In.Te.S.A. S.p.A.

Certification Practice Stetement:

Certificati qualificati di firma elettronica

ai sensi del Regolamento (UE) 910/2014 (eIDAS**)**

Codice documento: *INTQS-QC_CPS*
OID: *1.3.76.21.10.100.4*
Redazione: *Antonio Raia*
Approvazione: *Franco Tafini*
Data emissione: *13/03/2017*
Revisione: *01*

Questa pagina è intenzionalmente priva di contenuto.

Revisioni

Revisione n°: 01	**Data Revisione:**	**13 marzo 2017**
Descrizione modifiche:	Nessuna	
Motivazioni:	Prima emissione	

Sommario

1 Introduzione

Questo documento descrive le regole e le procedure operative del TSP INTESA per l'emissione dei certificati qualificati di firma elettronica, come definiti nel Regolamento (UE) 910/2014 (eIDAS).

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 e a quanti utilizzino tali certificati 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-QC_CPS*
Policy di riferimento	ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 411-3
Certificate Policy	0.4.0.194112.1.2 0.4.0.2042.1.2
OID In.Te.S.A. S.p.A.	1.3.76.21
servizi qualificati eIDAS	1.3.76.21.10
presente documento	*1.3.76.21.10.100.4*

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*
N. di fax	+39.011.19216.375
Indirizzo di posta elettronica	*marketing@intesa.it*
Indirizzo (URL) registro dei certificati	*ldap://x500.e-trustcom.intesa.it*
ISO Object Identifier (OID)	1.3.76.21.1

1.2.2 Contatti

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

posta elettronica:	*e-trustcom@intesa.it*
Telefono:	+39.011.19216.111
N. di fax	+39.011.19216.375
HelpDesk - per le chiamate dall'Italia	800.80.50.93
HelpDesk - per le chiamate dall'estero	+39 02.871.193.396

1.3 Riferimenti di 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.
CAD	Decreto Legislativo 7 Marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale"*; modificato dal D.Lgs 179/2016 (cfr.).
D.Lgs 179/2016	DECRETO LEGISLATIVO 26 agosto 2016, n. 179 - "*Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche*".
DLGS 196/03	Decreto Legislativo n.196 del 30 giugno 2003 - "*Codice in materia di protezione dei dati personali"*.
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.
DETERMINAZIONE DIGITPA, n.69/2010	Determinazione commissariale DigitPA 28/07/2010, n.69 – "*Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante Regole per il riconoscimento e la verifica del documento informatico…<<omissis>>"*.
DPCM	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 - *"Regole tecniche in materia di generazione, apposizionee 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).
ETSI-319.401	ETSI EN 319 401 v2.1.1 - *Electronic Signatures and Infrastructures (ESI);General Policy Requirements for Trust Service Providers*
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;* *Part 1: General requirements*
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;* *Part 2: Requirements for trust service providers issuing EU qualified certificates*
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates;* *Part 3: Policy requirements for Certification Authorities issuing public key certificates*
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 1: Overview and common data structures*
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 2: Certificate profile for certificates issued to natural persons*
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 5: QCStatements*
Rec ITU-R	Recommantadione ITU-R TF.460-6, *Annex 1 – Time Scales*.
RFC5905	Network Time Protocol (Protocollo NTP)
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	Recommantadione 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 vigilanza. Nel seguito anche solo *Agenzia*.
TSP	Trust service provider – Prestatore di servizi fiduciari (già *Certificatore*) Persona fisica o giuridica che presta uno o piu servizi fiduciari.
Certificatore Accreditato	TSP presente nell'elenco pubblico dei Certificatori Accreditati tenuto da AgID. (nelle more del Regolamento (UE) N. 910/2014).
CP	Certificate Policy - Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
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 Eng: 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

2.1 Procedura per la modifica

Ogni proposta di modifica al presente CPS sarà notificata all'Agenzia.

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

2.1.1 Modifiche senza preavviso

Senza preavviso possono essere apportate solamente modifiche di carattere editoriale, tipografiche, correzione di errori o variazioni dei contatti.

2.1.2 Modifiche con preavviso

Fatta eccezione per le modifiche di cui al punto precedente:

- ogni parte del presente documento può essere modificata con un preavviso di 90 giorni
- parti non considerate riguardanti l'infrastruttura PKI possono essere modificate con un preavviso di 30 giorni

2.2 Meccanismo di notifica dei cambiamenti

Ogni proposta di modifica al presente CPS sarà notificata all'Organismo di Vilgianza.

