IN.TE.S.A. S.p.A.

Manuale Operativo:

Procedura di Firma Digitale

con autorizzazione alla firma del Titolare

attraverso tecniche di tipo grafometrico

Codice documento: MO-GRAF

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 13/10/2016

Revisione: 02

Firmato da:
ANTONIO RAIA
Certificato emesso da: IN.TE.S.A. Certification Authority, IN.TE.S.A. S.p.A., IT

REVISIONI

Revisione n°:	**01**	**Data Revisione:**	**08 Dicembre 2012**
Descrizione modifiche:	Nessuna		
Motivazioni:	Prima emissione		
Revisione n°:	**02**	**Data Revisione:**	**13 ottobre 2016**
Descrizione modifiche:	Variazione dati societari e logo Aggiornamento definizioni e riferimenti normativi Formattazione Documento		
Motivazioni:	Aggiornamenti normativi: Regolamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 Variazioni organizzative Revisione documentale		

Sommario

Introduzione – Riferimenti Normativi & Acronimi

Riferimenti di legge

Testo Unico DPR 445/00	Decreto del Presidente della Repubblica del 28 dicembre 2000, n.445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*". (G.U. n.42 del 20 febbraio 2001). Nel seguito indicato anche solo come *TU*.
DLGS 196/03	Decreto Legislativo n.196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali*". (G.U. n.174 del 29 luglio 2003, suppl. ord.). Nel seguito indicato anche solo come *DLGS196/03*
CAD DLGS 82/05	Decreto Legislativo 7 Marzo 2005, n. 82. "*Codice dell'amministrazione Digitale".* (G.U. n.112 del 16 Maggio 2005). Nel seguito indicato anche solo come *CAD*.
DLGS 235/2010	Decreto Legislativo 30 dicembre 2012, n. 235 "*Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante Codice dell'amministrazione digitale, a norma dell'articolo 33 della legge 18 giugno 2009, n.69*". (G.U. n.3 del 4 Gennaio 2013)
DELIBERAZIONE CNIPA n.45	Deliberazione CNIPA 21 Maggio 2009, n.45. *Regole per il riconoscimento e la verifica del documento informatico*. (G.U. n.282 del 3 dicembre 2009) Modificata dalla Determ. DigitPA n.69/2010. Nel seguito indicato anche solo come *DELIBERAZIONE*
DETERMINAZIONE COMMISSARIALE DIGITPA, n.69	Determinazione commissariale DigitPA 28/07/2010, n.69 *Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante Regole per il riconoscimento e la verifica del documento informatico, pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 282*.
DPCM 22/02/2013 *Nuove Regole Tecniche*	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizionee verifi ca delle fi rme elettroniche avanzate, qualifi cate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b), 35, comma 2, 36,comma 2, e 71" (del CAD, ndr).* (G.U. n.117 del 21 maggio 2013). Nel seguito indicato anche solo come *DPCM*
DPCM 19/07/2012	Decreto del Presidente del Consiglio dei Ministri 19 luglio 2012 "*Definizione dei termini di validita' delle autocertificazioni circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza di cui al decreto del Presidente del Consiglio dei Ministri 30 ottobre2003, e dei termini per la sostituzione dei dispositivi automatici di firma.*" (G.U. n. 237 del 10 ottobre 2012)
DPCM 05/02/2015	Decreto del Presidente del Consiglio dei Ministri 5 febbraio 2015 "*Modifiche al decreto del Presidente del Consiglio dei Ministri 19 luglio 2012.*"
Regolamento (UE) N. 910/2014 (eIDAS	Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE Nel seguito indicato anche solo come *eIDAS*
D.Lgs 26 agosto 2016, n. 179	DECRETO LEGISLATIVO 26 agosto 2016, n. 179 "*Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche.*" (GU Serie Generale n.214 del 13-9-2016)

Definizioni & Acronimi

Sono qui riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

Termine o acronimo	*Significato*
AgID	Agenzia per l'Italia Digitale (già CNIPA e DigitPA): ***www.agid.gov.it*** Nel seguito anche solo *Agenzia*.
Certificato Qualificato	Attestato elettronico, che contiene un insieme di informazioni che creano una stretta e affidabile correlazione fra una chiave pubblica e i dati che identificano il Titolare. E' rilasciato da un Certificatore Accreditato
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*) Persona fisica o giuridica che presta uno o piu servizi fiduciari.
Certificatore Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID. (nelle more del Regolamento (UE) N. 910/2014).
CP	Certificate Policy - Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore / TSP che li ha emessi.
Doc.Informatico	Documento Informatico: documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Doc. Analogico	Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA	Firma elettronica Avanzata – ex Art.26 Reg.UE 910/2014 (eidas), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
Firma Digitale	Particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici
Firma remota	Particolare procedura di firma qualificata o di firma digitale che consente di garantire il controllo esclusivo del dispositivo di firma;
Firma automatica	Particolare procedura informatica di fi rma elettronica qualificata o di fi rma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
HSM	Hardware Security Module - Insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PKI	Public Key Infrastructure - Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA	Certification Authority: Entità della PKI che rilascia i certificati
RA Registration Authority	Autorità di Registrazione che su incarico del TSP esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al TSP. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del TSP (INTESA S.p.A.).
Parametri Grafometrici	Un insieme di parametri (velocità, pressione, ritmo, accelerazione, movimenti aerei) che vengono "catturati" nel momento in cui si appone una firma con una particolare penna e che rendono l'autenticazione del Titolare assolutamente certa.

Termine o acronimo	*Significato*
Validazione temporale	Informazione elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel momento
Titolare	Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.
TSA	Time Stamping Authority - Autorità che rilascia marche temporali.

A. Il Manuale Operativo

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A. (di seguito anche "INTESA"), che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di Prestatore di servizi fiduciari è coperto da diritti sulla proprietà intellettuale.

A.2. Applicabilità

Il presente documento costituisce il Manuale Operativo del Prestatore di Servizi Fiduciari IN.TE.S.A. S.p.A., al quale d'ora in poi si farà riferimento anche solo come *INTESA* ovvero *TSP* (Trust Service Provider) o anche *TSP INTESA*.

Il contenuto del Manuale Operativo è conforme con quanto definito nelle regole tecniche contenute nel DPCM e nel CAD (e relative modifiche e integrazioni).

Questo documento descrive le regole e le procedure operative del TSP INTESA per l'emissione dei certificati qualificati, la generazione e la verifica della firma digitale e le procedure del servizio di validazione temporale, in conformità con la vigente normativa in materia.

Le attività descritte sono svolte in conformità con il Regolamento (UE) 910/2014 (eIDAS).

Il servizio fornito dal TSP INTESA descritto in questo manuale prevede che il Titolare di un certificato di firma digitale possa avviare un processo di firma utilizzando una procedura di riconoscimento grafometrico, effettuato sui seguenti parametri della firma autografa: velocità, pressione, ritmo, accelerazione, movimenti aerei.

Perché ciò avvenga, nel rispetto della normativa vigente e garantendo la massima sicurezza della procedura, è previsto che, durante l'identificazione de visu del Titolare, queste nuove tecniche siano utilizzate per registrare dati e parametri specifici della firma autografa del Titolare. Al momento della firma, al posto dei tradizionali PIN e OTP (One Time Password) solitamente utilizzati in questa tipologia di servizi, al Titolare è richiesto di autenticarsi al servizio utilizzando specifici dispositivi grafometrici su cui riprodurre la propria firma autografa.

