In.Te.S.A. S.p.A.
Qualified Trust Service Provider
ai sensi del Regolamento (UE) N. 910/2014 (eIDAS)

CPS - Certification Practice Statement
e CP - Certificate Policy
per i Certificati Qualificati
di Firma Elettronica e di Sigillo Elettronico

Codice documento: INTQS-QCSS_CPS

OID: 1.3.76.21.10.100.5

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 23/06/2020

Versione: 02

Intesa
An IBM Company

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

Questa pagina è intenzionalmente priva di contenuto.

Revisioni

Versione n°: 02	***Data Revisione: 23/06/2020***
Descrizione modifiche:	7.1.1: nuovo certificato di root 6.8.8: aggiornamento descrittivo
Motivazioni:	rinnovo chiavi di certificazione puntualizzazione sul controllo del sincronismo dei TSS
Note:	servizi di firma elettronica qualificata
Versione n°: 01	***Data Revisione: 23/04/2020***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio
Note:	integra e sostituisce il documento *CPS per i Certificati qualificati di firma elettronica, ver.01* (cod. documento INTQS-QC_CPS, OID: 1.3.76.21.10.100.4)

Sommario

1 Introduzione

1.1 Generalità

Questo documento costituisce il Practice Statement del Prestatore di Servizi Fiduciari Qualificati (QTSP) In.Te.S.A. S.p.A. e descrive le regole e le procedure operative per l'emissione dei certificati qualificati di firma elettronica e di sigillo elettronico, come definiti nel Regolamento (UE) 910/2014 (eIDAS).

Quanto descritto in questo documento si applica al QTSP 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 elettronica, un sigillo elettronico e/o una validazione temporale elettronica (time-stamping).

Il documento è emesso in conformità allo standard *RFC 3647* e ne segue la struttura ivi descritta.

NOTA: Il presente documento integra e sostituisce il documento *CPS per i Certificati qualificati di firma elettronica, ver.01* (cod. documento *INTQS-QC_CPS*, OID: 1.3.76.21.10.100.4).

1.2 Identificazione del documento

Il presente documento è la versione n. **02**, rilasciata il **23/06/2020** del *CPS - Certification Practice Statement e CP - Certificate Policy per i certificati qualificati di firma elettronica e di sigillo elettronico* del QTSP INTESA (nel seguito, anche solo *CPS*).

Il contenuto di questo documento è conforme a quanto stabilito dalle regole tecniche contenute nel *Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013* (di seguito, *DPCM*), dal *D. lgs. 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione Digitale"* come successivamente modificato e integrato (di seguito, *CAD*) ed è conforme al *Regolamento UE 910/2014* (di seguito, anche solo *Reg. eIDAS*).

Codice documento	*INTQS-QCSS_CPS*
OID	*1.3.76.21.10.100.5*
Policy di riferimento	ETSI EN 319 411-1 ETSI EN 319 411-2 ETSI EN 319 411-3
Certificate Policy *eIDAS*	0.4.0.194112.1.2 0.4.0.194112.1.3
Certificate Policy *INTESA - certificati qualificati*	1.3.76.21.10.2.1.1 1.3.76.21.10.2.1.2
Certificate Policy *agIDCert*	1.3.76.16.6
Certificate Policy *ante eIDAS*	0.4.0.2042.1.2 0.4.0.1456.1.1
OID In.Te.S.A. S.p.A.	1.3.76.21
servizi qualificati eIDAS	1.3.76.21.10
servizi accreditati AgID	*1.3.76.21.1*
presente documento	*1.3.76.21.10.100.5*

1.3 PKI Participants

Il QTSP (*Prestatore di Servizi Fiduciari Qualificati*) è la società ***In.Te.S.A. S.p.A.***, di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289 - 10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**N. Iscrizione 1692/87**
N. di Partita I.V.A.	**05262890014**
N. di telefono (centralino)	**+39.011.19216.111**
HelpDesk - per le chiamate dall'Italia	**800.80.50.93**
HelpDesk - per le chiamate dall'estero	**+39 02.871.193.396**
Sito Internet	***www.intesa.it***
Indirizzo di posta elettronica	***marketing@intesa.it***
Indirizzo (URL) registro dei certificati	***ldap://x500.e-trustcom.intesa.it***
ISO Object Identifier (OID)	**1.3.76.21.1**

All'interno della struttura del QTSP 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 QTSP, espletando, per la parte di propria competenza, le attività a loro attribuite.

1.3.1 CA - Certification Authority

Il QTSP 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, sigilli elettronici* e *validazioni temporali* (cfr. eIDAS, art. 3, comma 16 e 17).

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

- *Responsabile della sicurezza.*
- *Responsabile del servizio di certificazione e validazione temporale.*
- *Responsabile della conduzione tecnica dei sistemi.*
- *Responsabile dei servizi tecnici e logistici.*
- *Responsabile delle verifiche e delle ispezioni (auditing).*

Le figure sopra elencate sono tutte appartenenti all'organizzazione di INTESA

1.3.2 RA - Registration Authority

INTESA ha costituito al suo interno un'entità denominata *Ufficio RA* che ha funzioni di Registration Authority.

In particolare, essa espleta le seguenti attività:

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

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

Il QTSP INTESA può inoltre demandare lo svolgimento di alcune funzioni della propria RA ad entità esterne (par. 1.3.3.4) vedi . Nel Contratto di Mandato, sottoscritto da entrambe le parti, saranno definite le attività in carico alla LRA esterne e riportati gli obblighi delle parti.

La RA INTESA e le LRA sono oggetto di audit e vigilanza da parte del QTSP, al fine di verificare il rispetto della normativa vigente.

1.3.3 Altre entità

1.3.3.1 Titolare del certificato qualificato

Persona fisica o giuridica cui è attribuita la firma elettronica o il sigillo elettronico, che ha accesso ai dispositivi per la creazione della firma elettronica o del sigillo elettronico.

È il soggetto intestatario del certificato.

1.3.3.2 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 l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato.

1.3.3.3 Utilizzatore (Relying Party)

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

1.3.3.4 LRA – Local Registration Authority

Il QTSP 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'Ufficio RA di INTESA ovvero, previo accordo, trattenuta e conservata dalla LRA con le stesse modalità.

Le LRA esterne sono attivate dal QTSP 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 identificazione posta in essere si svolga nel rispetto della normativa vigente;
- impedire ai propri dipendenti la prosecuzione dell'attività di identificazione 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 identificazione in accordo con il GDPR.
- segnalare senza indugio al QTSP INTESA, per tramite dell'Ufficio RA (*uff_ra@intesa.it*) ovvero dei propri riferimenti INTESA, ogni evento o incidente inerente i punti precedenti, nonché tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi o sui dati personali.

1.4 Utilizzo dei certificati qualificati

I certificati qualificati emessi dal QTSP INTESA secondo il presente documento sono utilizzati per la validazione di Firme Elettroniche Qualificate / Firme Digitali e di Sigilli Elettronici Qualificati.

Il QTSP INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, art. 13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto nel presente CPS, nel Manuale Operativo di riferimento e/o dalla mancata osservanza della normativa vigente.

I certificati possono contenere eventuali limiti d'uso, specificati nell'estensione *certificatePolicies* (*OID:2.5.29.32*) del certificato. In tale estensione è specificato se il certificato è utilizzato in una procedura automatica di firma o sigillo.

I certificati qualificati emessi in conformità alle LLGG riportano la codifica, nel campo *certificatePolicies* (OID 2.5.29.32), di un elemento PolicyIdentifier con valore *agIDcert* (OID 1.3.76.16.6).

Tutti i certificati qualificati, emessi dalla CA di INTESA in conformità alle LLGG, riportano solo ed esclusivamente il *Key Usage* corrispondente al "*Type A*" della ETSI 319 412-2i: *keyUsage (OID 2.5.29.15) = nonRepudiation*.

I profili dei certificati sono descritti al par. *7 - Profili dei certificati e CRL - Certificate Policy*.

1.5 Gestione delle specifiche contenute nel CPS

Il documento CPS è interamente gestito all'interno dell'organizzazione del QTSP INTESA, i cui riferimenti sono riportati al par. *1.3*.

Il documento CPS è redatto in collaborazione con i responsabili coinvolti nelle attività inerenti la PKI (par. *1.3.1*) e finalmente approvato dal *Responsabile della Sicurezza* (par. *1.3.1*).

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

1.5.1 Procedura per le revisioni

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

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

Una volta ottenuto parere positivo dall'Agenzia, il documento sarà pubblicato dal QTSP all'URL specificato al par.*1.3*.

Quanto sopra include eventuali modifiche di carattere editoriale o tipografiche.

1.6 Definizioni e Riferimenti

1.6.1 Definizioni e acronimi

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

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP - Qualified Trust Service Provider (già Certificatore Accreditato)	*Prestatore di Servizi Fiduciari Qualificati*. Persona fisica o *giuridica* che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A. Nel presente documento, indicato indifferentemente come *QTSP*, *Certificatore Accreditato* o più semplicemente *Certificatore.*
CAB - Conformity Assessment Body	*Organismo di valutazione della conformità.* Ente accreditato a norma di detto regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati.
EUTSL	*EU Trusted List - Elenco di Fiducia* - Elenco che include le informazioni relative ai prestatori di servizi fiduciari qualificati, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati. Tale elenco è mantenuto e pubblicato dal singolo stato membro (in Italia, a cura di AgID).

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 / QTSP nell'emettere e gestire certificati.
MO	*Manuale Operativo* - Documento redatto in conformità all'art. 40 del *Decreto del Presidente del Consiglio dei Ministri del 22 febbraio 2013* e soggetto ad approvazione dell'Organismo di Vigilanza (AgID).
CRL	*Certificate Revocation List* - Un elenco firmato (dalla CA) che riporta un insieme di certificati non più considerati validi dal Certificatore / QTSP che li ha emessi.
OCSP	*Online Certificate Status Protocol* - servizio di verifica dello stato di validità del certificato, secondo il protocollo OCSP.
HSM	*Hardware Security Module* - Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014 (eIDAS) e, *mutatis mutandi*, per la generazione del sigillo elettronico qualificato. Anche detti *Dispositivi di Firma Remota*.
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 certificati basati su crittografia a chiave pubblica. Per estensione, si includono i sistemi di validazione temporale elettronica qualificata.
CA	*Certification Authority* - Entità della PKI che rilascia i certificati di firma e/o sigillo.
RA *Registration Authority*	Autorità di Registrazione che su incarico del QTSP esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al QTSP. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del QTSP (INTESA S.p.A.).
TSA	*Time-Stamping Authority* - Entità della PKI che rilascia i certificati relativi alle chiavi di validazione temporale.
TSU	*Time-Stamping Unit*- Insieme di HW e SW che emette le validazioni temporali elettroniche. Ogni TSU ha un proprio Certificato di validazione temporale che sottoscrive le marche temporali emesse. Nel presente documento, tali certificati sono chiamati anche *Certificati di TSU.*
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario *per firmare*. La FEQ è creata da un dispositivo per la creazione di una firma elettronica qualificata ed è basata su un certificato qualificato per firme elettroniche. La FEQ coincide, in Italia, con la Firma Digitale definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
SEQ - Sigillo elettronico Qualificato	Dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica utilizzati *per garantire l'origine e l'integrità* di questi ultimi. Il SEQ soddisfa i requisiti sanciti all'art. 36 del Reg. eIDAS ed è creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici.
Validazione temporale elettronica	Informazione elettronica contenente la data e l'ora che viene associata ad un documento informatico, al fine di provare che quest'ultimo esisteva in quel momento. Altrimenti detta *marca temporale* ovvero *time-stamp*.
Certificato Qualificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica ad una *persona fisica*. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'*Allegato I* del Reg. UE 910/2014 (eIDAS).

