disponibilità di uno o più apparati sicuri di firma digitale automatica su cui operare.

❖

4 APPLIANCE APES™ 2D-PLUS®

4.1 L'APPLIANCE

L'apparato che si occupa di operare i processi di ADS è definito **Appliance αPeS™ 2D-Plus®**

Tipicamente è un computer in una scatola da rack da 1U, che espone due interfacce web: una dedicata all'amministratore dell'appliance stesso [PAdm] ed una dedicata ai titolari delle smart card [TSC] dedicate alla ADS, che l'appliance gestisce ed utilizza.

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

αPeS™ 2D-Plus®inoltre espone sulla rete un ulteriore accesso https, che permette di richiedere una serie di servizi, tra cui quello di firma digitale automatica e quello di generazione di timbro digitale.

Tutte le interazioni con l'appliance avvengono in mutua autenticazione forte.

> *I dettagli sull'operatività dell'appliance, sulle interfacce di amministrazione e sui processi interni si trovano nel documento:*
> ***Manuale dell'amministratore (PeS Administrator) del Software Core Appliance αPeS™ 2D-Plus®***
> *disponibile all'indirizzo* ***http://www.timbrodigitale.com/Appliance_PeS/doc/***

4.2 LA SCBOX™

La presenza di più Titolari di ADS, quindi di più Smart Card, aumenta la complessità della loro gestione sicura.

Allo scopo di essere aderenti alle norme sopra citate, c'è quindi la necessità di disporre di un apparato che permetta di gestire la custodia consapevole delle Smart Card da parte dei singoli Titolari.

Secure Edge mette a disposizione un apparato, definito SCBox™, che consente di mettere on-line più smart card, fornendo ad ognuna un'area protetta con misure di sicurezza tamper evident.

Le SCBox™ sono delle scatole metalliche da rack, comprensive di alimentazione e di connettività USB, fornite in due modelli:

- ✓ il modello 1U (una unità) per la gestione di massimo 4 smart card;
- ✓ il modello 3U (tre unità) per la gestione di massimo 12 smart card.

Le SCBox™ possono essere connesse tra loro in daisy-chain --via USB-- fino ad avere un massimo di dieci SCBox™ connesse ad un singolo Appliance αPeS™ 2D-Plus®.

> *La scheda sulle SCBox™ è presente nel documento:*
> ***Brochure SCBox™ Secure Edge***
> *disponibile all'indirizzo* ***http://www.timbrodigitale.com/Appliance_PeS/doc/***

❖

5 ATTIVAZIONE DI UN SERVIZIO DI TIMBRO DIGITALE

Ricordiamo che le procedure e le sequenze operative qui riportate sono da intendersi come suggerimento all'Azienda o Ente, che intende adottare la soluzione per il rilascio di timbri digitali.

Ciò nonostante, ci sono alcuni dati che sono assolutamente necessari alla piattaforma software, per poter operare in completa integrità e sicurezza. Questi dati, devono comunque essere formalizzati.

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

Di seguito vengono definiti: i ruoli identificati per una corretta operatività della piattaforma Appliance αPeS™2D-Plus®, gli interventi organizzativi che l'Azienda/Ente dovrebbe approntare ed infine le procedure operative necessarie ad operare.

5.1 I RUOLI DEL PROCESSO

- ✓ **PeSAdmin [PAdm]**: amministratore della piattaforma e del Software Core Appliance αPeS 2D-Plus®;
- ✓ **Titolare della Smart Card [TSC]**: persona fisica, che fa la richiesta ed a cui è assegnata una Smart Card di firma digitale (automatica), di cui quindi risulta intestatario e responsabile;
- ✓ **Responsabile Applicazione [RAp]**: persona fisica/ufficio che è responsabile del corretto funzionamento dell'applicazione informatica che si interfaccia all'appliance, per richiedere i timbri digitali per specifici documenti.

❖

5.2 PREMESSE ORGANIZZATIVE

Per ogni ruolo vengono riportate alcune note organizzative.