La firma digitale è poi realizzata tramite un sistema di coppie di chiavi asimmetriche, una pubblica e una privata, che consentono al Titolare di rendere manifesta l'autenticità e l'integrità di un documento informatico ad uno o più destinatari che ne possono verificare la validità.

In linea con quanto previsto dal DPCM, le chiavi di firma sono conservate, su dispositivi sicuri, denominati Hardware Security Module (di seguito anche solo HSM); l'uso esclusivo di tali chiavi è garantito dall'utilizzo del sistema di autenticazione di tipo grafometrico.

A.3. Validità

Quanto descritto in questo documento si applica al Certificatore Accreditato INTESA, cioè alle sue infrastrutture logistiche e tecniche, al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma digitale relativa ad essi, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 del DPCM, che, al comma 4, distingue le chiavi e i correlati servizi secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati e alle loro liste di revoca (CRL) o sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e relative regole utilizzate dal TSP INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei Certificatori accreditati tenuto da AgID.

Pertanto, in funzione delle normative menzionate, vengono coinvolte più entità che saranno meglio identificate nel proseguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.02 del Manuale Operativo del Prestatore di Servizi Fiduciari INTESA per la *Procedura di Firma digitale con autorizzazione alla firma del Titolare attraverso tecniche di tipo grafometrico*, rilasciata il 13/10/2016 in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è 1.3.76.21.1.3.1.50.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica anche presso l'indirizzo Internet

http://e-trustcom.intesa.it/ca_pubblica/manuale_operativo_grfmtr.pdf

La pubblicazione di versioni aggiornate del Manuale Operativo avverrà sul sito sopra indicato solo successivamente al loro inoltro all'Agenzia.

INTESA ha adottato, come propria Certificate Policy, quanto indicato all'interno del documento ETSI 101 456 (OID 0.4.0.1456.1.1). Tale decisione è stata confortata dal fatto che la maggior parte dei certificatori europei hanno adottato tali indicazioni per le proprie certificate policy. Inoltre, tale certificate policy è stata riconosciuta comparabile alla US Federal Bridge CA Certificate Policy, Medium Level. L'adozione di tale policy permetterà quindi una più facile interoperabilità in sede europea e un'eventuale più agevole interazione con le amministrazioni del governo USA.

B.2. Dati identificativi del Certificatore

Il TSP di cui il presente documento costituisce il "Manuale Operativo" ai sensi dell'Art.40 del DPCM è la società INTESA, di cui di seguito sono forniti i dati identificativi.

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289** **10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**N. Iscrizione 1692/87**

N. di Partita I.V.A.	**05262890014**
N. di telefono (centralino)	**+39.011.19216.111**
Sito Internet	**www.intesa.it**
N. di fax	**+39.011.19216.375**
Indirizzo di posta elettronica	**marketing@intesa.it**
Indirizzo (URL) registro dei certificati	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo è di INTESA, nella persona di Antonio Raia (DPCM Art.40, comma 3.c), il quale ne cura la stesura, la pubblicazione e l'aggiornamento.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, INTESA ha predisposto i seguenti strumenti:

un recapito di posta elettronica:	***e-trustcom@intesa.it***
un recapito telefonico:	+39 011.192.16.111
un recapito fax:	+39 011.192.16 375
un servizio di HelpDesk	per le chiamate dall'Italia 800.80.50.93 per le chiamate dall'estero +39 02.871.193.396

B.4. Entità coinvolte nei processi

All'interno della struttura del TSP INTESA vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal certificatore accreditato INTESA espletando, per la parte di loro competenza, le attività a loro attribuite.

Pertanto saranno di seguito descritti gli ambiti nei quali il TSP opera e, di conseguenza, le entità coinvolte.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti:

a) Responsabile della sicurezza.
b) Responsabile del servizio di certificazione e validazione temporale
c) Responsabile della conduzione tecnica dei sistemi
d) Responsabile dei servizi tecnici e logistici.
e) Responsabile delle verifiche e delle ispezioni (auditing).
f) Le figure sopra elencate sono tutte appartenenti all'organizzazione del TSP INTESA.

B.4.1. Certification Authority (Certificatore Accreditato)

INTESA, operando nell'ottemperanza di quanto previsto nelle Regole Tecniche (DPCM) e al Codice dell'Amministrazione Digitale (CAD) e del Regolamento eIDAS, espleta le attività di Prestatore di Servizi Fiduciari per le attività di emissione, pubblicazione, revoca e sospensione di certificati qualificati.

I dati identificativi del TSP INTESA sono riportati al precedente paragrafo B.2.

B.4.2. Registration Authority (Ufficio RA)

INTESA ha costituito al suo interno un'entità denominata Ufficio RA che ha funzioni di Registration Authority. In particolare, essa espleta le seguenti attività:

- Identificazione dei titolari.
- Registrazione dei titolari.
- Inizializzazione dei dispositivi sicuri di firma.
- Distribuzione dei dispositivi di firma.

- Gestione dell'inventario dei dispositivi di firma.
- Supporto al titolare.

L'Ufficio RA, all'interno di specifici accordi, ha inoltre l'incarico d'istruire il personale di entità esterne per la costituzione di Local Registration Authority (LRA). Queste ultime operano sul territorio svolgendo, anche solo in parte, le attività sopra elencate su incarico di INTESA.

C. Obblighi

C.1. Obblighi del Prestatore di Servizi Fiduciari

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dalla normativa vigente (vedi *Riferimenti di legge*).

In particolare, INTESA:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- identifica con certezza la persona che fa richiesta della certificazione;
- specifica nel certificato qualificato, su richiesta dell'istante e con il consenso del Terzo Interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi secondo quanto indicato nel cap. F.1;
- informa i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali;
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato, di perdita del possesso della chiave, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
- garantisce il funzionamento efficiente, puntuale e sicuro dei servizi di elencazione, nonché garantisce un servizio di revoca e sospensione dei certificati elettronici sicuro e tempestivo;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- non copia, nè conserva le chiavi private di firma del soggetto cui il TSP ha fornito il servizio di certificazione;
- assicura che il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il TSP;

- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- raccoglie i dati personali direttamente dalla persona cui si riferiscono o, previo suo esplicito consenso, attraverso personale esterno da lui delegato. I dati così raccolti saranno soltanto quelli necessari al rilascio e al mantenimento del certificato, accompagnati dall'informativa prevista dalla disciplina in materia di dati personali.

La generazione dei certificati qualificati è conforme all'Art.18 del DPCM e secondo quanto disposto dalla Deliberazione 45/2009. Quindi:

- prima di emettere il certificato qualificato il TSP deve:
  a) accertarsi dell'autenticità della richiesta
  b) verificare il possesso della chiave privata e il corretto funzionamento della coppia delle chiavi;
- il certificato qualificato deve essere generato con un sistema conforme a quanto previsto dall'art.33 del DPCM;
- il termine del periodo di validità del certificato qualificato precede di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verifi carne l'autenticità;
- l'emissione dei certificati qualificati è registrata nel giornale di controllo con la specificazione della data e dell'ora della generazione;

Secondo quanto stabilito dall'Art.14 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il Certificatore:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati (Art.42 DPCM);
- garantisce l'interoperabilità del prodotto di verifica (DPCM, Art.42, comma 2);
- mantiene copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione e la rende rende accessibile per via telematica (DPCM, Art.42, comma 3).