Certificato Qualificato di sigillo elettronico	Attestato elettronico che collega i dati di convalida di un sigillo elettronico ad una *persona giuridica*. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui *all'Allegato III* del Reg. UE 910/2014 (eIDAS).
CRL	*Certificate Revocation List* - Un elenco firmato (dalla CA) che riporta un insieme di certificati non più considerati validi dal Certificatore / QTSP che li ha emessi.
OCSP	*Online Certificate Status Protocol* - servizio di verifica dello stato di validità del certificato, secondo il protocollo OCSP.
HSM	*Hardware Security Module* - Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014 (eIDAS) e, *mutatis mutandis*, per la creazione del sigillo elettronico qualificato. Anche detti *Dispositivi di Firma Remota*.
Titolare (di Certificato Qualificato)	Persona fisica o giuridica cui è attribuita la firma elettronica o il sigillo elettronico e che ha accesso ai dispositivi per la creazione della firma elettronica. Soggetto intestatario del certificato.
Sottoscrittore o Richiedente	Ai fini del presente documento, è chi richiede al QTSP l'accesso al servizio (persona fisica o giuridica).
Utente	L'utilizzatore del servizio fiduciario.
Utilizzatore (Relying Party)	Chi utilizza il certificato, il sigillo e/o la marca temporale nella fase di verifica del documento elettronico.
Terzo Interessato	Persona fisica o giuridica (impresa, associazione di categoria, ente, ecc.) che richiede o autorizza l'emissione del certificato qualificato.
Cliente	Persona fisica o giuridica che sottoscrive un contratto con il QTSP INTESA.
Giornale di controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il Certificatore, tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza (DPCM 22/02/2013, art. 36).

1.6.2 Riferimenti normativi e tecnici

Regolamento (UE) N. 910/2014 (eIDAS) e ss.mm.ii.	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel presente documento, indicato anche solo come *Reg. eIDAS* (electronic Identification Authentication and Signature).
CAD - DLGS 82/05 e ss.mm.ii.	Decreto Legislativo 7 marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale".* Nel presente documento, indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e ss.mm.ii.	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 - *"Regole tecniche in materia di generazione, apposizione verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4, 28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36,comma 2, e 71"* (del CAD, n.d.r.). Nel presente documento, indicato anche solo come *DPCM*.
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	Decreto Legislativo n.196 del 30 giugno 2003 - "*Codice in materia di protezione dei dati* REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Nel presente documento, indicato anche solo come *GDPR*.
DETERMINAZIONE N. 147/2019 (Linee Guida) e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel presente documento, indicato anche solo come *DETERMINAZIONE* ovvero *LLGG*.
DELIBERAZIONE 45, 21/05/2009	Deliberazione CNIPA 21 maggio 2009, n.45 – "*Regole per il riconoscimento e la verifica del documento informatico"*; abrogata dalla Determinazione 147/2019. Nel presente documento, indicato anche solo come *DELIBERAZIONE*.

Comunicazione AgID 0016101 del 07-06-2016	AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016, avente oggetto "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*".
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-319.412-3	ETSI EN 319 412-2 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 3: Certificate profile for certificates issued to legal persons.*
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles;* *Part 5: QCStatements.*
ETSI-319.421	ETSI EN 319 421 v1.1.1 - *Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps.*
ETSI-319.422	ETSI EN 319 422 v1.1.1 - *Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles.*
Rec ITU-R	Recommendation ITU-R TF.460-6, *Annex 1 – Time Scales*.
RFC5280	*Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile.*
RFC5905	*Network Time Protocol (Protocollo NTP).*
RFC3647	*Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework.*
ENISA - Art. 19 Incident Reporting (Linee Guida)	*"Article 19 Incident Reporting – Incident reporting framework for eIDAS Article 19" – December 2016.* Nel presente documento, indicato anche solo come *LLGG ENISA (Art. 19)*.

2 Repository e pubblicazione

L'indirizzo di pubblicazione del presente CPS e della documentazione relativa ai servizi qualificati del QTSP INTESA è il seguente:

- *https://www.intesa.it/e-trustcom/*

L'accesso ai documenti, da parte degli utenti, è in sola lettura.

La gestione delle pubblicazioni sul sito del QTSP è a cura dello stesso.

I documenti soggetti ad approvazione dell'Organismo di Vigilanza sono inoltre pubblicati e reperibili anche sul sito della stessa Agenzia (*www.agid.gov.it*).

Ulteriori aspetti operativi sono reperibili sui *Manuali Operativi*: il QTSP INTESA è tenuto, dalla normativa italiana, a pubblicare un Manuale Operativo che descriva le procedure e le relative regole utilizzate dal QTSP per l'emissione dei certificati qualificati, la generazione e la verifica della firma elettronica qualificata, del sigillo elettronico qualificato e della validazione temporale elettronica.

Come per il CPS, anche i Manuali Operativi sono soggetti ad approvazione e pubblicazione da parte dell'Agenzia, la quale autorizza formalmente il QTSP all'applicazione di quanto riportato su tali documenti.

2.1 Pubblicazione dei certificati

Il QTSP 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 firma / sigillo dei titolari (dietro consenso)

Il QTSP 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*

NB: la pubblicazione del certificato sul servizio di LDAP è su richiesta esplicita del Titolare. Il consenso alla pubblicazione non necessariamente ne prevede la pubblicazione stessa.

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: *https://e-trustcom.intesa.it/CERTS/<<nomecert>>*.

3 Identificazione e Autenticazione (I&A)

Il QTSP INTESA emette certificati qualificati conformi al Regolamento eIDAS e a quanto raccomandato dalle LLGG di AgID.

Nello specifico, gli standard ETSI di riferimento per la profilazione del certificato qualificato sono:

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-319.412-3	ETSI EN 319 412-2 V1.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons*
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - *Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements*

Il *Titolare* del certificato qualificato può essere una persona fisica (rif. *ETSI-319.412-2*), nel qual caso si parla di *firma elettronica*, ovvero una persona giuridica (rif. *ETSI-319.412-3*), per cui si parla di *sigillo elettronico*.

3.1 Identificazione e registrazione degli utenti: Distinguished Name (DN)

Nel campo *SubjectDN* del certificato è riportato un set minimo di informazioni, in conformità alle LLGG e alle ETSI di riferimento, tramite le quali il Titolare (persona fisica o giuridica) è chiaramente identificato.

Altri attributi facoltativi possono essere valorizzati, ai fini di una migliore limitazione degli utilizzi.

3.1.1 SubjectDN Persona Fisica

Per i certificati emessi ad una persona fisica, saranno valorizzati almeno i seguenti attributi:

ATTRIBUTO	OID
countryName	2.5.4.6
givenName	2.5.4.42
surname	2.5.4.4
commonName	2.5.4.3
serialNumber	2.5.4.5
dnQualifier	2.5.4.46

Attributi facoltativi o alternativi di uso più comune, soggetti a restrizioni:

ATTRIBUTO	OID
organizationName	2.5.4.10
organizationIdentifier	*2.5.4.97*
organizationalUnitName	2.5.4.11
description	2.5.4.13
title	2.5.4.12
pseudonym	2.5.4.65

3.1.2 SubjectDN Persona Giuridica

Per i certificati emessi ad una persona giuridica, saranno valorizzati almeno i seguenti attributi:

ATTRIBUTO	OID
countryName	2.5.4.6
organizationName	2.5.4.10
organizationIdentifier	*2.5.4.97*
commonName	2.5.4.3
dnQualifier	2.5.4.46

3.1.3 Valorizzazione degli attributi

La valorizzazione degli attributi dei certificati segue le regole descritte dalle ETSI di riferimento e le raccomandazioni delle LLGG.

Si riportano nel seguito alcune specificità.

3.1.3.1 Identificativo univoco del Titolare

Al titolare del certificato è assegnato un codice, univoco presso il QTSP, riportato nell'attributo *dnQualifier*.

L'univocità del campo Subject e la riconducibilità certa del certificato al Titolare è assicurata dagli attributi:

- *serialNumber* per le persone fisiche
- *organizationIdentifier* per le persone giuridiche

Tali attributi contengono:

- *serialNumber*: contiene il codice fiscale (TIN) del Titolare indicato con il prefisso "`TINIT-`"
  Esclusivamente nel caso in cui al Titolare non sia stato assegnato un codice fiscale dall'autorità italiana è possibile indicare analogo numero di identificazione fiscale rilasciato da altra autorità dell'Unione utilizzando il prefisso `TIN` ovvero gli estremi di un documento di identità utilizzando i prefissi `IDC` o `PAS` ovvero un numero di registrazione nazionale utilizzando il prefisso PNO. . Dopo tali prefissi è indicato il codice ISO 3166 del paese che ha rilasciato il documento. Nei casi in cui la legge dello Stato di residenza della persona fisica non consenta l'utilizzo di nessuno dei precedenti codici, si utilizza il prefisso NS per identificare lo schema nazionale. In tale evenienza, il prestatore di servizi fiduciari deve inserire un codice univoco, eventualmente derivato da uno dei già menzionati.
- *organizationIdentifier*: contiene la partita IVA (VAT) della persona giuridica titolare del certificato. Dopo tale prefisso è indicato il codice ISO 3166 del paese che ha rilasciato il codice.

3.1.3.2 countryName

L'attributo *countryName* è valorizzato come segue:

- *persone fisiche*: se è presente l'attributo *organizationName*, è il codice ISO 3166 dello stato ove ha sede l'organizzazione ivi indicata; altrimenti, si fa riferimento allo stato di residenza del Titolare
- *persone giuridiche*: è il codice ISO 3166 dello stato ove ha sede il Titolare

3.1.3.3 organizationName

Attributo facoltativo. È eventualmente utilizzato per indicare l'appartenenza o l'affiliazione del Titolare all'organizzazione e esclusivamente nel caso in cui il prestatore di servizi fiduciari abbia avuto e conservi prova

della volontà dell'organizzazione medesima a tale uso e che la stessa si assuma l'obbligo di richiedere la revoca del certificato nel caso in cui il titolare del certificato lasci l'organizzazione.

