Certificati qualificati di Firma elettronica e Sigillo elettronico TI Trust Technologies CA eIDAS

CERTIFICATION PRACTICE STATEMENT

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione (sostituisce il precedente Manuale Operativo del QTSP TI Trust Technologies CERTQUAL.TT.SOMO16000.00)	10/04/2017
01	Aggiornamento dei riferimenti normativi in occasione dell'entrata in vigore del Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE	25/05/2018
02	• Incorporazione delle informazioni contenute ndegli Addendum seguenti (da considerarsi superati contestualmente alla pubblicazione del presente documento) o CERTQUAL.TT.SOMO17400.00 - Addendum Manuale Operativo CREDEM o CERTQUAL.TT.SOMO17999.00 - Addendum Manuale Operativo Cassa Risparmio Bolzano o CERTQUAL.TT.SOMO17700.00 - Addendum Manuale Operativo Banca del Piemonte o CERTQUAL.TT.SOMO16888.00 - Addendum Manuale Operativo Gruppo Crédit Agricole – (SELFIE) o CERTQUAL TT SOMO16777 00 - Addendum Manuale Operativo CartaLIS One-Shot o CERTQUAL.TT.SOMO14001.01 - Certificati di sottoscrizione per Banca Sella - Manuale Operativo Addendum o CERTQUAL.TT.SOMO14002.00 - Certificati di sottoscrizione per CREDEM - Manuale Operativo Addendum • Recepimento delle modifiche alla Deliberazione n. 45/2009 • Introduzione di un nuovo certificato di Certificazione	01/08/2018
03	• Revisione profilo certificati qualificati e precisazioni sull'utilizzo degli O.I.D. • Sostituzione AD	28/12/2018
04	• Modificato protocollo di accesso al registro dei certificati • Inseriti nuovi O.I.D.: • 1.3.76.16.5 per certificati rilasciati tramite identità Spid • 1.3.76.16.6 per certificati conformi alle raccomandazioni di cui alla DETERMINAZIONE N. 121/2019	06/09/2019
05	• Inserimento chiarimenti su O.I.D.e limitazioni di utilizzo dei certificati qualificati • Revisione informazioni contenute nei certificati qualificati per Sigillo Elettronico	18/12/2020

Indice degli argomenti

1 INTRODUZIONE

Telecom Italia Trust Technologies S.r.l. (nel seguito **TI Trust Technologies**, TI.TT o TSP, v. anche par. 1.3.1) opera come Certification Authority, gestore delle Identità Digitali in ambito SPID, gestore di servizi di PEC e Conservatore Accreditato. L'offerta di TI Trust Technologies si compone di diverse tipologie di Certificati e relativi servizi di gestione.

TI Trust Technologies è QTSP accreditato dall'aprile 2000 (come Saritel S.p.A., poi come I.T. Telecom S.p.A. ed, infine, come I.T. Telecom S.r.l.).

1.1 Scopo del documento

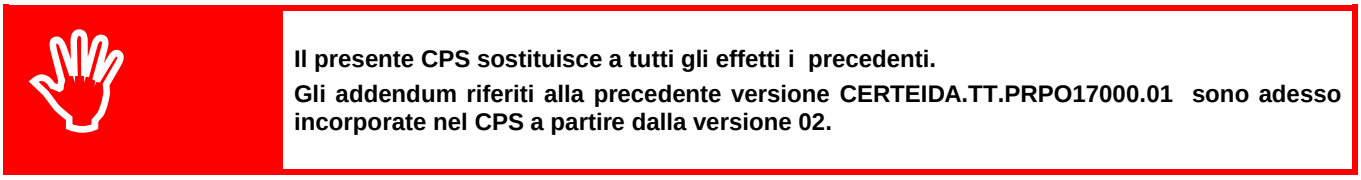
Il presente documento costituisce Certification Pratice Statement (di qui innanzi CPS) della Certification Authority di TI Trust Technologies. Conformemente a quanto previsto dal Regolamento eIDAS 910/2014 dell'UE illustra le modalità, i processi operativi, i ruoli, le responsabilità e le pratiche di tutti i soggetti coinvolti nel ciclo di vita, uso e gestione dei Certificati Qualificati di Firma elettronica e Sigillo elettronico emessi da TI Trust Technologies come Qualified Trust Service Provider in ambito eIDAS. Di seguito i certificati emessi dalla CA di TI Trust Technologies:

- *Certificati Qualificati di Firma elettronica custoditi su dispositivo QSCD*
- *Certificati Qualificati di Firma elettronica custoditi su dispositivo remoto QSCD*
- *Certificati Qualificati di Sigillo elettronico custoditi su dispositivo remoto QSCD*

Le procedure utilizzate per l'emissione dei Certificati Qualificati di Firma elettronica e Sigillo elettronico sono riportate sul sito https://www.trusttechnologies.it/.

La struttura ed il contenuto di questo CPS si basano sulla specifica pubblica RFC3647.

Completa tale documento una Certificate Policy (CP), che definisce il framework operativo per l'emissione e la gestione del ciclo di vita dei Certificati Qualificati (di Firma e Sigillo) emessi dalla Certification Authority TI Trust Technologies.



I servizi basati su certificati descritti nel presente CPS, sono erogati in tutto o in parte da TI Trust Technologies tramite specifiche ed idonee infrastrutture tecnologiche, come descritto nella seguente documentazione ed in altri documenti eventualmente in essa richiamati:

- il presente CPS
- le descrizioni delle tipologie di servizi pubblicate da TI Trust Technologies sul proprio sito https://www.trusttechnologies.it/download/documentazione;

Nell'ambito dei rapporti contrattuali si identificano i soggetti di seguito indicati:

- **Venditore**: soggetto che stipula il contratto di vendita dei servizi nei confronti del cliente finale e degli utilizzatori;
- **Cliente Finale o Cliente**: il soggetto che acquisisce tramite il venditore i servizi erogati da TI Trust Technologies;
- **Utilizzatore** (v. tabella al par. 1.3.3): il soggetto che usa i servizi erogato da TI Trust Technologies.

I servizi basati su certificati descritti nel presente CPS ed erogati da TI Trust Technologies sono regolati dalla documentazione di natura contrattuale descritta di seguito, cui si fa riferimento secondo l'ordine di prevalenza indicato in caso di contestazione o di discordanza tra le condizioni ed i termini convenuti tra le Parti:

1. Contratto di vendita del singolo servizio intercorrente tra il venditore ed il cliente finale;
2. Scheda di attivazione del servizio;
3. Modulo di accettazione delle condizioni di utilizzo del servizio e informativa privacy;
4. Condizioni specifiche per l'utilizzo del servizio;
5. Condizioni generali per l'utilizzo del servizio.

TI Trust Technologies rende disponibili le versioni aggiornate di tutta la documentazione rilevante da un punto di vista contrattuale mediante pubblicazione agli indirizzi seguenti (o comunque opportunamente ed idoneamente referenziati):

- https://www.trusttechnologies.it/download/documentazione/;
- https://www.trusttechnologies.it/download/legale-e-privacy/ .

1.2 Identificazione del CPS

L'OID per **TI Trust Technologies** è

{*iso(1) identified-organization(3) uninfo(76) telecomtrusttec (33)*}: **1.3.76.33**

Questo CPS è indicato, nei certificati, col seguente Object Identifier (OID): 1.3.76.33.1.1.**1** .

Il TSP definisce ed organizza i suoi OID per i certificati e documenti di cui al presente CPS (che potrà essere ulteriormente aggiornato), in conformità al Regolamento eIDAS e al *Codice dell'Amministrazione Digitale (CAD)*:

TI Trust Technologies	1.3.76.33
Trusted Service Provider	1.3.76.33.1
Certification Practice Statements	1.3.76.33.1.1
CPS TI Trust Technologies CA eIDAS	1.3.76.33.1.1.1
Certificati Qualificati di Firma elettronica custoditi su dispositivo remoto QSCD (conforme alla policy QCP-n-qscd 0.4.0.194112.1.2)	• 1.3.76.33.1.1.20[1] • 1.3.76.33.1.1.21 • 1.3.76.33.1.1.22 • 1.3.76.33.1.1.23 • 1.3.76.33.1.1.24 • 1.3.76.33.1.1.25 • 1.3.76.33.1.1.26 • 1.3.76.33.1.1.27 • 1.3.76.33.1.1.28 • 1.3.76.33.1.1.29
Certificati Qualificati di Firma elettronica custoditi su dispositivo QSCD (conforme alla policy QCP-n-qscd 0.4.0.194112.1.2)	1.3.76.33.1.1.1.10[2]
Certificati Qualificati di Sigillo elettronico custoditi su dispositivo remoto QSCD (conforme alla policy QCP-l-qscd 0.4.0.194112.1.3)	1.3.76.33.1.1.1.21[3]
Certificate Policies	1.3.76.33.1.2
Manuali Operativi	1.3.76.33.1.3
Manuale Operativo Certificati Qualificati di Firma Digitale ai sensi del D. Lgs. 82/2005, Marcatura Temporale, Carta Nazionale dei Servizi	1.3.76.33.1.3.10

OID aggiuntivi possono essere presenti nel certificato, anche ad indicare l'esistenza di limiti d'uso.

[1] Gli OID utilizzati nei servizi di firma remota variano in base alla finalità, alle modalità di identificazione dei Titolari ed alle modalità di utilizzo del certificato. Si veda il paragrafo 4.5.3 per ulteriori approfondimenti.
[2] L'OID ***1.3.76.33.1.1.1.10*** è in uso a partire dal ***10/10/2018***. I certificati qualificati su QSCD emessi fino a tale data contengono l'OID 1.3.76.33.1.1.1
[3] l'O.I.D. indicato può essere abbinato agli altri O.I.D. previsti per i Certificati Qualificati per Firma Elettronica quando la modalità operativa di utilizzo è la stessa (ad es. procedure automatiche di firma). Si veda il paragrafo 4.5.3 per ulteriori approfondimenti.

1.3 Partecipanti alla PKI

1.3.1 Certification Authority

La **Certification Authority** è il soggetto terzo e fidato che emette i certificati, firmandoli con le proprie chiavi private (chiavi di CA). La CA, inoltre, gestisce lo stato dei certificati.

Nell'ambito del servizio qui descritto, il ruolo di CA è svolto da **TI Trust Technologies**, identificata come segue e referenziata nel resto del documento come "CA TI Trust Technologies":

Denominazione sociale:	Telecom Italia Trust Technologies S.r.l.
Indirizzo della sede legale:	S. R.148 Pontina Km.29,100 – 00071 Pomezia
Legale rappresentante:	Salvatore Nappi (Amministratore Delegato)
P.IVA e Codice Fiscale:	04599340967
N° di telefono per contatti o richieste di revoca:	800 28 75 24
ISO Object Identifier (OID):	1.3.76.33
Sito web generale (informativo):	https://www.trusttechnologies.it/
Indirizzo di posta elettronica:	CRPresidio_CA@telecomitalia.it

1.3.2 Registration Authority

La Registration Authority (RA) è il soggetto (persona, struttura od organizzazione) che svolge le seguenti attività:

- accoglimento e validazione delle richieste di emissione e gestione dei certificati,
- registrazione del Titolare (v. par. 1.3.3) e del Cliente Finale,
- autorizzazione all'emissione, da parte della CA, del certificato richiesto,
- fornitura al *subject* del certificato e o degli eventuali strumenti e informazioni per il suo utilizzo.

L'attività di RA è svolta da Incaricati appartenenti all'organizzazione di TI Trust Technologies, ovvero della CA, a seguito di un adeguato addestramento del personale impiegato. Può essere svolta da Incaricati non appartenenti alla CA, persone fisiche o giuridiche cui viene affidato tramite delega lo svolgimento delle attività di identificazione del Soggetto richiedente (si veda in proposito quanto contenuto nel par.3.2.3).

Per l'emissione dei certificati qualificati di Firma e Sigillo la CA TI Trust Technologies obbliga i soggetti richiedenti al rispetto di tutti i requisiti applicabili indicati dal *Regolamento* eIDAS (ed incorporati per riferimento dalla CA stessa).