C.2. Obblighi del Titolare

Il Titolare è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, Art.32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal TSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- indicare esplicitamente nella richiesta di certificazione le informazioni che egli desidera non siano inserite nel certificato;
- comunicare al TSP eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici o di Internet, ecc.;
- utilizzare dispositivi di firma conformi all'Art.11 del DPCM, nel caso in cui non sia il TSP a fornirlo. Le informazioni relative a tale dispositivo dovranno comunque essere comunicate al TSP, in quanto INTESA intende conservare il controllo delle caratteristiche di sicurezza dei dispositivi di firma utilizzati dai Titolari e mantiene la corrispondenza tra certificato qualificato e dispositivo;

- conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza (DPCM, Art.8, comma 5);
- non duplicare la chiave privata né il dispositivo che la contiene (DPCM Art.8, comma 1), fatto salvo quanto disposto al medesimo Articolo, ai commi 2.3 e 4;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave (DPCM, Art.8, comma 5, lett. b);
- conservare con la massima diligenza i codici segreti, ricevuti dal TSP al fine di garantirne la massima riservatezza;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (DPCM, Art.5, comma 5);
- utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso nel caso la firma venga apposta per mezzo di una procedura automatica (DPCM, Art.5, comma 5);
- utilizzare esclusivamente il dispositivo fornito dal TSP, ovvero un dispositivo scelto tra quelli indicati dal TSP stesso (DPCM, Art.7, comma 6);
- richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso. chiave (DPCM, Art.8, comma 5, lett. C);
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua durata (DPCM, Art.28, comma 1);
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua decorrenza (DPCM, Art.24, comma 1);
- sporgere denuncia alle Autorità competenti in caso di smarrimento o sottrazione del dispositivo di firma.

C.3. Obblighi degli utilizzatori dei certificati

Coloro che utilizzino messaggi elettronici e/o evidenze informatiche firmati digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato allo standard ISO 9594-8, e il momento della sua emissione;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e il momento della sua emissione;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori e su eventuali certificati derivanti da accordi di mutua certificazione tra il proprio TSP e quelli altrui;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del TSP che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, si tratti di persona fisica o di organizzazione (impresa, associazione di categoria, ente, ecc.), ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato, previa sua autorizzazione, al Titolare.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza;
- variazione dei dati identificativi dell'azienda (es. denominazione sociale, sede legale, etc.), cessazione dell'attività da parte dell'organizzazione e ogni altro dato rilevante o che influisca ai fini dell'uso del certificato.

La richiesta di revoca o sospensione da parte del Terzo Interessato deve essere inoltrata per iscritto e corredata di documentazione giustificativa. Inoltre, il Terzo Interessato è tenuto a porre a conoscenza dei Titolari, che a lui afferiscono, delle tematiche di sicurezza concernenti l'uso della firma digitale: custodia del dispositivo, accesso ai sistemi, nonché a quanto esposto nel presente Manuale Operativo.

C.5. Obblighi delle LRA esterne

Il TSP INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale, ai sensi dell'Art.1717 del codice civile, di ulteriori soggetti (nel seguito denominati LRA esterne) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. In particolare, le LRA esterne espletano le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- raccolta della richiesta di registrazione e certificazione compilata e sottoscritta dal Titolare;
- consegna del dispositivo di firma.

La documentazione raccolta deve essere trasmessa all'Uffico RA di INTESA ovvero, previo accordo, trattenuta e conservata dalla LRA con le stesse modalità.

Le LRA esterne sono attivate dal TSP a seguito di un adeguato addestramento del personale indicato dall'Azienda o Ente con il quale viene stipulato un regolare Contratto di Mandato sottoscritto da entrambe le parti. In tale contratto sono esplicitati gli obblighi cui si deve attenere l'Azienda o Ente cui INTESA assegna l'incarico di LRA; in particolare deve:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente;
- impedire ai propri dipendenti la prosecuzione dell'attività di riconoscimento e curare l'immediato ritiro di ogni materiale qualora, per qualsiasi causa, si interrompa il rapporto in essere tra l'Azienda e il dipendente stesso, dandone tempestivamente notizia per iscritto a INTESA;
- custodire i dispositivi di firma fino alla consegna degli stessi ai Titolari destinatari, rispondendo direttamente della loro sottrazione o perdita per qualsiasi causa, con obbligo di comunicare senza ritardo tali eventi all'Ufficio di Registrazione di INTESA;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il Dlgs. 196/03.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Prestatore di Servizi Fiduciari

INTESA è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle proprie attività, come previsto dalla normativa vigente (vedi *C.1*).

INTESA non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dal DPCM, e in particolare, dal mancato rispetto da parte del Titolare, degli utilizzatori dei certificati e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e dalla mancata osservanza da parte degli stessi della normativa vigente.

Si ricorda pertanto di conservare con speciale diligenza il dispositivo di firma per garantirne l'integrità e la massima riservatezza e di conservare sempre separatamente dal dispositivo stesso le informazioni di abilitazione all'uso dello stesso.

Per quanto non esplicitamente riportato si fa specifico riferimento a quanto espresso nel *CAD, Capo II, Sezione II Firme elettroniche e Certificatori, Art.32 Obblighi del Titolare e del Prestatore di servizi di firma elettronica qualificata*.

INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo di esempio: calamità naturali, disfunzioni tecniche e logistiche al di fuori del proprio

controllo, interventi dell'autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

D.2. Assicurazione

INTESA ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è stato inviata al DigitPA apposita dichiarazione di stipula.

La copertura Assicurativa prevede i seguenti massimali:

- 250.000,00 (duecentocinquantamila) euro per singolo sinistro.
- 1.500.000,00 (unmilionecinquecentomila) euro per annualità.

D.3. Limitazioni agli indennizzi

Il TSP INTESA, fatto salvo i casi di dolo e colpa grave, esclude ogni responsabilità per danni subiti dagli utenti o da terzi in conseguenza di:

- mancato rispetto delle procedure e delle regole stabilite dal TSP;
- danno causato da disservizio;
- uso improprio dei certificati di sottoscrizione da parte di applicazioni di terze parti.

INTESA non si ritiene, peraltro, responsabile dei danni causati agli utenti Titolari e utilizzatori o a terzi conseguenti al non rispetto, da parte del Titolare, delle regole definite nel presente Manuale Operativo.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal certificatore accreditato.

E. Tariffe

Le tariffe per l'emissione, il primo rinnovo, la revoca e la sospensione dei certificati saranno definite su base progettuale.

Ulteriori informazioni sono reperibili sul sito del TSP INTESA, tenendo comunque conto che tali tariffe potranno variare in funzione delle quantità trattate e soggette all'andamento del mercato.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

Il TSP verifica con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato. Il riconoscimento è eseguito mediante presenza fisica della persona (*de visu*). Per i successivi rinnovi tale attività non sarà più ripetuta: sarà cura del Titolare comunicare al TSP eventuali cambiamenti relativi ai propri dati di registrazione.

L'attività di identificazione del richiedente viene effettuata:

- da INTESA, tramite le persone del proprio Ufficio RA;
- da LRA esterne; ad es. personale dell'Azienda o dell'Ente Cliente oppure di terze parti appositamente autorizzate dal Certificatore (vedi anche *C.5*)

In ogni caso la persona che fa richiesta della certificazione viene identificata con certezza e viene archiviata da INTESA la fotocopia di almeno un documento ufficiale per lo Stato di appartenenza.