Una volta ottenuto parere positivo dall'Agenzia, la notifica di modifica sarà resa pubblica ai sottoscrittori all'URL specificato al paragrafo *1.2.1*.

Commenti alle modifiche proposte devono essere inviate:

- entro 45 giorni per le notifiche di modifica con preavviso di 90 giorni
- entro 15 giorni per le notifiche di modifica con preavviso 30 giorni

I commenti saranno presi in considerazione a discrezione del TSP.

I sottoscrittori che non intendono accettare le proposte di modifica possono chiedere la rescissione del servizio: il nuovo CPS sarà considerato accettato dai sottoscrittori fino al ricevimento di tale richiesta.

2.3 Procedura di approvazione del CPS

Il documento CPS è approvato dal *Responsabile della Sicurezza*, dopo formale approvazione dei manager coinvolti nelle attività inerenti la PKI.

Il documento modificato è quindi inviato per approvazione all'Organismo di viglianza.

Le modifiche apportate al presente CPS potranno essere adottate solo in seguito alla pubblicazione del medesimo sul sito internet dell'Agenzia.

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 e del Titolare del Certificato

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

Il Titolare è tenuto ad ottemperare agli obblighi previsti nel presente documento (par. *5.3.4.1*).

3.4 Obblighi degli utilizzatori dei certificati e delle validazioni temporali

Coloro che utilizzino documenti elettronici, anche validati temporalmente, sono tenuti a ottemperare agli obblighi previsti nel presente documento (par. *5.3.4.3*).

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 (par. *5.3.4.2*).

4 Profili dei Certificati e Certificate Policy

4.1 CA - Certification Authority

I Certificati root del TSP INTESA dedicati al servizio fiduciario qualificato di generazione dei certificati qualificati per la firma elettronica hanno i seguenti OID:

- 1.3.76.21.1.3.1
- 1.3.76.21.1.5.1

4.1.1 Dati contenuti nei certificati root

I Certificati di root e i dati contenuti sono strutturati come disposto dalla Deliberazione e conformi al Regolamento eIDAS.

4.1.1.1 1.3.76.21.1.3.1

field	value
Version	v3
Serial Number	4b b1 eb 5b
Signature	sha1WithRSAEncryption
Hash	Sha1
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Validity (20 yrs)	martedì 30 marzo 2010 13:45:24 domenica 30 marzo 2025 14:15:24
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	1d 75 8b d9 cf 85 83 82 f3 26 b7 56 77 8a ce 50 db 2c cb 3d
Authority KeyIdentifier	1d 75 8b d9 cf 85 83 82 f3 26 b7 56 77 8a ce 50 db 2c cb 3d
Certificate Policies	Policy: 1.3.76.21.1.3.1 CPS: *http://e-trustcom.intesa.it*

CRL Distribution Points	Full Name: URI:*http://e-trustcom.intesa.it/CRL/INTESA_CA.crl*
Basic Constraint	CA:TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)

4.1.1.2 1.3.76.21.1.5.1

field	value
Version	v3
Serial Number	27 7d 09 de 55 2f 88 07
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. CA - Certification Authority**
Validity (20 yrs)	venerdì 9 gennaio 2015 14:48:32 mercoledì 9 gennaio 2030 14:48:32
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. CA - Certification Authority**
Public Key	rsaEncryption (2048)
Subject KeyIdentifier	b0 e0 26 b6 2b 34 1c 74 78 71 ca 05 90 96 c1 d0 2c 05 8c 44
Authority KeyIdentifier	b0 e0 26 b6 2b 34 1c 74 78 71 ca 05 90 96 c1 d0 2c 05 8c 44
Certificate Policies	Policy: 1.3.76.21.1.5.1 CPS: *http://e-trustcom.intesa.it*
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/INTESA_eCA.crl*
Basic Constraint	CA:TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)

4.2 Certificato qualificato rilasciato a persona fisica

I certificati qualificati emessi dalle CA di cui al par. *4.1*, avranno il seguente Policy OID:

- **0.4.0.194112.1.2**

4.2.1 Dati contenuti nel certificato qualificato

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
Hash	sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=<<ca emittente>>**
Validity	Definito contrattualmente