5.2.1 TSC: TITOLARE DELLA SMART CARD

I processi di cui si parla prevedono che il TSC abbia già disponibile una smart card dedicata alla firma automatica di un documento.

In caso contrario, il TSC dovrebbe richiedere ad un Certificatore Accreditato una smart card indicando esplicitamente il suo utilizzo per firma digitale automatica (ADS);

Se il TSC fosse già in possesso di smart card per ADS, il TSC ha la facoltà di usare una delle sue smart card per la firma automatica già in uso, anche per firmare un ulteriore DT, senza doverne richiedere una nuova.

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

Inoltre, prima di utilizzare la piattaforma αPeS, il TSC dovrebbe richiedere al PAdm un certificato X.509 di autenticazione (XAT), valido per l'accesso all'interfaccia web presente sull'appliance e dedicata al TSC, per la cui descrizione si rimanda al documento Signer Guide u.v.

Questa interfaccia permette di attivare/disattivare la/e smart card del TSC e di abilitare/disabilitare le configurazioni ad essa/e associata/e.

5.2.2 RAp: Responsabile dell'Applicazione

Il RAp, responsabile dell'applicazione software che richiede i servizi alla piattaforma αPeS™ 2D-Plus®, deve definire identificativi univoci di queste procedure software (IDA) e deve procurare per ogni applicazione che le ospita un certificato di autenticazione forte XAA.

La definizione dei parametri e dei valori, sui quali basare la configurazione ICP (vedi cap. 7) da applicare per la creazione del timbro digitale, è di responsabilità congiunta del RAp e dell'Ufficio competente per il documento IDD a cui applicare un Timbro Digitale .

5.2.3 PAdm: Amministratore dell'Appliance

Il PAdm, oltre a supervisionare i processi che operano sulla piattaforma, deve occuparsi di gestire in modo opportuno le relazioni che intercorrono tra smart card, configurazioni, certificati di autenticazione dell'applicazione e titolari di smart card.

Sul PAdm ricade inoltre la responsabilità della definizione degli identificativi di configurazione (ICP) , il loro inserimento e la loro gestione informatizzata.

La descrizione dell'interfaccia PAdm è presente nel documento:
Manuale dell'amministratore (PeS Administrator) del Software Core Appliance αPeS™ 2D-Plus®
disponibile all'indirizzo ***http://www.timbrodigitale.com/Appliance_PeS/doc/***

Una nota sui dati presenti all'interno di una configurazione è nel capitolo 7 .

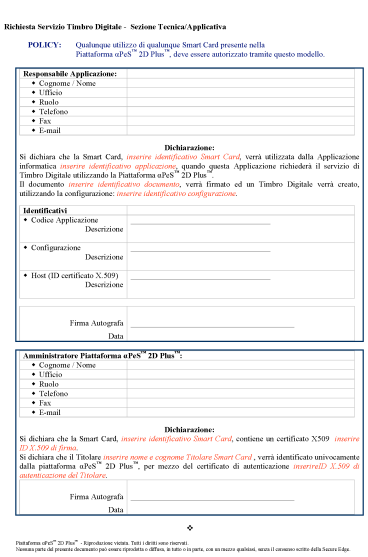
❖

5.3 Assicurazione e controllo delle operazioni

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

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

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



Richiesta Servizio Timbro Digitale - Sezione Tecnica/Applicativa

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

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

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

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

Firma Autografa
Data

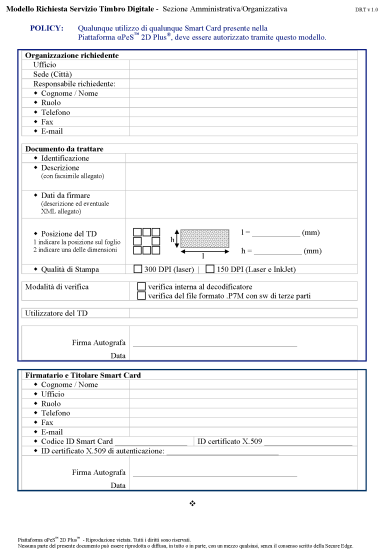
Amministratore Piattaforma αPeS™ 2D Plus™:
- Cognome / Nome
- Ufficio
- Ruolo
- Telefono
- Fax
- E-mail

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

Firma Autografa
Data

❖

Piattaforma αPeS™ 2D Plus™ - Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto della Secure Edge.