Il Titolare ovvero il Terzo Interessato sottoscrivono:

- Il contratto di servizio, in duplice copia, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Digitale*, in duplice copia, in cui riporta i propri dati, tra cui:
  - Ente richiedente.
  - Cognome e nome.
  - Data e luogo di nascita.
  - Codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano).
  - Numero di telefono (fisso o cellulare).
  - Indirizzo di posta elettronica.
  - Tipo, numero ed Ente di rilascio del documento di identità esibito.
- Il documento *Presa visione del Manuale Operativo INTESA*, in duplice copia, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del DLgs 196/03.

Nel caso la chiave debba essere utilizzata da dispositivi HW con procedura automatica (DPCM, Art.5, comma 2 e 3), saranno notificati al richiedente gli estremi di detti apparati (es. produttore, modello e numero di serie).

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il TSP (che non verifica la validità dell'indirizzo) userà in seguito tale indirizzo per comunicare con il richiedente.

La documentazione precedentemente descritta, relativa alla registrazione dei Titolari, viene conservata da INTESA per 20 (venti) anni dalla scadenza del certificato a cura del *Responsabile dei servizi tecnici e logistici*.

Contestualmente alla fase di riconoscimento, viene avviata una procedura finalizzata alla registrazione di quei dati grafometrici che serviranno nel seguito come strumento di autenticazione/autorizzazione per permettere l'utilizzo delle chiavi di firma.

Al titolare è richiesto di apporre da quattro a sei firme su di un tablet, utilizzando una particolare penna resa disponibile dall'operatore di RA / LRA. Grazie ad uno specifico software dedicato a tali riconoscimenti, il sistema è in grado di "catturare" una serie di informazioni relative al modo di firmare del Titolare, informazioni che saranno utilizzate successivamente per permettere al Titolare di accedere al servizio di firma digitale.

Questa fase che prende il nome di *enrollment* del titolare è pertanto particolarmente delicata, la qualità del profilo di firma grafometrica che viene definito e associato al Titolare diventerà fondamentale per il buon esito di tutte le operazioni di firma che verranno poi eseguite, per questo motivo alla descrizione di questa procedura dedichiamo il prossimo paragrafo.

F.2. Procedure di Enrollment

La procedura di enrollment è uno dei più importanti aspetti di sicurezza dell'intero sistema e, come detto in precedenza al Titolare, in questa fase viene richiesto di firmare in successione più volte su di un specifico tablet. L'enrollment è sempre svolto in presenza e con l'eventuale supporto dell'operatore di RA / LRA, sia presso i locali della RA / LRA, sia presso altra ubicazione (ad es. presso il il domicilio del richiedente). Gli aspetti di sicurezza della procedura sono descritti in F.3.

Vengono così memorizzate ad ogni firma effettuata una serie di parametri (pressione,accelerazione, velocità, ritmo e movimenti aerei) con cui la firma è stata eseguita e che sono tipici del modo di eseguire la firma stessa da parte del Titolare.

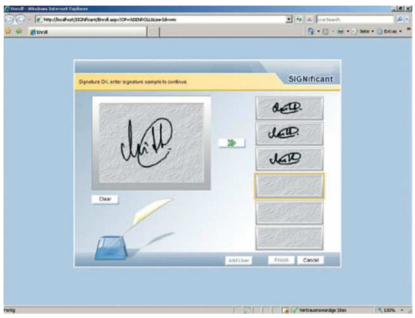
Se una o più firme apposte, durante la procedura, non dovessero risultare congruenti con le altre e magari differire in modo esplicito queste firme potrebbero essere scartate dal sistema ed al Titolare verrebbe richiesto di apporne delle altre fino ad arrivare ad un profilo consistente.

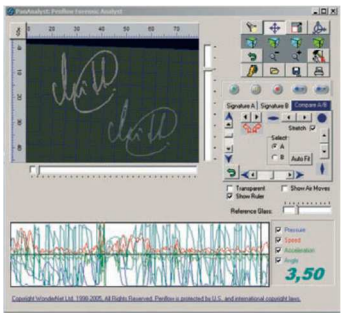
Il tutto per cercare poi di minimizzare in una successiva fase di verifica sia i "False Rejection Rate" che i "False Acceptance Rate":

- Il False Rejection Rate (FRR) rappresenta la percentuale di firme valide che dovessero essere rigettate dal sistema
- Mentre il false Acceptance Rate (FAR) rappresenta la percentuale di firme riconosciute come valide pur non avendone tutte le caratteristiche

Il riconoscimento della firma grafometrica ribadiamo non avverrà mai confrontando solo l'immagine della stessa (facilmente falsificabile), ma sfruttando tutti i parametri grafometrici precedentemente raccolti. Più precisamente, l'autenticazione di tipo grafometrico prevede la verifica contemporanea di più fattori, quali:

- il ritmo
- la velocità
- la pressione
- l'accelerazione
- il movimento





Uno degli aspetti più delicati da affrontare nei riconoscimenti di tipo grafometrico è come garantire nel tempo la qualità del servizio quando un Titolare per varie circostanze dovesse modificare il suo modo di firmare (pensiamo ad un giovane che diventa adulto, così come un anziano che inevitabilmente potrebbe avere una scrittura più incerta).

Per questo motivo è importante notare che nella nostra soluzione il processo di enrollment non si esaurisce in un'unica sessione ; infatti anche successivamente,ogni qual volta il Titolare firmerà per autenticarsi al sistema, le informazioni raccolte verranno utilizzate per aggiornare il suo profilo grafometrico. Per questo motivo la nostra soluzione, prevedendo un enrollment continuo nel tempo, può considerarsi oggi unica nel suo genere.

E' facile, infatti, intuire come questa procedura di enrollment continuo nel tempo non solo garantisca prestazioni ottimali ma è l'unica in grado di dare una risposta alla problematica appena evidenziata

Questo profilo (generato al momento dell'identificazione e successivamente aggiornato nel tempo) sarà infatti poi utilizzato per autenticare il Titolare al sistema di firma.

Per poter accedere alle proprie chiavi di firma il Titolare dovrà autenticarsi apponendo una nuova firma di tipo grafometrico su di un dispositivo tablet, con caratteristiche simili a quello, utilizzato in fase di enrollment. I parametri grafometrici rilevati in questa fase verranno confrontati con quelli raccolti durante la fase di enrollment e se considerati sufficientemente "attendibili" con percentuale di riconoscimento uguale o superiore almeno all'80% potranno permettere lo sblocco delle chiavi di firma.

F.3. Aspetti di sicurezza nel processo di Enrollment

Tutto il processo di enrollment è stato studiato per garantire la massima sicurezza ai nostri Titolari.

Cerchiamo di seguito di dare una breve illustrazione del processo evidenziando appunto gli aspetti di sicurezza che caratterizzano la soluzione.

