Qualified Trust Service Provider
ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

CPS - Certification Practice Statement
e CP - Certificate Policy
per il Servizio Fiduciario Qualificato di Validazione temporale elettronica

Codice documento: INTQS-TSA_CPS

OID: 1.3.76.21.10.100.3

Redazione: Antonio Raia

Approvazione: Simone Baldini
(Resp. servizio di certificazione e validazione temporale)

Data emissione: 30/12/2021

Versione: 02

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A.

Questa pagina è intenzionalmente priva di contenuto.

Revisioni

Versione n°: 02	***Data Revisione:***	***30 dicembre 2021***
Descrizione modifiche:	*Par. 1.2.2*:aggiornamento riferimenti helpdesk *Par. 1.3*: aggiornamenti normativi *Par. 2*: aggiornamento *Par. 4.2.1*: correzione refusi *Par. 7.7*:aggiornamento descrittivo Aggiornamento dati societari e logo	
Motivazioni:	Modifica numero telefonico helpdesk per chiamate dall'estero Integrazione riferimenti OID Puntualizzazione sul controllo del sincronismo dei TSS Variazione proprietà, direzione e coordinamento della società	
Versione n°: 01	***Data Revisione:***	***11 gennaio 2017***
Descrizione modifiche:	Nessuna	
Motivazioni:	Prima emissione	

Sommario

1 Introduzione

La *validazione temporale* (o *marcatura temporale*) è un servizio che permette di associare date e ora certe e legalmente valide a un documento informatico o un evento (es. ricezione di un messaggio, generazione di un documento o firma di un documento), consentendo quindi di associare una validazione temporale opponibile a terzi.

Il servizio consiste nella generazione, da parte di una *TSA* (*Time-Stamping Authority*), di una validazione temporale elettronica (*TST – Time-Stamping Token*), che permette di associare a documenti elettronici (o altri dati in form elettronica) l'informazione relativa ad una data e ad un'ora certa, così da approvare che i documenti esistevano in quel momento.

Il servizio di marca temporale può essere utilizzato sia su file **non** firmati digitalmente; garantendone una collocazione temporale certa e legalmente valida, sia su documenti informatici sui quali è stata apposta una Firma Digitale; in tal caso la marca temporale attesterà il preciso momento temporale in cui il documento è stato creato, firmato, trasmesso o archiviato

Questo documento descrive le regole e le procedure operative del TSP INTESA per l'emissione dei certificati relativi al servizio fiduciario di validazione temporale e la generazione e la verifica delle validazioni temporali, in conformità con la vigente normativa.

Quanto descritto in questo documento si applica al TSP INTESA, cioè alle sue infrastrutture logistiche e tecniche e al suo personale, ai titolari dei certificati da esso emessi, agli utenti del servizio di validazione temporale e a quanti utilizzino tali certificati/marche temporali per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma digitale e/o una marca temporale.

Il presente *CPS - Certification Practice Statement* (nel seguito solo CPS) è di esclusiva proprietà di In.Te.S.A. S.p.A. (di seguito anche *INTESA*, *TSP INTESA* oppure solo *TSP*), che è titolare di ogni relativo diritto intellettuale.

Quanto fornito da INTESA ai Sottoscrittori e ai propri operatori per utilizzare la funzioni della Public Key Infrastructure (PKI) gestita da INTESA è coperto da diritti sulla proprietà intellettuale.

Per estensione, si considerano i servizi fiduciari qualificati di Time-Stamping come servizi erogati dalla struttura di PKI.

1.1 Identificazione CPS

Il presente documento costituisce il *CPS - Certification Practice Statement* del TSP INTESA.

Il contenuto del CPS è conforme con quanto definito nelle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013, nel Codice dell'Amministrazione Digitale (così come modificato dal D.Lgs 179/2016) e nel Regolamento (UE) 910/2014 (eIDAS).

Nome *CPS - Certification Practice Statement*	*INTQS-TSA_CPS*
Policy di riferimento	ETSI EN 319 421 (0.4.0.2023.1.1) ETSI EN 319 411-n ETSI EN 319 401
OID In.Te.S.A. S.p.A.	1.3.76.21
servizi qualificati eIDAS	1.3.76.21.10
presente documento	*1.3.76.21.10.100.3*
servizi di Validazione temporale qualificata	1.3.76.21.10.1
OID TS-CA root	1.3.76.21.10.1.1
OID TSU	1.3.76.21.10.1.1.1

1.2 Riferimenti

1.2.1 TSP INTESA

Nel seguito, i dati identificativi del Prestatore dei Servizi Fiduciari descritti nel presente documento:

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*
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

1.2.2 Contatti

Per eventuali osservazioni e richieste di chiarimenti, sono disponibili i seguenti recapiti:

posta elettronica:	*uff_ra@intesa.it*
Telefono:	+39.011.19216.111
Helpdesk - per le chiamate dall'Italia	800.80.50.93
Helpdesk - per le chiamate dall'estero	+39 02.39 30 90 66

1.3 Riferimenti di normativi

Regolamento (UE) N. 910/2014 (eIDAS) e ss.mm.ii.	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 presente documento, indicato anche solo come *Reg. eIDAS* (electronic Identification Authentication and Signature).
CAD - DLGS 82/05 e ss.mm.ii.	Decreto Legislativo 7 marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale".* Nel presente documento, indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e ss.mm.ii.	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 - *"Regole tecniche in materia di generazione, apposizione verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36,comma 2, e 71"* (del CAD, n.d.r.). Nel presente documento, indicato anche solo come *DPCM.*
DELIBERAZIONE	Deliberazione CNIPA 21 maggio 2009, n.45 – "*Regole per il riconoscimento e la verifica del documento informatico"*; modificata dalla Determ. DigitPA n.69/2010.
DLGS 196/03 e ss.mm.ii.	Decreto Legislativo n.196 del 30 giugno 2003 - "*Codice in materia di protezione dei dati personali*".
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	Decreto Legislativo n.196 del 30 giugno 2003 - "*Codice in materia di protezione dei dati* REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Nel presente documento, indicato anche solo come *GDPR.*
DETERMINAZIONE N. 147/2019 (Linee Guida) e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel presente documento, indicato anche solo come *DETERMINAZIONE* ovvero *LLGG.*

ETSI-319.401	ETSI EN 319 401 v2.3.1 - *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*
ETSI-319.421	ETSI EN 319 421 v1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic *Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles*
Rec ITU-R	Recommendation ITU-R TF.460-6, *Annex 1 – Time Scales*.
RFC5905	Network Time Protocol (Protocollo NTP)

1.4 Definizioni e acronimi

Sono qui riportati i significati di alcuni acronimi e termini specifici utilizzati nel presente documento. Un elenco più completo è presente sul Regolamento eIDAS (*Art.3 Definizioni*) e sul CAD (*Art.1 Definizioni*, così come modificato dall'*Art.1* del D.Lgs 179/2016).