1.3.3 Titolare (Subject) ed altri soggetti

Nel presente CPS si individuano i soggetti seguenti:

Titolare **(anche menzionato come "utilizzatore")**	Soggetto che possiede la chiave privata del certificato, associata alla relativa chiave pubblica. Può essere una delle tipolgie seguenti: a) la persona fisica, oppure b) la persona fisica associata ad una persona giuridica, oppure c) la persona giuridica (anche identificata come elemento a sé state associato ad un'organizzazione), oppure d) la persona che esercita la libera professione Il Titolare è identificato nel certificato al campo **"SUBJECT"** (il Titolare può anche non coincidere con il Cliente Finale menzionato al par. 1.1 o con il Richiedente)
Richiedente	È il soggetto che per proprio conto o per conto di altri richiede un certificato, sottoscrivendo la modulistica di attivazione, sulla base di uno specifico legame esistente e comprovabile di associazione/rappresentanza con il Titolare. Nell'ambito della normativa ETSI di riferimento è individuato come il "**SUBSCRIBER**".
Soggetto che fa affidamento sui servizi o sulle informazioni contenute nel	È il soggetto che nella normativa ETSI è identificato come **Relying Party** e che fa affidamento sulle informazioni contenute in un certificato di firma elettronica o di sigillo emesso da TI Trust Technologies.

certificato	
Terzo interessato	È la persona fisica o giuridica o l'Ente che presta attesta le informazioni riguardanti l'appartenenza del Titolare ad una determinata organizzazione, l'abilitazione a svolgere determinate attività ovvero la detenzione di poteri di rappresentanza e/o cariche afferenti il Titolare o il Cliente finale.

A completamento di quanto indicato nella tabella che precede, si specificano le casistiche seguenti:

a) Un certificato di cui sia Titolare una persona fisica, può essere richiesto dai soggetti seguenti:
   i. la persona fisica stessa; oppure
   ii. una persona fisica diversa con idoneo potere di rappresentanza legale; oppure
   un qualunque altro soggetto che può rappresentare legalmente la persona giuridica individuata nel campo "Organizzazione" del certificato, cui la persona fisica Titolare è riferita;

b) Un certificato di cui sia Titolare una persona giuridica, può essere richiesto dai soggetti seguenti:
   i. un qualunque soggetto con idoneo potere di rappresentanza legale della persona giuridica; oppure
   ii. un legale rappresentante della persona giuridica che acquista il servizio in favore di sue controllate o di sue unità o di suoi dipartimenti.

Allo scopo di evitare ogni genere di conflitto di interesse, il richiedente e il soggetto che opera come RA sono soggetti distinti, salvo il caso in cui quest'ultima stia richiedendo un certificato per se stessa o un certificato di cui sia Titolare una persona ad essa associata o collegata.

1.3.4 Terze Parti

TI Trust Technologies identifica i fornitori critici ai fini dell'erogazione del servizio e, applicando specifiche politiche nel rispetto delle policy di Gruppo, assicura che i controlli per la sicurezza, le definizioni di servizio e i livelli di erogazione inclusi negli accordi di erogazione di servizi di terze parti, siano attuati, condotti e mantenuti attivi.

Inoltre tutti cambiamenti relativi all'erogazione di servizi di terze parti sono originati e supervisionati dalla Direzione tenendo in considerazione la criticità dei sistemi relativi al business e dei processi coinvolti.

1.4 Uso dei certificati

Ogni uso dei certificati qualificati di firma e sigillo, emessi da TI Trust Technologies, che violi quanto riportato dal presente CPS è proibito e comporta, qualora TI Trust Technologies ne venga a conoscenza, la revoca immediata del certificato.

Si assume che tutti i soggetti coinvolti nell'utilizzo di un certificato posseggano le competenze e gli strumenti necessari per il suo uso appropriato, come di seguito descritto.

1.4.1 Uso appropriato del certificato

I certificati qualificati rilasciati dalla CA TI Trust Technologies possono essere utilizzati per le transazioni che richiedono:

- Non ripudio (*Non-Repudiation*)

L'uso non autorizzato di certificati può comportare un annullamento delle garanzie offerte dalla CA TI Trust Technologies agli utenti e parti coinvolte.

1.4.2 Uso proibito del certificato

L'uso del certificato è limitato a quanto specificato nel presente CPS e dalle condizioni per il suo utilizzo (v. par. 1.1 e cap. 9) e comunque a quanto specificato nell'estensione *keyUsage* del certificato. Qualsiasi utilizzo in contrasto con quanto definito non è permesso.

1.4.3 Formato del certificato

La composizione dei Certificati Qualificati emessi dalla Certification Authority TI Trust Technologies è conforme allo standard X.509 v3 secondo la specifica RFC-5280

Lo standard definisce il formato dei certificati qualificati basati su sistemi di crittografia a chiave pubblica, ma non specifica un particolare algoritmo di crittografia.

Nello standard X.509 v3 un certificato si compone dei seguenti campi:

- Versione;
- Numero seriale;
- ID dell'algoritmo di firma;
- Nome di chi ha emesso il certificato;
- Periodo di validità;
- Nome dell'utente;

- Informazioni sulla chiave pubblica dell'utente;
- Identificatore (unico) dell'emittente (versione 2 e 3);
- Identificatore (unico) dell'utente (versione 2 e 3);
- Estensioni (solo versione 3);
- Firma dei campi precedenti.

Il certificato è firmato dall'emittente per autenticare il legame tra i campi descrittivi del certificato (in particolare il nome del soggetto) e la chiave pubblica del soggetto.

La valorizzazione dei campi che compongono i certificati avviene secondo le Linee Guida AgID [Det. 121/2019], contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate".

La conformità alle Linee Guida AgID è dichiarata all'interno dei certificati attraverso la codifica, nel campo CertificatePolicies (OID 2.5.29.32), di un elemento PolicyIdentifier con valore AgIDcert (OID 1.3.76.16.6).

1.4.3.1 Caratteristiche comuni

Tutti i titolari di certificato sono individuati da un ***Distinguished Name* chiaro ed univoco**, conforme al corrispondente standard X.500. Il *distinguished name* deve essere riconoscibile come nome di persona o entità. L'utilizzo di pseudonimi nel common name relativo al *distinguished name* del certificato, è soggetto a valutazione da parte di TI Trust Technologies.

TI Trust Technologies non emette certificati anonimi.

TI Trust Technologies emette Certificati qualificati caratterizzati da campi contenenti i valori sotto indicati:

- il campo emittente (*Issuer*) è caratterizzato da questi valori:
  - **CN** = **TI Trust Technologies < *identificativo della CA* >**
  - **O = Telecom Italia Trust Technologies S.r.l.**
  - **OU = Servizi di certificazione**
  - **C = IT**
- il campo *Subject* per le cui caratteristiche si rimanda al paragrafo 3.1;
- nel campo *estensioni* vengono inserite informazioni addizionali (ad esempio sulla policy di certificazione o sulle restrizioni per l'utilizzo della chiave).

1.4.3.2 Estensioni del certificato

La composizione dei Certificati qualificati emessi dalla Certification Authority TI Trust Technologies è conforme allo standard X.509 v3.

TI Trust Technologies utilizza alcune estensioni secondo la definizione della International Standards Organisation (ISO). Tali estensioni possono limitare il ruolo e la posizione di un certificato; ad esempio l'estensione *keyUsage* limita i fini tecnici per i quali può essere utilizzata una chiave in un certificato.

Per tutti i certificati dovranno essere almeno comprese le estensioni:

- *Certificate Policy*
- *cRLDistribution Point*
- *authorityInformationAccess*
- *basicConstraints*
- *keyUsage*

Per i dettagli si rimanda al paragrafo 7.1.

1.5 Amministrazione del CPS

Questo CPS è redatto, pubblicato ed aggiornato da TI Trust Technologies. Inoltre è sottoposto a revisione (almeno) annuale per garantire la conformità ai requisiti previsti dal *Regolamento* eIDAS e dal *Codice dell'Amministrazione Digitale (CAD)*.

Richieste di informazioni o chiarimenti sul presente CPS possono essere inoltrate via posta elettronica all'indirizzo CRPresidio_CA@telecomitalia.it .

Questo CPS è approvato dalla Direzione di TI Trust Technologies, previo consulto con le funzioni aziendali coinvolte nell'erogazione del servizio.

1.6 Definizioni e acronimi

AgID	Agenzia per l'Italia Digitale
CA	Certification Authority
CC	**Common Criteria**: criteri per la valutazione della sicurezza nei sistemi informatici.
CDP	CRL Distribution Point
CP	Certificate Policy
CPS	Certification Practice Statement
CRL	Certificate Revocation List
CSL	Certificate Suspension List
CS	Centro Servizi
CSR	Certificate Signing Request
DN	Distinguished Name
eIDAS	electronic IDentification Authentication and Signature
FIPS	Federal Information Processing Standard
HSM	Hardware Security Module
HTTP	**Hyper-Text Transfer Protocol**: protocollo di trasmissione che permette lo scambio di file su World Wide Web.
HTTPS	**Secure Hyper-Text Transfer Protocol**: protocollo di trasmissione che permette la cifratura e decifrazione dei dati trasmessi (durante la consultazione di siti e pagine Internet). Corrisponde ad un'estensione del protocollo Internet standard HTTP (Hypertext Transfer Protocol), attraverso il protocollo SSL.
ISO	**International Standards Organization**: organizzazione internazionale per la standardizzazione. Ha stabilito numerosi standard nell'area dei sistemi informativi (l'ANSI-American National Standards Institute è uno dei principali organismi appartenenti all'ISO).
ITSEC	**Information Technology Security Evaluation Criteria**: criteri europei per la valutazione della sicurezza nei sistemi informatici.
ITU	**International Telecommunication Union**: organizzazione internazionale che funge da ente regolatore per gli standard nelle telecomunicazioni.
ITU–T	ITU–Telecommunication Sector
OCSP	**On-line Certificate Status Protocol**: protocollo utilizzato dalle applicazioni per determinare lo stato di un certificato (può essere utilizzato per soddisfare alcuni requisiti operativi fornendo informazioni di revoca più attuale possibile che con CRL e può anche essere utilizzato per ottenere ulteriori informazioni di stato).
OID	**Object Identifier**: sequenza numerica univoca che identifica un oggetto (struttura, algoritmo, parametro, sistema) nell'ambito di una gerarchia generale definita dall'ISO.
PIN	**Personal Identification Number**: codice di sicurezza riservato che permette l'attivazione delle funzioni del dispositivo di firma.
PDF	Portable Document Format
PKCS	**Public Key Cryptography Standard**: standard tecnici per applicazioni crittografiche, realizzati dalla RSA Data Security Inc.
PKI	**Public Key Infrastructure**: infrastruttura informatica costituita da applicazioni che utilizzano tecniche crittografiche a chiave pubblica (include servizi di generazione e distribuzione di chiavi, emissione e pubblicazione di certificati, gestione dei registri dei certificati emessi e delle liste di sospensione e revoca, altri servizi come l'emissione di marche temporali).
Portale	Applicazione Web attraverso la quale il Cliente eroga I propri servizi
QSCD	Qualified Signature Creation Device
QTSP	Qualified Trusted Service Provider
RA	Registration Authority
RFC	**Request For Comments**: definizioni scritte di protocolli o standard in uso su Internet emessi dalla Internet Engineering Task Force (IETF).
SSCD	Secure Signature Creation Device
SSL	**Secure Socket Layer**: protocollo standard per la gestione di transazioni sicure su Internet, basato sull'utilizzo di algoritmi crittografici a chiave pubblica.
X.509	**Recommendation X.509**: specifica ITU-T che definisce la struttura e la terminologia da utilizzare per la compilazione dei certificati e delle liste di revoca/sospensione ad essi associate.