- il Tablet (1) comunica con l'applicazione Client (2), la quale potrebbe essere un'applicazione INTESA, ma anche un'applicazione di sportello di una banca, ovvero un'applicazione utilizzata da un agente assicurativo, piuttosto che in un ambito sanitario dove si richieda la firma digitale di referti. La connessione fra Tablet e Client è comunque sempre cifrata.
- Il Client (2) comunica poi con il Server(3); il server designato a verificare la validità delle firme appena apposte e alla gestione delle procedure di enrollment precedentemente descritte. Anche in questo caso tutte le connessioni sono protette e cifrate via HTTPs.
- Il Server (3) necessita infine di un Database (4) dove sono stati memorizzati (cifrati) tutti i profili dei Titolari. Questi profili potranno essere recuperati al momento opportuno, decifrati nella memoria del Server e, una volta utilizzati, immediatamente rilasciati senza che alcunché di tale profili possa essere modificato in maniera dolosa e/o colposa. Sarà sempre il Server che ritornerà al Client l'esito del confronto (Verify_Match/Verify_NoMatch)

Oltre a quanto appena descritto altri aspetti di sicurezza vengono gestiti dall'applicazione, fra questi :

- utilizziamo solo dispositivi tablet capaci di encrypting communication;
- tutte le comunicazioni fra i vari sistemi coinvolti sono cifrate;
- i dati grafometrici non sono mai in chiaro ma sempre cifrati;
- il codice del software che gestisce i dati grafometrici è sempre compilato per evitare rischi di code injection;
- il permesso all'accesso di tali sistemi viene gestito tramite un sistema di Kerberos authentication;
- tutti gli accesi ai sistemi vengono registrati nell'audit log del sistema e resi disponibili al giornale di controllo.

F.4. Altri attributi del Certificato qualificato

F.4.1. Titoli e abilitazioni professionali

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a

dimostrazione dell'effettiva sussistenza di tali abilitazioni professionali o documentazione equivalente (es. autocertificazione), così come indicato nella Deliberazione CNIPA n.45. Una copia di tale documentazione viene conservata dal TSP.

La documentazione atta a supportare la richiesta d'inserimento di titoli o abilitazioni professionali all'interno del certificato qualificato non può essere antecedente a 10 (dieci) giorni dalla data di presentazione della richiesta di emissione del suddetto certificato.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative ad abilitazioni professionali.

INTESA, in caso di autocertificazione, non si assume alcuna responsabilità, salvo i casi di dolo o colpa grave, per l'eventuale inserimento nel certificato d'informazioni autocertificate dal titolare.

F.4.2. Poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di poteri di rappresentanza (es. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un Cliente, etc.), il richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza di tali poteri di rappresentanza.

Per la rappresentanza di persone fisiche, il richiedente dovrà produrre una copia autentica della delega o procura notarile sottoscritta dalla persona rappresentata insieme all'attestazione di consenso di quest'ultima all'inserimento del ruolo nel certificato.

Nel caso in cui sia richiesta l'indicazione nel certificato di un ruolo relativo alla rappresentanza di organizzazioni o enti di diritto privato, il titolare dovrà presentare documentazione atta a comprovare il ruolo di cui si chiede l'inserimento nel certificato ed una dichiarazione dell'ente di appartenenza nel quale l'organizzazione autorizza il TSP all'inserimento dello specifico ruolo nel certificato. Quest'ultimo documento non dovrà essere antecedente 20 (venti) giorni rispetto alla data di richiesta di emissione del certificato qualificato.

L'inserimento nel certificato qualificato d'informazioni relative all'esercizio di funzioni pubbliche o poteri di rappresentanza in enti od organizzazioni di diritto pubblico sarà subordinato a specifici accordi con gli enti stessi. Sulla base di tali accordi sarà possibile specificare il ruolo del titolare all'interno dell'ente o organizzazione pubblica.

La documentazione prodotta sarà conservata dal TSP per un periodo di 20 (venti) anni.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative a poteri di rappresentanza.

F.4.3. Limitazioni d'uso

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, il richiedente deve sottoscrivere idonea documentazione attestante la richiesta. Una copia di tale documentazione viene conservata dal TSP.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.4.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno pseudonimo in alternativa ai propri dati reali. Anche in questo caso, poiché comunque ci si riferisce a certificati qualificati, il TSP conserverà le informazioni relative alla reale identità dell'utente per 20 (venti) anni dopo la scadenza del certificato stesso.

F.5. Contratto di servizio tra INTESA ed Ente cliente

Nel caso in cui il cliente sia un Ente o una Azienda, i cui dati identificativi saranno definiti a contratto, si applicano anche le norme seguenti, fermo restando quanto specificato al paragrafo F.1, dal punto 2 in poi, per l'identificazione e la registrazione dei singoli Titolari.

1. Le persone delegate ad indicare il personale del Cliente abilitato ad essere certificato da INTESA faranno pervenire al TSP gli elenchi delle persone alle quali INTESA sarà autorizzata a rilasciare i certificati qualificati. In tali elenchi sarà possibile anche indicare eventuali limitazioni all'uso delle coppie di chiavi, poteri di rappresentanza o abilitazioni professionali.
2. Questi elenchi saranno resi disponibili agli addetti interessati: il personale dell'Ufficio RA e dell'Help Desk.
3. Le persone autorizzate esibiranno alle LRA documenti analoghi a quelli indicati al paragrafo F.1.
4. La LRA verificherà che la persona sia autorizzata ad essere certificata e opererà in conformità a quanto indicato al paragrafo F.1.

F.6. Registrazione degli utenti

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi del TSP. Questa operazione viene sempre eseguita dal personale dell'Ufficio RA di INTESA.

Durante la registrazione dei dati del Titolare viene generato l'identificativo univoco del Titolare presso il TSP.

G. Modalità di generazione delle chiavi

G.1. Generazione delle chiavi di certificazione

La generazione delle chiavi di Certificazione all'interno dei dispositivi di firma custoditi nei locali del TSP avviene in presenza del *Responsabile dei servizi di certificazione*, come previsto dal DPCM all'Art.7, comma 1, ed è preceduta dall'inizializzazione dei dispositivi di firma.

Il tutto avviene inoltre alla presenza di un numero di responsabili aziendali ritenuto adeguato e sufficiente ad evitare operazioni illecite.

Una volta generate le coppie di chiavi, quelle private vengono suddivise in più parti, ciascuna delle quali viene trascritta su più dispositivi di backup (token USB), secondo una logica *m di n*: gli n dispositivi sono suddivisi e consegnati alle n figure aziendali presenti, le quali vi associeranno una propria password.

La lunghezza delle chiavi del sistema di certificazione è di 2048 bit.

G.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'Art.49 del DPCM.

La lunghezza delle chiavi del sistema di validazione temporale è di 2048 bit.

G.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del TSP, è possibile procedere alla generazione delle chiavi di sottoscrizione.

Il Titolare una volta terminate le operazioni di identificazione e di enrollment precedentemente descritte potrà avviare immediatamente dopo la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato

Da quel momento il riconoscimento grafometrico precedentemente descritto permetterà al Titolare di conservare in modo esclusivo il controllo delle proprie chiavi di firma ai sensi del DPCM.

Lo stesso riconoscimento grafometrico (rafforzato da un'identificazione de visu svolta da personale INTESA o di società da essa delegata) sarà richiesto in ogni occasione che il Titolare voglia firmare un documento digitale, in ottemperanza dell'art.35, comma 2 del CAD.

Le coppie di chiavi di sottoscrizione vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa vigente.

Le coppie di chiavi per la creazione e la verifica della firma (la cui lunghezza è di almeno 2048 bit) sono attribuite ad un solo Titolare, che ne mantiene il controllo esclusivo secondo le modalità appena descritte.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo ***G.1***, vengono generati i certificati delle chiavi pubbliche conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia attraverso il sistema di comunicazione di cui all'Art.16, comma 1, del DPCM.

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

H.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel paragrafo ***G.3,*** è possibile generare una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

La CA elabora immediatamente la richiesta ricevuta, in conformità con quanto previsto dal DPCM all'Art.18.