Subject DN	*ETSI-319.412-2* *DELIBERAZIONE*
Public Key	rsaEncryption (2048)
Key Usage	Non Repudiation
Basic Constraint	CA:FALSE
Authority KeyIdentifier	AKI della CA emitente
Authority Information Access	CA Issuers - URI:http://e-trustcom.intesa.it/CERTS/<<*nomeCAcert*>>.cer OCSP - URI:http://e-trustcom.intesa.it/ocsp
qcStatements	1. Questo è un Certificato Qualificato conforme agli Annex I, III or IV del Regolamento EU 910/20142. 2. Questo certificato riporta un periodo di "retention" da parte della CA pari a 20 anni. 3. La chiave pubblica certificata risiede in un Dispositivo Sicuro per la Creazione di Firme (QSCD) 4. Attestazione conformità: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.2 CPS: *http://e-trustcom.intesa.it/INTQS-QC_CPS.pdf* - eventuale limite d'utilizzo Policy: 0.4.0.2042.1.2
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specifico per il certificato

4.3 Entità coinvolte nei processi

4.3.1 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.

4.3.1.1 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.

4.3.1.2 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:

- Identificazione dei titolari.
- Registrazione dei titolari.
- Inizializzazione dei dispositivi individuali di firma.
- Distribuzione dei dispositivi individuali di firma.
- Gestione dell'inventario dei dispositivi individuali di firma.
- Supporto al titolare

L'Ufficio RA, all'interno di specifici accordi, ha inoltre l'incarico d'istruire il personale di entità esterne per la costituzione di Local Registration Authority (LRA).

4.3.2 Altre entità

4.3.2.1 Titolare del certificato qualificato

Persona fisica cui è attribuita la firma elettronica e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.

4.3.2.2 Terzo interessato

Il Terzo Interessato è la persona fisica o giuridica (impresa, associazione di categoria, ente, ecc.) che richiede o autorizza l'emissione del certificato qualificato. Ha facoltà di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato.

4.3.2.3 Utilizzatore

L'Utilizzatore è colui che, verificando il documento elettronico, utilizza i certificati (e le eventuali marche temporali) emesse dal TSP INTESA.

4.3.2.4 LRA – Local Registration Authority

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

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

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

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

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

5 Modalità Operative

Ulteriori aspetti operativi sono reperibili sui Manuali Operativi del TSP INTESA, il quale è tenuto, dalla normativa italiana, a pubblicare un Manuale Operativo che descriva le procedure e le relative regole utilizzate dal TSP per l'emissione dei Certificati Qualificati, la generazione e la verifica della firma elettronica qualificata e la validazione temporale.

5.1 Pubblicazione dei Certificati

Il TSP utilizza un registro dei certificati "LDAP", dove pubblica:

- I certificati delle chiavi di certificazione.
- I certificati delle chiavi di sottoscrizione del sistema di validazione temporale.
- I Certificati per le chiavi di firma dell'Agenzia.
- Le liste di revoca e sospensione.
- I certificati di sottoscrizione dei Titolari (dietro consenso)

Il TSP mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno, la quale aggiorna in tempo reale le copie operative, accessibili da parte degli utenti con protocollo LDAP all'indirizzo: *ldap://x500.e-trustcom.intesa.it*.

Inoltre, all'interno del certificato qualificato è indicato il luogo in cui è disponibile gratuitamente il certificato della CA che ha sottoscritto il certificato stesso (CA Issuers - URI: *http://e-trustcom.intesa.it/CERTS*).

5.2 Identificazione e registrazione degli utenti

5.2.1 Registrazione iniziale

5.2.1.1 Dati contenuti nel Certificato – Campo Subject DN

I dati del Titolare saranno contenuti nel Certificato, nel campo subject, strutturati in conformità al Reg. eIDAS e alla DELIBERAZIONE.

ATTRIBUTO	OID
countryName	2.5.4.6
OrganizationName	2.5.4.10
localityName	2.5.4.7
organizationalUnitName	2.5.4.11
givenName	2.5.4.42
surname	2.5.4.4
commonName	2.5.4.3
pseudonym	2.5.4.65
title	2.5.4.12
serialNumber	2.5.4.5
dnQualifier	2.5.4.46

5.2.1.2 Identificativo univoco

Al titolare è assegnato un identificativo univoco presso il Certificatore.

5.2.1.3 Titoli e Abilitazioni professionali

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a dimostrazione dell'effettiva sussistenza di tali abilitazioni professionali o documentazione equivalente (es. autocertificazione), così come indicato nella Deliberazione CNIPA n.45. Una copia di tale documentazione viene conservata dal TSP.

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

5.2.1.4 Poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di poteri di rappresentanza (es. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un Cliente, etc.), il

richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza di tali poteri di rappresentanza.