1.7 Riferimenti

Riferimento	Descrizione
[TUDA]	DPR 445/2000 Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa.
[CAD]	“Decreto Legislativo 26 agosto 2016, n. 179 Modifiche ed integrazioni al Codice dell'amministrazione digitale, di cui al decreto legislativo 7 marzo 2005, n. 82, ai sensi dell'articolo 1 della legge 7 agosto 2015, n. 124, in materia di riorganizzazione delle amministrazioni pubbliche”.
[Regolamento eIDAS]	“Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE”.
[Normativa Privacy]	Regolamento Generale sulla Protezione dei Dati n. 2016/679/UE e s.m.i. Decreto Legislativo 30 giugno 2003, n. 196, “Codice in materia di protezione dei dati personali”, pubblicato nel Supplemento Ordinario n.123 della Gazzetta Ufficiale n. 174, 29 luglio 2003 e s.m.i.
[Codice Penale]	Fattispecie di reato applicabili ai seguenti ambiti: • Falsità in sigilli o strumenti o segni di autenticazione, certificazione o riconoscimento (capo II) • Falsità in atti (capo III) • Falsità personale, con particolare riguardo agli art. 495 bis (Falsa dichiarazione o attestazione al QTSP di firma elettronica sull’identità o su qualità personali proprie o di altri), art. 495 ter (Fraudolente alterazioni per impedire l'identificazione o l'accertamento di qualita' personali), art. 496 (False dichiarazioni sulla identità o su qualità personali proprie o di altri).
[RFC2251]	"Lightweight Directory Access Protocol (v3)", (http://www.ietf.org/rfc/rfc2251.txt)
[RFC2986]	"PKCS #10: Certification Request Syntax Specification Version 1.7", (http://www.ietf.org/rfc/rfc2986.txt)
[RFC6960]	“Online Certificate Status Protocol - OCSP”, (http://www.ietf.org/rfc/rfc6960.txt)
[RFC3647]	"Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", (http://www.ietf.org/rfc/rfc3647.txt)
[RFC5280]	"Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile", (http://www.ietf.org/rfc/rfc5280.txt)
[RFC6818]	“Updates to the Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile”, (http://www.ietf.org/rfc/rfc6818.txt)
[X.509]	ITU-T Recommendation X.509 (2005)|ISO/IEC 9594-8:2005, Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.
[ETSI TS 101 862]	“Qualified Certificate profile”.
[ETSI TS 102 280]	“X.509 V.3 Certificate Profile for Certificates Issued to Natural Persons”.
[ETSI EN 319 412-1]	“Electronic Signatures and Infrastructures; Certificate Profiles; Part 1: Overview and common data structures”.
[ETSI EN 319 412-2]	“Electronic Signatures and Infrastructures; Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons”.
[ETSI EN 319 412-3]	“Electronic Signatures and Infrastructures; Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons”.
[ETSI EN 319 412-5]	“Electronic Signatures and Infrastructures; Certificate Profiles; Part 5: QCStatements”.
[ETSI TS 101 456]	“Electronic Signatures and Infrastructures; Policy requirements for certification authorities issuing qualified certificates”.
[Requisiti per la Nomina]	CERTQUAL.TT.PRPO17999.00 - Requirement Incaricati esterni – Contiene i riferimenti ed i requirement fissati dai riferimenti normativi applicabili: • eIDAS, art. 24, c. 1.2 e lett. a) • eIDAS, art. 24, c. 2 lett. b) • DM 20/6/12 n. 145 artt. 1, 3 e 5 • eIDAS, art. 24, c. 2, lett. c)

	• [ETSI 319 411-2] Clause 6.4.4 e [ETSI 319 401] Clause 7.2 • [ETSI 319 411-2] Clause 6.5.6 e [ETSI 319 401] Clause 7.7 • [ETSI 319 411-2] Clause 6.5.7, [ETSI 319 401] Clause 7.8 e [ETSI 319 411-1] Clause 6.5.7 a e b • [ETSI 319 411-2] Clause 6.8.4 e [ETSI 319 401] Clause 7.13
[Det. 189/2017]	Modifiche alla Deliberazione n. 45 del 21 maggio 2009
[Avviso 17]	Avviso n. 17 - Utilizzo identità digitali SPID al fine di rilasciare certificati qualificati
[Det. 121/2019]	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.

2 PUBBLICAZIONI E REPOSITORY

Per “repository” si intende un insieme di archivi o registri on-line contenenti informazioni di interesse pubblico relative ai certificati e al servizio di emissione e gestione degli stessi descritto in questo CPS.

2.1 Gestione del repository

Il “repository” di TI.TT è costituito dal sito web che gestisce in proprio e di cui è direttamente responsabile, disponibile all’indirizzo web https://www.trusttechnologies.it/download/documentazione/.

La CA gestisce in proprio il repository e ne è direttamente responsabile.

2.2 Informazioni pubblicate

La CA pubblica almeno la seguente documentazione sul proprio sito web:

- Certification Practice Statement (CPS)
- Certificate Policy (CP)
- Condizioni generali di utilizzo dei servizi
- Modulistica

La CA, inoltre, pubblica le CRL e, ove previsto, i certificati.

Ulteriori informazioni sulle CRL si rimanda alla sezione 4.10.

2.3 Tempi e frequenza delle pubblicazioni

TI.TT notifica con un preavviso di 30 giorni solari le modifiche che intende apportare al CPS, pubblicando nella sezione del sito in cui è disponibile una apposita nota informativa.

Allo scadere del preavviso il nuovo CPS e, se necessario anche la documentazione annessa, vengono pubblicati sul sito web di TI.TT.

Eventuali modifche che non influiscono sull’attuazione della CP o sull’accetabilità dei certificati saranno effettuate senza nessuna informativa preventiva.

I certificati vengono pubblicati – quando richiesto del Titolare – al momento della loro emissione.

2.4 Controllo degli accessi

L’accesso al repository in sola lettura (“read-only”) è completamente libero per chiunque.

L’accesso al repository per la pubblicazione di informazioni nuove o aggiornate è possibile solo da postazioni di lavoro attestate sulla medesima rete del repository, previa autenticazione.

3 IDENTIFICAZIONE ED AUTENTICAZIONE

3.1 Regole di Naming

Tutti i titolari di certificato sono individuati da un *distinguishedName* (DN) chiaro ed univoco, conforme al corrispondente standard X.500. Il *distinguishedName* deve essere riconoscibile come nome di persona (fisica o giuridica) o entità.

Il campo *subject* del certificato contiene informazioni facilmente comprensibili che consentono l'individuazione del titolare del certificato. Sono consentiti pseudonimi o nomi diversi dall'effettiva denominazione sociale (o altra denominazione ufficiale) del Titolare: in tal caso la CA TI Trust Technologies si riserva di valutare singolarmente le richieste di emissione di certificati contenenti pseudonimi.

La CA TI Trust Technologies rilascia certificati qualificati ai richiedenti che presentano una richiesta opportunamente documentata contenente un nome verificabile.

I Richiedenti non possono utilizzare nelle richieste di certificazione nomi che violino diritti di proprietà intellettuale di altri. TI Trust Technologies rimarrà estranea a qualsivoglia controversia riguardante la proprietà dei nomi, né si adopererà per risolvere eventuali controversie riguardanti la proprietà di nomi commerciali, marchi commerciali o di servizi. TI Trust Technologies si riserva la facoltà di respingere una richiesta di certificazione e di revocare un certificato a fronte di una tale controversia.

3.1.1 Contenuti dei certificati qualificati

I Certificati qualificati emessi dalla CA TI Trust Technologies e oggetto del presente CPS sono conformi alla normativa vigente e, in particolare, alle specifiche [RFC5280] e [RFC6818] ed alle specifiche [ETSI TS 101 862] V1.3.3, recante "Profilo dei Certificati Qualificati" e [ETSI TS 102 280] V1.1.1, recante "Profilo dei certificati X.509 V.3 per certificati rilasciati a persone fisiche" e successive modificazioni ed integrazioni.

Inoltre, sono conformi al [Regolamento eIDAS] e agli standard [ETSI EN 319 412-2] V2.1.1 (Electronic Signatures and Infrastructures;Certificate Profiles;Part 2:Certificate profile for certificates issued to natural persons), [ETSI EN 319 412-3] V1.1.1 (Electronic Signatures and Infrastructures;Certificate Profiles;Part 3:Certificate profile for certificates issued to legal persons) e [ETSI EN 319 412-5] V2.1.1 (Electronic Signatures and Infrastructures;Certificate Profiles;Part 5:QCStatements).

Di seguito sono elencati i dati standard riportati nei certificati, secondo quanto previsto dalla normativa:

- indicazione che si tratta di un certificato qualificato di firma elettronica ovvero di sigillo elettronico;
- numero di serie del certificato;
- ragione o denominazione sociale del TSP qualificato e Stato nel quale è stabilito;
- codice identificativo univoco del Titolare presso il TSP;
- nome, cognome e codice fiscale (o uno pseudonimo chiaramente indicato come tale[4]) ovvero ragione o denominazione sociale del Titolare (ove applicabile);
- eventuali poteri di rappresentanza;
- eventuali abilitazioni professionali;
- valore della chiave pubblica;
- algoritmi crittografici utilizzati per l'emissione del certificato;
- data di inizio e fine della validità del certificato;
- tipologia di utilizzo delle chiavi;
- firma elettronica avanzata o sigillo elettronico del TSP che ha rilasciato il certificato.

Su richiesta del Titolare o del terzo interessato il certificato può contenere le seguenti informazioni, purché pertinenti allo scopo per il quale il certificato é richiesto:

- **qualifiche specifiche del Titolare**, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza;
- **limiti d'uso del certificato**. Ai sensi dell'art. 12, comma 6, lettera c) della [DLB 45/09], la CA TI Trust Technologies, su richiesta del Titolare o della persona giuridica che ha richiesto il certificato, prevede la possibilità di inserire all'interno del certificato qualificato i seguenti limiti d'uso:
    a. Il Titolare fa uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato;
    b. Il certificato è valido solo per firme apposte con procedura automatica. La dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati.
    c. L'utilizzo del certificato è limitato ai rapporti con [*indicare il soggetto*]
    d. Qualunque altra limitazione d'uso, concordata con il QTSP (*max 200 caratteri*);
- **limiti del valore** degli atti unilaterali e dei contratti per i quali il certificato può essere usato, ove applicabili.

[4] L'ammissibilità dell'uso di pseudonimi è valutata caso per caso dalla CA.

3.2 Validazione iniziale dell'identità

Questo paragrafo descrive le procedure utilizzate per l'identificazione del richiedente al momento della richiesta di emissione del certificato qualificato.

La procedura di identificazione comporta che il richiedente sia riconosciuto dalla CA TI Trust Technologies, attraverso la RA o un suo Incaricato, che ne verificherà l'identità attraverso una delle modalità definite nel presente CPS.

3.2.1 Dimostrazione del possesso della chiave privata

Nell'ambito dei propri servizi, la CA TI Trust Technologies non consente la generazione da parte dei Titolari o dei Richiedenti di coppie di chiavi per sottoscrizione. Il possesso ed il controllo delle chiavi private è garantito dalle modalità di consegna al Titolare dei dispositivi e/o delle relative credenziali.

3.2.2 Autenticazione dell'organizzazione richiedente

Nel caso di Certificati Qualificati di Sigillo elettronico l'identità dell'organizzazione è verificata tramite la consultazione del database della CCIAA (Camera di Commercio, Industria e Artigianato) o, nel caso di Pubbliche Amministrazioni, dell'Indice delle Pubbliche Amministrazioni (IPA).

Nel caso di mancata corrispondenza, la richiesta di certificato è respinta.

Tale verifica non è prevista per il rilascio dei Certificati Qualificati di Firma elettronica.

3.2.3 Identificazione del Richiedente persona fisica

Se non diversamente disposto dal presente CPS e in connessione con il [Regolamento eIDAS] si applicano le seguenti regole.

I certificati possono essere emessi soltanto dopo l'identificazione del Richiedente. L'identificazione è effettuata dal QTSP tramite gli Incaricati, i quali possono essere:

- *afferenti all'organizzazione della CA TI Trust Technologies*
- *afferenti alla struttura del Cliente*

Gli Incaricati afferenti all'organizzazione della CA TI Trust Technologies possono identificare qualsiasi soggetto richiedente.

Gli Incaricati afferenti alla struttura del Cliente possono identificare e registrare i seguenti soggetti richiedenti, secondo i casi riportati in tabella.

INCARICATI DEL CLIENTE / RICHIEDENTI	Privato[5]	P.A.[6]
Soggetti appartenenti alla struttura del Cliente	SI	SI
Soggetti Terzi con rapporto contrattuale con il Cliente	Solo per Clienti [DL 385/93][7] o [Regolamento eIDAS art.24, comma 1 e 2] [8]	SI
Soggetti Terzi senza rapporto contrattuale con il Cliente	NO	SI

Tabella 1: Soggetti richiedenti identificabili da Incaricati afferenti alla struttura del Cliente

In ogni caso, l'autenticazione delle richieste di emissione nonché l'autorizzazione all'emissione dei certificati sono responsabilità della CA TI Trust Technologies, nella persona del responsabile della Registrazione dei Titolari.