NB: L'organizationName non è utilizzato nel caso in cui il Titolare sia un semplice cliente dell'organizzazione (rif. *LLGG*).

3.1.3.4 title

Nel caso in cui l'*organizationName* sia presente, i medesimi vincoli si applicano anche all'eventuale codifica dell'attributo *title*. L'attributo *title*, se presente, contiene il ruolo del Titolare nell'ambito dell'organizzazione indicata nell'attributo *organizationName*, secondo la semantica indicata nelle *LLGG*.

3.1.3.5 pseudonym

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 QTSP conserverà le informazioni relative alla reale identità dell'utente per 20 (venti) anni dopo la scadenza del certificato stesso.

L'attributo *pseudonym* (OID 2.5.4.65) deve essere utilizzato in alternativa a *givenName + surname.*

Utilizzando uno pseudonimo, il subject DN sarà valorizzato come segue:

- countryName "c=IT"
- *pseudonym* pseudonimo univoco presso il QTSP
- commonName "pseudonym"
- serialNumber come da LLGG
- *dnQualifier* identificativo univoco presso il QTSP

3.2 Identificazione certa iniziale del richiedente il certificato

Il QTSP 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 QTSP, tramite le persone del proprio Ufficio RA ovvero proprio personale adeguatamente formato;
- LRA esterne: ad esempio il personale dell'Azienda o dell'Ente Cliente oppure di terze parti appositamente delegate dal QTSP e adeguatamente formato.

La persona che fa richiesta della certificazione viene identificata con certezza dall'operatore di RA e viene archiviata dal QTSP, INTESA (o dalla LRA incaricata) copia di almeno un documento ufficiale di identità per lo Stato di appartenenza.

Se il titolare del certificato sarà una persona giuridica, la richiesta di certificazione dovrà essere avanzata dalla persona fisica che rappresenta la persona giuridica, fornendo opportuna documentazione aggiuntiva atta alla verifica dei poteri di rappresentanza (es. la visura camerale). Tipicamente, il richiedente potrà essere il Legale Rappresentante, o persona da questo formalmente delegato.

La verifica certa dell'identità del Titolare può essere effettuata nelle seguenti modalità:

- *De visu, in presenza*: per l'identificazione è necessaria la presenza fisica del richiedente davanti all'operatore di RA
- *De visu, da remoto*: l'identificazione è effettuata mediante un sistema di videoconferenza con caratteristiche di qualità certificate da un *CAB* (organismo di valutazione della conformità)
- *Per identificazione precedente*: avvalendosi di un'identificazione certa già effettuata da un *Intermediario finanziario* o da altro *Soggetto Esercente Attività Finanziaria*, che, ai sensi delle norme antiriciclaggio tempo per tempo vigenti, è obbligato all'identificazione dei propri clienti
- *Altre modalità*, purché conformi all'art. 24, comma 1, del Reg. eIDAS

Ulteriori dettagli sulle procedure di identificazione del Titolare attualmente poste in essere sono reperibili sui Manuali Operativi del QTSP, pubblicati al seguente link:

- *https://www.intesa.it/e-trustcom/*

3.3 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 QTSP o da altro ente incaricato.

3.4 Identificazione per richiesta di revoca o sospensione

La richiesta di revoca o sospensione di un certificato qualificato (par. 4.9) può essere avanzata da:

- QTSP INTESA
- Titolare
- Terzo Interessato

La richiesta di revoca / sospensione dei certificati avanzata dal Titolare o dal Terzo interessato verso il QTSP deve essere sottoscritta dal richiedente e accompagnata da copia di un documento di identità.

Una volta verificata la congruenza dei dati riportati nella richiesta, il certificato è revocato / Sospeso dalla Certification Authority del QTSP.

4 Ciclo di vita dei certificati

I certificati qualificati 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.

4.1 Richiesta di certificazione

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

In casi particolari, è possibile l'emissione prima della conclusione della fase di identificazione (par. 7.1.3).

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

4.1.1 Richiedente generico - persona fisica

Il richiedente, cioè la *persona fisica* che sarà il *Titolare* del certificato, sottoscrive:

- Il contratto di servizio, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Qualificato P.F.*, in cui riporta i dati necessari all'emissione del certificato, 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 cellulare.
  - Indirizzo di posta elettronica.
  - Tipo, numero, ente di rilascio e data di scadenza del documento di identità esibito.
- Il documento *Presa visione del Manuale Operativo INTESA*, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del GDPR.

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il QTSP (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 dal QTSP (ovvero dalla LRA incaricata, se previsto dal contratto di mandato) per 20 (venti) anni dalla scadenza del certificato.

4.1.2 Richiedente generico - persona giuridica

Il richiedente, cioè la persona fisica rappresentante la *persona giuridica* che sarà il *Titolare* del certificato (par. 3.2), sottoscrive:

- Il contratto di servizio, in cui sono riportati gli obblighi di ambo le parti.
- Il documento *Modulo Richiesta Certificato Qualificato P.G.*, in cui riporta i dati necessari all'emissione del certificato, 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 cellulare.
  - Indirizzo di posta elettronica.
  - Tipo, numero, ente di rilascio e data di scadenza del documento di identità esibito.
  - Denominazione della persona giuridica
  - Sede della persona giuridica
  - P.IVA o Codice Fiscale (VAT o analogo per organizzazioni con sede all'estero)
- Il documento *Presa visione del Manuale Operativo INTESA*, in cui dichiara di aver preso visione del Manuale Operativo.
- Il documento *Dichiarazione di autorizzazione al trattamento dei dati personali*, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del GDPR.

È responsabilità del richiedente fornire un indirizzo valido di posta elettronica, poiché il QTSP (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 dal QTSP (ovvero dalla LRA incaricata, se previsto dal contratto di mandato) per 20 (venti) anni dalla scadenza del certificato.

4.1.3 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 par. *3* 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 documentazione analoga a quella indicata al paragrafo precedente.

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

4.1.4 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 QTSP.

4.1.5 Abilitazioni professionali e poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di firma elettronica 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.), ovvero 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. Copia di tale documentazione viene conservata dal QTSP.

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.

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 QTSP, ovvero dalla LRA incaricata, per un periodo di 20 (venti) anni.

4.2 Processo di recepimento della richiesta

Il processo di valutazione della richiesta è svolto dal QTSP tramite la propria RA, ovvero dalla LRA cui sono state demandate le funzioni di Registration Authority.

Nello svolgimento di tale processo, CA, RA/LRA e richiedente/titolare sono vincolati al rispetto degli obblighi di cui al par. *9.6 - Obblighi*.

4.3 Emissione del certificato

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

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

Dopo la generazione della coppia di chiavi di firma / sigillo, 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 conseguentemente il corretto funzionamento della coppia di chiavi).

Il QTSP 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.

4.3.1 Generazione chiavi e relativo certificato su dispositivo di firma

In linea generale, per l'emissione di un certificato su di un dispositivo di firma, sono effettuate le seguenti operazioni:

- L'operatore di RA 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 Individuale di firma, l'applicazione blocca il PIN di accesso al dispositivo di firma. Al Titolare sarà 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.

4.4 Accettazione del certificato

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 (par. *4.9.2*).

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

Il richiedente sottoscrive la presa visione del pertinente *Manuale Operativo*, dove sono riportati gli obblighi del Titolare e delle altre entità coinvolte nel servizio cui aderisce (par. *9.6 - Obblighi*).

Il Manuale Operativo è disponibile sul sito del QTSP all'URL *https://www.intesa.it/e-trustcom/*

4.5 Utilizzo del certificato e delle chiavi

4.5.1 Utilizzo della chiave privata e del certificato - obblighi del Titolare

Il Titolare è tenuto a conservare le informazioni necessarie all'utilizzo della chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

In particolare, deve conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata, sia essa depositata su di un dispositivo di firma individuale (smartcard, token) ovvero su di un dispositivo di firma remota (HSM). Stessa diligenza deve porre nei confronti dei dispositivi di autenticazione forte (es. chiavette OTP, smartphone o cellulare).

La chiave privata relativa al certificato non può essere utilizzata da terzi.

Il Titolare della chiave deve, tra gli altri obblighi (par. *9.6.2*):

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- comunicare al QTSP, anche per tramite della LRA, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente CPS o nel Manuale Operativo di propria pertinenza.

4.5.2 Utilizzo della chiave pubblica e del certificato - obblighi dell'Utilizzatore

Utilizzatore (*Relying Party*) è chiunque riceva un documento firmato digitalmente e, al fine di verificarne la validità, si avvalga del certificato qualificato utilizzato dal Titolare per firmare il documento stesso.

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in conformità al Reg. eIDAS.

Coloro che si avvalgono di un certificato qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato dagli standard vigenti al momento della sua emissione;
- verificare lo stato di validità del certificato mediante il protocollo OCSP o tramite l'accesso alle Liste di Revoca;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei QTSP;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del QTSP che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

Gli obblighi sopra descritti sono automaticamente espletati dai Software di Verifica conformi alle normative vigenti (art. 14 del DPCM).

4.6 Rinnovo del certificato

Non è previsto il rinnovo del certificato qualificato, inteso come prolungamento della validità. In prossimità della scadenza, su richiesta del Titolare, sarà generata una nuova coppia di chiavi e sarà emesso un nuovo certificato.

4.7 Rinnovo delle chiavi

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

I certificati digitali emessi dalla CA INTESA hanno una validità standard 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.

È possibile per cui procedere all'emissione del certificato nelle modalità descritte al par. *4.3*.

4.8 Modifica del certificato

Le informazioni riportate sul certificato non sono modificabili. Eventuali correzioni o variazioni possono essere apportate solo con l'emissione di un nuovo certificato.

4.9 Revoca o Sospensione del certificato

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

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato (art.24, comma 1, DPCM).

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*:

- *CRLReason* ***Superceded*** sostituzione del certificato senza compromissione della chiave privata;
- *CRLReason* ***Key Compromise***: compromissione (perdita delle caratteristiche di sicurezza e univocità) della chiave privata;
- *CRLReason* ***Affiliation Changed***:i dati del certificato sono obsoleti oppure errati;
- *CRLReason* ***Cessation of Operation***: cessazione preventivata ovvero repentina, in condizioni di conflittualità o non, del Titolare dalle mansioni per le quali gli erano stati rilasciati i certificati ();
- *CRLReason* ***Privilege Withdrawn***: mancato rispetto da parte del Titolare degli obblighi specificati nel CPS o nel Manuale Operativo, in misura tale che il Terzo Interessato o la CA ritengano necessario una revoca immediata.