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

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

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

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

5.2.1.5 Limitazioni d'uso

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

5.2.1.6 Uso di pseudonimi

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

5.2.2 Identificazione certa iniziale del richiedente il certificato

Il TSP verifica con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

L'attività di identificazione del richiedente viene effettuata da:

- Il Certificatore, tramite le persone del proprio Ufficio RA;
- LRA esterne: ad esempio il personale dell'Azienda o dell'Ente Cliente oppure di terze parti appositamente autorizzate dal Certificatore;

La persona che fa richiesta della certificazione viene identificata con certezza e viene archiviata da INTESA (o dalla LRA incaricata) la fotocopia di almeno un documento ufficiale per lo Stato di appartenenza.

5.2.3 Identificazione per riemissione del certificato

Fatta salva ogni verifica completa e approfondita sulla richiesta di riemissione, la verifica *de visu* del Titolare non è richiesta in caso di soggetto già precedentemente riconosciuto da TSP o da altro ente incaricato.

5.2.4 Identificazione per richiesta di revoca o sospensione

La richiesta di Revoca o sospensione di un Certificato di sottoscrizione può essere avanzata da:

- TSP INTESA
- Titolare
- Terzo Interessato

La revoca / sospensione dei certificati viene asseverata dal loro inserimento nella lista di revoca CRL.

Il profilo delle CRL 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.

Le informazioni di revoca e sospensione sono anche disponibili attraverso il protocollo OCSP.

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato, il TSP notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

La revoca / sospensione è effettuata al massimo entro 24h dal ricevimento della richiesta.

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

- sostituzione del certificato senza compromissione della chiave privata (CRLReason: Superceded);
- compromissione (ovvero la perdita delle caratteristiche di sicurezza e univocità) della chiave privata del Titolare (*CRLReason: Key Compromise*);
- i dati del certificato sono modificati o obsoleti; in questo caso ricade anche l'eventualità che un Titolare non accetti i certificati emessi a suo nome in quanto i dati sono errati (*CRLReason: Affiliation Changed*);
- cessazione repentina, in condizioni di conflittualità o non, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati (*CRLReason: Cessation of Operation*);
- cessazione preventivata dalle mansioni per le quali sono stati rilasciati i certificati al Titolare (*CRLReason: Cessation of Operation*);
- mancato rispetto da parte del Titolare degli obblighi specificati nel Manuale Operativo, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata (*CRLReason: Unspecified*);
- altri casi aventi carattere d'urgenza a giudizio del Terzo Interessato (*CRLReason*: *Unspecified*);
- altri casi non urgenti (*CRLReason*: *Unspecified*).

In fase di richiesta, dovranno essere specificate la data e l'ora a partire dalla quale il certificato dovrà risultare revocato o sospeso e l'eventuale periodo di sospensione.

5.2.4.1 Revoca su iniziativa del Certificatore

Il TSP INTESA può revocare i certificati dei Titolari nei casi indicati al paragrafo precedente.

In ogni caso informerà dell'avvenuta revoca i Titolari interessati tramite posta elettronica, altrimenti tramite posta ordinaria.

5.2.4.2 Revoca su richiesta del Titolare

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

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

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

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

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

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

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

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

5.2.4.3 Revoca su richiesta del Terzo Interessato

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

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

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

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

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

La richiesta dovrà indicare chiaramente:

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

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

5.2.4.4 Sospensione di certificato

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba essere revocato o no (ad esempio nei casi in cui si tema la compromissione della chiave privata o lo smarrimento/furto del dispositivo di firma, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

Per una sospensione il codice di CRLReason è *certificateHold* e ha come conseguenza l'emissione immediata della lista aggiornata di sospensione/revoca.

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per la Richiesta di Revoca.

5.2.4.5 Durata del periodo di sospensione

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

In assenza di comunicazioni, il certificato verrà automaticamente revocato dopo il periodo di sospensione, non superiore ai 90giorni, indicato dal Titolare nella richiesta, con la *CRLReason* indicata al momento della richiesta stessa.

5.3 Ciclo di vita dei certificati

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

Entro la data di scadenza del certificato, al Titolare del dispositivo di firma sarà spedito, ove possibile per posta elettronica altrimenti per posta ordinaria, un avviso di prossima scadenza.

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

5.3.1 Richiesta di certificazione

Completata positivamente la fase di identificazione e registrazione, è possibile procedere alla generazione delle chiavi di sottoscrizione generate dal Certificatore.