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP - Qualified Trust Service Provider (già Certificatore Accreditato)	*Prestatore di Servizi Fiduciari Qualificati*. Persona fisica o *giuridica* che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A. Nel presente documento, indicato indifferentemente come *QTSP*, *Certificatore Accreditato* o più semplicemente *Certificatore.*
CAB - Conformity Assessment Body	*Organismo di valutazione della conformità.* Ente accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati.
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.
MO	Manuale Operativo
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.
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.).
Validazione temporale elettronica	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. Altrimenti detta *marca temporale* ovvero *time-stamp*.
Marca temporale	Vedi: Validazione temporale elettronica

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 (TSP) che rilascia marche temporali.
TSU	Time-Stamping Unit
TST	Time-Stamping Token - Marca temporale.
Sottoscrittore Richiedente	Ai fini del presente Manuale Operativo, è chi richiede al TSP l'accesso al servizio (persona fisica o guridica).
Utente	L'utilizzatore del servizio di richiesta e apposizione della marca temporale.
Utilizzatore	Chi utilizza la marca temporale nella fase di verifica del documento elettronico al quale la stessa è stata apposta dall'Utente.

2 Gestione delle specifiche contenute nel CPS

Il documento CPS è interamente gestito all'interno dell'organizzazione del QTSP INTESA, i cui riferimenti sono riportati al par. *1.2*.

Il documento CPS è redatto in collaborazione con i responsabili coinvolti nelle attività inerenti la PKI (par. *5.1.1.1*) e finalmente approvato dal *Responsabile della Sicurezza* (ex art. 38 DPCM).

Il documento è quindi inviato per approvazione all'Organismo di Vigilanza: le procedure descritte nel presente CPS potranno essere adottate solo in seguito all'autorizzazione formale dell'Agenzia. A questa segue la pubblicazione del documento sul sito internet del QTSP INTESA e sul sito dell'Agenzia.

1.1.1 Procedura per le revisioni

Fermo restando il ciclo approvativo interno al QTSP, ogni nuova versione del presente CPS sarà notificata all'Agenzia.

Il documento modificato non potrà infatti essere adottato senza il nulla osta dell'Organismo di vigilanza.

Una volta ottenuto parere positivo dall'Agenzia, il documento sarà pubblicato dal QTSP all'URL specificato al par. *1.2*.

Quanto sopra include eventuali modifiche di carattere editoriale o tipografiche.

3 Condizioni Generali

3.1 Obblighi del TSP

Nello svolgimento della sua attività, il TSP INTESA opera in conformità con quanto specificato nel presente documento.

3.1.1 Obblighi del TSP come Certificatore

Nello svolgimento della sua attività come Certificatore, il TSP INTESA opera in conformità con quanto disposto da:

- Decreto Legislativo del 7 marzo 2005, n. 82. Codice dell'Amministrazione digitale;
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013;
- Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104.

3.2 Obblighi della RA INTESA

Gli Operatori di RA sono dipendenti INTESA, attraverso i quali il TSP ottempera a quanto specificato nel presente documento.

3.3 Obblighi del Sottoscrittore

Il Sottoscrittore è tenuto ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.4 Obblighi degli utilizzatori dei certificati e delle validazioni temporali

Coloro che utilizzino documenti elettronici validati temporalmente, sono tenuti a ottemperare agli obblighi previsti nel presente documento.

3.5 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 ottemperare agli obblighi previsti nel presente documento.

4 Profili dei Certificati e Certificate Policy

4.1 TSCA - Time-Stamping Certification Authority

Il Certificato root di TSA dedicato al servizio fiduciario qualificato di validazione temporale ha il seguente OID:

- **1.3.76.21.10.1.1**

4.1.1 Dati contenuti nel certificato

Il ***Certificato di root*** e i dati contenuti sono strutturati come disposto dalla Deliberazione e conformi al Regolamento eIDAS:

field	value
Version	v3
Serial Number	58 96 3d 6d 49 d8 78 56
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN= IN.TE.S.A. QUALIFIED TSA**
Validity (20 yrs)	lunedì 16 gennaio 2017 14:00:28 domenica 11 gennaio 2037 14:00:28
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN= IN.TE.S.A. QUALIFIED TSA**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	03 2b e3 ec 1d 3e b8 07 6f 21 b7 0e b2 f7 2b 29 d6 03 a4 e2
Authority KeyIdentifier	03 2b e3 ec 1d 3e b8 07 6f 21 b7 0e b2 f7 2b 29 d6 03 a4 e2
Certificate Policies:	OID *1.3.76.21.10.1.1*
CRL Distribution Points	Full Name: URI:*http://e-trustcom.intesa.it/CRL/INTESA_QTSA.crl*
Basic Constraint	CA:TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)
Algoritmo di identificazione personale	sha1
Identificazione personale	`21 33 10 d8 52 27 be 4d f5 88 b6 71 2f 37 b7 db aa 0d 7f ed`

4.2 TSU -Time-stamping Unit Certificate

I certificati di validazione temporale, emessi dalla TSCA di cui al par. 4.1, in confomità alla *ETSI 319-422, Annex A*, avranno uno dei seguenti OID:

- 0.4.0.2023.1.1 (ETSI 319-421, Clause 5.2)
- 1.3.76.21.10.1.1.1 (identificativo proprio del TSP)

4.2.1 Dati contenuti nel certificato

Il Certificato e i dati contenuti sono strutturati come disposto dalla Deliberazione e conformi al Regolamento eIDAS:

field	value
Version	v3
Serial Number	Definito dalla CA e univoco all'interno della stessa CA
Signature	sha256WithRSAEncryption
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. QUALIFIED TSA**
Validity	10 years
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **organizationIdentifier=VATIT-05262890014** **OU:QUALIFIED TSA** **CN=IN.TE.S.A. Time-Stamping Unit XXXNN**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	RFC 5280 - Method 1
Basic Constraint	CA:FALSE
Authority KeyIdentifier	03 2b e3 ec 1d 3e b8 07 6f 21 b7 0e b2 f7 2b 29 d6 03 a4 e2
Certificate Policies	Policy: 0.4.0.2023.1.1 or 1.3.76.21.10.1.1.1 Rif. CPS: *https://e-trustcom.intesa.it*
CRL Distribution Points	Full Name: URI:*http://e-trustcom.intesa.it/CRL/INTESA_QTSA.crl*
Key Usage	digitalSignature
Extended Key Usage	Timestamp

4.3 Sostituzione dei certificati e delle chiavi

Le procedure di sostituzione delle chiavi e dei relativi certificati sono descritte all'interno del par. *5.10.1-Sostituzione pianificata delle chiavi di validazione temporale*.