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

4.9.1 Revoca su iniziativa del Certificatore

Il QTSP 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.

4.9.2 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 internet *https://www.intesa.it/e-trustcom/*. Oltre al documento di richiesta di revoca, il messaggio dovrà contenere i dati relativi al certificato da revocare (o informazioni 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 e allegando un proprio documento di identità:
    a. via fax, al numero indicato all'URL *https://www.hda.intesa.it* nell'orario di servizio ivi riportato.
    b. via posta ordinaria, all'indirizzo del QTSP (par. *1.3*).
- Eccezionalmente, nel caso in cui la motivazione della richiesta di revoca sia *Key Compromise*, il Titolare potrà telefonare al numero fornito dal QTSP 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 *https://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, e-mail, telefono, ente di riferimento)
- motivazione della richiesta
- momento di decorrenza del provvedimento.

Altri 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 disponibile (es. tipo di dispositivo e numero seriale, organizzazione di riferimento, numero seriale del certificato, data di rilascio…).

Il QTSP, 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).

4.9.3 Revoca su richiesta del Terzo Interessato

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

Il QTSP 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'indirizzo internet *https://www.intesa.it/e-trustcom/*. 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 *https//www.hda.intesa.it/* nell'orario di servizio ivi riportato;
    b. via posta ordinaria, all'indirizzo del QTSP (par. *1.3*).

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 *https//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 QTSP, 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.

4.9.4 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, oppure 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*.

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

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per la richiesta di revoca.

4.9.4.1 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 90 (novanta) giorni, indicato dal Titolare nella richiesta, con la *CRLReason* indicata al momento della richiesta stessa.

In caso di revoca di un certificato sospeso, la data di revoca coinciderà con la data di sospensione.

4.10 Informazioni sullo stato del certificato

In conformità al Reg. eIDAS, le informazioni sullo stato del certificato sono disponibili via protocollo OCSP, all'URL indicato sul certificato stesso.

La revoca e la sospensione dei certificati possono essere asseverate anche dal loro inserimento nella lista CRL (art. 22 del DPCM). Il profilo delle CRL è conforme con lo standard RFC 3280. Tale lista, firmata dalla Certification Authority emittente il certificato, viene aggiornata con periodicità prestabilita e conforme alla normativa vigente.

L'indirizzo internet della lista CRL è indicato sul certificato nel campo *CDP - CRL Distribution Point*.

La lista CRL è disponibile anche sul registro dei certificati.

Tutti i servizi di pubblicazione sopra descritti sono disponibili h24.

4.11 Termine contratto

Salvo accordi particolari con il cliente, il contratto che lega il Titolare al QTSP cessa di esistere con la scadenza del certificato.

4.12 Key Escrow & Key Recovery

Non applicabile per le chiavi private relative ai certificati qualificati emessi dal QTSP INTESA.

5 Sicurezza fisica e controlli procedurali

Questo componente descrive i controlli di sicurezza non tecnici (cioè, i controlli fisici, procedurali e del personale) utilizzati dal QTSP per eseguire in sicurezza le funzioni di generazione delle chiavi, gestione del ciclo di vita del certificato qualificato (identificazione, rilascio, revoca, etc.), auditing e archiviazione.

Il QTSP, ai sensi dell'art. 35 del DPCM, predispone e mantiene aggiornato un *Piano della Sicurezza*, di cui ne è inviata copia cifrata all'Agenzia. Il documento è classificato come *Riservato INTESA*.

5.1 Sicurezza fisica

Il sistema PKI INTESA e i suoi componenti HW e SW sono gestiti all'interno di installazioni sicure (c.d. *Data Center* o *Server Farm*), protette da accessi non autorizzati attraverso sistemi di controllo degli accessi 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.

5.1.1 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.

5.1.2 Accessi fisici

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

Gli accessi alle aree PKI sono limitati al personale autorizzato, abilitato a percorsi specifici all'interno delle strutture ed eventualmente soggetto ad un servizio di escorting da parte del personale della server farm: norme specifiche regolano il numero e il tipo di figure professionali richieste per ogni rilevante operazione sui sistemi ospitati nelle facility.

L'accesso di visitatori occasionali è permesso solamente se accompagnati dal personale autorizzato (in numero dipendente dall'area specifica). L'accesso di persone non autorizzate (es. personale di servizio) avviene solo in presenza del numero minimo di personale autorizzato.

Tutti gli accessi sono tracciati.

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

5.1.3 Energia e Condizionamento

Le Server Farm 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.

Sono attivi generatori supplementari indipendenti di energia elettrica, locati esternamente all'edificio e testati periodicamente.

5.1.4 Rischio d'allagamento

I Data Center utilizzati sono dotati di sistemi per la rilevazione di eventuali allagamenti.

5.1.5 Prevenzione e protezione antincendio

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

5.1.6 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.

5.1.7 Smaltimento rifiuti

I rifiuti sono conferiti secondo la normativa vigente in materia.

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

5.1.8 Off-site Backup

I backup sono conservati in luoghi differenti dal luogo di origine.

5.2 Controlli procedurali

In questa sezione sono descritti i requisiti per il riconoscimento di ruoli fidati, insieme alle responsabilità per ciascun ruolo.

5.2.1 Ruoli del personale addetto alla PKI

Il personale responsabile delle attività di certificazione, in conformità con l'art. 38, comma 1, 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)*.

Non sono attribuite al medesimo soggetto più funzioni tra quelle sopra previste (DPCM, art. 38 comma 2).

Il personale di cui sopra ha maturato un'esperienza professionale nelle tecnologie informatiche e delle telecomunicazioni almeno quinquennale (DPCM, art 38,comma 1).

Le figure sopra elencate sono appartenenti all'organizzazione di INTESA: tutte le mansioni relative a compiti di certificazione sono assegnate formalmente, mediante lettera di incarico sottoscritta, al personale dipendente di INTESA S.p.A.

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 (c.d. *Tempo di preavviso*), essi cessano immediatamente dall'occuparsi del sistema, vengono disabilitati dalle funzioni relative e restituiscono tempestivamente ogni dispositivo e documento di identità che consenta loro di accedere alle aree e ai documenti riservati e di continuare ad esercitare le mansioni relative al servizio fiduciario.

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.

Nessuno delle figure sopra citate sarà dettagliata in seguito, fatta eccezione per il *Responsabile del servizio di certificazione e validazione temporale*, unico ruolo con responsabilità operative.

Ferma restando la responsabilità del QTSP, alcune delle seguenti responsabilità possono essere affidate ad altre organizzazioni. In questo caso il responsabile della sicurezza, o altro dipendente appositamente designato, gestisce i rapporti con tali fi gure professionali (DPCM, art. 38, comma 3).

5.2.1.1 Responsabile del servizio di certificazione e validazione temporale.

Tale figura è responsabile della generazione dei certificati: è incaricato della supervisione del processo di emissione e gestione dei certificati, inclusa la custodia dei dispositivi di firma (HSM) del QTSP.

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 custoditi dal QTSP;
- l'attivazione dei dispositivi di firma del sistema di emissione dei certificati (CA), del sistema di marcatura temporale (TSA) e dei titolari

- la generazione delle chiavi del sistema di emissione dei certificati (CA) e del sistema di marcatura temporale (TSA); la loro sostituzione in condizioni di emergenza e di normale avvicendamento;
- la sostituzione delle chiavi dei titolari;
- la corretta emissione delle marche temporali e la loro conservazione;
- il rilascio, la sospensione, la revoca, la sostituzione dei certificati;
- la pubblicazione delle informazioni sullo stato del certificato (OCSP / CRL);
- 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.

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.

5.2.1.2 CA Operator

I CA Operator sono responsabili della installazione, della gestione e dell'aggiornamento del sistema di emissione dei certificati, incluso i dispositivi di firma del QTSP.

La mansione di CA Operator è ricoperta da più addetti, includendo nel computo anche il *Responsabile del servizio di certificazione e validazione temporale*.

Alcune attività proprie dell'attività del CAO sono effettuate in modalità dual-control.

5.2.1.3 RA / LRA Operator

Gli operatori di Registration Authority ricoprono le funzioni di interfaccia con i richiedenti la certificazione e con i titolari, durante tutte le fasi di registrazione, certificazione, revoca e sospensione.

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

5.2.1.4 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 afferenti la PKI (sistema di generazione dei certificati e di validazione temporale). Ove necessario, essi possono accedere alle sale in cui si trovano i citati sistemi, se accompagnati da almeno una persona autorizzata: 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 PKI. Ove necessario, essi possono accedere alle sale in cui si trovano i citati sistemi, se accompagnati da almeno una persona autorizzata: il loro ingresso e la loro permanenza vengono registrate nel Giornale di controllo. Le loro azioni vengono registrate sui log.

5.3 Controlli sul personale addetto

5.3.1 Qualifica ed esperienza

Tutto il personale ricoprente i ruoli menzionati al precedente paragrafo è dipendente INTESA e possiede un'esperienza pluriennale su analisi, sviluppo, pianificazione o gestione di sistemi informativi. Fanno eccezione gli operatori di LRA, che possono essere semplicemente formati per il ruolo specifico.

È inviato all'Agenza, inizialmente e ad ogni aggiornamento organizzativo, l'organigramma del personale responsabile per il servizio fiduciario (DPCM, art. 38, comma 1), comprensivo di dettagliato e aggiornato CV.

5.3.2 Verifica dei requisiti del personale addetto

È tenuto un repository dei CV del personale INTESA.

Parimenti, per i fornitori esterni, è richiesta una dichiarazione di adeguata formazione, eventualmente accompagnata da un estratto del CV.

Prima dell'assunzione è richiesta un'autocertificazione dell'assenza di carichi pendenti e di condanne penali. Entro 180 gg dall'assunzione il dipendente dovrà produrre il relativo certificato rilasciato dalla procura.

Sono definite linee guida aziendali per ridurre al minimo eventuali conflitti di interesse che potrebbero evidenziarsi in ambito lavorativo o familiare.

5.3.3 Formazione

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 di data privacy e sulle variazioni organizzative. Per ogni aggiornamento apportato al sistema di certificazione è previsto un apposito addestramento.

5.3.4 Sanzioni disciplinari

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.

5.3.5 Controlli sul del personale esterno

Il QTSP INTESA predispone piani di audit periodici sia verso i fornitori di servizi strategici, sia verso le organizzazioni cui è demandata la funzione di LRA.

5.4 Audit logging (Giornale di Controllo)

Il giornale di controllo (DPCM, art. 36) è costituito dall'insieme delle registrazioni effettuate, anche automaticamente, dai dispositivi installati presso il QTSP. Le registrazioni possono essere effettuate indipendentemente anche su supporti distinti e di tipo diverso.