Le chiavi di sottoscrizione sono generate su dispositivi di firma che rispondono ai requisiti previsti dall'Annex II del Reg. eIDAS (QSCD – Qualified Signature Creation Device).

5.3.1.1 Richiedente generico

Il Titolare sottoscrive:

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

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

La documentazione precedentemente descritta, relativa alla registrazione dei Titolari, viene conservata da INTESA (ovvero dalla LRA incaricata) per 20 (venti) anni dalla scadenza del certificato.

5.3.1.2 Contratto di servizio tra INTESA ed Ente/Azienda cliente

Nel caso in cui il cliente sia un Ente o un'Azienda, i cui dati identificativi saranno definiti a contratto, si applicano anche le norme seguenti, fermo restando quanto specificato al paragrafo 5.2 per l'identificazione e la registrazione dei singoli Titolari.

- Le persone delegate a indicare il personale del Cliente abilitato ad essere certificato da INTESA faranno pervenire al Certificatore gli elenchi delle persone alle quali INTESA sarà autorizzata a

rilasciare i certificati qualificati. In tali elenchi sarà possibile anche indicare eventuali limitazioni all'uso delle coppie di chiavi, poteri di rappresentanza o abilitazioni professionali.

- Questi elenchi saranno resi disponibili agli addetti interessati: il personale dell'Ufficio RA ovvero della LRA.
- Le persone autorizzate esibiranno alle LRA documenti analoghi a quelli indicati al paragrafo precedente (*5.3.1.1*).

La LRA verificherà che la persona sia autorizzata ad essere certificata e opererà come indicato nel paragrafo precedente (*5.3.1.1*), con l'eccezione del primo punto di tale paragrafo.

5.3.2 Emissione del certificato

Dopo la generazione della coppia di chiavi di sottoscrizione, è possibile generare una richiesta di certificazione ad essa relata, nel formato PKCS#10; essa fornisce la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

La CA elabora immediatamente la richiesta ricevuta, accertandosi dell'autenticità della richiesta e che il Titolare sia effettivamente in possesso della chiave privata (verificando conseguentemene il corretto funzionamento della coppia di chiavi).

Il TSP emette il certificato con un sistema conforme con l'Art.33 del DPCM 22/02/2013 e al Reg. eIDAS.

Dietro consenso del Titolare, il certificato così generato è pubblicato sul registro dei certificati.

La generazione del certificato è registrata nel giornale di controllo.

Più in dettaglio, sono effettuate le seguenti operazioni:

- L'operatore si autentica all'applicazione, seleziona i dati di registrazione del Richiedente e attiva la procedura di richiesta di certificato.
- L'applicazione accede al dispositivo di firma con il PIN di default e genera la coppia di chiavi.
- L'applicazione attivata dall'operatore di RA, dopo la generazione delle chiavi, genera la richiesta di certificato.
- La richiesta viene direttamente inoltrata alla CA; essa è firmata elettronicamente dall'operatore e trasmessa su canale sicuro.
- Il certificato emesso viene ricevuto dall'applicazione e inserito sul dispositivo di firma con le dovute verifiche.
- In caso di Dispositivo di firma individuale, l'applicazione blocca il PIN di accesso al dispositivo di firma. Al Titolare verrà consegnata, separatamente, una busta contenente il PUK del dispositivo per l'attivazione del medesimo.
- In caso di firma remota, saranno consegnate al Titolare le credenziali di accesso

5.3.3 Accettazione del certificato

Il TSP informa preventivamente il cliente circa termini e condizioni per l'utilizzo dei certificati qualificati di firma elettronica.

Il richiedente sottoscrive la presa visione del Manuale Operativo del TSP INTESA, dove sono riportati gli obblighi del Titolare e delle altre entità coinvolte nel processo.

Il Manuale Operativo è disponibile sul sito del TSP all'URL *http://e-trustcom.intesa.it/ca_pubblica/manuale.htm*.

I titolari sono tenuti a verificare la correttezza delle informazioni contenute nel Certificato loro consegnato e segnalare immediatamente eventuali errori al Certificatore.

In tal caso, il titolare deve sottoscrivere una richiesta di Revoca per il Certificato contenente dati errati.