4.4 Revoca dei certificati

Le revoca dei certificati è descritta all'interno del par. .5.5.

5 Modalità Operative

5.1 Entità coinvolte nei processi

5.1.1 Entità del TSP coinvolte nei processi

All'interno della struttura del TSP INTESA sono identificate delle entità che prendono parte ai processi oggetto del presente CPS. Tali attori operano in ottemperanza alle regole e ai processi posti in essere dal TSP, espletando, per la parte di propria competenza, le attività a loro attribuite.

5.1.1.1 Certification Authority (CA/TSCA)

INTESA, operando nell'ottemperanza di quanto previsto nelle Regole Tecniche (DPCM), del Codice dell'Amministrazione Digitale (CAD) e del Regolamento eIDAS, espleta le attività di Prestatore di Servizi Fiduciari Qualificati per la *creazione, verifica e convalida di firme elettroniche* e *validazioni temporali* (cfr. eIDAS, Art.3, comma 16 e 17).

Il personale responsabile delle attività afferenti i servizi di certificazione e validazione temporale, 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).

Le figure sopra elencate sono tutte appartenenti all'organizzazione del TSP INTESA.

5.1.1.2 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, nell'ambito dei Servizi oggetto del presente MO, le seguenti attività:

- Verifica estremi contrattuali
- Registrazioni Utenze
- Rilascio Credenziali per l'accesso al servizio

5.1.2 Altre entità

5.1.2.1 Sottoscrittore / Richiedente

L'Utente è colui che usufruisce del servizio per Validare temporalmente un documento elettronico. Utilizzando le credenziali di accesso al sistema, richiede la marca temporale e la appone sul Documento da validare.

5.1.2.2 Utilizzatore

L'Utilizzatore è colui che, verificando il documento elettronico, utilizza le marche temporali emesse dal TSP INTESA e apposte dall'Utente. Può essere o meno un sottoscrittore.

5.2 Richiesta di Validazione Temporale

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

Tali applicazioni effettuano la richiesta di marca temporale con la seguente procedura:

- Selezione, da parte dell'utente, del documento a cui associare la marca temporale.
- Generazione dell'impronta da parte dell'applicazione.
- Invio alla TSA della richiesta di marca temporale con la stessa impronta.
- 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 le stesse applicazioni l'utente può, in qualsiasi momento, verificare le marche temporali ricevute e verificarne le informazioni contenute. Tra queste:

- 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.

5.2.1 Verifica delle validazioni temporali

Come previsto dall'Art.14, comma 1, del DPCM, al fine di effettuare la verifica delle firme digitali e delle validazioni temporali, il TSP INTESA fornisce l'applicazione ***DigitalSign Reader***.

Il software è disponibile per il download, assieme alla relativa documentazione, all'indirizzo:

http://e-trustcom.intesa.it/softwarediverifica.html

L'utilizzo del software è gratuito.

L'applicazione permette di verificare qualunque archivio informatico firmato e validato temporalmente e di visualizzarne il contenuto, qualora la stazione di lavoro sia dotata del software adatto a processare quella tipologia d'archivio. A titolo d'esempio, l'applicazione sarà in grado di visualizzare i documenti caratterizzati dall'estensione ".pdf" qualora sia stata preventivamente installata l'applicazione Acrobat Reader.

Per l'utilizzo dell'applicazione non è necessario disporre di alcun dispositivo di firma.

La procedura di verifica della firma digitale apposta ad un documento informatico esegue i seguenti controlli:

- verifica delle struttura della busta crittografica;
- verifica che il certificato del firmatario non sia scaduto;
- verifica che il certificato del firmatario non sia stato revocato o sospeso;
- verifica che il certificato del firmatario sia stato emesso da una Autorità di Certificazione inclusa nell'elenco pubblico dei certificatori accreditati;
- verifica delle informazioni presenti nel certificato qualificato, nonché le estensioni obbligatorie (DPCM, Art.14, comma 2b);
- consente l'aggiornamento, per via telematica, delle informazioni pubblicate nell'elenco pubblico dei certificatori accreditati (DPCM, Art.14, comma 2c);
- verifica della marca temporale;
- verifica della validità del certificato di certificazione (CA e TSCA);

Per ulteriori dettagli relativi all'applicazione, si rimanda al manuale utente disponibile sull'applicazione stessa.

5.2.2 Piattaforma proprietaria DeSigner

Il TSP INTESA mette a disposizione della propria clientela una soluzione in grado di erogare servizi Firma Digitale e Marcatura Temporale Remota puntuale e/o massiva, riducendo al minimo i costi di adozione da parte degli utilizzatori del servizio.

La piattaforma Intesa ***DeSigner*** consente di:

- apporre Firme Digitali Qualificate puntuali (complete di marca temporale) ai documenti oggetto del servizio protette da Strong Authentication
- apporre firme massive qualificate (complete di marca temporale) su singoli documenti o su tutti i documenti contenuti in un'area definita
- apporre una marca temporale ad uno specifico documento o a tutti i documenti contenuti in un'area definita
- verificare firma e/o marcatura temporale apposte su uno specifico documento o a tutti i documenti contenuti in un'area definita.

Gli elementi base che compongono la soluzione DeSigner di Firma Remota di Intesa sono:

- Il server di firma DeSigner (la componente applicativa di firma in grado di interfacciare i dispositivi crittografici di firma) che sarà operante nella Server farm di Intesa,
- La componente Client DeSigner esposta tramite interfaccia web services di tipo SOAP e REST per essere integrata nell'applicazione Cliente.
- I Dispositivi crittografici di firma (HSM) dimensionati opportunamente sulla base delle esigenze (numerosità degli utenti da gestire e dalla configurazione scelta HA, DR), operativi presso la Server Farm di Intesa
- L'integrazione con i Timestamp Server che erogano le marche temporali per collocare nel tempo il documento o la firma apposta al documento.
- L'integrazione con la soluzione di autenticazione DeAuth per le operazioni di Strong Authentication inerenti la firma: generazione, invio, verifica token di autenticazione.
- L'integrazione con la soluzione di verifica Firma e Marcatura Temporale DeVerify
- La Certification Authority di Intesa

La soluzione proposta permette di interfacciare i servizi di Marcatura Temporale sia direttamente dalle applicazioni Cliente, rispettando lo standard RFC3161, sia con l'ausilio della componente DeSigner.