5.4.1 Tipi di eventi registrati

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

Sul Giornale di controllo sono registrati, tra gli altri eventi:

- Gli accessi ai sistemi di PKI
- Gli accessi fisici ai data center
- Gli eventi riguardanti il certificato (emissione e ciclo di vita)
- La personalizzazione del dispositivo di firma

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 errori imputabili ad un operatore (es. il tentativo di eseguire un'operazione non autorizzata) o nel caso di malfunzionamenti HW o SW.

5.4.2 Frequenza dei LOG

Gli eventi sono raccolti in tempo reale da un SW dedicato. Tali dati vengono monitorati e verificati giornalmente per garantire un audit completo.

5.4.3 Conservazione dei LOG

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

5.4.4 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. Lo stesso SW di gestione e raccolta dei log ha un sistema di controllo che rende impossibile la modifica dei log raccolti.

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

5.4.5 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.

5.4.6 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.

5.4.7 Notifica ai soggetti causa di eventi

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

5.4.8 Verifiche della vulnerabilità

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

5.5 Archivio dei documenti

5.5.1 Tipologia di documenti ed eventi archiviati

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

5.5.1.1 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).

La copia del documento di identità è parte della documentazione prodotta.

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

5.5.1.2 Documentazione elettronica

Comprende i dati registrati dal Giornale di Controllo e gli eventi del sistema di validazione temporali.

In particolare, tutte le marche temporali emesse dal sistema di validazione sono conservate in un apposito archivio digitale non modificabile per un periodo non inferiore a 20 (venti) anni ovvero, su richiesta dell'interessato, per un periodo maggiore.

5.5.1.3 Documentazione che può essere elettronica oppure cartacea

Tutti i documenti relativi alle richieste di sospensione o revoca operate dal Certificatore, dal Titolare o dal Terzo Interessato.

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

5.5.1.4 Documenti addizionali

Verbali, tra cui quelli della generazione delle chiavi di CA e TSA, eventualmente in formato digitale e digitalmente firmati dal personale incaricato.

5.5.2 Periodo di archiviazione

Tutti gli elementi indicati al precedente par. *5.5.1* sono conservati per un periodo di 20 (venti) anni.

5.5.3 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.

5.5.4 Procedure di backup degli archivi

5.5.4.1 Archivio cartaceo

Le informazioni contenute sui documenti cartacei sono conservate in modo sicuro presso il QTSP ovvero, se convenuto, presso i siti delle LRA incaricate.

5.5.4.2 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.

5.5.5 Requisiti per il riferimento temporale dei record

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

5.5.6 Verifica di integrità

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

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

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

Ai sensi del Reg. (UE) 2016/679 (GDPR), è possibile 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.

5.6 Rinnovo delle chiavi del QTSP

In questo paragrafo è trattata la sostituzione pianificata delle chiavi del QTSP, ovverosia le chiavi del sistema di certificazione (CA e TSA) e del sistema di validazione temporale.

5.6.1 Rinnovo delle chiavi di CA

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alle coppie di Chiavi di certificazione (CA e TSA), utilizzate dai sistemi di emissione dei certificati di firma / sigillo e dei certificati di TSA, il QTSP procederà in base a quanto stabilito dall'art. 30 del DPCM.

L'operazione è effettuata in modalità dual-control, in presenza del *Responsabile del servizio 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, come richiesto dal DPCM (art. 18, comma 3).

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

5.6.2 Rinnovo delle chiavi di validazione temporale

In conformità con quanto indicato all'art. 49, comma 2, del DPCM, ai fini 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 emissione. Contestualmente, un certificato è emesso relativamente alla nuova coppia di chiavi (senza revocare il precedente, relativo alla coppia di chiavi sostituita).

5.7 Compromissione e disaster recovery

5.7.1 Gestione degli incidenti di sicurezza

Ai sensi dell'art. 19(2) del Reg. eIDAS, il QTSP è tenuto a notificare all'organismo di vigilanza (AgID) e, ove applicabile, ad altri organismi interessati, quali l'ente nazionale competente per la sicurezza delle informazioni o l'autorità di protezione dei dati, tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

Qualora sia probabile che la violazione della sicurezza o la perdita di integrità abbia effetti negativi su una persona fisica o giuridica a cui è stato prestato il servizio fiduciario, il prestatore di servizi fiduciari notifica senza indugio anche alla persona fisica o giuridica la violazione di sicurezza o la perdita di integrità.

Di seguito sono riportati i livelli di *severity* codificati nelle *LLGG ENISA ART.19 Incident Reporting*:

1. No impact
2. Insignificant impact: provider assets were affected but no impact on core services
3. Significant impact: part of the customers/services is affected
4. Severe impact: large part of the customers/services is affected
5. Disastrous: the entire organisation, all services, all certificates are affected

Per ogni livello di severity, il documento ENISA riporta, a titolo di esempio, una serie di eventi classificati come incidenti di sicurezza. Per ulteriori approfondimenti, si rimanda al documento stesso, reperibile sul sito di ENISA (*https://www.enisa.europa.eu/publications/article19-incident-reporting-framework*).

5.7.2 Guasto del dispositivo di firma della CA INTESA

Nel caso di guasto del dispositivo di firma contenente le chiavi di certificazione, potrebbe essere necessario, a seconda del tipo di guasto, o ri-inizializzare il dispositivo stesso o inizializzarne uno nuovo, al fine di ricreare le chiavi originali.

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

Tale evento sarà notificato all'organismo di vigilanza come incidente di sicurezza.

5.7.3 Compromissione delle chiavi di certificazione

Nel caso di compromissione delle chiavi di certificazione, è applicata la procedura di revoca del certificato root. Il QTSP INTESA genererà una nuova coppia di chiavi, come riportato al par. *5.6.1*.

Nel caso di compromissione delle chiavi di marcatura temporale, il relativo certificato sarà revocato e le chiavi saranno ricreate, come descritto in *5.6.2*.

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, art. 23). Viene applicato quanto descritto in precedenza e i certificati riemessi con la procedura usuale. Nota: questa possibilità è stata valutata e pianificata per completezza, poiché è ragionevole che non si verifichi mai.

L'incidente di sicurezza è notificato all'organismo di vigilanza e, ove applicabile, agli altri organismi interessati.

5.7.4 Gestione degli eventi catastrofici

La presenza di sistemi configurati in modalità *dual-site*, con repliche distribuite in più punti consente comunque, in caso di interruzione di funzionamento di una delle sedi, di accedere ai servizi se almeno una delle sedi dei data center è operativa.

Il QTSP INTESA è dotata di un piano di emergenza per la gestione degli eventi catastrofici che prevede le seguenti fasi:

- *gestione dell'emergenza:* attivazione delle soluzioni di *disaster recovery*
- *gestione del transitorio*: servizio attivo e ripristino di ulteriori soluzioni di *disaster recovery*;
- *ritorno dell'esercizio a regime*: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica off-site dei dati e l'intervento entro 24 ore di personale atto ad attivare le funzionalità del sito di DR.

5.8 Cessazione della CA o RA

Un'eventuale cessazione di uno o più servizi del QTSP deve minimizzare il disservizio provocato nei confronti di coloro che hanno sottoscritto contratti per l'utilizzo dei servizi dismessi e per le terze parti collegate. In particolare, deve essere fornita una continuità delle informazioni necessarie per verificare la correttezza dei servizi fiduciari.

La cessazione dei Servizi può avvenire programmaticamente, nel caso in cui il QTSP INTESA decidesse deliberatamente di non fornire, da una certa data prestabilita, i servizi per cui è QTSP, ovvero in maniera indipendente dalla volontà del QTSP.

In conformità al Reg. eiDAS, il QTSP INTESA predispone un *Piano di Cessazione delle Attività* (*Termination Plan*), di cui copia aggiornata è inviata all'organismo di vigilanza. Il documento ha come obiettivo la descrizione, in termini generali, delle procedure previste dal QTSP INTESA in caso di cessazione del servizio fiduciario fornito.

Con un periodo di preavviso non inferiore ai sei mesi rispetto alla prevista data di cessazione, il QTSP 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 Interessato

- • Le Terze parti coinvolte nei processi, quali
  - – le Local RA esterne (par. 1.3.3.4)
  - – i fornitori di servizi / prodotti
  - – i fornitori dei servizi logistici (server farm)
- • Eventuali altri QTSP con cui sussistono rapporti di collaborazione

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

I titolari dei certificati saranno anche avvisati della prevista revoca del certificato di firma / sigillo.

5.8.1 Storni contrattuali

La cessazione del servizio comporterà lo storno dei contratti in essere con:

- • Local RA esterne, con revoca del mandato ad operare per conto del QTSP
- • Cliente o Azienda / Ente cliente

Tutti gli aspetti economici relativi saranno valutati e presi in carico dalla Direzione Generale.

5.8.2 Revoca dei certificati e distruzione delle chiavi

La cessazione del servizio comporterà la revoca dei certificati relativi alle chiavi di certificazione e di validazione temporale.

Successivamente, si procederà all'eliminazione delle chiavi di certificazione dai dispositivi.

Le operazioni menzionate saranno svolte in presenza dei responsabili dei servizi del QTSP (par. 1.3): dell'operazione sarà fatto verbale, sottoscritto almeno dal *Responsabile del servizio di certificazione e validazione temporale* e dal *Responsabile delle verifiche e delle ispezioni (auditing*).

Entro 24 ore, il Certificatore notificherà l'avvenuta revoca all'Agenzia e ai titolari.

Prima di procedere alla revoca dei certificati relativi alle chiavi di certificazione, sarà attivata una procedura di revoca di tutti i certificati di firma / sigillo firmati dalla CA.

Un volta revocati i certificati, saranno cancellate le chiavi relative ai certificati di firma remota risiedenti sui dispositivi di firma remota custoditi dal Certificatore. Per gli eventuali dispositivi custoditi per conto del Certificatore da soggetti terzi (DPCM, art. 3, comma 4), si renderà necessaria una visita ispettiva (audit).presso i locali ove è custodito il dispositivo per accertare l'avvenuta cancellazione delle chiavi di firma / sigillo.

Dell'operazione sarà fatto verbale, sottoscritto almeno dal *Responsabile del servizio di certificazione e validazione temporale* e dal *Responsabile delle verifiche e delle ispezioni (auditing)*.

Per quanto riguarda i dispositivi di firma individuali distribuiti (smartcard/token usb), sarà inviata specifica comunicazione ai titolari, consigliando la distruzione del dispositivo a seguito della revoca del certificato relativo alle chiavi di firma / sigillo ivi contenute.

6 Controlli Tecnici di Sicurezza

6.1 Generazione e Installazione delle chiavi

6.1.1 Generazione della coppia di chiavi di certificazione (CA e TSA)

La generazione delle chiavi di Certificazione all'interno dei dispositivi di firma custoditi nei locali del QTSP e in presenza del *Responsabile del servizio di certificazione e validazione temporale*, 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 conservati in luoghi fisici differenti, così come le password dei dispositivi autorizzativi.