5.3.4 Obblighi del Titolare, Terzo interessato, Utilizzatori

5.3.4.1 Obblighi del Titolare

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal TSP, garantendone l'attendibilità sotto la propria responsabilità;

- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- indicare esplicitamente nella richiesta di certificazione le informazioni che egli desidera non siano inserite nel certificato;
- comunicare al TSP eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici o di Internet, ecc.;
- utilizzare dispositivi di firma conformi all'Annex II del Reg. eIDAS, nel caso in cui non sia il TSP a fornirlo. Le informazioni relative a tale dispositivo dovranno comunque essere comunicate al TSP, in quanto INTESA intende conservare il controllo delle caratteristiche di sicurezza dei dispositivi di firma utilizzati dai Titolari e mantiene la corrispondenza tra certificato qualificato e dispositivo;
- conservare con la massima diligenza la chiave privata o il dispositivo che la contiene al fine di garantirne l'integrità e la massima riservatezza;
- non duplicare la chiave privata né il dispositivo che la contiene;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
- conservare con la massima diligenza i codici segreti, ricevuti dal TSP al fine di garantirne la massima riservatezza;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia;
- utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso nel caso la firma venga apposta per mezzo di una procedura automatica;
- utilizzare esclusivamente il dispositivo fornito dal TSP, ovvero un dispositivo scelto tra quelli indicati dal TSP stesso;
- richiedere immediatamente la revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma difettosi o di cui abbia perduto il possesso. chiave;
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua durata;
- sottoscrivere la richiesta di revoca specificandone la motivazione e la sua decorrenza;
- sporgere denuncia alle Autorità competenti in caso di smarrimento o sottrazione del dispositivo di firma.

5.3.4.2 Obblighi del terzo interessato

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

A titolo esemplificativo si riportano le seguenti circostanze:

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

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

5.3.4.3 Obblighi degli utilizzatori dei certificati

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

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato allo standard ISO 9594-8, e il momento della sua emissione;
- verificare l'assenza del certificato dalle Liste di Revoca e Sospensione (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;

- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del TSP che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

5.3.5 Rinnovo dei certificati di sottoscrizione

Non è previsto il rinnovo del certificato di sottoscrizione. Alla scadenza, sarà generata una nuova coppia di chiavi e sarà emesso un nuovo certificato.

5.3.6 Rinnovo delle chiavi

5.3.6.1 Rinnovo delle chiavi di sottoscrizione

Il periodo di vita delle chiavi di sottoscrizione del Titolare non è inferiore al periodo di validità del certificato relativo.

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

Entro la data di scadenza del certificato, al Titolare del dispositivo di firma sarà spedito, ove possibile per posta elettronica altrimenti per posta ordinaria, un avviso di prossima scadenza.

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

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

E' possibile per cui procedere all'emissione del certificato nelle modalità descritte al paragrafo *5.3.2*.

5.3.6.2 Sostituzione pianificata delle chiavi del Certificatore

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.

L'attività è pianificata in modo da garantire la continuità dei servizi, compatibilmente al fatto che Il termine del periodo di validità di un certificato qualificato deve precedere di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità (DPCM, art.18, comma 3).

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

5.3.7 Certificate modification

Se uno degli attributi del Certificato non è più valido (es. cambio di Cognome, variazione del campo Organization, etc,), il Titolare può chiedere l'emissione di un nuovo Certificato a lui intestato.

5.3.8 Revoca e sospensione del Certificato

Oltre a quanto indicato in *5.2.4*, si fa presente che un certificato in stato Revocato non può essere riportato allo stato Valido, a meno che non sia stato Sospeso (la sospensione è una particolare revoca con crlReason pari a *certificateHold*).

5.3.9 Certificate status services

Conformemente al Reg. eIDAS, il TSP pubblica l'informazione sullo stato del Certificato sia attraverso un servizio OCSP, sia tramite le liste di Revoca e Sospensione (CRL).

Entrambe le informazioni sono raggiungibili 24/7 agli URL indicati all'interno del certificato stesso (cfr. par. *4*).

6 Sicurezza fisica e controlli procedurali

6.1 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 - ruoli

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 e coincide con il *Responsabile dei servizi di certificazione e validazione temporale*.

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 par. *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.

6.4 Procedure di Audit della SicurezzaProcedure di Audit della Sicurezza

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

6.4.1 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.

6.4.2 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.

6.4.3 Conservazione dei LOG

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

6.4.4 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.

6.4.5 Procedure di backup dei Log

I Log sono conservati in triplice copia su tre server dedicati, collocati fisicamente sul sito primario e di DR. A saturazione dello spazio fisico sui server, se ne prevede la storicizzazione su sistema NAS.

