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

Manuale Operativo per il Servizio Fiduciario Qualificato di Validazione temporale elettronica

Codice documento: INTQS-TSA_MO

OID: 1.3.76.21.10.100.2

Redazione: Antonio Raia

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

Data emissione: 30/12/2021

Versione: 03

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

Questa pagina è intenzionalmente priva di contenuto.

Revisioni

Versione n°: 03		***Data Revisione: 30 dicembre 2021***
Descrizione modifiche:	Aggiornamento riferimenti normativi (*B.1*) Aggiornamento riferimenti QTSP Aggiornamento par. *N.1.1* Aggiornamento dati societari e logo	
Motivazioni:	Modifica riferimenti telefonici helpdesk e fax Puntualizzazione sul controllo del sincronismo dei TSS Aggiornamenti e correzione refusi Variazione proprietà, direzione e coordinamento della società	
Versione n°: 02		***Data Revisione: 29 gennaio 2019***
Descrizione modifiche:	Aggiornamento riferimenti normativi (*B.1*) Variazione indirizzo di posta elettronica (*A.3*) Aggiornamento paragrafo dei massimali assicurativi (*E.2*) Riferimenti URL al punto *A.2* e *N.2.1* Formattazione documento	
Motivazioni:	Aggiornamenti	
Versione n°: 01		***Data Revisione: 2 gennaio 2017***
Descrizione modifiche:	Nessuna	
Motivazioni:	Prima emissione	

Sommario

Revisioni **3**
Sommario **4**
A. Introduzione **6**
A.1. Proprietà intellettuale 6
A.2. Dati identificativi della versione del Manuale Operativo 6
A.3. Dati identificativi del Prestatore di Servizi Fiduciari 6
A.4. Responsabilità del Manuale Operativo 6
B. Riferimenti e definizioni **7**
B.1. Riferimenti normativi 7
B.2. Definizioni & Acronimi 7
C. Generalità **8**
C.1. Manuale Operativo (MO) 8
C.2. Entità coinvolte nei processi 8
C.2.1. Certification Authority (CA/TSCA) 8
C.2.2. Registration Authority (Ufficio RA) 9
C.2.3. Utente / Richiedente 9
C.2.4. Utilizzatore 9
D. Obblighi **9**
D.1. Obblighi del Prestatore di Servizi Fiduciari 9
D.2. Obblighi dell'Utente / Richiedente 9
D.3. Obblighi degli utilizzatori delle marche temporali 10
E. Responsabilità e limitazioni agli indennizzi **10**
E.1. Responsabilità del Prestatore di Servizi Fiduciari 10
E.2. Assicurazione 10
E.3. Limitazioni agli indennizzi 10
F. Tariffe **11**
G. Infrastruttura del servizio di Validazione Temporale **11**
H. Modalità di generazione delle chiavi **11**
H.1. Generazione delle chiavi di certificazione (TSCA) 11
H.2. Generazione delle chiavi del sistema di validazione temporale (TSU) 12
I. Modalità di emissione dei certificati **12**
I.1. Procedura di emissione dei Certificati di certificazione (TSCA) 12
I.2. Procedura di emissione dei Certificati di validazione temporale (TSU) 12
J. Modalità di revoca e sospensione dei certificati **12**
J.1.1. Revoca dei certificati 12
J.1.2. Revoca dei certificati relativi alle Chiavi di certificazione 12
J.1.3. Revoca dei certificati relativi alle Chiavi di validazione temporale 12
K. Modalità di sostituzione delle chiavi **13**
K.1. Sostituzione delle chiavi di Certificazione (TSCA) 13
K.1.1. Sostituzione pianificata delle Chiavi di certificazione 13
K.1.2. Sostituzione in emergenza delle Chiavi di certificazione 13
K.2. Sostituzione delle Chiavi di validazione temporale 13
K.2.1. Sostituzione pianificata delle Chiavi di validazione temporale 13
K.2.2. Sostituzione in emergenza delle chiavi del sistema di validazione temporale 13
L. Modalità di protezione della riservatezza **13**
M. Conservazione delle validazioni temporali **13**
N. Procedure per la validazione temporale **13**
N.1. Servizio di validazione temporale 13
N.1.1. Controllo del sincronismo con l'ora campione 14
N.1.2. TST – Marca temporale 14
N.2. Modalità di richiesta e verifica marche temporali 14