Gli Incaricati effettuano l'identificazione e la registrazione secondo le modalità previste nel presente CPS per le seguenti categorie di soggetti

a. richiedente il certificato in qualità di **persona fisica non appartenente ad alcuna organizzazione**:

I. il richiedente, purché abbia compiuto il diciottesimo anno di età, sottopone la sua richiesta di adesione all'Incaricato che provvede ad accertare la sua identità mediante l'esibizione in originale di uno dei documenti

[5] Il Cliente è una persona fisica o una persona giuridica privata.

[6] Il Cliente è un soggetto o un Ente della Pubblica Amministrazione.

[7] Il Cliente e le sue strutture sono dotati dei requisiti di onorabilità richiesti ai soggetti che svolgono funzione di amministrazione, direzione e controllo presso le banche di cui all'art. 26 del Testo Unico delle leggi in materia bancaria e creditizia (cfr.[DL385/93] e successive modificazioni), oppure sono tenuti ad effettuare nell'ambito delle loro attività statutarie attività di identificazione dei propri utenti con livelli di robustezza pari o superiori a quanto effettuato dal Certificatore o dalle predette aziende..

[8] Il Cliente e le sue strutture soddisfano i requisiti espressi in [Requisiti per la Nomina].

d'identificazione indicati dall'art. 35 del [TUDA] in corso di validità. Il richiedente esibisce anche il Codice Fiscale in originale.

II. I richiedenti residenti all'estero, purché abbiano compiuto il diciottesimo anno di età, ai fini dell'identificazione esibiscono in originale un documento in corso di validità valido ai fine della verifica dell'identità[9]:. Inoltre, devono esibire il codice fiscale rilasciato loro in Italia, oppure, in mancanza di esso il codice fiscale rilasciato dall'autorità fiscale del paese di residenza o, in mancanza, un analogo codice identificativo, quale ad esempio un codice di previdenza sociale o un codice identificativo generale. In mancanza di tale codice identificativo potrà essere utilizzato il numero del passaporto.

b. richiedente il certificato in qualità di **persona fisica appartenente ad un'organizzazione**:

III. il richiedente, oltre alla documentazione di cui al punto a., deve fornire anche la documentazione necessaria all'identificazione dell'organizzazione a cui appartiene. Quando il Richidente appartiene alla stessa organizzazione degli Incaricati, tale documentazione non viene raccolta.

In entrambi i casi il richiedente può richiedere un certificato in cui sia specificato:

- l'eventuale ruolo di **rappresentante e/o delegato di una persona fisica e/o giuridica**;
- l'eventuale **potere di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite**;
- l'eventuale **denominazione o marchio registrato**.

In questi casi il richiedente deve produrre alla CA TI Trust Technologies la documentazione che attesti il consenso del Terzo Interessato. L'eventuale utilizzo di marchi richiede la produzione al QTSP della documentazione comprovante la loro titolarità/registrazione.

3.2.3.1 ID-VISU Identificazione del Richiedente mediante esibizione 'a vista' di un documento di identità ('de visu')

In questa modalità di identificazione il Richiedente viene identificato '*de visu*' dall'Incaricato della CA TI Trust Technologies, ossia di persona tramite esibizione a vista di un valido documento d'identità. L'Incaricato provvede poi a verificare la validità della documentazione fornita dal Richiedente.

L'identificazione può essere effettuata anche da parte di un Pubblico Ufficiale in base a quanto disposto dalle normative che disciplinano la loro attività (ad es. dichiarazione sostitutiva di atto notorio): in tal caso il Richiedente compila la richiesta di certificazione e la sottoscrive di fronte al Pubblico Ufficiale, facendo autenticare la propria firma ai sensi delle normative vigenti; la richiesta è poi presentata alla CA TI Trust Technologies (o ad un suo Incaricato).

3.2.3.2 ID-SIGN Identificazione del Richiedente mediante utilizzo della firma elettronica qualificata emessa da un TSP qualificato

In questa modalità di identificazione la CA TI Trust Technologies si basa sul riconoscimento già effettuato da un altro Qualified TSP che ha emesso il certificato qualificato, utilizzato dal Richiedente per firmare digitalmente la richiesta (in formato elettronico) di certificazione. L'Incaricato della CA TI Trust Technologies provvede a verificare la corrispondenza tra i dati contenuti nel certificato qualificato e quelli forniti dal Richiedente nella richiesta.

In conformità all' [Avviso 17], qualora il certificato qualificato in questione sia stato rilasciato tramite identità digitale SPID, questa modalità di Identificazione avrà come effetto l'inserimento nel nuovo certificato qualificato dell'OID 1.3.76.16.5, registrato a cura dell'Agenzia, con la seguente limitazione d'uso: "Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require others SPID digital identity";

3.2.3.3 ID-OTHER Identificazione del Richiedente mediante modalità alternative

Rientrano in questa tipologia tutte quelle modalità alternative di identificazione che prevedono l'utilizzo di procedure analoghe eseguite da soggetti destinatari degli obblighi di Identificazione e Adeguata Verifica, ai sensi delle normative vigenti, di recepimento della Direttiva 2005/60/CE del Parlamento Europeo e del Consiglio, relative alla prevenzione dell'uso del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo, e delle successive ulteriori normative comunitarie di esecuzione.

Con specifico riferimento al contesto italiano, i soggetti destinatari degli obblighi acquisiscono i dati in base a procedure definite in autonomia nel rispetto di quanto previsto dal D.Lgs. 231/2007 e s.m.i., oppure alle analoghe procedure adottate secondo le norme antiriciclaggio vigenti alla data dell'identificazione oppure in conformità ad ulteriori normative che consentono di pervenire alla verifica dell'identità in modo conforme alla normativa a cui fa riferimento il QTSP.

Secondo le suddette normative, le aziende che operano in ambito finanziario sono tenute "ad acquisire i dati identificativi e ad effettuare il riscontro su una copia - acquisita tramite fax, a mezzo posta, in formato elettronico o con modalità analoghe - di un documento di identità non scaduto" e a provvedere ad "un'ulteriore verifica dei dati acquisiti secondo le modalità ritenute più opportune, in relazione al rischio specifico".

[9] Si fa riferimento al database PRADO pubblicato dalla Commissione Europea per quanto concerne i cittadini provenienti dai paesi UE. Per cittadini extra-UE si valuterà caso per caso l'idoneità del documento ai fini delle verifiche richieste al QTSP.

A titolo esemplificativo e non esaustivo, l'ulteriore verifica può essere effettuata con le seguenti modalità riferite all'ambito bancario:

- Bonifico: Ricezione di un Bonifico bancario da conto corrente di altro Istituto Bancario di cui il Titolare risulti intestatario (in modalità tali da assolvere gli obblighi a carico della Banca in materia di esecuzione degli obblighi di adeguata verifica della clientela)
- Selfie + welcome call: il Richiedente invia alla Banca, in modalità elettronica, la fotografia di due documenti d'identità e un selfie, tutte eseguite contestualmente all'esecuzione dell'operazione, senza poter richiamare immagini già preventivamente memorizzate sul proprio device. La Banca, per mezzo degli Addetti del proprio backoffice, si accerta dell'autenticità delle informazioni fornite sia eseguendo una serie di controlli su banche dati proprie e pubbliche (quali SCIPAFI per il controllo del documenti di identità), sia effettuando una chiamata telefonica al richiedente ("welcome call") con la richiesta di una serie di informazioni a conferma di quanto rilevato tramite Portale.

Questa modalità di identificazione è applicabile esclusivamente all'emissione di Certificati il cui utilizzo è limitato ai rapporti fra il Titolare ed il Cliente o qualsiasi ente controllato o altro ente per conto del quale sono erogati prodotti o servizi.

La limitazione di utilizzo è realizzata sia attraverso l'inserimento nel certificato del testo (in lingua Italiana ed Inglese) che ne descrive il contesto, sia applicativamente impedendo l'utilizzo dei certificati al di fuori del contesto previsto.

3.2.3.4 ID-VIDEO Identificazione del Richiedente da remoto, mediante procedura audio-video

Nella modalità di identificazione del richiedente tramite sessione web remota, le operazioni di identificazione e di registrazione, avvengono nel corso di una sessione audio video registrata automaticamente, alla quale il richiedente partecipa assieme ad un operatore incaricato designato da TI Trust Technologies. Il richiedente opera utilizzando un opportuno dispositivo dotato delle necessarie prestazioni (quali ad es. PC, smart TV, smartphone, altro device mobile e/o analoghi) collegato ad una webcam e ad un sistema audio funzionanti.

Prima dell'avvio della sessione, l'operatore si identifica con il suo numero operatore e chiede il consenso alla registrazione. Il richiedente compila con i propri dati anagrafici la modulistica on line (v. par. 3.2.3) e presta il proprio consenso alla video registrazione del processo di identificazione, nel corso del quale:

1. l'operatore chiede di mostrare un documento di identità in corso di validità, sul quale sia presente una foto recente e riconoscibile, una firma autografa, un timbro di un'Amministrazione dello Stato;
2. l'operatore verifica in aggiunta anche l'esattezza del numero di cellulare e l'indirizzo e-mail dichiarati dal richiedente tramite una OTP (one time password) inviata via SMS o via email;
3. l'operatore chiede all'utente di effettuare azioni casuali (così come definito nelle procedure interne del QTSP, classificate come riservate);
4. l'operatore chiede all'utente di esprimere espressa volontà a dotarsi di firma digitale;
5. il sistema utilizzato dal QTSP registra in idoneo formato elettronico l'intera sessione di identificazione e di validazione dei dati, appone ad essa la propria firma digitale ed una marcatura temporale e la sottopone al processo di conservazione a norma, per la durata necessaria. Si precisa che i dati conservati dal QTSP constano del file audio-video della sessione e dei relativi metadati strutturati in formato elettronico. La loro conservazione in forma protetta per la durata richiesta, risponde ai requisiti indicati all'art. 32, comma 3, lettera j) del CAD.

Ad identificazione completata i dati confermati nella sessione remota, sono utilizzati per l'emissione del certificato di firma digitale remota, previa accettazioni delle condizioni contrattuali. Tale modalità soddisfa quanto richiesto dall'art. 32, comma 3, lettera a) del CAD relativamente alla certezza della identificazione della persona che fa richiesta della certificazione.

3.2.4 Identificazione del Richiedente persona giuridica

L'identificazione del Richiedente persona giuridica viene effettuata da una persona fisica identificata con una delle modalità previste (cfr. 3.2.3). Il Richiedente presenta la documentazione relativa alla persona giuridica (cfr. 3.2.2) e la documentazione attestante i poteri di rappresentanza conferiti alla persona fisica: visura camerale (rilasciata da una CCIAA) o, in alternativa, della copia dell'atto notarile di procura legale (firmata dal Richiedente).

3.2.5 Ulteriori verifiche svolte dalla CA TI Trust Technologies

La policy di TI Trust Technologies è limitata dalle Leggi sulla protezione dei dati e dei consumatori e dalle limitazioni di garanzia applicabili, come esposto in questo CPS (cfr. sezione 9).

La CA TI Trust Technologies si riserva la facoltà di effettuare ulteriori verifiche con modalità non prestabilite.

3.2.6 Informazioni non verificate dalla CA TI Trust Technologies per l'emissione dei certificati

La CA TI Trust Technologies non verifica gli indirizzi di posta elettronica indicati nelle richieste di emissione dei certificati.

In generale, la CA TI Trust Technologies non verifica la correttezza delle informazioni ricevute dal Richiedente che non sono destinate ad essere incluse in campi critici del certificato (ai fini della sicurezza) e che non sono necessarie per l'emissione e successiva gestione del certificato.

3.2.7 Dati archiviati per la registrazione del Richiedente

La CA TI Trust Technologies registra tutte le informazioni utilizzate per verificare l'identità del Richiedente e mantiene i dati del contratto e qualsiasi informazione e/o documentazione a supporto della registrazione del Richiedente, che includono anche ma non sono limitati a:

- Condizioni di Utilizzo dei Servizi;
- Dichiarazione del Richiedente che le informazioni contenute nel certificato sono corrette e complete;
- Nome e Cognome del Richiedente (persona fisica);
- Nome completo e forma giuridica della persona giuridica o altra entità organizzativa;
- Tutte le pertinenti informazioni di registrazione esistenti (ad esempio, registrazione della società) della persona giuridica o altra entità organizzativa.

3.3 Identificazione e Autenticazione per le richieste di rinnovo

Le attività di identificazione e di autenticazione in caso di rinnovo si svolgono in maniera simile a quella per le richieste di prima emissione, descritta nel paragrafo 3.2 del presente CPS.