6.4.6 Sistema di accumulazione dei Log

L'accumulazione dei Log è interna ai sistemi coinvolti e tramite un'applicazione dedicata al c.d. Giornale di Controllo.

6.4.7 Notifica ai soggetti causa di eventi

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

6.4.8 Verifiche della vulnerabilità

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

6.5 Archivio documentazione

6.5.1 Tipologia di eventi registrati

Come richiesto dal DPCM 22/02/2013, la seguente documentazione e i seguenti eventi sono oggetto di archiviazione.

6.5.1.1 Archivio cartaceo

Comprende tutta la documentazione sottoscritta dal Titolare al momento della richiesta di registrazione e ogni altro documento presentato (es. documentazione atta a dimostrare eventuali poteri di rappresentanza o limitazioni d'uso).

E' parte della documentazione prodotta la copia del documento di identità.

La suddetta documentazione, di base cartacea, sarà in seguito oggetto di archiviazione ottica per un'agevole consultazione del personale autorizzato di INTESA.

6.5.1.2 Documentazione elettronica

Comprende:

- Personalizzazione del dispositivo di firma
- Generazione Certificato
- Revoca Certificato
- Sospensione Certificato
- Accessi del personale nelle aree protette dove sono installati i sistemi i CA
- Inizio e termine del processo della sessione di emissione certificato

- Ogni differenza riscontata tra il registro dei certificati risiedente sul MASTER e le copie operative (SHADOW)
- Le operazioni che riguardano il contenuto del registro dei certificati
- Inizio e termine della mancata o ridotta disponibilità del Registro dei certificati
- Ogni anomalia o tentativo di manomissione al sistema di marcatura temporale
- Marche temporali emesse

Le informazioni di cui ai punti precedenti sono registrate dai relativi programmi applicativi e accessibili dal personale autorizzato.

6.5.1.3 Documentazione che può essere elettronica oppure cartacea

Tutti i documenti relativi alle richieste di sospensione o revoca operate dal Certificatore, dai Titolari o dai Terzi Interessati.

Se la predetta documentazione è cartacea, sarà in seguito oggetto di archiviazione ottica per un'agevole consultazione del personale autorizzato di INTESA.

6.5.1.4 Documenti addizionali

Verbali della generazione delle chiavi di CA e TSS, eventualmente in formato digitale e digitalmente firmati dal personale incaricato.

6.5.2 Periodo di archiviazione

Tutti gli elementi indicati al precedente paragrafo *6.5.1* sono conservati per un periodo di 20 (venti) anni.

6.5.3 Protezione dell'archivio

L'integrità dei dati archiviati è garantita, a seconda della specifica procedura, attraverso la firma digitale.

I dati classificati come confidenziali sono protetti contro la divulgazione non autorizzata.

6.5.4 Procedure di backup degli archivi

6.5.4.1 Archivio cartaceo

Le informazioni contenute sui documenti cartacei sono conservate in modo sicuro sia centralmente che presso I siti di LRA.

6.5.4.2 Archivio elettronico

I dati sono salvati giornalmente. Settimanalmente gli archivi sono consolidati e salvati. Analogamente, l'ultimo sabato di ogni mese è operato il salvataggio mensile.

6.5.5 Requisiti per il riferimento temporale dei record

I record sono oggetto di evidenza temporale, come descritto nel presente documento.

6.5.6 Verifica di integrità

L'integrità dell'archivio della CA INTESA è verificato:

- periodicamente, in occasione degli Audit di sicurezza schedulati;
- ogni volta in cui sia richiesto un audit di sicurezza completo.

6.5.7 Procedure per l'acquisizione e la verifica delle informazioni archiviate

Chiunque può richiedere in qualsiasi momento l'accesso ai propri dati personali e alle informazioni correlate.

Le informazioni riguardanti i sistemi ad accesso controllato possono essere esaminate solo dal personale incaricato e dagli Auditor nominati.

Gli archivi non sono interessati dai fermi per guasto dei sistemi INTESA PKI.

Nel caso INTESA termini la propria operatività, all'ente che le succederà nella gestione della CA sarà affidato l'archivio dati ed esso dovrà garantirne gli stessi criteri di disponibilità.

6.6 Gestione del disaster recovery

6.6.1 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.

6.6.2 Guasto del dispositivo di firma della CA 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 più avanti in *7.1*, al fine di ricreare le chiavi originali.