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.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

6.1.2 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.

L'operazione è svolta in presenza del *Responsabile del servizio di certificazione e validazione temporale* ovvero da persona da questi delegata.

Della chiave pubblica viene generato il certificato, avente validità 10 (dieci) 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.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

6.1.3 Generazione della coppia di chiavi di firma / sigillo

Le chiavi di firma / sigillo possono essere generate dal Titolare o dal Certificatore.

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

6.1.4 Dimensioni delle chiavi e Algoritmi di firma

L'algoritmo crittografico utilizzato è RSA, con algoritmo di firma SHA-256.

La lunghezza delle chiavi di certificazione è conforme alla normativa tempo per tempo vigente.

6.1.5 Utilizzo delle chiavi (keyUsage)

In conformità con le LLGG e il Reg. eIDAS, , il campo keyUsage dei certificati è impostato come segue:

- CA - TSA (certificato di root) — keyUsage: keyCertSign + cRLSign
- TSU (certificato di validazione temporale) — keyUsage: digitalSignature; extKeyUsage: timeStamping
- Firma elettronica / Sigillo elettronico (certificato qualificato) — keyUsage: nonRepudiation

6.2 Protezione della chiave privata

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

6.2.1 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 conformi ai requisiti dell'Allegato II del Reg. eIDAS (QSCD).

E' fatta segnalazione all'Agenzia dei dispositivi in uso, e della loro eventuale dismissione, secondo le modalità da questa definite.

6.2.2 Controllo Multi-Persona della chiave privata

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

6.2.3 Deposito presso terzi della chiave privata

Le chiavi private di non sono depositate presso terzi.

6.2.4 Backup della chiave privata

Le chiavi private di certificazione sono oggetto di backup.

Le chiavi di validazione temporale non sono oggetto di backup.

6.2.5 Archiviazione della chiave privata

Il backup cifrato delle chiavi private è archiviato off-site.

6.2.6 Introduzione della chiave privata in modulo crittografico

Il QTSP INTESA implementa la generazione della coppia di chiavi solamente all'interno del dispositivo crittografico.

Il restore del backup delle chiavi di certificazione avviene in modalità *dual-control*, sempre comunque alla presenza del *Responsabile del servizio di certificazione e validazione temporale*.

6.2.7 Memorizzazione della chiave privata

Le chiavi private sono generate all'interno del dispositivo e ivi memorizzate e protette secondo i meccanismi di sicurezza del dispositivo stesso.

6.2.8 Attivazione della chiave privata

I dispositivi crittografici di CA, TSU e Firma remota possono essere attivati solo in modalità *dual-control*, sempre comunque alla presenza del *Responsabile del servizio di certificazione e validazione temporale*.

6.2.9 Disattivazione della chiave privata

I dispositivi crittografici di CA, TSU e Firma remota possono essere attivati solo in modalità *dual-control*, sempre comunque alla presenza del *Responsabile del servizio di certificazione e validazione temporale*.

6.2.10 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/TSA, TSU, firma / sigillo). Qualora tale dispositivo venga manomesso o anche asportato (quindi non più alimentato), automaticamente si disattiva. Per togliere il dispositivo da tale stato è necessario riattivarlo mediante l'utilizzo degli appositi dispositivi di sicurezza.

In caso di compromissione della chiave privata, in conseguenza del blocco del dispositivo come prima descritto, alla presenza *Responsabile del servizio di certificazione e validazione temporale* e in modalità *dual-control*, il dispositivo sarà inizializzato, in modo da cancellarne il contenuto e i suoi backup saranno ri-inizializzati o distrutti.

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

6.3 Ulteriori aspetti concernenti la gestione delle chiavi

6.3.1 Archiviazione delle chiavi pubbliche

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

6.3.2 Periodo di validità per le chiavi

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

Il periodo di validità dei certificati relativi alle chiavi di TSU è di almeno 10 (dieci) anni. Le chiavi di TSU sono comunque sostituite, senza che il relativo certificato sia revocato, al massimo ogni 90 (novanta) giorni, al fine di limitare il numero di validazioni temporali emesse per ciascuna coppia di chiavi.

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

6.4 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/TSA e di TSU.

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

6.5 Controlli di sicurezza sulle macchine

6.5.1 Requisiti specifici di sicurezza

Oltre alla separazione dei ruoli (par.1.3), tutte le attività svolte sono oggetto di log (di sistema e applicativi).

6.5.2 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.

6.6 Gestione dei controlli di sicurezza

INTESA ha in essere norme, procedure e processi per la gestione e gli aggiornamenti dei controlli di sicurezza.

6.7 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 dei siti INTESA PKI e delle LRA sono protette e avvengono attraverso porte di comunicazione espressamente autorizzate.

Come da normativa vigente, sono periodicamente effettuati *Penetretion Test* e *Vulnerability Assessement*.

6.8 Sincronismo con l'ora campione

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata mediante il protocollo *NTP* (*Network Time Protocol*). L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi, a loro volta, sono sincronizzati alla scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

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

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

6.8.1 Controllo del sincronismo con l'ora campione

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

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

7 Profili dei certificati e CRL - Certificate Policy

I profili dei certificati e delle CRL emessi dal QTSP INTESA sono conformi alla specifiche riportate nella RFC5280 (Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile) e agli standard ETSI EN di riferimento del Reg. eIDAS e delle LLGG.

7.1 Profili dei certificati

Sono riportati nel seguito i profili dei certificati *root* delle CA del QTSP INTESA e i certificati da esse emessi.

Tutte i certificati di root sotto descritti sono presenti nella EUTSL - EU Trusted List dei prestatori di servizi fiduciari.

7.1.1 CA - Certification Authority - Firma Elettronica Qualificata

In questo paragrafo sono descritti i certificati afferenti il *servizio qualificato di firma elettronica*.

A. Certificato di root

I certificati root del QTSP 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

I certificati di root e i dati contenuti sono strutturati come disposto dalla *Deliberazione* (per i certificati emessi quando in vigore), dalla *LLGG* e conformi al *Regolamento eIDAS*.

- ***OID 1.3.76.21.1.3.1 - CA root (30.03.2010 - rinnovo 16.06.2020))***
  https://e-trustcom.intesa.it/CERTS/CAINTESA2.cer
  Tabella riepilogativa:

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)

- ***OID 1.3.76.21.1.3.1 - CA root (rinnovo 16.06.2020)***
  https://e-trustcom.intesa.it/CERTS/CAINTESA2R.cer
  Tabella riepilogativa:

field	value
Version	v3
Serial Number	4c 39 3a d0
Signature	sha256WithRSAEncryption
Hash	Sha256
Issuer DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Validity (20 yrs)	martedì 16 giugno 2020 15:16:05 sabato 16 giugno 2035 15:46:05
Subject DN	**C=IT** **O=IN.TE.S.A. S.p.A.** **CN=IN.TE.S.A. Certification Authority**
Public Key	rsaEncryption (4096)
Subject KeyIdentifier	F7:29:FB:D8:B4:D8:40:7D:EC:28:BB:5F:F3:7E:50:3D:A1:59:4C:C4
Authority KeyIdentifier	F7:29:FB:D8:B4:D8:40:7D:EC:28:BB:5F:F3:7E:50:3D:A1:59:4C:C4
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_CA1.crl*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)

- ***OID 1.3.76.21.1.5.1 - CA root (09.01.2015)***
  https://e-trustcom.intesa.it/CERTS/CAINTESA3.cer
  Tabella riepilogativa:

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)

B. *Certificato qualificato di firma elettronica*

Il certificato qualificato di firma elettronica e i dati contenuti sono strutturati come disposto *Deliberazione* (per i certificati emessi quando in vigore), dalle *LLGG* e sono conformi al *Regolamento eIDAS*.

I certificati qualificati emessi dalle CA di cui al par. precedente hanno il seguente Policy OID:

- 0.4.0.194112.1.2

Contengono inoltre, nell'estensione *certificatePolicies*, in riferimento alla CA root che li ha emessi, i segg. OID:

- 1.3.76.21.1.3.1.1
- 1.3.76.21.1.5.1.1

I certificati qualificati emessi in conformità alle LLGG riportano la codifica, nel campo *certificatePolicies* (OID 2.5.29.32), di un elemento PolicyIdentifier con valore *agIDcert*:

- OID 1.3.76.16.6

Tabella riepilogativa:

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	*PROFILO CONFORME A:* *ETSI-319.412-2* *LLGG*
Public Key	rsaEncryption (2048) o superiore
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	AKI della CA emittente
Authority Information Access	CA Issuers - URI:*https://e-trustcom.intesa.it/CERTS/*<<nomeCAcert>>.cer OCSP - URI:*https://e-trustcom.intesa.it/<<nomeOCSP>>*
qcStatements	**qcStatement:** RIF. ETSI 319 412-5 punti 4.2 - 4.3 (4.2.1) 1. Questo è un Certificato Qualificato conforme agli Annex I, III o IV del Regolamento (EU) No 910/2014 (4.2.2) 2. La chiave pubblica certificata risiede in un Dispositivo Sicuro per la Creazione di Firme (QSCD) (4.2.3) 3. Tipo del certificato: id-etsi-qct-esign (4.3.3) 4. Questo certificato riporta un periodo di "retention" da parte della CA pari a 20 anni. (4.3.4) 5. Attestazione conformità: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.2 Policy: 1.3.76.21.1.3.1.1 oppure 1.3.76.21.1.5.1.1 CPS: *https://www.intesa.it/e-trustcom/* - ed eventuali limiti d'uso Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specifico per il certificato

7.1.2 CA - Certification Authority - Sigillo e Firma Elettronici Qualificati

In questo paragrafo sono descritti i certificati afferenti la CA dedicata ai *servizi qualificati di sigillo elettronico e firma elettronica*.

A. Certificato di root (OID 1.3.76.21.10.2.1)

Il certificato root del QTSP INTESA dedicato al servizio fiduciario qualificato di generazione dei *certificati qualificati per il sigillo elettronico e per la firma elettronica* ha il seguente OID:

- 1.3.76.21.10.2.1

Il certificato di root e i dati contenuti sono strutturati come disposto dalle *LLGG* e sono conformi al *Regolamento eIDAS*.