Nei casi di certificati custoditi su dispositivi gestiti da CA TI Trust Technologies, è possibile procedere al riemissione dei certificati prima della scadenza, senza specifica richiesta da parte del Titolare, allo scopo di garantire la continuità dei servizi erogati.

Nel caso in cui i dati di identificazione del Titolare contenuti nella prima richiesta non abbiano subito modifiche, è sufficiente effettuare una richiesta di rinnovo della certificazione.

3.3.1 Identificazione e Autenticazione per rinnovo dopo la revoca

Nel caso di rinnovo successivo alla revoca, si procede sempre come per la validazione iniziale dell'identità (3.2).

3.4 Identificazione e Autenticazione per le richieste di revoca

La modalità di identificazione ed autenticazione delle richieste di sospensione o revoca dipende dal canale usato per la richiesta:

- per poter inoltrare richieste di sospensione o revoca attraverso il canale di comunicazione sicuro predisposto dalla CA TI Trust Technologies, è necessario disporre delle credenziali (che sono fornite in fase di registrazione);
- nel caso delle richieste di sospensione o revoca inviate alla CA TI Trust Technologies, si procede come descritto nel paragrafo 3.2.3.

4 REQUISITI OPERATIVI DI GESTIONE DEI CERTIFICATI

Se non diversamente disposto dal presente CPS in connessione con il [Regolamento eIDAS], i seguenti requisiti operativi si applicano al ciclo di vita dei certificati.

Tutte le entità all'interno del dominio TI Trust Technologies (RA, Subscribers o altri partecipanti) hanno il dovere continuo di informare la CA TI Trust Technologies di tutte le variazioni delle informazioni presenti in un certificato durante il periodo operativo del certificato e fino a che non scade o viene revocato.

La CA TI Trust Technologies emette, revoca o sospende i certificati solo a seguito di richieste autenticate ed approvate.

4.1 Richiesta del certificato

4.1.1 Modalità base

Per la richiesta di certificati qualificati il cui titolare sia una **persona fisica**, all'atto della registrazione il Richiedente deve fornire all'Incaricato almeno le seguenti informazioni:

- Nome e cognome;
- Codice Fiscale o analogo codice identificativo (v. par. 3.2.3);
- Luogo e Data di nascita;
- Estremi del documento di riconoscimento presentato per l'identificazione;

- Indirizzo e-mail ed eventuale numero di telefonia mobile, per le comunicazioni dalla CA TI Trust Technologies al Soggetto;
- Eventuale documentazione per la richiesta di certificati in cui sia specificato ruolo, titolo o potere di rappresentanza.

Per la richiesta di certificati qualificati il cui titolare sia una **persona giuridica**, all'atto della registrazione il Richiedente – individuato nel legale rappresentante o persona fisica dotata di procura – deve fornire all'Incaricato almeno le seguenti informazioni:

- Nome e cognome del Richiedente;
- Codice Fiscale o analogo codice identificativo del Richiedente (v. par. 3.2.3);
- Estremi del documento di riconoscimento presentato per l'identificazione del Richiedente;
- Indirizzo e-mail per le comunicazioni dalla CA TI Trust Technologies al Richiedente;
- Nome del Soggetto persona giuridica;
- Partita IVA ovvero numero di Registro Imprese per soggetti italiani, VAT code o altro identificativo per soggetti stranieri;
- Sede legale della persona giuridica.

I dati di registrazione raccolti sono utilizzati per la generazione del certificato del Titolare e per le comunicazioni del QTSP, in conformità a quanto disposto dalla normativa vigente.

Il Richiedente, all'atto della richiesta attesta:

- di aver preso **visione del presente CPS** e aver **ricevuto informazioni accurate e complete** riguardo al servizio di certificazione;
- di conoscere i **principi generali** di funzionamento del servizio;
- di conoscere gli **obblighi** e le **responsabilità** che egli assume in merito alla protezione della segretezza della chiave privata e alla conservazione e uso dei dispositivi di firma, previsti dalla legge;
- il consenso al trattamento dei suoi dati, secondo quanto previsto dalla [Normativa Privacy], nei limiti e modi riportati nel capitolo 9 del presente documento e illustrati nell'informativa fornita al Titolare.

L'Incaricato all'atto della richiesta attesta:

- che il Richiedente questi è la persona identificata e che ha richiesto il servizio;
- che le informazioni fornite, fatte salve quelle che non può verificare di persona (ad es. ruoli, titoli e incarichi da esso ricoperti), sono accurate.

Una volta terminata la fase di registrazione l'Incaricato non ha alcun ulteriore obbligo di verifica della validità delle informazioni relative al Richiedente e contenute nel Certificato.

Nel caso di Titolare distinto dal Richiedente i requisiti sopra elencati sono soddisfatti dal Titolare. Il Cliente ed il Titolare sono tenuti ad accettare Condizioni di utilizzo dei Servizi.

4.1.2 Modalità multifase

Qusta modalità viene utilizzata quando il contesto operativo e la finalità della firma richiedono che questa sia disponibile ed utilizzabile prima che tutte le verifiche previste sull'identità del Titolare siano state completate.

Questa modalità si avvale generalmente di un Portale del Cliente per acquisire le richieste di attivazione dei Servizi (Tipicamente Finanziari) ed esporre e rendere scaricabile per il Titolare le condizioni contrattuali per l'utilizzo della firma elettronica qualificata. In questo modo il Cliente consente propri Titolari di effettuare operazioni (ad es.i apertura di conti correnti) senza doversi necessariamente recare fisicamente in una filiale o sede.

Conclusa con successo la fase di apertura del Servizio, le usuali operazioni saranno svolte dal Titolare usando i servizi offerti dal Portale.

4.1.2.1 Fasi di attivazione del certificato

Il processo di attivazione del certificato prevede le seguenti fasi:

1) *Compilazione del form di attivazione del Servizio.* Il Titolare/Richiedente accede al Portale e compila il form di attivazione del Servizio, inserendo i dati anagrafici, il numero telefonico, e-mail e gli altri dati richiesti dal fornitore del servizio. Tramite lo stesso Portale, il Titolare/Richiedente può consultare e scaricare le condizioni contrattuali per l'utilizzo della firma digitale;
2) *Emissione del certificato digitale e firma della documentazione.* Il Portale richiede al QTSP di generare un certificato digitale qualificato che viene emesso ed immediatamente sospeso. Esso sarà utilizzato per la firma della richiesta del Servizio, della documentazione prevista dal QTSP per l'emissione del certificato e per eventuali servizi accessori.

3) *Verifica dell'identità del Richiedente:* Tutte le informazioni raccolte dal Portale saranno verificate dagli Addetti del Cliente. La verifica dell'identità del richiedente viene effettuata secondo una delle modalità previste al par. 3.2.3.3
4) *Attivazione definitiva del Certificato Digitale.* A seguito dell'esecuzione con successo di tutte le verifiche previste, il fornitore del servizio richiede al QTSP l'attivazione definitiva del certificato digitale, che potrà essere usato dal Titolare/Richiedente per le operazioni di firma eseguite sul Portale.
5) *Revoca del Certificato Digitale.* In caso di mancato superamento delle verifiche, oppure di cessazione del rapporto contrattuale tra Titolare e Cliente, il Cliente richiede al QTSP la revoca del certificato digitale, che non potrà più essere usato dal Titolare/Richiedente in nessuna circostanza. In caso di mancato richiesta di attivazione del certificato da parte del Cliente entro 60 giorni dalla sua emissione, il QTSP revoca automaticamente il certificato.

4.1.2.2 Limitazioni d'uso nei certificati

La modalità multifase è applicabile esclusivamente in presenza di Certificati contenenti limiti d'uso (in lingua Italiana ed Inglese) ai rapporti fra il Titolare ed il Cliente o qualsiasi ente controllato o altro ente per conto del quale sono erogati prodotti o servizi.

4.2 Elaborazione delle richieste

Alla ricezione di una richiesta di certificazione la RA svolge opportune attività di verifica:

- provvede al censimento del richiedente nel database di registrazione;
- verifica che le informazioni identificative contenute nella CSR siano coerenti con quelle fornite nel modulo di richiesta;
- verifica l'identità del richiedente ed il suo possesso della chiave privata corrispondente alla CSR, come descritto nella sezione 3.2;
- verifica la coerenza fra i dati contenuti nella richiesta e quelli riportati sulla documentazione ricevuta;
- verifica l'univocità del nome X.500 (*Distinguished Name*) nell'ambito dei certificati emessi dalla CA;
- effettua, se necessario, ulteriori controlli.

4.3 Emissione del certificato

Se le verifiche di cui alla sezione precedente vengono superate, la RA invia alla CA TI Trust Technologies una richiesta di emissione del certificato.

Dopo l'approvazione di una richiesta di registrazione, la CA TI Trust Technologies emette il certificato firmandolo con una propria chiave di certificazione.

Contestualmente all'emissione del certificato, ove previsto, la CA TI Trust Technologies lo pubblica nel registro dei certificati che ha emesso. Le modalità di gestione del registro dei certificati sono riportate in 4.3.3.

La generazione di un certificato è registrata nel giornale di controllo della CA TI Trust Technologies. La traccia dell'avvenimento è conservata per almeno venti anni dalla data di emissione del certificato, secondo quanto previsto dalla normativa.

Emettendo il certificato, la CA TI Trust Technologies garantisce al Titolare che:

- il certificato non contiene errori o inesattezze originati dal QTSP o giunti in qualsiasi modo a conoscenza della CA TI Trust Technologies;
- il certificato è conforme a tutti i requisiti illustrati nel presente CPS, nonché a quanto richiesto dalla normativa vigente;
- l'esecuzione di tutte le procedure finalizzate al rilascio del certificato da parte dell'organizzazione della CA TI Trust Technologies è stata eseguita a regola d'arte.

Ogni certificato, emesso in seguito alla richiesta di registrazione da parte del relativo Titolare, è inserito in un dispositivo sicuro di firma contenente la chiave privata relativa alla chiave pubblica riportata nel certificato medesimo.

4.3.1 Emissione del certificato su dispositivo QSCD custodito dal Titolare

La coppia di chiavi crittografiche viene generata direttamente su dispositivo sicuro di firma – censito preventivamente dalla CA TI Trust Technologies, consegnato materialmente al Titolare e mantenuto sotto il suo controllo esclusivo (ad esempio, smartcard o Token USB) – utilizzando le applicazioni messe a disposizione dalla CA TI Trust Technologies, previa autenticazione sicura.

In questo contesto operativo, il QTSP consegna al Titolare un "KIT" per l'utilizzo del servizio che comprende:

- un dispositivo sicuro di firma (smartcard con lettore o token USB) e,
- i codici riservati per l'utilizzo del certificato (PIN e PUK).

La verifica dell'identità del Titolare al momento della consegna del KIT è effettuata direttamente dalla CA TI Trust Technologies o per il tramite di suoi incaricati (cfr. sezione 3).

4.3.2 Emissione del certificato su dispositivo QSCD custodito dalla CA TI Trust Technologies

La coppia di chiavi crittografiche viene generata direttamente su dispositivo sicuro di firma centralizzato – Hardware Security Module (HSM) – attivabile esclusivamente dal Titolare solo a seguito di un'**autenticazione forte**, effettuata mediante una delle seguenti modalità:

- **Mobile**
- **Token OTP**
- **SMS OTP**
- **Biometrica**
- **semplificata**

In questo contesto operativo, al momento della sua identificazione e registrazione, al Titolare viene associato un dato identificativo verificabile mediante un'autenticazione forte e, ove previsto, gli vengono consegnati i codici segreti per l'utilizzo del servizio.

In base alla modalità di autenticazione forte utilizzata, sono previste differenti tipologie di attivazione e utilizzo del servizio, come descritto di seguito.

4.3.2.1 Con autenticazione *Mobile*

Al momento della registrazione, al Titolare viene associata un'**utenza telefonica cellulare** e consegnata una busta contenente i codici segreti per l'utilizzo del servizio.

Nella fase di autenticazione forte (dell'operazione di firma), grazie alle prestazioni tecnologiche della rete radiomobile, la CA TI Trust Technologies effettua la verifica dell'identità del Titolare accertandosi che egli stia usando esattamente l'utenza telefonica cellulare che ha dichiarato al momento della sua registrazione. A tal fine, il Titolare esegue una chiamata ad un **Numero Verde** dall'utenza telefonica cellulare ad egli associata e digita in post selezione un codice numerico OTP. Il **codice OTP** è una password dinamica valida per un periodo di tempo definito, che identifica in modo univoco la transazione ed il richiedente.