N.2.1. Verifica delle validazioni temporali 15
N.2.2. Piattaforma proprietaria DeSigner 15
N.2.3. Software di firma e verifica – DigitalSign 16
N.2.4. Software di firma e verifica – firma4ng 17
N.3. Formato dei documenti 17
O. Procedura di gestione degli eventi catastrofici 17

A. Introduzione

Il presente documento ha come obiettivo la descrizione delle procedure e relative regole messe in atto da In.Te.S.A. S.p.A. per la distribuzione del *Servizio Fiduciario Qualificato di Validazione Temporale.*

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

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di *Prestatore di Servizi Fiduciari Qualificati* (*QTSP – Qualified Trust Service Provider*) è coperto dai diritti sulla proprietà intellettuale.

A.2. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la revisione n.***03*** del *Manuale Operativo per il Servizio Fiduciario Qualificato di Validazione Temporale del Prestatore di Servizi Fiduciari In.Te.S.A. S.p.A.*, rilasciata il 30/12/2021, conforme al Regolamento (UE) 910/2014 (eIDAS).

L'object identifier di questo documento è ***1.3.76.21.1.100.2***.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica all'url della pagina internet *www.intesa.it/e-trustcom*, nonché sul sito di AgID - Agenzia per l'Italia Digitale (*www.agid.gov.it*).

La pubblicazione di versioni aggiornate del presente Manuale Operativo avverrà sul sito di In.Te.S.A. S.p.A. solo successivamente al loro inoltro all'Agenzia.

A.3. Dati identificativi del Prestatore di Servizi Fiduciari

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

A.4. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo è del Prestatore di servizi fiduciari In.Te.S.A. S.p.A., che ne cura la stesura, la pubblicazione e l'aggiornamento.

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

B. Riferimenti e definizioni

Nel presente capitolo sono descritti i Riferimenti normativi e tecnici e le definizioni dei termini correntemente utilizzati con i relativi acronimi.

B.1. Riferimenti normativi

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* - e successive modificazioni e integrazioni.
CAD	Decreto Legislativo 7 Marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale*" - e successive modificazioni e integrazioni.
GDPR	*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)* - e successive modificazioni e integrazioni.
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 - e successive modificazioni e integrazioni.
DPCM	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 - *"Regole tecniche in materia di generazione, apposizione e 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, ndr) - e successive modificazioni e integrazioni.
DETERMINAZIONE (LLGG)	*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	Recommandation ITU-R TF.460-6, *Annex 1 – Time Scales*.
RFC5905	Network Time Protocol (Protocollo NTP)

B.2. Definizioni & 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* Nel seguito anche solo *Agenzia*.
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*) Persona fisica o giuridica che presta uno o più 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.
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
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.
Richiedente	Ai fini del presente Manuale Operativo, è chi richiede al TSP l'emissione di una marca temporale.
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.

C. Generalità

C.1. Manuale Operativo (MO)

Questo documento descrive le regole e le procedure operative del *servizio fiduciario qualificato di validazione temporale* fornito dal 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*.

Quanto descritto in questo documento si applica al TSP INTESA, cioè alle sue infrastrutture logistiche e tecniche, al suo personale, agli utenti del Servizio e a quanti utilizzino le marche temporali emesse da INTESA.

C.2. Entità coinvolte nei processi

All'interno della struttura del TSP INTESA sono identificate delle entità che prendono parte ai processi oggetto del presente MO. 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.

C.2.1. 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.

C.2.2. 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

C.2.3. Utente / 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.

C.2.4. Utilizzatore

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

D. Obblighi

D.1. Obblighi del Prestatore di Servizi Fiduciari

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dalla normativa vigente (cfr. ***B.1***).