Modello Richiesta Servizio Timbro Digitale - Sezione Amministrativa/Organizzativa — DRT v 1.0

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

Organizzazione richiedente
- Ufficio
- Sede (Città)

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

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

Modalità di verifica — ☐ verifica interna al decodificatore ☐ verifica del file formato .P7M con sw di terze parti

Utilizzatore del TD

Firma Autografa
Data

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

Firma Autografa
Data

❖

Piattaforma αPeS™ 2D Plus™ - Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto della Secure Edge.

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

5.3.1 LA RICHIESTA

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

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

❖

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

5.3.2 I DATI DEL TITOLARE

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

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

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

❖

5.3.3 IL RAP E LE GARANZIE SULL'APPLICAZIONE INFORMATICA

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

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

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

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

Nella sezione di sua competenza:

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

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

l'applicazione richiedente e l'host che la ospita ed infine le smart card che potranno operare una ADS;

❖

5.3.4 IL PADM E LE GARANZIE SULL'OPERATIVITÀ DELL'APPLIANCE

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

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

5.3.5 COMPLETAMENTO DEL FORM: ACCETTAZIONE DA PARTE DEL FIRMATARIO

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

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

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

6 OPERAZIONI SUL CAMPO

6.1 TSC: PERSONALIZZAZIONE SMART CARD

All'arrivo di una nuova smart card, è buona prassi che il TSC sostituisca le originali credenziali di attivazione della smart card stessa: il PIN ed il PUK.

Il TSC dovrebbe utilizzare un PC off-line ed utilizzando il lettore di smart card ed il software fornito dal Certificatore Accreditato, operare per cambiare PIN e PUK assegnati inizialmente alla smart card.

Una volta che la Smart Card è stata personalizzata in questo modo, può essere sottoposta al rilascio ed attivazione, presso il centro che ospita l'Appliance αPeS e la SCBox.

❖

6.2 PADM: AGGIORNAMENTO DB APPLIANCE

Il PAdm, anche sollecitato dai RAp e dai TSC, aggiorna le strutture dati presenti nel Software Core Appliance αPeS 2D-Plus® come segue:

- ☞ su richiesta di un RAp, assegna un nuovo XAA ad un host applicativo, se questo non è ancora conosciuto dall'appliance; è cura del RAp, l'inserimento e l'uso dell'XAA da parte dell'applicazione software che richiede l'accesso all'appliance;
- ☞ su richiesta di un TSC, assegna a quest'ultimo un nuovo XAT; è cura del TSC l'integrazione e l'uso dell'XAT sul client/browser usato per accedere alle funzioni riservate al titolare della smart card, presente sull'appliance;
- ☞ su richiesta di un TSC, il PAdm prende in carico una nuova smart card di firma digitale automatica; alle funzioni pertinenti la smart card, viene programmato un accesso riservato al solo TSC, per mezzo dell'XAT in suo possesso;
- ☞ la configurazione ICP, indicata nel documento DRT, deve essere aggiornata con tutte le informazioni provenienti dal DRT stesso; in questa entry vengono registrate tutte le informazioni necessarie ad operare (vedi Cap.**7**).
  Naturalmente se la configurazione a cui si riferisce il DRT non fosse esistente, il PAdm ne crea una nuova nel DB delle configurazioni, con identificativo univoco ICP;

❖

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

6.3 TSC/PADM: CERIMONIA DI RILASCIO SMART CARD

La SCBox alloggia al suo interno le Smart Card che utilizza, sia per ragioni di sicurezza che in ottemperanza al CAD; in genere quindi il TSC è presente nella fase di inserimento della propria Smart Card nell'SCBox, per certificare che questa è stata inserita nell'apparato e nel luogo concordato.