Nei casi in cui sia necessaria una maggiore garanzia dell'identità del Titolare, è possibile eseguire l'autenticazione forte mediante ***outgoing call*** (chiamata, eseguita dalla CA TI Trust Technologies, all'utenza telefonica dichiarata dal Titolare).

4.3.2.2 Con autenticazione *tramite Token OTP*

Al momento della registrazione, al Titolare viene associato **il numero seriale univoco di un Token OTP** a lui consegnato insieme alla busta contenente i codici segreti per l'utilizzo del servizio.

Nella fase di autenticazione forte (dell'operazione di firma), la CA TI Trust Technologies accerta l'identità del Titolare, verificando l'associazione del codice OTP generato dal Token utilizzato al numero seriale dello stesso.

Il Token può essere anche di tipo software (ad esempio App per dispositivo mobile); in questo caso il seriale univoco viene sostituito da analogo codice generato da una procedura ad-hoc di attivazione del Token.

4.3.2.3 Con autenticazione *tramite SMS OTP*

Al momento della registrazione, al Titolare viene associata un'**utenza telefonica cellulare**.

Nella fase di autenticazione forte (dell'operazione di firma), la CA TI Trust Technologies genera un codice OTP e lo invia tramite SMS all'utenza telonica cellulare registrata sul sistema; il Titolare inserisce l'OTP ricevuto nell'applicazione di firma e la CA TI Trust Technologies ne accerta l'identità verificando che l'OTP corrisponda con quello inviato.

E' prevista la possibilità di fare scegliere al Titolare il PIN di firma.

I codici segreti che completano il servizio (PUK, Codice di revoca) vengono inviati al Titolare tramite email e/o SMS ai contatti verificati in fase di attivazione del certificato.

4.3.2.4 Con autenticazione *Biometrica*

Al momento della registrazione, al Titolare viene associato un insieme di **informazioni caratteristiche della sua firma autografa**, rilevate da un apposito **dispositivo di tipo *grafometrico*** e consegnata una busta contenente i codici segreti per l'utilizzo del servizio.

Nella fase di autenticazione forte (dell'operazione di firma), il Titolare dovrà apporre su un dispositivo grafometrico la propria firma autografa per consentire alla CA TI Trust Technologies di verificarne la corrispondenza alle informazioni rilevate per essa al momento della registrazione[10].

Per l'autenticazione forte Biometrica è prevista le possibilità di non distribuire ai Titolari i codici segreti per l'utilizzo del servizio al momento della registrazione. In tal caso:

- nell'operazione di firma, il Titolare appone la propria firma autografa esclusivamente su un dispositivo grafometrico installato presso una postazione presidiata da un addetto dell'organizzazione del Cliente o della CA TI Trust Technologies che accerta direttamente l'identità del Titolare e, dunque, non viene effettuata la verifica del codice PIN;
- l'utilizzo della firma del Titolare viene limitato ("*Firma per Scopo*"). A tal fine, nei certificati dei Titolari sarà presente un limite d'uso (cfr. par. 4.5.2).

[10] Sebbene con una terminologia impropria, si parla diffusamente di Firma Digitale Biometrica.

4.3.2.5 Con autenticazione *semplificata*

In aderenza alla prescrizione nazionale specificata nelle "linee guida per la conformità del sistema e degli strumenti di autenticazione utilizzati nella generazione della firma elettronica – CAD art. 35 comma 5" (Rif. 4) pubblicate da AgID, è prevista la possibilità di utilizzare metodi di autenticazione alternativi che, pur mantenendo le caratteristiche di sicurezza richieste dalla natura del servizio, semplificano l'utilizzo dello strumento di firma.

Il QTSP, con l'obiettivo di favorire la diffusione della firma digitale, ha provveduto ad adeguare l'esperienza d'uso in favore dell'utente, comunque garantendogli il controllo esclusivo della chiave utilizzata per la generazione della firma.

Tali metodi di autenticazione si caratterizzano nel fatto che per poter attivare una firma remota è necessario fornire al dispositivo di firma un PIN segreto, previa verifica di un ulteriore fattore di autenticazione, nel nostro caso:

- Firma Biometrica
- Chiamata telefonica effettuata da/verso un dispositivo registrato
- OTP generato da un token hardware
- OTP ricevuto dal titolare via SMS o App

I contesti d'uso dove questi metodi di autenticazione sono utilizzabili sono specifici e circoscritti a limitati rapporti tra titolare e proprio fornitore di servizio (banca/correntista – assicurazione/assicurato - …) .

La semplificazione nasce dalla condivisione di uno dei fattori di autenticazione fra il sistema di firma e le applicazioni del Cliente, che già lo utilizzano per l'autenticazione preventiva per l'accesso da parte del Titolare al proprio Portale,

In tutti i contesti d'uso previsti l'SSCD è comunque sempre custodito e gestito dal QTSP che ne garantisce l'integrità come previsto dai livelli di sicurezza logica e fisica già dichiarati nel proprio Piano della Sicurezza.

4.3.3 Registro dei Certificati

4.3.3.1 Gestione e Sicurezza

Nel Registro dei Certificati sono registrate le seguenti attività della CA TI Trust Technologies:

- pubblicazione dei certificati emessi, ove richiesto dal Titolare;
- sospensione dei certificati;
- riabilitazione dei certificati sospesi;
- revoca dei certificati.

La gestione del registro è attuata in conformità con le norme vigenti. In particolare:

- le registrazioni sono conservate per il periodo previsto dalla normativa in funzione della tipologia di registrazione e con le modalità richieste;
- i certificati emessi sono pubblicati solo se richiesto esplicitamente dal Titolare. In tal caso, il Titolare deve inviare l'apposito modulo, disponibile sul sito della CA TI Trust Technologies (https://www.trusttechnologies.it), firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione, seguendo la procedura descritta sul sito stesso.

Nel registro dei certificati sono presenti i seguenti elementi:

- i certificati emessi dalla CA TI Trust Technologies, per la cui pubblicazione, se prevista, i Titolari hanno espresso liberamente esplicito consenso;
- la lista dei certificati revocati o CRL;
- la lista dei certificati sospesi o CSL (che coincide con la lista dei certificati revocati, la CRL).

Il registro dei certificati è accessibile secondo le modalità previste dalla normativa e descritte in 4.3.3.2 del presente documento.

L'effettuazione delle operazioni che modificano il contenuto del registro dei certificati è possibile solo per il personale espressamente autorizzato della CA TI Trust Technologies. In particolare, il ***Responsabile della conduzione tecnica dei sistemi, del Sistema di Riferimento Temporale e della sicurezza dei dati e dei log*** incaricato dalla CA TI Trust Technologies, garantisce la corretta gestione del registro dei certificati e i processi di pubblicazione, sospensione e revoca dei certificati.

Tutte le attività di modifica del registro dei certificati sono opportunamente segnalate e archiviate dalla CA TI Trust Technologies. Inoltre sono annotati i seguenti eventi relativi al registro:

- la data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il registro dei certificati non risulta accessibile dall'esterno;
- ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile.

Il registro dei certificati è tenuto in doppia copia e almeno una copia di sicurezza della copia operativa e di quella di riferimento del registro dei certificati è conservata in armadi di sicurezza distinti, situati in locali diversi da quelli dei dispositivi tecnologici della CA TI Trust Technologies.

Il registro dei certificati viene aggiornato in maniera automatica ogni volta che viene emesso un certificato o una lista dei certificati sospesi o revocati.

4.3.3.2 Accesso e Consultazione

Le modalità di accesso al registro dei certificati sono stabilite in conformità con le norme vigenti.

Il registro dei certificati è pubblicato sotto forma di *url http accessibili pubblicamente.* L'accesso avviene tramite rete Internet all'indirizzo DNS del sito Web della CA TI Trust Technologies, nonché nell'Elenco Pubblico dei Certificatori tenuto da AgID, ai sensi della normativa vigente.

Il registro dei certificati può essere consultato mediante il protocollo HTTPS collegandosi all'indirizzo *https://www.trusttechnologies.it/registrocertificati*.

4.4 Accettazione del certificato

Il Richiedente deve informare la CA TI Trust Technologies di eventuali imprecisioni o difetti in un certificato subito dopo il ricevimento del certificato o comunicare precedentemente le informazioni da includere nel certificato.

L'uso pubblico del certificato, anche se temporaneo, implica in ogni caso l'accettazione del certificato da parte del titolare.

La CA TI Trust Technologies mette a disposizione del Titolare gli strumenti e le informazioni per l'utilizzo del servizio sia direttamente sia per il tramite di un Incaricato, sempre curandosi di accertare l'identità del Titolare. All'atto della consegna il Titolare sottoscrive una dichiarazione per attestare l'avvenuta ricezione degli strumenti e delle informazioni per l'utilizzo del servizio.

Gli strumenti e le informazioni per l'utilizzo del servizio sono posti nella disponibilità dei rispettivi Titolari con modalità sicure, allo scopo di garantire che nessuna persona, ad eccezione del Titolare, possa venirne contemporaneamente in possesso.

I codici segreti per l'utilizzo dei dispositivi di firma sono costituiti da:

- codice segreto di **attivazione del dispositivo** (codice **PIN**);
- codice segreto di **sblocco del dispositivo** (codice **PUK**, quando applicabile, in relazione alle modalità di erogazione del servizio);
- codice segreto di **revoca del certificato (ove previsto)**;
- ove previste, credenziali di accesso per l'utilizzo del sistema di comunicazione sicuro con la CA TI Trust Technologies, tramite rete Internet (cfr. 4.9).

Dal momento in cui li riceve, il Titolare è l'unico responsabile della protezione della segretezza di tali codici.

4.5 Uso della coppia di chiavi e del certificato

Il Titolare deve proteggere la propria chiave privata, avendo cura di evitare la divulgazione a terzi; se presente, deve custodire il dispositivo di firma (QSCD), ovvero gli strumenti di autenticazione per la firma (remota) in maniera; inoltre, deve conservare le informazioni di abilitazione all'uso della chiave privata separatamente dal dispositivo.

Nelle Condizioni di utilizzo dei servizi, la CA TI Trust Technologies sono evidenziati gli obblighi del Titolare rispetto alla protezione della chiave privata.

Le chiavi private devono essere utilizzate solo come specificato nel campo *keyUsage* come indicato nel relativo certificato.

Le chiavi private generate all'interno di dispositivi sicuri di firma non possono essere in alcun caso esportate, pertanto il loro utilizzo può avvenire solo all'interno del dispositivo che le custodisce.

4.5.1 Uso del certificato da parte del Soggetto che fa affidamento sui servizi o sulle informazioni contenute nel certificato

Il Soggetto che fa affidamento sui servizi o sulle informazioni contenute nel certificato deve conoscere l'ambito di utilizzo del certificato riportati nel presente CPS e nel certificato stesso.

Deve verificare la validità del certificato controllando, all'interno delle relative liste, che lo stesso non risulti sospeso o revocato.

Deve inoltre verificare l'esistenza ed il contenuto di eventuali limitazioni d'uso della coppia di chiavi, poteri di rappresentanza ed abilitazioni professionali.

4.5.2 Limiti d'uso e di valore

TITT garantisce la possibilità di inserire all'interno dei certificati qualificati almeno i limiti d'uso seguenti (fra parentese la versione in lingua inglese):

- *I titolari fanno uso del certificato solo per le finalità di lavoro per le quali esso è rilasciato. (The certificate holder must use the certificate only for the purposes for which it is issued.)*

- *Il presente certificato è valido solo per firme apposte con procedura automatica. La presente dichiarazione costituisce evidenza dell'adozione di tale procedura per i documenti firmati. (The certificate may be used only for automatic procedure signature purposes.)*
- *L'utilizzo del certificato è limitato ai rapporti con* <indicazione del soggetto>*. (The certificate may be used only for relations with the* <declare the subject>*.)*

Eventuali ulteriori limiti d'uso possono essere concordati con i Clienti.