- ***OID 1.3.76.21.10.2.1 - CA root (18.03.2020)***
  https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer

Tabella riepilogativa:

field	value
Version	v3
Serial Number	59CB 51E D 07 46 5 CC3
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Validity (20 yrs)	mercoledì 18 marzo 2020 17:52:05 domenica 18 marzo 2040 17:52:05
Subject DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Public Key	rsaEncryption (4096)
Subject KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Certificate Policies	Policy: X509v3 Any Policy CPS: *https://intesa.it/e-trustcom/*
Basic Constraint	CA: TRUE, pathlen:0
Key Usage	Firma certificato, Firma CRL offline, Firma CRL (06)

B. Certificato qualificato di sigillo elettronico (OID 1.3.76.21.10.2.1.1)

Il certificato qualificato di sigillo elettronico e i dati contenuti sono strutturati come disposto dalle *LLGG* e sono conformi al *Regolamento eIDAS*.

I certificati qualificati di sigillo elettronico emessi dalle CA di cui al par. precedente hanno il seguente Policy OID:

- 0.4.0.194112.1.3

Contengono, inoltre, nell'estensione *certificatePolicies*, in riferimento alla CA root che li ha emessi, il seg. OID:

- 1.3.76.21.10.2.1.1

I certificati qualificati emessi in conformità alle LLGG riportano la codifica, nel campo *certificatePolicies* (OID 2.5.29.32), di un elemento PolicyIdentifier con valore *agIDcert*:

- OID 1.3.76.16.6

Tabella riepilogativa:

field	value
Version	v3
Serial Number	Definito dalla CA e univoco all'interno della stessa CA
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Validity	Definito contrattualmente
Subject DN	*PROFILO CONFORME A:* *ETSI-319.412-3* *LLGG*
Public Key	rsaEncryption (2048) o superiore
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority Information Access	CA Issuers - URI:*https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer* OCSP - URI:*https://e-trustcom.intesa.it/ocsp*
qcStatements	**qcStatement:** RIF. ETSI 319 412-5 punti 4.2 - 4.3 (4.2.1) 1. Questo è un Certificato Qualificato conforme agli Annex I, III o IV del Regolamento (EU) No 910/2014 (4.2.2) 2. La chiave pubblica certificata risiede in un Dispositivo Sicuro per la Creazione di Firme (QSCD) (4.2.3) 3. Tipo del certificato:*id-etsi-qct-eseal* (4.3.3) 4. Questo certificato riporta un periodo di "retention" da parte della CA pari a 20 anni. (4.3.4) 5. Attestazione conformità: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.3 Policy: 1.3.76.21.1.10.2.1.1 CPS: *https://www.intesa.it/e-trustcom/* - ed eventuali limiti d'uso Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specifico per il certificato

C. *Certificato qualificato di firma elettronica (OID 1.3.76.21.10.2.1.2)*

Il certificato qualificato di firma elettronica e i dati contenuti sono strutturati come disposto dalle *LLGG* e sono conformi al *Regolamento eIDAS*.

I certificati qualificati di firma elettronica emessi dalle CA di cui al par. precedente hanno il seguente Policy OID:

- 0.4.0.194112.1.2

Contengono, inoltre, nell'estensione *certificatePolicies*, in riferimento alla CA root che li ha emessi, il seg. OID:

- 1.3.76.21.10.2.1.2

I certificati qualificati emessi in conformità alle LLGG riportano la codifica, nel campo *certificatePolicies* (OID 2.5.29.32), di un elemento PolicyIdentifier con valore *agIDcert*:

- OID 1.3.76.16.6

Tabella riepilogativa:

field	value
Version	v3
Serial Number	Definito dalla CA e univoco all'interno della stessa CA
Signature	sha256WithRSAEncryption
Hash	sha256
Issuer DN	**C: IT** **organizationIdentifier: VATIT-05262890014** **O: In.Te.S.A. S.p.A.** **CN: Intesa SpA - eIDAS Qualified Trust Services**
Validity	Definito contrattualmente
Subject DN	*PROFILO CONFORME A:* *ETSI-319.412-2* *LLGG*
Public Key	rsaEncryption (2048) o superiore
Key Usage	Non Repudiation
Basic Constraint	CA: FALSE
Authority KeyIdentifier	0B:27:99:23:AA:F1:B3:30:6E:65:AE:56:DA:BB:67:67:FB:A8:8E:C5
Authority Information Access	CA Issuers - URI:*https://e-trustcom.intesa.it/CERTS/CAINTESASIG.cer* OCSP - URI:*https://e-trustcom.intesa.it/ocspsl*
qcStatements	**qcStatement:** RIF. ETSI 319 412-5 punti 4.2 - 4.3 (4.2.1) 1. Questo è un Certificato Qualificato conforme agli Annex I, III o IV del Regolamento (EU) No 910/2014 (4.2.2) 2. La chiave pubblica certificata risiede in un Dispositivo Sicuro per la Creazione di Firme (QSCD) (4.2.3) 3. Tipo del certificato:*id-etsi-qct-esign* (4.3.3) 4. Questo certificato riporta un periodo di "retention" da parte della CA pari a 20 anni. (4.3.4) 5. Attestazione conformità: EN: *https://e-trustcom.intesa.it/DOCS/INTQS-QC_PDS.pdf*
Certificate Policies	Policy: 0.4.0.194112.1.2 Policy: 1.3.76.21.1.3.1.1 oppure 1.3.76.21.1.5.1.1 CPS: *https://www.intesa.it/e-trustcom/* - ed eventuali limiti d'uso Policy: 1.3.76.16.6
CRL Distribution Points	Full Name: URI: *http://e-trustcom.intesa.it/CRL/<<nomeCRL>>.crl*
Subject Key Identifier	Specifico per il certificato

7.1.3 Certificati di firma digitale in particolari ambiti chiusi di utenti

È possibile l'emissione di un certificato di validità temporale limitata (30 / 60 minuti) prima che sia conclusa l'identificazione del Titolare solamente nel caso sussistano particolari circostanze riconducibili a limitati utilizzi della firma digitale in contesti chiusi di utenti che non consentono alle firme digitali generate di produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non termini con esito positivo.

Questa possibilità è stata confermata dall'Agenzia con la comunicazione alle CA del 7 giugno 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", avente per oggetto "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*".

La comunicazione sopra menzionata riporta le seguenti restrizioni:

1) Il processo è riconducibile esclusivamente a sistemi di firma remota;
2) L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;

3) Nel certificato qualificato del Titolare devono essere presenti stringenti limiti d'uso afferenti il rapporto specifico (ad esempio, cliente e istituto finanziario) fra Titolare e cointeressato e cofirmatario;
4) Con l'obiettivo di distinguere chiaramente questi certificati da quelli emessi con procedure più tradizionali, il certificato qualificato del Titolare deve contenere uno specifico OID, riscontrabile nel manuale operativo, in cui è descritto questo particolare processo e il suo ristretto ambito;
5) Devono sussistere stringenti limiti applicativi: l'applicazione di firma remota deve limitare i possibili oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario. I documenti oggetto della sottoscrizione devono essere giuridicamente imperfetti, cioè privi di effetto fino all'apposizione della firma del cointeressato e cofirmatario. A titolo di esempio, si citano i contratti per l'adesione ad un servizio;
6) Nel caso in cui la verifica dell'identità del Titolare avvenga per mezzo di un incontro fisico fra Titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del Certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario se diverso dal Certificatore;
7) Il cointeressato e cofirmatario può espletare la verifica dell'identità in vece del Certificatore, attraverso sessioni audio-video (alle ben note condizioni) ovvero in applicazione della normativa afferente la verifica dell'identità di cui al D.lgs. 231/2007, ove applicabile. Qualora, nell'ambito della verifica ai sensi di tale D.lgs. sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;
8) All'apposizione della firma del Titolare non deve essere apposta la marca temporale che deve essere apposta obbligatoriamente dopo la firma del cointeressato e cofirmatario che rende l'atto giuridicamente perfetto;
9) Fino all'apposizione della firma e della marca di cui al precedente punto 8, l'oggetto sottoscritto dal solo Titolare non deve essere fornito ad alcuno e, qualora la verifica dell'identità del Titolare non avesse buon fine, deve essere distrutto conservando traccia degli eventi in appositi log.

Per ottemperare al punto 4), il certificato emesso sotto queste condizioni deve essere distinguibile dagli altri: a tal fine, il QTSP INTESA ha individuato i tre seguenti OID, per mantenere il riferimento alla CA di root che ha emesso il certificato:

- *1.3.76.21.1.3.1.1.1*
- *1.3.76.21.1.5.1.1.1*
- *1.3.76.21.10.2.1.2.1*

La descrizione della procedura di rilascio, di apposizione della firma e dei limiti applicativi saranno riportati nei manuali operativi pertinenti.

7.2 Profilo delle 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

7.2.1 Estensioni delle entry

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

7.3 Profilo dell'OCSP

Il Reg. eIDAS rende obbligatoria fornire l'informazione sullo stato del certificato tramite il protocollo OCSP.

Il formato della *response* è conforme alle specifiche RFC 6960.

7.4 Profilo delle validazioni temporali

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

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

- Version
- Policy
- messageImprint
- serialNumber
- genTime
- accuracy
- TSA

8 Audit di conformità

Il QTSP INTESA è soggetto ad Audit periodico ai fini del rilascio e mantenimento della certificazione per le qualifica dei propri servizi fiduciari ai sensi del Reg. eIDAS.

Lo stesso regolamento prevede una verifica della conformità dell'organizzazione e dei servizi da parte di un *organismo di valutazione della conformità* (*CAB - Comformity Assessment Body*) accreditato dall'*Ente di Accreditamento* nazionale (per l'Italia: Accredia - *https://www.accredia.it*).

Il QTSP trasmette all'Organismo di Vigilanza i report di conformità entro tre giorni dalla ricezione.

8.1 Periodicità delle verifiche

I prestatori di servizi fiduciari qualificati sono sottoposti, ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità.

Inoltre, l'organismo di vigilanza (AgID) può, in qualsiasi momento, condurre una verifica o chiedere a un organismo di valutazione della conformità di eseguire una valutazione di conformità.

Sono pianificati, infine, ispezioni di verifica presso i fornitori di servizi, ivi incluse le organizzazioni cui è demandata l'attività di Local Registration Authority. Tali audit sono svolti da personale interno all'organigramma del QTSP.

8.2 Identità e qualificazioni degli auditor

Le verifiche di sono effettuate a cura di un organismo di valutazione della conformità accreditato, che a sua volta si avvale di figure professionali qualificate e accreditate.

8.3 Relazioni tra QTSP e Auditor

Gli auditor incaricati dall'*organismo di valutazione della conformità* non hanno alcuna relazione con il QTSP INTESA.

Il *Responsabile delle verifiche e delle ispezioni* (par. *1.3*) appartiene ad una direzione aziendale differente da quella del *Responsabile del servizio di certificazione e validazione temporale*.

8.4 Oggetto delle verifiche

Gli audit condotti dall'organismo di valutazione delle conformità vertono sugli aspetti procedurali e organizzativi del QTSP nello svolgimento delle attività connesse ai servizi fiduciari. Quindi una disamina completa dei requisiti richiesti dal Reg. eIDAS e dalle norme ETSI di riferimento.