Tra tali obblighi, INTESA, in qualità di TSP:

- 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;
- si attiene alle misure di sicurezza per il trattamento dei dati personali;
- procede alla pubblicazione della revoca / sospensione dei certificati elettronici (rif.), assicurando la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- fornisce le informazioni utili ai soggetti che richiedono il servizio di validazione temporale (e.g. termini e condizioni relative all'utilizzo del servizio, le procedure di reclamo e di risoluzione delle controversie, etc.);
- fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle validazioni temporali;
- mantiene copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione e la rende accessibile per via telematica (DPCM, Art.42, comma 3).

D.2. Obblighi dell'Utente / Richiedente

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

Al Richiedente / Utente del servizio è richiesto inoltre di:

- fornire tutte le informazioni richieste dal TSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta per l'emissione della marca temporale secondo le modalità indicate in questo Manuale Operativo;
- comunicare al TSP eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici o di posta elettronica, ecc.;

- conservare le informazioni di abilitazione all'utilizzo del servizio con la massima diligenza;

D.3. Obblighi degli utilizzatori delle marche temporali

Coloro che utilizzino messaggi elettronici e/o evidenze informatiche validati temporalmente, sono tenuti a:

- verificare l'assenza del certificato di TSA dalle Liste di Revoca (CRL) 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;

E. Responsabilità e limitazioni agli indennizzi

E.1. Responsabilità del Prestatore di Servizi Fiduciari

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

INTESA, fatti salvi i casi di colpa o dolo (*eIDAS, Art.13*), non assume alcuna responsabilità per le conseguenze derivanti da un uso del servizio di Validazione temporale differente da quanto disposto dal DPCM, e in particolare, dal mancato rispetto da parte dell'Utente e degli Utilizzatori delle marche temporali di quanto indicato nel presente Manuale Operativo e, più in generale, dalla mancata osservanza da parte degli stessi della normativa vigente.

Si ricorda pertanto di conservare con speciale diligenza le credenziali di accesso al sistema di Validazione temporale. Si raccomanda altresì di conservare sempre con la massima cura le informazioni di abilitazione all'uso dei dispositivi di firma.

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* e nel Reg. eIDAS, *Art.13 Responsabilità e onere della prova*.

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 e validazione temporale.

E.2. Assicurazione

INTESA è beneficiaria di contratti assicurativi per la copertura dei rischi derivanti dall'esercizio delle proprie attività e dei danni causati a terzi. Il contenuto di tali contratti è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è resa disponibile all'Agenzia apposita dichiarazione di stipula.

E.3. Limitazioni agli indennizzi

Il TSP INTESA è responsabile di danni causati, per colpa o dolo, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al regolamento eIDAS e alla normativa vigente, fatti salvi i casi in cui i danni siano causati da un utilizzo, da parte dei sottoscrittori, che ecceda i limiti indicati su *CPS*, *Manuale Operativo* e *Contratto di servizio*.

INTESA non si ritiene responsabile dei danni causati agli utenti e utilizzatori o a terzi conseguenti al non rispetto, da parte del sottoscrittore, delle regole definite in *CPS*, *Manuale Operativo* e *Contratto di servizio*.

INTESA non si ritiene responsabile dei danni causati agli utenti e utilizzatori o a terzi conseguenti ad un uso improprio del sistema di validazione temporale da parte di applicazioni di terze parti.

L'utente, 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 TSP INTESA.