Il DeSigner, infatti, è in grado di interfacciare direttamente il servizio di Marcatura Temporale fornendo allo stesso tutte le informazioni necessarie e ottenute dalla componente web services del Client e di richiedere, di conseguenza, l'apposizione delle marche temporali sul singolo documento o su un lotto di documenti.

La soluzione DeSigner è in grado di interfacciare direttamente anche i servizi di verifica Firma e Marcatura Temporale esposti dalla componente ***DeVerify***.

DeVerify è il servizio offerto da Intesa per la verifica delle Firme e delle Marche Temporali e che offre le seguenti funzionalità:

- Verifica Firma Digitale, con o senza Marcatura Temporale, su un documento singolo o su un lotto di documenti per tutti i profili di Firma normati: CADES (P7M), PADES (PDF), XADES (XML).
- Verifica Marcatura Temporale su un documento singolo o su un lotto di documenti
- Verifica di Firme/Marche temporali multiple all'interno dello stesso documento
- Verifica di Firme/Marche temporali a 3 livelli: check integrità, rispetto requirements normativi, verifica alla data con download delle CRL
- Generazione report sintetici o di dettaglio con l'esito delle verifiche

Le funzionalità sopracitate saranno gestite anch'esse direttamente dal DeSigner, nell'ambito dell'integrazione con la soluzione DeVerify, con l'ausilio delle informazioni fornite dal web services Client.

5.2.3 Software di firma e verifica – DigitalSign

DigitalSign (*CompEd Software Design Srl*) è l'applicazione distribuita dal TSP INTESA per la generazione e la verifica di firme digitali e l'apposizione di marche temporali.

Alla prima attivazione, occorre procedere alla configurazione del dispositivo di firma e aggiornare l'elenco dei certificati di CA con le relative CRL. Queste informazioni vengono reperite dalla lista dei Certificati di certificazione tenuta da AgID.

Attivando la funzione di Firma, è richiesto di selezionare il documento da sottoscrivere e di inserire il dispositivo di firma (smartcard ovvero token USB), se non ancora presente. Il documento selezionato viene visualizzato mediante l'applicazione e viene quindi richiesto di digitare il codice PIN del dispositivo di firma. Finalmente, all'utente è richiesto di salvare il documento firmato (Cades o Pades) e/o marcato temporalmente, se richiesto.

Nel processo di generazione della firma digitale vengono effettuate le seguenti operazioni:

- Verifica che il certificato di sottoscrizione indicato dall'utente non sia scaduto.
- Verifica della corrispondenza tra chiave privata presente sul dispositivo di firma e certificato del Titolare.

L'applicazione *DigitalSign* permette anche l'apposizione di firme multiple allo stesso documento.

Alla firma può associata una marca temporale generata dal servizio di validazione temporale del TSP INTESA.

Oltre alla funzioni di generazione di firme, il prodotto offre le seguenti funzionalità:

- Verifica firma: tale funzione è analoga a quella descritta nella sezione **Errore. L'origine riferimento non è stata trovata.**.
- Cifra: tale funzione permette di cifrare un documento, disponendo di un certificato utilizzabile per la cifratura di dati.
- Decifra: tale funzione permette la decifratura di dati precedentemente cifrati.

Per ulteriori dettagli relativi all'applicazione *DigitalSign* si rimanda al manuale utente, disponibile nel prodotto stesso.

5.2.4 Software di firma e verifica – firma4ng

Il TSP INTESA distribuisce anche il software di firma e verifica ***firma4ng*** *(Bit4id)*, un'applicazione professionale di firma digitale, compatibile con i sistemi operativi Windows, Linux e Mac OS X. Permette la firma e la verifica di qualsiasi tipo di documento elettronico.

Per ulteriori dettagli relativi all'applicazione *firma4ng* si rimanda al manuale utente, disponibile nel prodotto stesso.

5.3 Formato dei documenti

Le applicazioni fornite dal TSP INTESA permettono l'apposizione della firma digitale e della validazione temporale su tutti i formati di documenti elettronici.

È tuttavia importante sottolineare che alcune tipologie di documento informatico non potrebbero comunque ottenere gli effetti descritti nell'Art.21 del CAD, poiché potrebbero contenere macroistruzioni o codice eseguibile tali da attivare funzionalità che possano modificare gli atti o i dati nello stesso rappresentati.

5.4 Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

- I certificati delle chiavi di sottoscrizione del sistema di validazione temporale.
- I certificati delle chiavi di certificazione.
- I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
- Certificati per le chiavi di firma dell'Agenzia (DPCM).
- 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.

La copia di riferimento (MASTER) 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/CSL.

La copia di riferimento aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

L'accesso è possibile sulla copia operativa (SHADOW) all'indirizzo ***ldap:x500.e-trustcom.intesa.it*** (via protocollo LDAP).

5.5 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 dalla CA, viene aggiornata con periodicità prestabilita (24h) e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

5.5.1 Revoca dei certificati relativi alle Chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- malfunzionamento del dispositivo sicuro (HSM) con rischio di compromissione delle chiavi,
- cessazione dell'attività del TSP,

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

Entro 24 ore, il TSP notificherà la revoca all'Agenzia e agli Utenti del Servizio.

5.5.2 Revoca dei certificati relativi alle Chiavi di validazione temporale

Nei casi di:

- compromissione della chiave di validazione temporale,
- malfunzionamento del dispositivo sicuro (HSM) con rischio di compromissione delle chiavi,
- cessazione dell'attività del TSP,

il TSP procede con la revoca dei certificati di validazione temporale e disattiva la TSU relativa.

5.6 Pubblicazione CRL

Il rinnovo delle CRL è schedulato ogni 24 ore. L'emissione delle CRL è altresì contestuale ad una Revoca o Sospensione operate sul sistema.