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

6.6.3 Compromissione delle chiavi di certificazione

Nel caso di compromissione delle chiavi di certificazione, è applicata la procedura di revoca, come descritto in *7.9*. Il TSP INTESA genererà una nuova coppia di chiavi, come riportato in *7.1.1*.

Nel caso di compromissione delle chiavi di marcatura temporale, il relativo certificato sarà revocato e le chiavi saranno ricreate, come descritto in *7.1.2*.

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.

7 Controlli Tecnici di Sicurezza

7.1 Generazione e Installazione delle chiavi

7.1.1 Generazione della coppia di chiavi di certificazione (CA e 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 almeno 2048 bit.

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 di almeno 2048 bit.

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.

Al fine di sostituire le chiavi e il certificato di TSU come previsto dall'art. 49, comma 2, del DPCM, l'operazione è pianificata con una periodicità massima di 3 mesi (cfr. *7.13*).

7.1.3 Generazione della coppia di chiavi di sottoscrizione

Le chiavi di sottoscrizione possono essere generate dal titolare o dal certificatore.

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

Per la fi rma remota, è consentita l'esportazione sicura delle chiavi private.

Per la firma remota, è consentita la replicazione in sicurezza delle chiavi presenti su HSM, al fine di realizzare una configurazione ad alta affidabilità del dispositivo sicuro.

7.1.4 Dimensioni delle chiavi e Algoritmi di firma

L'algoritmo crittografico utilizzato è RSA.

Le chiavi di certificazione (CA e TSCA) hanno lunghezza di almeno 2048bit.

Le chiavi di validazione temporale (TSU) hanno lunghezza di almeno 2048bit

Le chiavi di sottoscrizione hanno lunghezza di almeno 2048bit.

Algoritmo utilizzato: SHA-256.

7.1.5 Utilizzo delle chiavi (keyUsage)

In conformità con la Deliberazione e con il reg. eIDAS, , il campo keyUsage dei certificati è impostato come segue:

- CA - TSCA: keyCertSign + cRLSign
- TSU: digitalSignature
- Sottoscrizione: nonRepudiation

Il certificato TSU 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+)

I dispositivi di firma remota sono certificati ai sensi del Reg. eIDAS (QSCD).

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 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, TSU e Firma remota 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, TSU e Firma remota 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), validazione temporale e firma remota sono utilizzati dispositivi HSM tamperproof dedicati alla generazione e conservazione delle chiavi (CA/TSCA, TSU, sottoscrizione). 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 compromisione della chiave privata, in conseguenza del 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-inizilizzzati 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 certificazone 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. Le chiavi di TSU sono comunque sostituite, senza che il relativo certificato sia revocato, al massimo ogni 90 giorni, al fine di limitare il numero di validazioni temporali emesse per ciascuna coppia di chiavi (cfr. *7.13.1*).

Il periodo standard di validità dei certificati di sottoscrizione è di 24 mesi, salvo differenti accordi con il cliente.

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 di CA/TSCA e di TSU.

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 (par. *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 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).

7.7.1 Controllo del sincronismo con l'ora campione

E' posto in essere un software di controllo che prevede 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.

7.8 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).

7.9 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.

7.9.1 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.

7.9.2 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.

7.9.3 Revoca dei certificati di sottoscrizione

Vedi *5.2.4*.

7.10 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.

7.10.1 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)

7.11 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).

7.12 Modalità di sostituzione delle Chiavi di Certificazione (CA e TSCA)

7.12.1 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 di TSU, 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.

L'attività è pianificata in modo da garantire la continuità dei servizi, compatibilmente al fatto che Il termine del periodo di validità di un certificato qualificato deve precedere di almeno due anni il termine del periodo di validità del certificato delle chiavi di certificazione utilizzato per verificarne l'autenticità (DPCM, art.18, comma 3).

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

7.12.2 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 alla sezione *6.6*.

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

7.13.1 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.

7.13.2 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 alla sezione *6.6*.

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 termporale 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 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.
- Il TSP INTESA si farà carico di conservare le informazioni relative alle attività svolte. Eventualmente, si farà carico di trasferire ad una terza parte, da definire, gli obblighi di mantenere, per un periodo congruo alla normativa vigente, tali informazioni.

9.2 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.

10 Verifica delle Firme e delle Validazioni temporali

10.1 Software di firma e verifica

10.1.1 Software verifica – DigitalSign Reader

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.

10.1.2 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.

10.1.3 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 *10.1.1*.
- 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.

10.1.4 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.

10.2 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.

Questa pagina è intenzionalmente priva di contenuto.

Fine del documento