In particolare:

- si accerta dell'autenticità della richiesta (comma 1.a);
- si accerta che il Titolare sia effettivamente in possesso della chiave privata e verifica il corretto funzionamento della coppia di chiavi (comma 1.b).

Il certificato così generato è pubblicato sul registro dei certificati, dietro consenso del Titolare.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

Il TSP mantiene le informazioni per l'identificazione del Titolare di un dispositivo sicuro di firma e dei certificati in esso contenuti, per un periodo pari a 20 (venti) anni dalla data di emissione del certificato qualificato, salvo quanto previsto dall'Art.11 del decreto legislativo n. 196/03.

Al termine del processo, sul dispositivo del Titolare saranno stati registrati, oltre alla chiave privata di firma:

- il certificato di sottoscrizione;
- il certificato elettronico relativo alla chiave pubblica del Certificatore la cui corrispondente chiave privata è stata utilizzata per sottoscrivere il certificato qualificato relativo alle chiavi di sottoscrizione del Titolare, come da Art.11, comma 5, del DPCM.

I seguenti paragrafi descrivono le operazioni effettuate per l'emissione dei certificati nelle due modalità previste dal Certificatore per la generazione delle chiavi.

H.3. Informazioni contenute nei certificati

I certificati qualificati emessi dal certificatore INTESA sono conformi a quanto indicato nella deliberazione CNIPA n.45 del 21/05/09 e successive modificazioni e sono conformi al regolamento eIDAS.

H.4. Codice di Emergenza

Come previsto dal DPCM, Art.21, ad ogni emissione di un certificato di sottoscrizione viene consegnato al Titolare un *codice di emergenza* riservato da utilizzare nel corso del ciclo di vita del certificato per richiedere la sospensione dello stesso.

Tale codice potrà essere, a titolo di esempio, una specifica password comunicata in busta cieca o un dispositivo fisico, come un token OTP qualora il Titolare ne possedesse già uno.

I. Modalità di revoca e sospensione dei certificati

I.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista di revoca CRL (DPCM, Art.20).

Il profilo delle CRL/CSL è conforme con lo standard RFC 5280.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita (24h) e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

Informazioni circa la validità del Certificato saranno rese diposnibili anche via OCSP.

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato (Artt. 23, 25, 27 e 29 del DPCM), il Certificatore notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

Un certificato può essere revocato nei seguenti casi, ad ognuno dei quali corrisponde un codice detto CRLReason indicato tra parentesi:

1. sostituzione del certificato senza compromissione della chiave privata (*CRLReason: Superseded*);
2. compromissione (perdita delle caratteristiche di sicurezza e univocità) della chiave privata del Titolare (*CRLReason: Key Compromise*);
3. i dati del certificato sono modificati o obsoleti; in questo caso ricade anche l'eventualità che un Titolare non accetti i certificati emessi a suo nome in quanto i dati sono errati (*CRLReason: Affiliation Changed*);
4. cessazione repentina, in condizioni di conflittualità o non, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati (*CRLReason: Cessation of Operation*);
5. mancato rispetto da parte del Titolare degli obblighi specificati nel Manuale Operativo, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata (*CRLReason: Unspecified*);
6. altri casi, che non ricadono nei precedenti (*CRLReason: Unspecified*); tuttavia, l'utilizzo di tale causale è deprecato e se ne sconsiglia l'utilizzo

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato e il motivo della revoca.

I.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca del proprio certificato secondo tre diverse modalità:

1. Qualora il Titolare disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo ***uff_ra@intesa.it*** contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata (il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'indirizzo inernet ***http://e-trustcom.intesa.it/ca_pubblica/mod_revoca.doc***). Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che che permettano di identificare univocamente il certificato da revocare - vedi più sotto) e il motivo della richiesta (eventualmente facendo riferimento a quelli indicati al paragrafo. *I.1*).
2. Nei casi in cui il Titolare non disponga di un proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente:
   a. via fax, al numero indicato all'URL ***http://www.hda.intesa.it***/ nell'orario di servizio ivi riportato.

b. via posta ordinaria, all'indirizzo sempre indicato all'URL di cui al punto a.

3. Eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia *Key Compromise*, il Titolare potrà telefonare al numero fornito dal TSP al momento del rilascio del primo certificato qualificato a lui intestato. Egli dovrà fornire i dati relativi al certificato e il *Codice di Emergenza* (DPCM, Art.21). In questo caso il certificato indicato sarà temporaneamente sospeso in attesa della richiesta scritta del Titolare.

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'Art.24, comma 1, del DPCM.

Al di fuori degli orari di assistenza indicati all'URL *http://www.hda.intesa.it/*, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente, per quanto riguarda il Titolare interessato:

- generalità (es. nome, cognome, email, telefono, ente di riferimento)
- motivazione della richiesta
- momento di decorrenza del provvedimento.

Altri dati dati aggiuntivi possono essere utili al fine di identificare univocamente il certificato da revocare. Tali dati possono essere recuperati dal Titolare dalla documentazione rilasciata in fase di emissione, se ancora dispponibile (es. tipo di dispositivo e numero seriale, organizzazione di riferimento, numero seriale del certificato, data di rilascio…).

Il TSP, accertata la correttezza della richiesta, darà notizia della revoca al Titolare tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca (CRL).

I.1.2. Revoca su richiesta del Terzo Interessato

Il Terzo Interessato può richiedere la revoca del certificato del Titolare.

Il Certificatore dispone tre diverse modalità per la richiesta di revoca da parte del Terzo Interessato:

1. Qualora il Terzo Interessato disponga del proprio dispositivo di firma, invierà un messaggio di posta elettronica all'indirizzo ***uff_ra@intesa.it*** contenente in allegato il documento di richiesta di revoca debitamente compilato e firmato con la propria chiave privata (il modulo *Richiesta di Revoca Certificati Digitali* è disponibile all'URL ***http://e-trustcom.intesa.it/ca_pubblica/mod_revoca.doc***). Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni che permettano di risalire univocamente al certificato da revocare) e il motivo della richiesta (eventualmente facendo riferimento a quelli indicati al paragrafo. *I.1*).
2. Nei casi in cui il Terzo Interessato non disponga del proprio dispositivo di firma, potrà alternativamente inoltrare la richiesta specificando i dati di cui al punto precedente:
    a. via fax, al numero indicato all'URL ***http://www.hda.intesa.it***/ nell'orario di servizio ivi riportato;
    b. via posta ordinaria, all'indirizzo sempre indicato all'URL di cui al punto precedente.
3. Eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia *Key Compromise*, il Terzo Interessato potrà telefonare al numero fornito dal TSP al momento del rilascio del primo certificato qualificato a lui intestato. Egli dovrà fornire i dati relativi al certificato e il Codice di Emergenza (DPCM, Art.21). In questo caso il certificato indicato sarà temporaneamente sospeso in attesa della richiesta scritta del Titolare.

La richiesta presentata in una delle modalità sopra descritte diventa la documentazione giustificativa prevista dall'Art.25 comma 1 del DPCM.

Al di fuori degli orari di assistenza indicati all'URL *http://www.hda.intesa.it/*, sarà a disposizione del richiedente solamente la modalità d'accesso tramite numero verde.