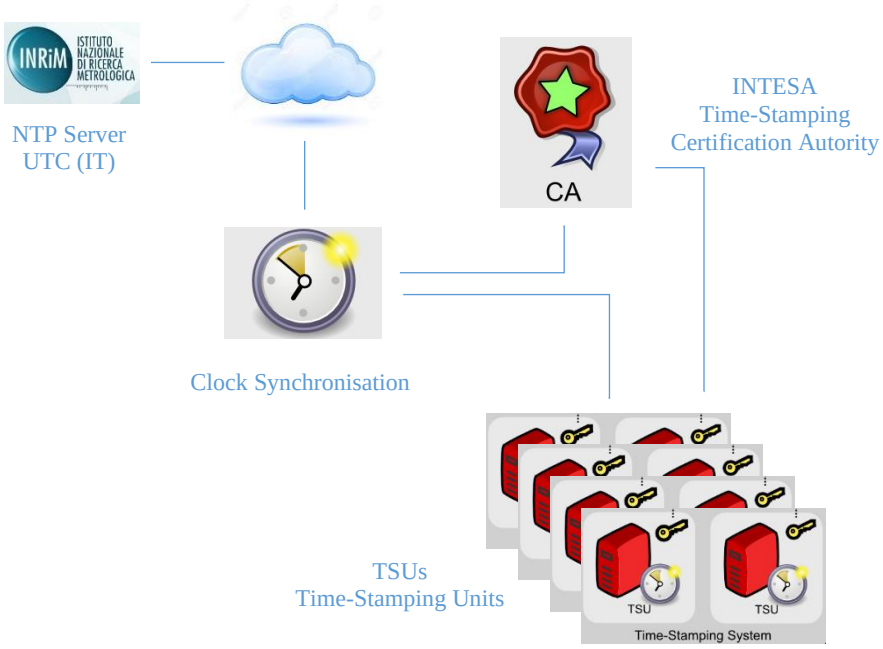
F. Tariffe

Le tariffe per l'utilizzo del Sistema di Validazione temporale sono in funzione delle quantità trattate e soggette all'andamento del mercato.

Offerte dedicate possono essere richieste contattando il TSP INTESA agli indirizzi riportati in *A.3* o al proprio referente commerciale.

G. Infrastruttura del servizio di Validazione Temporale

L'infrastruttura del servizio può essere schematizzata, nei suoi elementi essenziali, come segue:



La TSA INTESA si avvale di una CA root dedicata (nel seguito anche solo TSCA), le cui chiavi sottoscrivono i *Certificati di validazione temporale* (o di *marcatura temporale*), le cui corrispondenti chiavi private (*Chiavi di validazione temporale* o di *marcatura temporale*) sono utilizzate dalle TSU per sottoscrivere le marche temporali.

I *Certificati di validazione temporale* emessi dalla TSCA identificano univocamente la specifica TSU, per cui è possibile, data la singola marca temporale, risalire alla TSU emittente.

Data e ora certa sono garantite dalla sincronizzazione con l'ora campione fornita da un cospicuo numero di server NTP distribuiti a livello planetario (par. *N.1*).

Nei successivi paragrafi sono descritte le politiche di generazione delle chiavi e della gestione dei relativi certificati dell'infrastruttura di TSA del TSP INTESA.

H. Modalità di generazione delle chiavi

H.1. Generazione delle 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 di 2048 bit.

H.2. Generazione delle chiavi del sistema 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 di 2048 bit.

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

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione (TSCA)

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo ***H.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.

L'operazione è svolta in presenza del Responsabile dei servizi di certificazione.

I.2. Procedura di emissione dei Certificati di validazione temporale (TSU)

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo ***H.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.

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

J. Modalità di revoca e sospensione dei certificati

J.1.1. 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 dalla CA, viene aggiornata con periodicità prestabilita (24h) e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

J.1.2. 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.

J.1.3. 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.

K. Modalità di sostituzione delle chiavi

K.1. Sostituzione delle chiavi di Certificazione (TSCA)

K.1.1. Sostituzione pianificata delle Chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, 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, come descritto al paragrafo ***H.1***.

K.1.2. 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. *O*.

K.2. Sostituzione delle Chiavi di validazione temporale

K.2.1. 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.

K.2.2. 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. *O*.

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. Conservazione delle 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).

N. Procedure per la validazione temporale

N.1. Servizio di validazione temporale

Il TSP INTESA offre un servizio qualificato di validazione temporale di documenti elettronici conforme alla normativa vigente.

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 software 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).

N.1.1. 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.

N.1.2. TST – Marca temporale

Il formato della Marca temporale è conforme con quanto richiesto dal Regolamento eIDAS e, nello specifico, con la *ETSI-319.422*.

N.2. Modalità di richiesta e verifica marche temporali

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.

N.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'URL della pagina internet *www.intesa.it/e-trustcom*.

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.

N.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 dei requirement 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.

N.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, descritto al par. *N – Procedure per la validazione temporale*.

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

- Verifica firma: tale funzione è analoga a quella descritta al par. *N.2.1*.
- 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.

N.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.

N.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.

O. 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.

Fine del documento