5.6.1 Requisiti per la consultazione delle CRL/CSL

Le parti interessate, nella verifica di validità di un documento firmato digitalmente e/o validato temporalmente, devono verificarne la validità:

- scaricando le ultime CRL/CSL pubblicate dal TSP INTESA all'URL specificato
- verificando la validità delle CRL/CSL scaricate, verificandone la firma
- verificando la validità delle CRL/CSL scaricate, verificando che la data e l'ora del prossimo aggiornamento non siano state superate
- verificando che il certificato non sia inserito nella CRL/CSL
- verificare l'autenticità del certificato e/o la marca temporale attraverso il rispettivo di certificazione la Lista Pubblica dei Certificatori (EUTSL)

5.7 Procedure di Audit della Sicurezza

Tutti i sistemi e componenti coinvolti nei processi descritti in questo *CPS* tengono traccia degli eventi rilevanti.

5.7.1 Tipi di eventi registrati

Tutti i sistemi INTESA, ivi inclusi i sistemi di LRA, tengono traccia delle operazioni rilevanti: i file di *Log* prodotti sono tenuti e gestiti in modo da evitare qualsiasi manomissione.

Gli eventi vengono classificati in base al livello di rilevanza: il livello minimo è quello di tipo informativo come quando trattasi di normali attività (es. una richiesta di certificato, l'emissione di una nuova CRL), il livello massimo è relativo ad eventi critici, come nel caso di sbagli imputabili ad un operatore (es. il tentativo di eseguire un'operazione non autorizzata) o di malfunzionamenti HW o SW.

5.7.2 Frequenza dei controlli dei LOG

Tali dati vengono consultati e verificati giornalmente per garantire un audit completo. In caso di forza maggiore, è applicato quanto descritto nel Piano della Sicurezza INTESA.

5.7.3 Conservazione dei LOG

Tutti i dati di log sono conservati per una durata non inferiore ai 20 (venti) anni.

5.7.4 Protezione dei Log

La numerazione progressiva degli eventi, l'indicazione del momento in cui si sono verificati e l'utilizzo della firma digitale, rendono praticamente impossibile ogni alterazione del file stesso.

L'ispezione dei Log è di competenza del *Responsabile dell'Audit*, che vi può accedere accompagnato da almeno una figura autorizzata.

5.7.5 Procedure di backup dei Log

Il backup dei Log segue le procedure descritte più avanti in 4.6.4.

5.7.6 Sistema di accumulazione dei Log

L'accumulazione dei Log è interna ai sistemi coinvolti.

5.7.7 Notifica ai soggetti causa di eventi

Il *Responsabile della Sicurezza* notifica per iscritto i soggetti che hanno causato eventi e il loro manager.

5.7.8 Verifiche della vulnerabilità

Verifiche sulla vulnerabilità dei Log sono eseguite insieme al processo generale di Risk Assessment INTESA.

5.8 Archivio validazioni temporali

Tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a venti anni (DPCM, Art.53, comma 1).

5.9 Modalità di sostituzione delle Chiavi di Certificazione (TSCA)

5.9.1 Sostituzione pianificata delle Chiavi di certificazione

Almeno 90 (novanta) giorni prima della scadenza del certificato relativo alla coppia di *Chiavi di certificazione*, utilizzate dal sistema di emissione dei certificati, in presenza del *Responsabile del servizio di certificazione* e di responsabili aziendali in numero sufficiente a garantire la sicurezza dell'operazione, si procederà alla generazione di nuove chiavi di certificazione.

Quanto fatto sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza del certificato.

5.9.2 Sostituzione in emergenza delle Chiavi di certificazione

Il procedimento utilizzato in caso di guasto del dispositivo di firma o di disastro presso la sede centrale è trattato al par. *5.11*.

5.10 Modalità di sostituzione delle chiavi di validazione temporale (TSU)

5.10.1 Sostituzione pianificata delle chiavi di validazione temporale

In conformità con quanto indicato dal DPCM (Art.49, comma 2), al fine di limitare il numero di marche temporali generate con la medesima coppia di *Chiavi di validazione temporale*, queste sono sostituite entro 90 (novanta) giorni dalla data della loro creazione. Contestualmente, un nuovo certificato è emesso relativamente alla nuova coppia di chiavi, senza revocare il certificato corrispondente alla coppia di chiavi precedentemente in uso.

L'operazione è svolta in presenza del *Responsabile del Servizio* ovvero da suo delegato.

Quanto fatto sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza del certificato.

5.10.2 Sostituzione in emergenza delle chiavi del sistema di validazione temporale

Il procedimento utilizzato in caso di guasto del dispositivo di firma o di disastro presso la sede centrale è descritto al par. *5.11*.

5.11 Gestione del disaster recovery

5.11.1 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 dei token di autenticazione/gestione dei dispositivi HSM al fine di attivare la chiave privata di CA nel dispositivo di firma del sito di backup.

5.11.2 Guasto del dispositivo di firma della TSCA INTESA

Nel caso di guasto del dispositivo di firma contenente le chiavi di certificazione, sarà necessario, a seconda del tipo di guasto, o ri-inizializzare il dispositivo stesso o inizializzarne uno nuovo, come descritto al par. *7*, al fine di ricreare le chiavi originali.

Il tutto sarà verbalizzato, sottoscritto e conservato per 20 (venti) anni.

5.11.3 Compromissione delle chiavi di certificazione

Nel caso di compromissione delle chiavi di certificazione, è applicata la procedura di revoca, come descritto al par.13. Il TSP INTESA genererà una nuova coppia di chiavi, come riportato al par. *7.1*.

Nel caso di compromissione delle chiavi di marcatura temporale, il relativo certificato sarà revocato e le chiavi saranno ricreate, come descritto al par. *7.1*.

Nel caso i due eventi precedenti occorressero contemporaneamente, i certificati emessi e marcati temporalmente con le chiavi coinvolte saranno revocati per iniziativa del certificatore (DPCM). Viene applicato quanto descritto in precedenza e i certificati riemessi con la procedura usuale. Le liste CRL/CSL saranno firmate con il nuovo set di chiavi. Nota: questa possibilità è stata valutata e pianificata per completezza, poiché è ragionevole che non si verifichi mai.

6 Sicurezza fisica

Il sistema PKI INTESA e i suoi componenti HW e SW sono gestiti dentro e da installazioni sicure, protette da accessi non autorizzati attraverso sistemi di controllo accessi tradizionali e di sorveglianza, che forniscono registrazioni per audit di verifica.

Solamente il personale autorizzato ha accesso alle aree specifiche, sotto stringenti policy e procedure oggetto periodico di audit.

6.1.1 Ubicazione fisica e struttura dell'edificio

Ciascun edificio rilevante per la struttura PKI è dotato di misure di sicurezza rispondenti alle vigenti norme di legge.

Ogni edificio è sotto sorveglianza ed è monitorato da sistemi elettronici e da personale addetto.