4.5.3 Descrizione degli OID utilizzati nei servizi di firma remota

La tabella seguente elenca gli OID dei certificati qualificati di firma elettronica e sigillo elettronico con la descrizione della relativa modalità operativa di utilizzo:

OID	***Descrizione modalità operativa di utilizzo***
1.3.76.33.1.1.20	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata mediante il telefono del titolare ed* emessi in conformità alla normativa italiana sulla Firma Digitale, emessi in conformità alla normativa italiana sulla Firma Digitale. L'autenticazione può essere effettuata attraverso chiamata telefonica oppure OTP gestito con apposita App per dispositivi mobili (smartOTP).
1.3.76.33.1.1.21	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *utilizzate in procedure automatiche*, emessi in conformità alla normativa italiana sulla Firma Digitale.
1.3.76.33.1.1.22	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata mediante tecnologia biometrica*, emessi in conformità alla normativa italiana sulla Firma Digitale.
1.3.76.33.1.1.23	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *utilizzate in procedure automatiche per incaricati di identificazione*, emessi in conformità alla normativa italiana sulla Firma Digitale.
1.3.76.33.1.1.24	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata mediante OTP del cliente e il telefono del titolare* emessi in conformità alla normativa italiana sulla Firma Digitale.
1.3.76.33.1.1.25	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata mediante OTP via SMS del titolare*, emessi in conformità alla normativa italiana sulla Firma Digitale. I certificati nascono sospesi e vengono attivati in seguito alla conferma da parte del cliente.
1.3.76.33.1.1.26	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata con strumenti del cliente e con limite d'uso,* emessi in conformità alla normativa italiana sulla Firma Digitale. I certificati nascono sospesi e vengono attivati in seguito alla conferma da parte del cliente.
1.3.76.33.1.1.27	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata attraverso il cellulare del titolare e con limite d'uso,* emessi in conformità alla normativa italiana sulla Firma Digitale. I certificati nascono sospesi e vengono attivati in seguito alla conferma da parte del cliente. I certificati sono utilizzati per un'unica firma, per questo definiti "one-shot".
1.3.76.33.1.1.28 *1.3.76.33.1.1.29*	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su HSM *con autenticazione effettuata attraverso il cellulare del titolare e con limite d'uso,* emessi in conformità alla normativa italiana sulla Firma Digitale. I certificati nascono sospesi e vengono attivati in seguito alla conferma da parte del cliente dell'identità del titolare effettuata attraverso selfie, upload di documenti di identità e welcome call di verifica, registrata ed archiviata. I Certificati non sono utilizzabili al di fuori del contesto applicativo indicato nella limitazione d'uso.

Quando il certificato qualificato contenente uno dei sopramenzionati O.I.D. è rilasciato ad una persona giuridica, il certificato contiene anche lo O.I.D. specifico per il sigillo elettronico (1.3.76.33.1.1.1.21).

In ogni caso la natura del soggetto (persona fisica o persona giuridica) al quale è stato rilasciato il certificato qualificato è sempre univocamente individuabile dalla presenza dell'O.I.D. della corrispondente policy prescritta dalla norma ETSI EN 319 411-2:

- *Persone fisica - QCP-n-qscd - 0.4.0.194112.1.2*
- *Persone giuridica - QCP-l-qscd - 0.4.0.194112.1.3*

4.6 Rinnovo del certificato

Il Certificato ha una data di scadenza, oltre la quale perde ogni validità.

4.6.1 Rinnovo del certificato su dispositivo QSCD custodito dal Titolare

Per un certificato di questa tipologia, a scadenza, deve essere effettuata una nuova emissione in modalità analoga alla prima.

Nel caso in cui i dati di identificazione del Titolare contenuti nel modulo di richiesta di registrazione utilizzato in precedenza per l'emissione del certificato e per le comunicazioni con il Titolare non abbiano subito modifiche rispetto alla prima emissione, è sufficiente effettuare una nuova emissione con **richiesta di rinnovo della certificazione**.

L'emissione del nuovo certificato può avvenire sia utilizzando lo stesso dispositivo di firma sia mediante uno nuovo. In ogni caso si prevede la certificazione di una nuova coppia di chiavi generate anch'esse con le modalità già descritte.

4.6.2 Rinnovo del certificato su dispositivo QSCD custodito dalla CA TI Trust Technologies

Nel caso del servizio erogato in modalità remota, la nuova emissione avviene generando una nuova coppia di chiavi e comunicando al Titolare, ove previsto, le nuove informazioni necessarie per l'uso del servizio.

4.7 Rigenerazione della chiave (re-key)

Nel caso in cui il Titolare decida di utilizzare una nuova chiave, egli deve necessariamente fare richiesta di un corrispondente nuovo certificato.

4.8 Modifica del certificato

Un certificato, essendo firmato dalla CA emittente, non può essere modificato. Per rimediare ad eventuali errori nella generazione del certificato, dunque, è necessario emetterne uno nuovo (e revocare quello errato, per evidenti ragioni di sicurezza).

Nel caso in cui il certificato emesso contenga informazioni errate a causa di errori commessi dalla CA o dalla RA, il certificato errato sarà revocato e ne verrà emesso uno corretto, sollecitamente, senza oneri aggiuntivi per il cliente e senza richiedere ulteriori informazioni al cliente.

Nel caso in cui il certificato emesso contenga informazioni errate a causa di errori commessi dal richiedente (ad esempio, errata compilazione di uno o più campi del modulo di richiesta), il certificato errato sarà revocato.

4.9 Sospensione e Revoca del certificato

La sospensione determina un blocco temporaneo della validità di un certificato, a partire da un dato momento (data/ora).

La revoca determina la cessazione anticipata della validità di un certificato, a partire da un dato momento (data/ora). La revoca di un certificato è irreversibile e non retroattiva.

L'attuazione della sospensione o revoca consiste nella generazione e pubblicazione di una nuova CRL (Certificate Revocation List) che include il numero di serie del certificato sospeso o revocato. La CRL è liberamente accessibile a chiunque abbia necessità di verificare lo stato del certificato (cfr. la sezione 4.10).

4.9.1 Circostanze per la sospensione

Le condizioni che possono determinare la sospensione di un certificato sono le seguenti:

- una richiesta di revoca effettuata tramite le modalità – riportate al paragrafo 4.9.6 – *comunicazione telefonica*, oppure, *canale di comunicazione sicuro con il QTSP*;
- compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme/sigilli;
- guasto del dispositivo di firma/sigillo;
- perdita di possesso della chiave privata o delle informazioni necessarie al suo utilizzo;
- sospetti abusi e/o falsificazioni;
- altre cause che possono generare la perdita dei requisiti di riservatezza, integrità e disponibilità delle informazioni contenute nel certificato.

4.9.2 Chi può richiedere la sospensione

La sospensione può essere richiesta dal Cliente e/o dal Titolare del certificato, dal richiedente o dal terzo interessato. Il certificato può essere sospeso d'ufficio dalla CA.

L'identificazione del sottoscrittore che chiede la sospensione di un certificato è effettuata secondo una procedura interna (cfr. 3.2.3).

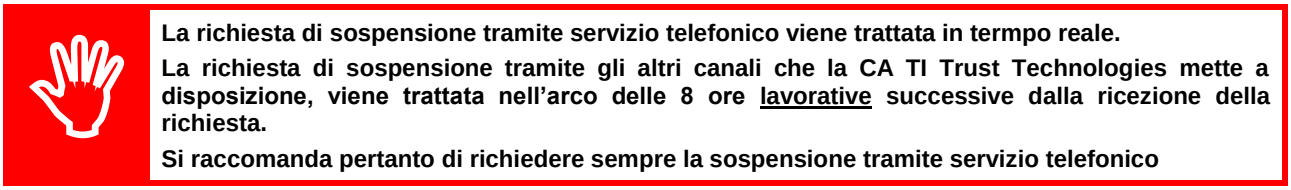
4.9.3 Procedura per la sospensione

Il Titolare o il terzo interessato che intendano ottenere la sospensione di un certificato devono inoltrare regolare richiesta di revoca secondo le modalità descritte nel presente CPS.

La CA TI Trust Technologies segnala al Titolare l'avvenuta sospensione inviando una notifica come descritto in 4.9.7.

Il Titolare, l'Incaricato o il terzo interessato che intendano ottenere la sospensione di un certificato devono inoltrare regolare richiesta secondo le modalità di seguito indicate:

- la **sospensione da parte del Titolare e dell'Incaricato** può essere richiesta con le modalità seguenti:
  - per **iscritto**, tramite fax inviato alla CA TI Trust Technologies, al numero riportato nel sito (https://www.trusttechnologies.it);
  - utilizzando il **servizio telefonico o il canale web sicuro** messi a disposizione dalla CA TI Trust Technologies.



Nei casi di sospensione telefonica o via web, la richiesta deve essere confermata per iscritto tramite fax inviato alla CA TI Trust Technologies, riportato nel sito (https://www.trusttechnologies.it).

Nella richiesta di sospensione per iscritto o nella conferma scritta della sospensione richiesta via telefono o via canale web sicuro devono essere chiaramente indicati:

- esplicita dichiarazione della volontà di sospendere il certificato (se la richiesta proviene dal Titolare);
- la motivazione della richiesta di sospensione ed il periodo di sospensione richiesto;
- il codice di registrazione del Titolare;
- i seguenti dati anagrafici del Titolare o dell'Incaricato se è lui a chiedere la sospensione:
  - nome e cognome;
  - data e luogo di nascita;
  - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
  - codice fiscale;
- fotocopia di un documento di riconoscimento del richiedente la sospensione;
- il momento a partire dal quale il certificato deve essere sospeso;
- il momento a partire dal quale il certificato deve essere riattivato.

- la **sospensione da parte del Terzo Interessato** può essere richiesta esclusivamente per **iscritto**, tramite fax inviato alla CA TI Trust Technologies, riportato nel sito (https://www.trusttechnologies.it), che deve contenere:
  - esplicita dichiarazione della volontà di sospendere il certificato;
  - la motivazione della richiesta di sospensione e il periodo di sospensione richiesto;
  - i seguenti dati anagrafici del richiedente:
    - nome e cognome;
    - data e luogo di nascita;
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza).
  - il momento a partire dal quale il certificato deve essere sospeso;
  - il momento a partire dal quale il certificato deve essere riattivato.

4.9.3.1 Attuazione della Sospensione del Certificato

La sospensione di un certificato determina l'immediata cessazione della sua validità, indipendentemente dalla data di scadenza del certificato medesimo, sino al momento della sua riattivazione.

La sospensione viene effettuata mediante l'inserimento del certificato nella lista dei certificati sospesi (CSL). La pubblicazione di tale lista determina il momento a partire dal quale il certificato si considera sospeso. Qualora la sospensione avvenga a causa della possibile compromissione della segretezza della chiave privata, la CA TI Trust Technologies garantisce l'immediata pubblicazione dell'aggiornamento della lista dei certificati sospesi riportante la sospensione in questione.

Le liste di sospensione sono conformi alla normativa vigente e, in particolare, alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Le Liste dei Certificati Sospesi sono pubblicate periodicamente, secondo quanto riportato nel paragrafo 4.9.8.

Nel caso in cui la sospensione debba essere immediata, la pubblicazione della nuova Lista dei Certificati Sospesi può essere effettuata in maniera non programmata.

La sospensione di un certificato viene comunicata a utenti terzi tramite la pubblicazione delle liste di sospensione.

La verifica della validità di un certificato è responsabilità di chiunque intenda fare affidamento sul medesimo.

Le chiavi private corrispondenti a chiavi pubbliche contenute in certificati sospesi e i dispositivi che le contengono, devono essere conservate con la massima diligenza da parte dei Titolari anche durante il periodo di sospensione. Analogamente, le informazioni riservate di abilitazione all'uso della chiave privata devono essere salvaguardate e conservate in luogo diverso dal dispositivo che contiene la chiave, come previsto dalla normativa vigente.

4.9.3.2 Riattivazione di Certificati sospesi

Il Titolare e il terzo interessato possono chiedere la riattivazione di un certificato sospeso.

Il Titolare, l'Incaricato o il terzo interessato che intendano ottenere la riattivazione di un certificato sospeso devono inoltrare regolare richiesta secondo le modalità di seguito indicate:

- le richieste di **riattivazione da parte del Titolare** di un certificato o dall'Incaricato sono accettate qualora siano inviate tramite fax al numero della CA TI Trust Technologies, riportato nel sito (https://www.trusttechnologies.it), e contengano:
  - esplicita dichiarazione della volontà di riattivare anticipatamente il certificato;
  - la motivazione della riattivazione anticipata e la decorrenza richiesta;
  - il *codice di registrazione* del Titolare;
  - i seguenti dati anagrafici del richiedente:
    - nome e cognome;
    - data e luogo di nascita;
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
    - codice fiscale;
    - fotocopia di un documento di riconoscimento.