Gli audit presso i fornitori di servizi ovvero presso le LRA vertono sugli aspetti specifici oggetto della fornitura ovvero delle funzioni demandate.

8.5 Rilevazione di non conformità

In caso di rilevazione di non conformità, è redatto un *Piano di Intervento* (*Action Plan*) che contiene le azioni necessarie per il rientro dalla non conformità segnalata.

La tempistica di presa in carico e risoluzione è correlata al livello (severity) della non conformità.

8.6 Comunicazione dei risultati

Il QTSP trasmette all'Organismo di Vigilanza i report di conformità entro tre giorni dalla ricezione da parte dell'organismo di valutazione delle conformità.

I risultati delle verifiche ispettive condotte dal QTSP sono condivisi con i responsabili di cui al par. *1.3* e con il management aziendale.

9 Condizioni generali

9.1 Tariffe

Le tariffe per il servizio di certificazione e di validazione temporale sono pubblicate sul sito del QTSP.

Per progetti specifici, le tariffe sono concordate a livello contrattuale con il singolo cliente.

L'accesso alle informazioni riguardanti lo stato del certificato (CRL e OCSP) è libero e gratuito.

Il QTSP mette a disposizione un software di verifica a titolo gratuito (https://www.intesa.it/e-trustcom/).

9.2 Responsabilità finanziaria - copertura assicurativa

Oltre a soddisfare il requisito minimo richiesto sul capitale sociale, INTESA è beneficiaria di contratti assicurativi per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è inviata ad AgID apposita dichiarazione di stipula.

9.3 Protezione delle informazioni confidenziali

Tutte le informazioni confidenziali di cui il QTSP INTESA viene in possesso nella gestione dei servizi oggetto di questo CPS sono conservate e trattate secondo la normativa vigente in tema di data privacy (D.Lgs. 196/03 e Reg. (UE) 2016/279 e loro ss.mm.ii.).

Sono considerate *Confidenziali* tutte le informazioni, personali o aziendali, che non compaiono sul certificato qualificato.

9.4 Protezione dei dati personali

Nella propria attività di QTSP per i servizi fiduciari oggetto di questo CPS, INTESA opera come *Titolare del trattamento dei dati personali*, ai sensi della normativa vigente in tema di data privacy (D.Lgs. 196/03 e Reg. (UE) 2016/279 e loro ss.mm.ii.).

Nello specifico, i dati personali trattati sono quelli raccolti in fase di identificazione e registrazione del Titolare.

9.5 Proprietà intellettuale

Il presente documento è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale: quanto qui descritto per l'espletamento delle attività di INTESA è coperto da diritti sulla proprietà intellettuale.

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

9.6 Obblighi

Nel seguito sono riportati gli obblighi cui devono sottostare i partecipanti alla PKI (par. *1.3*)

9.6.1 Obblighi del QTSP INTESA

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche (CAD)
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013 (DPCM)
- Regolamento (UE) 2016/679 (GDPR)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il QTSP INTESA:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'art. 29 del Reg. eIDAS;
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'art. 32 del CAD;
- informa i richiedenti, in modo esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni, in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza di INTESA) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.
- fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il QTSP INTESA:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati ai sensi dell'art. 42 del DPCM;
- indica un sistema di verifica della firma elettronica, di cui all'art. 14 del DPCM;
- mantiene copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di certificazione di cui all'art. 43 del DPCM, e la rende accessibile per via telematica come stabilito dall'art. 42, comma 3 del DPCM.

Il QTSP INTESA conduce periodicamente attività di ispezione (audit) presso la LRA per verificare che sia rispettato quanto previsto dalla normativa e dal presente CPS, nel pertinente Manuale Operativo, nonché di quanto riportato nel contratto di mandato, secondo un piano di campionamento condiviso con la LRA.

9.6.2 Obblighi del Titolare

Il Titolare al quale è stato attribuito un certificato qualificato per i servizi fiduciari del QTSP INTESA, oggetto nel presente CPS e descritti nel Manuale Operativo (MO) di riferimento, è tenuto a conservare le informazioni necessarie all'utilizzo della propria chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, art. 32, comma 1).

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo CPS e nel MO di riferimento;
- comunicare al QTSP INTESA, anche per tramite della LRA, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente CPS;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (art. 5, comma 5, del DPCM);
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma;
- revocare o sospendere il certificato digitale secondo quanto indicato nel presente CPS e nel MO di riferimento.

9.6.3 Obblighi degli utilizzatori dei certificati

L'Utilizzatore (*Relying Party*) è chiunque riceva un documento firmato digitalmente e, al fine di verificarne la validità, si avvalga del certificato qualificato utilizzato dal Titolare per firmare il documento stesso.

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in conformità al Reg. eIDAS.

Coloro che si avvalgono di un certificato qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato dagli standard vigenti al momento della sua emissione;
- verificare lo stato di validità del certificato mediante il protocollo OCSP o tramite l'accesso alle Liste di Revoca;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei QTSP;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

9.6.4 Obblighi del Terzo Interessato

Il Terzo Interessato, nei servizi oggetto del presente CPS, è tipicamente l'organizzazione (cliente) che stipula un contratto di fornitura di servizi fiduciari con il QTSP.

Il Terzo Interessato:

- autorizza formalmente il QTSP all'utilizzo del campo *organizationName* del certificato (par. 3.1.3.3)
- verifica che il Titolare sia in possesso di tutti i requisiti necessari e autorizza il medesimo a richiedere il rilascio del certificato qualificato di firma elettronica.
- indica al QTSP INTESA eventuali ulteriori limitazioni d'uso del certificato qualificato
- indica al QTSP INTESA eventuali titoli o poteri di rappresentanza del Titolare

Il Terzo Interessato si assume l'obbligo di richiedere la revoca del certificato nel caso in cui il titolare del certificato lasci l'organizzazione ovvero vengano meno i requisiti per cui è stato richiesto il certificato (ad es. subentri una variazione o cessazione dei poteri di rappresentanza)

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente comunicata alla CA quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato un certificato qualificato per la firma elettronica.

Il terzo interessato dovrà altresì comunicare ogni 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.

9.6.5 Obblighi delle LRA

INTESA, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale di ulteriori soggetti (nel seguito, *LRA – Local Registration Authority*) per svolgere una parte delle attività proprie dell'Ufficio di registrazione.

Tipicamente, una LRA è demandata ad espletare le seguenti attività:

- identificazione con certezza del richiedente la certificazione (titolare del certificato);
- registrazione del richiedente / Titolare;
- consegna al Titolare dei codici che gli permetteranno di accedere alla propria chiave di firma nel rispetto degli artt. 8 e 10 comma 2 del DPCM;
- invio della documentazione sottoscritta all'Ufficio RA di INTESA, salvo differenti accordi riportati sul contratto di mandato.

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere la LRA e sui quali INTESA ha l'obbligo di vigilare.

In particolare, si richiede alla LRA di:

- vigilare affinché l'attività di identificazione posta in essere si svolga nel rispetto della normativa vigente (CAD, DPCM, Reg. eIDAS ed eventualmente la normativa in materia di Antiriciclaggio);
- utilizzare e trattare i dati personali acquisiti in fase di identificazione in accordo con il GDPR;
- rendere disponibile ad INTESA il materiale raccolto nella fase di identificazione e registrazione.
- conservare in modo sicuro la documentazione raccolta nella fase di identificazione e registrazione, quindi inviarla all'Ufficio RA del QTSP INTESA su richiesta della QTSP stessa
- consentire l'accesso presso i propri locali di personale del QTSP, ovvero di terzi dallo stesso incaricati, per adempiere agli obblighi di ispezione (audit); tale accesso deve essere consentito anche agli auditor incaricati dall'Organismo di Vigilanza (AgID);
- segnalare senza indugio al QTSP INTESA, per tramite dell'Ufficio RA (*uff_ra@intesa.it*) ovvero dei propri riferimenti INTESA, ogni evento o incidente inerente i punti indicati precedentemente, nonché tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi oggetto del presente CPS e del Manuale Operativo di riferimento ovvero sui dati personali dei titolari.

9.7 Esclusione di garanzie

Non sono previsti ulteriori obblighi oltre a quelli riportati al par. *9.6.1*.

9.8 Limitazioni di responsabilità

Il QTSP INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, art. 13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'art. 5 del DPCM, e in particolare dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente CPS, nel Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

Parimenti, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

INTESA non sarà responsabile per i danni derivanti da un utilizzo non conforme del certificato qualificato in relazione alla limitazione d'uso specificata sul certificato stesso.

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

Se non altrimenti specificata, la limitazione di responsabilità è riportata nelle *Condizioni Generali di Contratto INTESA* (*www.intesa.it*).

9.9 Indennizzi

Se non altrimenti specificati, i termini di indennizzo sono riportati nelle *Condizioni Generali di Contratto INTESA* (*www.intesa.it*).

9.10 Termini e risoluzione del contratto

Se non altrimenti specificato, il Contratto avrà efficacia e decorrerà dalla sottoscrizione dello stesso. La Durata contrattuale è quella definita nello specifico Contratto di volta in volta.

Le clausole risolutive, se non altrimenti specificate, sono riportate nelle *Condizioni Generali di Contratto INTESA* (*www.intesa.it*).

9.11 Comunicazioni

Richieste di informazioni possono essere indirizzate ai riferimenti del QTSP, par.*1.3*.

9.12 Gestione delle modifiche

Vedi par. *1.5.1 - Procedura per le revisioni*.

9.13 Procedura per la risoluzione delle dispute

Per qualsiasi controversia sarà competente in via esclusiva il foro di Torino

9.14 Legge applicabile

La legislazione vigente è quella dello Stato italiano e della Comunità Europea.

9.15 Conformità alla normativa applicabile

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dalla normativa vigente e, in particolare, da:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche (CAD)
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013 (DPCM) ed eventuali ss.mm.ii.
- Regolamento (UE) 2016/679 (GDPR) ed eventuali ss.mm.ii.
- Regolamento (UE) 910/2014 (eIDAS) ed eventuali ss.mm.ii.

Un elenco più completo della normativa di riferimento è riportato al par. *1.6.2*.

10 Appendice: 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 QTSP INTESA fornisce l'applicazione ***DigitalSign Reader***.

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

- *https://www.intesa.it/e-trustcom/*

L'utilizzo del software è gratuito.

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

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

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

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

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

10.1.2 Piattaforma proprietaria DeSigner

Il QTSP 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 QTSP 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 firma / sigillo 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 QTSP INTESA.

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

- Verifica firma: tale funzione è analoga a quella descritta al par. *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 QTSP 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 QTSP INTESA permettono l'apposizione della firma elettronica, del sigillo elettronico 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.

Fine del documento