Gli impianti elettrici e di sicurezza sono certificati a norma di legge.

I sistemi PKI INTESA sono ospitati in edifici collocati in zone non sismiche, dotati di opportuni sistemi di scarico delle acque e lontani dai corsi d'acqua.

Nelle vicinanze non sono presenti fabbriche a rischio di emissioni nocive.

6.1.2 Accessi fisici

I sistemi di PKI INTESA (CA, RA, Directory, Time Stamp Server) sono ospitati in aree chiuse ed elettronicamente controllate.

Gli accessi alle aree PKI sono limitati al personale autorizzato, che in nessun caso può operare da solo: norme specifiche regolano il numero e il tipo di figure professionali richieste per ogni rilevante operazione sui sistemi di PKI.

L'accesso di visitatori occasionali è permesso solamente se accompagnati dal personale autorizzato (in numero dipendente dall'area specifica). Tale accesso è tracciato.

L'accesso di persone non autorizzate (es. personale di servizio) avviene solo in presenza del numero minimo di personale autorizzato.

Sono attivi sistemi di anti intrusione.

6.1.3 Energia e Condizionamento

Le aree PKI sono condizionate. I sistemi dell'aria condizionata sono regolarmente monitorati per prevenire la diffusione di sostanze nocive. Le condutture non aggirano i sistemi di controllo messi in essere tra le aree di sicurezza.

E' attivo un generatore supplementare indipendente di energia elettrica, locato esternamente all'edificio e testato periodicamente.

6.1.4 Rischio d'allagamento

Vedi 6.1.1.

6.1.5 Prevenzione e protezione antincendio

Le misure di prevenzione e protezione antincendio attivate sono conformi alle normative vigenti.

6.1.6 Supporti di memorizzazione dati

I supporti utilizzati per la memorizzazione dei dati sono stoccati in aree sicure. Sono attive procedure per la loro gestione durante l'intero ciclo di vita, dall'acquisto fino allo smaltimento.

6.1.7 Smaltimento rifiuti

Lo smaltimento di supporti media prevede la loro cancellazione o distruzione per prevenire la divulgazione di dati confidenziali.

I documenti classificati come confidenziali sono distrutti prima di essere smaltiti.

6.2 Controlli procedurali

E' applicata una restrittiva separazione dei ruoli (DPCM), che prevede le seguenti figure:

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)

Tutte le mansioni relative a compiti di certificazione sono assegnate formalmente al personale dipendente di INTESA S.p.A. a tempo indeterminato. Nessuno dei sopra citati sarà dettagliato in seguito, fatta eccezione per il *Responsabile del servizio di certificazione e validazione temporale*, unico ruolo con responsabilità operative. Saranno ugualmente definiti i ruoli operativi, con le proprie responsabilità e i requisiti di sicurezza

Il personale autorizzato alle aree ad accesso ristretto è tenuto a rispettare le specifiche procedure INTESA.

Quando viene stabilita la cessazione del rapporto di lavoro con gli addetti al sistema di certificazione, sia essa immediata o pianificata entro un lasso di tempo medio-breve (dell'ordine di pochi mesi al massimo), essi cessano immediatamente dall'occuparsi del sistema, vengono disabilitati dalle funzioni relative e restituiscono tempestivamente ogni dispositivo e documento di riconoscimento che consenta loro di accedere alle aree e ai documenti riservati e di continuare ad esercitare le mansioni relative e la documentazione riservata in loro possesso.

Viene inoltre loro ricordato l'obbligo di non rivelare le notizie riservate di cui siano a conoscenza, anche dopo la conclusione del rapporto di lavoro.

6.2.1 Responsabile della generazione dei certificati

Tale posizione è assegnata dalla Direzione Aziendale INTESA.

Il responsabile della generazione dei certificati è incaricato della supervisione del processo di emissione e gestione dei certificati, inclusa la custodia dei dispositivi di firma del Certificatore.

È responsabile quindi dei vari aspetti riguardanti la crittografia e della correttezza e del rispetto delle procedure previste per:

- la custodia di tutti i dispositivi di firma: quelli destinati ai titolari e quelli del Certificatore;
- l'attivazione dei dispositivi di firma del sistema di emissione dei certificati, del sistema di marcatura temporale e dei titolari
- la generazione delle chiavi del sistema di emissione dei certificati;
- la sostituzione delle chiavi dei titolari;
- la sostituzione delle chiavi del Certificatore in condizioni di emergenza e di normale avvicendamento;
- la corretta emissione delle marche temporali e la loro conservazione;
- il rilascio, la sospensione, la revoca, la sostituzione dei certificati;
- l'emissione delle CRL/CSL;
- la produzione e la gestione delle copie di sicurezza;
- la gestione delle funzioni relative a quanto sopra anche nel caso di emergenze e di disastri.

Abilita alle rispettive operazioni gli Operatori della CA (CA Operator – vedi punto 6.2.2), precedentemente incaricati dalla linea manageriale aziendale.

Collabora alla definizione, alla redazione e all'attuazione degli accordi di mutua certificazione.

Collabora con i Responsabili della Sicurezza e dell'Auditing alla definizione, alla redazione e all'attuazione delle misure di sicurezza concernenti quanto di sua competenza.

6.2.2 CA Operator

Gli operatori di CA sono nominati dalla Direzione Aziendale

I CA Operator sono responsabili della installazione, della gestione e dell'aggiornamento del sistema di emissione dei certificati, incluso il dispositivo di firma del Certificatore.

La mansione di CA Operator è ricoperta da più addetti, includendo nel computo anche il Responsabile della generazione dei certificati, per consentire le operazioni sul sistema.

Essi installano il sistema di emissione certificati, autorizzano ad operare sul sistema altri CA Operator, e autorizzano un primo nucleo di almeno due Responsabili della registrazione degli utenti (RA Operator).

6.2.3 Amministratori del registro dei certificati

Il ruolo di amministratore del Registro dei certificati è assegnato dalla Direzione Aziendale

Le sue responsabilità ricoprono l'installazione e la gestione e l'aggiornamento del registro dei certificati e del sistema di marcatura temporale.

La mansione di Directory Administrator è ricoperta da più addetti includendo nel computo anche il Responsabile del registro dei certificati, per consentire le operazioni sul sistema.

6.2.4 RA Operator

Gli Operatori di RA sono nominati dalla Direzione Aziendale.

Le loro responsabilità operative coprono l'installazione, la gestione e l'aggiornamento dei prodotti di RA.