La richiesta dovrà indicare chiaramente:

- per quanto riguarda il Terzo Interessato:
  - Azienda di appartenenza
  - generalità
  - riferimenti al documento che lo autorizza a chiedere l'emissione, la revoca o la sospensione del certificato del Titolare interessato
  - suoi recapiti: telefonici e di posta elettronica
- per quanto riguarda il Titolare interessato:
  - generalità
  - estremi del certificato di cui si chiede la revoca o la sospensione
  - tipo (revoca o sospensione) e motivazione della richiesta, come indicato al par. *I.1* (CRLReason).
  - momento di decorrenza del provvedimento.

Il TSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati tramite posta elettronica, in casi particolari tramite posta ordinaria, e inserirà il certificato nella lista di revoca, che sarà emessa immediatamente.

I.1.3. Revoca su iniziativa del Certificatore

Il TSP INTESA può revocare i certificati dei Titolari nei casi indicati al par. *I.1* (CRLReason), in aggiunta ai motivi riportati al paragrafo seguente.

In ogni caso informerà della revoca i Titolari interessati tramite posta elettronica, altrimenti tramite posta ordinaria.

I.1.4. Revoca dei certificati relativi a chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- malfunzionamento del dispositivo sicuro per la generazione delle firme,
- cessazione dell'attività,

il TSP procede con la revoca dei certificati di certificazione corrispondenti e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione.

Entro 24 ore, il TSP notificherà la revoca all'Agenzia e ai Titolari.

I.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al capitolo *I.1*.

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba effettivamente essere revocato (ad esempio nei casi in cui si tema la compromissione della chiave privata o lo smarrimento/furto del dispositivo di firma, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

Per una sospensione, il codice di CRLReason è *certificateHold* e ha come conseguenza l'inserimento del certificato nella lista aggiornata di revoca (CRL).

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli Artt. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

Sarà cura del richiedente comunicare all'Ufficio RA di INTESA, con modalità analoghe a quelle utilizzate per la richiesta di sospensione, la richiesta di riattivazione o di revoca del certificato precedentemente sospeso.

In assenza di comunicazioni, il certificato verrà automaticamente revocato dopo il periodo di sospensione indicato dal Titolare nella richiesta, con la CRLReason indicata al momento della richiesta stessa (vedi *0*) e con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione).

I.2.1. Sospensione su richiesta del Titolare

Le modalità da seguire in questo caso sono le medesime indicate al capitolo *I.1.1*, cui si aggiunge la possibilità di richiedere la sospensione immediata, che può essere inoltrata utilizzando il numero telefonico fornito dal Certificatore al momento del rilascio del primo certificato qualificato. Il Titolare comunicherà il *Codice di Emergenza* stabilito al momento dell'emissione del certificato (vedi paragrafo *H.2*) e specificherà il motivo della richiesta di sospensione, facendo riferimento a quelli indicati al par. *I.1* (CRLReason): durante la conversazione telefonica si farà comunicare il numero di fax o l'indirizzo postale, cui invierà la medesima richiesta su lettera a conferma della comunicazione telefonica.

Il Titolare specificherà nella richiesta la durata del periodo di sospensione, che in ogni caso non potrà superare i 90 (novanta) giorni.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione, con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione).

I.2.2. Sospensione su richiesta del Terzo Interessato

Le modalità da seguire in questo caso sono le medesime indicate al capitolo I.1.1.

Il Terzo interessato specificherà nella richiesta la durata del periodo di sospensione, che in ogni caso non potrà superare i 90 (novanta) giorni.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione, con la decorrenza della sospensione (la data di revoca assumerà il valore della data di sospensione).

I.2.3. Sospensione su iniziativa del TSP

Il Certificatore notifica la sospensione ai Titolari tramite posta elettronica oppure, in casi particolari, tramite posta ordinaria.

J. Modalità di sostituzione delle chiavi

J.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare

I certificati digitali emessi dalla CA INTESA hanno validità di 24 (ventiquattro) mesi dalla data di emissione, salvo accordo diverso con i singoli clienti.

Entro la data di scadenza del certificato, al Titolare del dispositivo di firma sarà spedito, all'indirizzo di posta elettronica comunicato, un avviso di prossima scadenza.

Il Titolare che intende rinnovare il proprio certificato deve darne comunicazione tempestiva all'Ufficio RA del Certificatore, in modo da garantire la continuità del servizio.

Le procedure per l'ottenimento di un nuovo certificato differiscono dalla prima emissione in quanto non vengono più ripetute le attività di identificazione e di registrazione dei dati del Titolare.

J.2. Sostituzione delle chiavi del Certificatore

Per quanto riguarda le procedure per la sostituzione delle chiavi di Certificazione e del sistema di Validazione Temporale, si rimanda a quanto indicato nel Manuale Operativo INTESA:

(***http://e-trustcom.intesa.it/ca_pubblica/manuale_operativo.pdf)***.

K. Registro dei certificati

K.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

1. I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
2. I certificati delle chiavi di certificazione.
3. I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
4. Certificati per le chiavi di firma del DigitPA.
5. Le liste di revoca e sospensione.

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il Certificatore mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno: questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

K.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL.

L'accesso è possibile all'indirizzo ***ldap://x500.e-trustcom.intesa.it*** secondo il protocollo LDAP.

K.3. Accesso fisico ai locali dei sistemi preposti al registo dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se presenti almeno nel numero ritenuto adeguato ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

L. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure minime previste dal DLgs 196/03.

M. Procedura di gestione della copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato alla sezione K.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del Certificatore (DPCM, Art.36).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (DPCM, Art.49, comma 1).

- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (DPCM, Art.52).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

N. Procedura di gestione degli eventi catastrofici

Il Responsabile della sicurezza gestisce un piano di gestione degli eventi catastrofici che prevede le seguenti fasi:

- gestione dell'emergenza: in questa fase è garantita la continuità di accesso alle CRL/CSL; la loro emissione può subire ritardi derivanti dalla necessità di attivare il server di back up della CA, situato nel sito di back up;
- gestione del transitorio: in questo periodo è assicurata l'emissione dei certificati e il ripristino di ulteriori soluzioni di disaster recovery;
- ritorno dell'esercizio a regime: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Va premesso che la presenza di repliche della copia operativa del registro dei certificati distribuite in più punti consente comunque, in caso di interruzione di funzionamento della sede principale, di accedere al contenuto del registro dei certificati aggiornato fino al momento dell'interruzione.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL/CSL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e dello HW, anche della situazione di emergenza. È previsto inoltre l'intervento entro il medesimo lasso di tempo dei depositari delle componenti la chiave privata della CA ai fini di ricostruirla nel dispositivo di firma del sito di backup.

In tutte le località interessate dalla gestione degli eventi catastrofici è depositata copia cartacea del piano di emergenza.

O. Procedure per la validazione temporale

O.1. Servizio di validazione temporale

Il TSP INTESA offre un servizio di validazione temporale di documenti informatici.

Data e ora certa sono garantite dalla sincronizzazione con l'ora campione italiana fornita dal servizio NTP di INRIM (vedi cap. P)

O.2. Modalità di richiesta e verifica marche temporali

Il TSP INTESA mette a disposizione dei propri Clienti un'applicazione per la richiesta e la verifica di marche temporali.

Tale applicazione effettua la richiesta di marca temporale con la seguente procedura:

1. Selezione, da parte dell'utente, del documento a cui associare la marca temporale.
2. Generazione dell'impronta da parte dell'applicazione.
3. Invio alla TSA della richiesta di marca temporale con la stessa impronta.
4. Ricezione della risposta da parte della TSA con il risultato della richiesta e, in caso di successo, la marca temporale che viene memorizzata nel file specificato dall'utente.