Contemporaneamente il TSC dovrà comunicare al PAdm, il proprio XAT, in modo da poter successivamente accedere alla "Interfaccia Titolare" che l'Appliance mette a disposizione.

❖

6.4 TSC: ATTIVAZIONE FISICA DELLA SMART CARD ED ABILITAZIONE ALLA ICP

Svolte le attività relative ad un nuovo servizio di timbro digitale (vedi Cap.5), non è ancora possibile operare per la generazione del timbro digitale.

Anche se il TSC ha firmato il DRT, ci sono ancora due operazioni da ottemperare:

- ☞ Attivare la smart card, se questa non fosse già attivata;
- ☞ Abilitare la smart card ad operare per la specifica configurazione;

I due step sono indipendenti tra loro; è possibile infatti che una smart card sia già attiva ed operi firme digitali automatiche su configurazioni diverse: bisogna quindi abilitare la smart card alla ulteriore configurazione ICP.

È anche possibile che una smart card sia abilitata per una o più configurazioni, ma non sia attiva; il TSC deve quindi attivarla in modo esplicito.

Per renderla operativa e permettere che generi firme digitali a fronte delle richieste degli applicativi, il TSC dovrà attivarla utilizzando l'opportuna "Interfaccia Titolare" via web a cui il TSC ha accesso tramite una connessione sicura in mutua autenticazione forte che l'Appliance attiva, riconoscendo l'XAT del TSC.

Una volta che la smart card sia attiva ed abilitata a lavorare per una specifica configurazione, sarà possibile generare timbri digitali.

La stessa interfaccia web permetterà al TSC di interrompere/disattivare la Smart Card una volta completato il ciclo di produzione dei documenti; questa modalità garantisce che il controllo reale sull'uso della Smart Card, rimanga nelle mani del Titolare.

> *La descrizione dell'interfaccia per il Titolare è presente nel documento:*
> ***Manuale dell'interfaccia web per il titolare di una Smart Card di firma digitale automatica***
> *disponibile all'indirizzo* ***http://www.timbrodigitale.com/Appliance_PeS/doc/***

❖

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50

7 LA CONFIGURAZIONE

Le informazioni, necessarie all'appliance per operare a seguito di una richiesta proveniente da una applicazione software, sono contenute in una struttura dati, definita **configurazione**.

L'identificativo di quale configurazione utilizzare (ICP) è una delle informazioni di contorno, inviate dall'applicazione software all'appliance, nel messaggio di richiesta di un timbro digitale: questo parametro è fondamentale per il risultato da ottenere.

Una configurazione è un'insieme di dati, che definisce:

- ✓ l'identificativo del documento su cui si opera: IDD;
- ✓ l'identificativo dell'applicazione che può richiedere il Timbro Digitale: IDA;
- ✓ il certificato di autenticazione forte presentato dall'applicazione che ospita la IDA: XAA
- ✓ i certificati di chiave pubblica associati alle smart card che possono operare la ADS con questa configurazione: XSG
- ✓ i metadati specifici per il timbro digitale da fornire:
  - PPI da usare per l'immagine del timbro digitale: [1200 | 600 | **300** | 150];
  - Dimensioni del *rettangolo di contenimento*[1] presente sull'IDD;
  - Compressione dei dati: [**T**rue | False]
  - Tipo di firma digitale: [**PKCS#7** | PGP/GPG | N.A. | RSA]
  - Tipo di codice 2D-Plus®: [**29** | 39 | 39c]
  - Formato dell'immagine del timbro digitale: [**GIF** | JPG | TIFF | BitMap]

❖

[1] Area, all'interno del layout del documento, dove verrà collocato il timbro digitale

© GT50 s.r.l Riproduzione vietata. Tutti i diritti sono riservati.
Nessuna parte del presente documento può essere riprodotta o diffusa, in tutto o in parte, con un mezzo qualsiasi, senza il consenso scritto di GT50