6.2.5 LRA Operator

Gli operatori di Local RA sono nominati dalla Direzione Aziendale.

Le loro responsabilità operative ricoprono le funzioni di interfaccia con i richiedenti la certificazione e con i titolari, durante tutte le fasi di registrazione, certificazione, revoca e sospensione

6.2.6 Amministratori della Rete e dei Sistemi

I gestori dei Sistemi e dell'infrastruttura di rete della CA sono nominati dalla Direzione Aziendale.

- Gli Amministratori di Sistema sono responsabili della gestione dei sistemi ove avviene la generazione dei certificati e l'emissione delle CRL/CSL, di quelli a cui fanno capo le LRA e i RA

Operator e di quelli ove operano il Registro dei certificati e il sistema di validazione temporale. Essi possono entrare nelle sale in cui si trovano i citati sistemi: il loro ingresso e la loro permanenza vengono registrate nel Giornale di controllo. Le loro azioni sullo specifico sistema vengono registrate sul log del sistema stesso.

- Gli Amministratori di Rete sono responsabili della rete locale su cui sono attestati i vari sistemi centrali della CA. Ove necessario essi possono entrare nelle sale in cui si trovano tali sistemi. Il loro ingresso e la loro permanenza vengono registrate nel Giornale di controllo. Le loro azioni vengono registrate sui log.

Essi possono accedere alle aree PKI solo se accompagnati da almeno una persona autorizzata, il quale è responsabile della registrazione della presenza degli amministratori suddetti nelle aree ad accesso ristretto.

6.3 Controlli sul personale addetto

Tutto il personale ricoprente i ruoli menzionati al precedente paragrafo è dipendente INTESA e possiede un'esperienza di almeno 5 (cinque) anni su analisi, sviluppo, pianificazione o gestione di sistemi informativi. Fanno eccezione gli operatori di LRA esterne (LRAE).

Il personale addetto ha ricevuto un adeguato addestramento ed è costantemente aggiornato sulle soluzioni tecnologiche adottate dalla PKI INTESA, sulle procedure, sulle politiche di sicurezza e sulle variazioni organizzative.

Nessuno tra il personale addetto ha avuto in passato sanzioni disciplinari dovute a violazione delle misure di sicurezza, né ha in essere altri incarichi incompatibili con quelli relativi ai servizi di certificazione.

7 Controlli Tecnici di Sicurezza

7.1 Generazione e Installazione delle chiavi

7.1.1 Generazione della coppia di chiavi di certificazione (TSCA)

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 sufficiente ad evitare operazioni illecite.

L'inizializzazione del dispositivo di firma prevede la creazione di più dispositivi (token USB) che consentono la gestione dell'HSM; essi vengono creati 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 conforme alla normativa tempo per tempo vigente.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza dei certificati.

In seguito alla generazione delle chiavi di certificazione, vengono generati i certificati delle chiavi pubbliche, 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.

7.1.2 Generazione della coppia di chiavi di validazione temporale (TSU)

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 conforme alla normativa tempo per tempo vigente.

L'operazione è svolta in presenza del *Responsabile dei servizi di certificazione* ovvero da persona da questi delegata.

Della chiave pubblica viene generato il certificato, avente validità 10 anni, firmato con la chiave privata appositamente generata dal Certificatore.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza dei certificati.

7.1.3 Dimensioni delle chiavi e Algoritmi di firma

L'algoritmo crittografico utilizzato è RSA.

Le chiavi di certificazione (CA e TSCA) hanno lunghezza conforme alla normativa tempo per tempo vigente.

Le chiavi di validazione temporale (TSU) hanno lunghezza conforme alla normativa tempo per tempo vigente

Algoritmo utilizzato: SHA-256.

7.1.4 Utilizzo delle chiavi (keyUsage)

In conformità con la Deliberazione e con il reg. eIDAS, , il campo keyUsage del Certificato di sottoscrizione formato X.509v3 è impostato come segue:

- CA - TSCA: **keyCertSign + cRLSign**
- TSS: **digitalSignature**

Il certificato TSS ha inoltre il campo **extKeyUsage** impostato come *keyPurposeId=timeStamping* (1.3.6.1.5.5.7.3.8).

7.2 Protezione della chiave privata

Tutte le coppie di chiavi sono generate internamente al dispositivo crittografico.

7.2.1 Standard per i moduli crittografici

Il Certificatore utilizza come dispositivi di firma per i propri sistemi (per l'emissione dei certificati e per la generazione delle marche temporali) moduli crittografici di tipo HSM (Hardware Security Module) collegati al sistema mediante protocollo TCP/IP su connessione di tipo Ethernet.

Essi sono dichiarati conformi con CC EAL 4+ (Common Criteria Assurance Level 4+)

Il contenuto del modulo viene disattivato quando viene individuato un tentativo di manomissione.

7.2.2 Controllo Multi-Persona della chiave privata

I dispositivi crittografici di CA e TSS possono essere attivati solo in presenza di un congruo numero di persone autorizzate (almeno due).

7.2.3 Deposito presso terzi della chiave privata

Le chiavi private di non sono depositate presso terzi.

7.2.4 Backup della chiave privata

Le chiavi private di certificazione sono oggetto di backup.

Le chiavi di validazione temporale non sono oggetto di backup.

7.2.5 Archiviazione della chiave privata

Le chiavi private non sono archiviate.

7.2.6 Introduzione della chiave privata in modulo crittografico

Non Applicabile: il TSP INTESA implementa solo la generazione della coppia di chiavi all'interno del dispositivo crittografico.

7.2.7 Attivazione della chiave privata

I dispositivi crittografici di CA e TSU possono essere attivati solo in presenza di un congruo numero di persone autorizzate (almeno due).

7.2.8 Disattivazione della chiave privata

I dispositivi crittografici di CA e TSU possono essere disattivati solo in presenza di un congruo numero di persone autorizzate (almeno due).

7.2.9 Distruzione della chiave privata

Su tutti i sistemi di CA (Primario e Disaster Recovery) e di validazione temporale sono utilizzati dispositivi HSM tamperproof dedicati alla generazione e conservazione delle chiavi (CA/TSCA e TSU). Qualora tale dispositivo venga estratto dal sistema, automaticamente si disattiva. Per togliere il dispositivo da tale stato è necessario riattivarlo mediante l'utilizzo degli appositi dispositivi di sicurezza.

In caso di compromissione della chiave privata, in conseguenza del blocco del dispositivo come prima descritto, alla presenza di un congruo numero di persone autorizzate e del Responsabile dell'audit, il dispositivo sarà inizializzato, in modo da cancellarne il contenuto e i suoi backup saranno ri-inizializzati o distrutti.