Mediante la stessa applicazione l'utente può, in qualsiasi momento, visualizzare e verificare le marche temporali ricevute.

Il comando di visualizzazione fornisce le seguenti informazioni relative alla marca temporale contenuta nel file selezionato:

- data ed ora di generazione della marca;
- versione del protocollo di Time Stamping utilizzato dal server che ha generato la marca temporale;
- identificatore dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale;
- valore dell'impronta dell'evidenza informatica;
- numero di serie della marca temporale;
- identificativo della policy di sicurezza implementata dalla TSA.

La verifica di una marca temporale richiede l'indicazione del file originale e del file contenente la marca temporale associata.

P. Modalità per l'apposizione e la definizione del riferimento temporale

Tutte le macchine del sistema di PKI del TSP INTESA sono sincronizzate con l'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata da un software specifico installato su ogni server che, mediante il protocollo NTP (Network Time Protocol), si collega al server remoto configurato.

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per passare l'informazione di tempo e di data sulla rete Internet. Esso permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.

L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

Il sofware installato presso il TSP INTESA si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l'ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (GG/MM/YYYY HH:MM:SS), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM, Art.51.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (DPCM, Art.41).

Q. Modalità operative per l'utilizzo del sistema firma

Come detto in precedenza le chiavi di firma non risiedono su di un dispositivo locale quale una smart card o di un token ma vengono generate e conservate su un HSM remoto.

Per firmare il titolare dovrà accedere all'applicazione web fornita da INTESA e una volta verificato il documento o i documenti da firmare avviare la procedura di firma stessa.

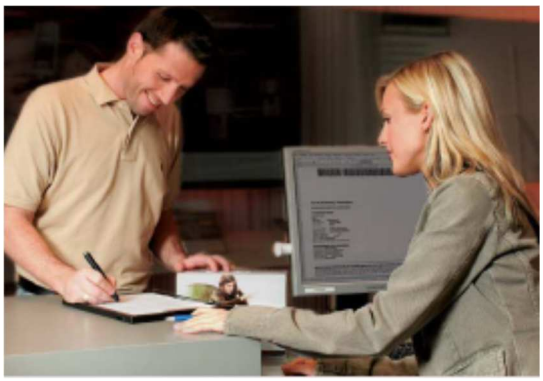
Normalmente per questa tipologia di servizi l'accesso al dispositivo di firma (HSM) viene gestito attraverso l'impiego di PIN e OTP (One Time Password), la novità descritta nel presente Manuale Operativo è l'introduzione di una tecnica grafometrica (basata sul riconoscimento della firma effettatuata su uno specifico device o tablet) come metodo alternativo per l'accesso al dispositivo di firma stesso (HSM).

Q.1. Modalità di Firma

Il Titolare anche al momento della firma sarà stato identificato dal personale INTESA o suoi delegati, tipica situazione è quella in cui un Istituto Bancario o un'Assicurazione svolgono per conto di INTESA le attività di Registration Authority.

In questo caso non solo il Titolare sarà stato precedemente identificato ma anche al momento della firma si troverà presso una filiale al cospetto del personale della società stessa che lo avrà nuovamente riconosciuto.

Dopo che questo nuovo riconoscimento sarà stato effettuato ed una volta che il titolare abbia potuto esaminare il/i documento/i da firmare egli potrà avviare tale procedura apponendo una firma su di un dispositivo tablet (in modo analogo a come aveva firmato nella fase di enrollment precedentemente descritta).

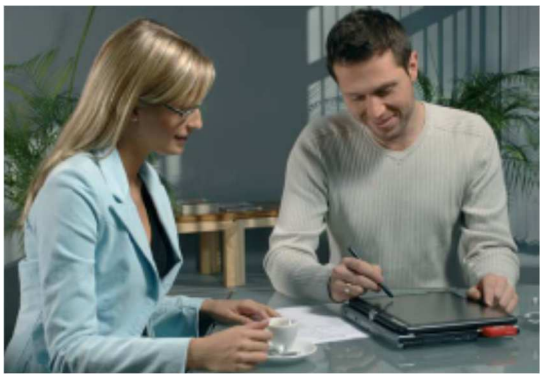


- Il sistema è in grado di rilevare alcune fra le caratteristiche grafometriche più salienti della firma appena apposta e confrontarle con il profilo precedentemente archiviato.

Uno score determinerà quanto la firma apposta per ultima si discosta dal profilo,registrato per quell'utente, se lo score di riconoscimento verà considerato sufficientemente alto (>=80%) ed in considerazione che il Titolare è stato nuovamente identificato dal personale del Certificatore (o di una Registration Authority) il processo di firma potrà essere avviato.

Qualora invece il confronto fra la firma appena apposta ed il profilo registrato non dovesse raggiungere lo score desiderato, nonostante l'identificazione appena effettuata, verrà richieso all'utente di apporre con maggiore attenzione una nuova firma.

Questo perché probabilmente il non raggiungimento dello score desiderato può essere dovuto a errori anche banali ma immediatamente rilevati dal sistema (mancanza di una lettera, omissione di vocali accentate, etc.).



La nuova apposizione eseguita con maggiore attenzione ha normalmente successo, e raggiunto lo score desiderato si potrà finalmente avviare la procedura di firma.

R. Modalità operative per l'utilizzo del sistema di verifica delle firma

Come previsto dall'Art.14, comma 1, del DPCM, il Certificatore indica l'applicazione che consente di effettuare la verifica delle firme digitali.

Poiché i documenti sottoscritti nell'ambito dei servizi descritti da questo Manuale Operativo sono esclusivamente in formato PDF (come previsto dall'art.21 comma 8 e 15 della delibera CNIPA n. 45), si suggerisce a tutti gli utilizzatori di scaricare il software Acrobat Reader DC reperibile gratuitamente sul sito ***www.adobe.com/it***.

S. Modalità operative per la generazione della firma digitale

Il TSP INTESA mette a disposizione dei propri Clienti strumenti per la generazione della firma digitale sia su documenti singoli che in modalità massiva mediante l'utilizzo di procedure automatiche. Tali strumenti sono conformi a quanto previsto dagli Artt. 4 e 11 del DPCM.

S.1. Firma con procedure automatiche e formato dei documenti

Il servizio offerto non prevede il rilascio di un'applicazione client e la distribuzione di smart card e/o token USB come dispositivi di firma, ma piuttosto un'applicazione remota accedibile attraverso un sistema di autenticazione basato sulla tecnologia di autorizzazione grafometrica precedentemente illustrata che offre una serie di funzionalità che permettono la sottoscrizione di uno o più documenti e l'apposizione per ogni singola firma di una marca temporale. generata dal servizio di validazione temporale del TSP INTESA descritto alla sezione O – *Procedure per la validazione temporale*.

In questo caso i certificati di sottoscrizione generati risiedono, con le rispettive chiavi private, come già anticipato su un dispositivo di firma di tipo Hardware Security Module (HSM).

Il servizio è conforme a quanto stabilito dalla normativa (DPCM, Art.5, comma 2 e 3) e il formato della busta crittografica e di firma è coerente con quanto descritto nello standard ISO/IEC 32000 – Portable Document Format (PDF) sviluppato in conformità alle specifiche ETSI TS 103 172 v.2.2.2.