Verbale del processo è steso dal Responsabile dell'Audit e conservato per 20 (venti) anni.

7.3 Ulteriori aspetti concernenti la gestione delle chiavi

7.3.1 Archiviazione delle chiavi pubbliche

Le chiavi pubbliche di certificazione sono archiviate da INTESA sul registro dei certificati.

7.3.2 Periodo di validità per le chiavi

Il periodo di validità dei certificati relativi alle chiavi di CA è di almeno 15 anni.

Il periodo di validità dei certificati relativi alle chiavi di TSU è di almeno 10 anni

7.4 Codici di attivazione

Gli operatori di CA sono forniti di codici di attivazione "m di n" per l'attivazione e la gestione dei dispositivi crittografici della CA e del TSS.

Ogni assegnatario di un dispositivo crittografico deve applicare la dovuta diligenza nella conservazione dei codici di attivazione

7.5 Controlli di sicurezza sulle macchine

7.5.1 Requisiti specifici di sicurezza

Oltre alla separazione dei ruoli (6.2), tutte le attività svolte sono oggetto di log (di sistema e applicativi).

7.5.2 Classificazione di sicurezza

I componenti della CA di INTESA sono conformi con i requisiti di verifica secondo i criteri di sicurezza richiesti dalla normativa vigente.

7.6 Controlli di sicurezza della rete

La rete INTESA è protetta da Firewall e IDS (Intrusion Detection System).

La rete PKI INTESA è una rete dedicata, protetta da un apposito Firewall, interna alla rete INTESA.

Le macchine dedicate alla PKI sono oggetto di hardening e permettono solo le funzioni necessarie.

Le comunicazioni tra le macchine del sito INTESA PKI, del sito di backup e delle LRA sono protette e avvengono attraverso porte di comunicazione espressamente autorizzate.

7.7 Sincronismo con l'ora campione

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata mediante il protocollo *NTP* (*Network Time Protocol*). 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, a loro volta, sono sincronizzati alla 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.

I riferimenti temporali apposti dalle applicazioni sono stringhe in formato data (DD/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 (Art.41 del DPCM).

7.7.1 Controllo del sincronismo con l'ora campione

I server dedicati ai servizi di marcatura temporale hanno inoltre un controllo software tra l'orario della macchina e un cospicuo numero di server NTP distribuiti a livello planetario: l'utilità di controllo, installata su ognuno dei server utilizzati dal QTSP INTESA nell'ambito della validazione temporale, periodicamente verifica l'allineamento del clock di sistema questi NTP Server di riferimento Se l'allineamento temporale non risulta conforme alle specifiche tecniche di riferimento tempo per tempo vigenti, il servizio di marcatura temporale erogato dallo specifico server che risultasse disallineato viene arrestato. Alla data, è previsto il blocco del sistema di validazione temporale in caso di superamento di una soglia di tolleranza fissata a 1 (un) minuto secondo (in valore assoluto).

In caso di blocco, una segnalazione è inviata al personale addetto, al fine di verificarne le cause e intervenire di conseguenza.

8 Profilo delle marche temporali e CRL

8.1 TST – Marca temporale

Il formato della Marca temporale è conforme con quanto richiesto dal Regolamento eIDAS e, nello specifico, con la *ETSI-319.422*. L'OID specificato nel campo policy dei TST sarà 0.4.0.2023.1.1.

La marca temporale contiene le informazioni richieste dalla normativa di riferimento (RFC3161, punto 2.4.2) fatto salvo quanto richiesto da *ETSI-319.422*:

- Version
- Policy
- messageImprint
- serialNumber
- genTime
- accuracy
- tsa

8.2 CRL – Certificate Revocation List

Il formato della CRL è conforme alla RFC 2459.

Sono valorizzati i seguenti campi:

- Versione
- Certificatore
- Data effettiva
- Prossimo aggiornamento
- Algoritmo di firma
- Authority key Identifier
- CRL Number

8.2.1 Estensioni delle entry

- Numero di serie del certificato
- Data di revoca
- Causale di revoca (**reasonCode**)

9 Cessazione dell'attività di TSP

Il TSP INTESA ha redatto Piano di Cessazione in conformità all'art.24 paragrafo 2 lettera h) del Regolamento (UE) n. 910 del 23 luglio 2014 (eIDAS).

Copia del Piano di Cessazione è stata inviata all'Agenzia.

9.1.1 Cessazione programmata dei servizi

Nel caso di cessazione programmata dei propri servizi, il TSP INTESA applicherà le seguenti procedure minime:

- Il TSP INTESA informerà tutti i sottoscrittori dei servizi e altre entità con cui ha accordi o relazioni di altro tipo
- Il TSP INTESA cesserà ogni contratto nei confronti di terze parti che agiscono su mandato del TSP stesso e revocherà ogni autorizzazione ad agire per suo conto;
- Il TSP INTESA provvederà alla distruzione delle chiavi private relative ai servizi fiduciari, fatte incluse le copie di backup, in modo che non possano essere recuperate.
- Ove possibile, il TSP INTESA trasferirà ad una terza parte, da definire, gli obblighi di mantenere, per un periodo ragionevole di tempo, informazioni circa l'esistenza dei servizi del TSP (a meno che non sia dimostrabile che il TSP, al momento della cessazione, non abbia più in proprio possesso tali informazioni).

9.1.2 Notifica di cessazione

Con un periodo di preavviso non inferiore ai sei mesi rispetto alla prevista data di cessazione, il TSP darà notifica di tale decisione e delle conseguenze derivanti ai soggetti interessati.

La comunicazione avverrà preferibilmente e ove possibile via PEC; in alternativa via posta elettronica e/o via posta ordinaria (o raccomandata per casi specifici).

I soggetti destinatari della comunicazione saranno:

- Le autorità di vigilanza e supervisione competenti
- I sottoscrittori dei servizi
- I titolari dei certificati, se differenti dal sottoscrittore del servizio
- Il Terzo Ineressato
- Le Terze parti coinvolte nei processi, quali
  - le Local RA esterne
  - i fornitori di servizi / prodotti
  - i fornitori dei servizi logistici (server farm)
- Eventuali altri TSP con cui sussistono rapporti di collaborazione

Analoga comunicazione sarà resa disponibile sul sito del TSP INTESA - *www.intesa.it*.

I titolari dei certificati saranno anche avvisati della prevista revoca del certificato di sottoscrizione.

Fine del documento