- le richieste di **riattivazione da parte del terzo interessato** sono accettate qualora pervengano tramite fax al numero della CA TI Trust Technologies, riportato nel sito (https://www.trusttechnologies.it), e contengano:
  - esplicita dichiarazione della volontà di riattivare anticipatamente il certificato;
  - la motivazione della richiesta di riattivazione anticipata e la decorrenza richiesta;
  - i seguenti dati anagrafici del richiedente:
    - nome e cognome;
    - data e luogo di nascita;
    - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza).

La CA TI Trust Technologies si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della riattivazione (anticipata) riportati sulla richiesta di riattivazione.

La riattivazione del certificato è sancita dalla sua eliminazione dalla Lista dei Certificati Sospesi (CSL), firmata da una chiave di certificazione e pubblicata.

Le Liste dei Certificati Sospesi sono pubblicate periodicamente, secondo quanto riportato nel paragrafo 4.9.7.

4.9.4 Circostanze per la revoca

Le condizioni che possono determinare la revoca di un certificato sono le seguenti:

- la perdita, il furto, la modifica, la rivelazione non autorizzata o altra compromissione della chiave privata del Titolare;
- il Titolare del certificato o chi per esso hanno violato un obbligo definito in questo CPS e previsto dalla normativa;
- variazione delle informazioni contenute nel certificato relative al Titolare;
- un errore nel processo di registrazione;
- provvedimento dell'autorità giudiziaria (ad esempio a seguito di attività illecite da parte dell'entità organizzativa Titolare);
- la cessazione dell'attività dell'entità organizzativa Titolare;
- la richiesta da parte del Titolare (ad esempio motivata da cessazione dell'uso del certificato);
- la richiesta da parte di "**terzi interessati secondo la normativa vigente**", quali, ad esempio:
  - un'organizzazione terza, dalla quale derivano in capo al Titolare i poteri di rappresentanza o altri titoli relativi all'attività professionale o a cariche rivestite presso o per conto dell'organizzazione terza medesima;
  - il cliente che ha stipulato il contratto di acquisto del certificato destinandolo ad una persona a lei, in qualunque maniera, afferente;
  - la persona fisica o giuridica rappresentata legalmente dal Titolare in virtù di una procura o di una delega.
- inadempienze contrattuali da parte del cliente (ad esempio mancato pagamento);
- la cessazione dell'attività della CA TI Trust Technologies;
- acquisizione della conoscenza di cause limitative della capacità del Titolare;
- sospetti abusi e/o falsificazioni;

- compromissione della chiave di certificazione che ha firmato il certificato in questione.

Oltre alle circostanze sopra riportate, sono motivo di revoca del certificato:

- la modifica o la scadenza del rapporto che intercorre tra il Titolare e l'organizzazione per conto della quale il certificato viene utilizzato;
- il decadere del titolo, della carica o del ruolo inerente i poteri di rappresentanza o la qualifica professionale in nome di cui il certificato viene utilizzato;
- il ritiro della procura o della delega da parte del rappresentato.

4.9.5 Chi può richiedere la revoca

La revoca può essere richiesta dal Titolare del certificato, dal Richiedente o terzo interessato, o dalla CA TI Trust Technologies o RA.

L'identificazione del soggetto che chiede la revoca di un certificato è effettuata secondo una procedura interna (cfr. 3.4).

In determinate circostanze il Titolare ha l'obbligo di richiedere la revoca del certificato (cfr. https://www.trusttechnologies.it/download/legale-e-privacy/).

La revoca viene effettuata direttamente dalla CA TI Trust Technologies o RA quando vengono a conoscenza di condizioni che compromettono l'attendibilità del certificato o costituiscono grave e ripetuta inadempienza contrattuale da parte del cliente o del Titolare.

Ai sensi della normativa, nel caso in cui non abbia la possibilità di accertare in tempo utile l'autenticità della richiesta di revoca, la CA TI Trust Technologies invece che alla revoca procede alla **sospensione** del certificato (cfr. 4.9.1).

4.9.6 Procedura per la revoca

Il Titolare o il terzo interessato che intendano ottenere la revoca di un certificato devono inoltrare la richiesta di revoca secondo le modalità descritte nel presente CPS.

La CA TI Trust Technologies segnala al cliente l'avvenuta revoca inviando una notifica come descritto in 4.9.7.

Qualora la revoca avvenga a causa della possibile compromissione della segretezza della chiave privata, la CA TI Trust Technologies garantisce l'immediata pubblicazione dell'aggiornamento della lista dei certificati revocati riportante la revoca in questione.

Il Titolare, l'Incaricato o il terzo interessato che intendano ottenere la revoca di un certificato devono inoltrare la richiesta secondo le modalità di seguito indicate:

- la richiesta di **revoca da parte del Titolare** di un certificato è accettata qualora redatta ed inoltrata per iscritto ed inoltre contenga:
  1) esplicita dichiarazione della volontà di revocare il certificato;
  2) la motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca;
  3) il *codice di registrazione* fornito al Titolare al momento della richiesta di registrazione relativa al certificato da revocare;
  4) almeno i seguenti dati anagrafici del richiedente:
     - nome e cognome;
     - data e luogo di nascita;
     - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
     - codice fiscale.

Qualora la richiesta di revoca sia sottoposta alla CA TI Trust Technologies secondo una delle seguenti procedure:

- **tramite il canale di comunicazione sicuro predisposto dalla CA TI Trust Technologies**,
- **per telefono**, chiamando il numero verde della CA TI Trust Technologies, riportato nel sito (https://www.trusttechnologies.it), fornendo le informazioni elencate in precedenza nei punti da 1 a 4 e, in aggiunta, dichiarando esplicitamente il **codice segreto di revoca**,

la CA TI Trust Technologies provvede a **sospendere cautelativamente il certificato** (v. par. 4.9) mentre il Titolare si impegna a confermare per iscritto la richiesta di revoca, inviandola tramite fax, al numero della CA TI Trust Technologies riportato nel sito (https://www.trusttechnologies.it). Il fax deve contenere le informazioni elencate in precedenza nei punti da 1 a 4 e, in aggiunta:

- fotocopia di un documento di riconoscimento;
- nel caso di richiesta di revoca motivata da smarrimento o furto degli strumenti per l'uso del servizio, la fotocopia della denuncia dell'avvenuto smarrimento o furto.

La CA TI Trust Technologies si riserva il diritto di non procedere alla revoca definitiva del certificato, bensì alla sua sospensione immediata sino al ricevimento della conferma della richiesta di revoca.

- la richiesta di **revoca da parte del terzo interessato** di un certificato è accettata qualora redatta ed inoltrata per iscritto ed inoltre contenga:
  1) esplicita dichiarazione della volontà di revocare il certificato;
  2) la motivazione della richiesta di revoca e la decorrenza richiesta per tale revoca;
  3) almeno i seguenti dati anagrafici di chi la richiede:
     - nome e cognome;
     - data e luogo di nascita;
     - indirizzo di residenza (costituito da via, numero civico, CAP, comune di residenza);
  4) la documentazione giustificativa della revoca (ad esempio, copia dei documenti ufficiali attestanti la modifica o terminazione del rapporto intercorrente tra Titolare e terzo interessato per conto di cui il certificato viene utilizzato, o il decadere del titolo, della carica o del ruolo in nome del quale il certificato viene utilizzato, revoca della procura o della delega).

4.9.6.1 Attuazione della Revoca del Certificato

La CA TI Trust Technologies si impegna a compiere ogni ragionevole sforzo per rispettare i tempi di decorrenza della revoca riportati sulla relativa richiesta. Nei casi di compromissione della chiave privata, furto o smarrimento del dispositivo, la CA TI Trust Technologies si impegna ad eseguire la revoca tempestivamente all'atto della ricezione della richiesta.

La revoca del certificato è sancita dal suo inserimento in una Lista dei Certificati Revocati firmata da una chiave di certificazione e pubblicata.

Le liste di revoca sono conformi alla normativa vigente, ed in particolare alla specifica pubblica PKCS#6 e PKCS#9 e successive modificazioni o integrazioni.

Le Liste dei Certificati Revocati sono pubblicate periodicamente, secondo quanto riportato nel paragrafo 4.9.8.

Nel caso in cui la revoca debba essere immediata, la pubblicazione di una Lista dei Certificati Revocati può essere effettuata in maniera non programmata.

La revoca di un certificato viene comunicata a utenti terzi tramite la pubblicazione delle liste di revoca.

La verifica della validità di un certificato è responsabilità di chiunque intenda fare affidamento sul medesimo.

In particolare, è responsabilità dell'utente terzo il controllo dell'eventuale presenza del certificato su una lista di revoca firmata dal QTSP che l'ha emessa. Tale controllo deve includere la verifica che la lista in esame non sia scaduta a causa della pubblicazione, in data od ora successiva, di una lista più aggiornata.

4.9.7 Notifica al Titolare

L'avvenuta revoca o sospensione o riattivazione di un certificato viene notificata al Titolare tramite qualsiasi mezzo considerato idoneo dalla CA TI Trust Technologies.

Analogamente viene notificato qualunque fatto noto al QTSP che possa compromettere la validità o affidabilità del certificato.

Secondo quanto previsto dalla normativa vigente, l'intenzione di revocare o sospendere un certificato è notificata anticipatamente al Titolare, salvo casi di motivata urgenza, ogni qual volta la revoca o sospensione avvenga per iniziativa della CA TI Trust Technologies o del terzo interessato; l'intenzione di riattivare un certificato è notificata anticipatamente al Titolare, salvo casi di motivata urgenza, ogni qual volta la richiesta provenga da un terzo interessato.

In alternativa ad una comunicazione diretta al Titolare, la CA TI Trust Technologies può fargli pervenire la notifica della revoca, sospensione o riattivazione del certificato (anche anticipata) tramite un proprio Incaricato.

4.9.8 Frequenza di emissione della CRL

Vedere il paragrafo 4.10.1.

4.10 Servizi informativi sullo stato del certificato

La CA TI Trust Technologies mette a disposizione servizi di controllo dello stato del certificato attraverso CRL e OCSP.

Lo stato dei certificati (attivo, sospeso, revocato) è quindi reso disponibile a tutti gli interessati mediante:

- pubblicazione della Certificate Revocation List (CRL) nel formato definito dalla specifica [RFC5280];
- servizio OCSP (On-line Certificate Status Provider) conforme alla specifica [RFC6960].

4.10.1 Caratteristiche operative

La CRL ed il servizio OCSP sono resi accessibili con la seguente modalità:

- protocollo HTTP [RFC2616]

CRL

L'indirizzo completo HTTP della CRL è inserito nell'estensione *CRLDistributionPoints* del certificato.

La CA TI Trust Technologies firma digitalmente ogni CRL che emette in modo da convalidarne l'integrità e la data e ora di emissione.

La CRL viene rigenerata e ripubblicata almeno ogni ora, anche in assenza di nuove sospensioni o revoche.

OCSP

L'indirizzo completo HTTP del server OCSP (*responder*) è inserito nell'estensione *AuthorityInformationAccess* del certificato.

La CA TI Trust Technologies o il *responder* OCSP produce messaggi di risposta firmati, che indicano lo stato del certificato; se la richiesta contiene informazioni errate o non è correttamente formattata il responder OCSP ritorna uno stato di "unknown" (sconosciuto).

Lo stato dei certificati fornito dai due servizi viene costantemente allineato in modo che l'informazione risulti consistente nel tempo; il tempo massimo richiesto dalle procedure di allineamento è di 15 minuti.

La CRL e il servizio OCSP sono liberamente consultabili da chiunque.

4.10.2 Disponibilità del servizio

L'accesso alla CRL e al servizio OCSP è disponibile in modo continuo (24x7), tranne in caso di fermi per manutenzione programmata e in caso di guasti.

4.11 Cessazione del contratto

Il contratto di servizio stipulato tra la CA TI Trust Technologies e cliente si intende terminato:

- alla data di scadenza naturale del certificato, oppure
- alla data di attuazione della revoca del certificato (vedere la sezione 4.9).

4.12 Segnalazioni di problemi

Oltre alla revoca di un certificato, CA TI Trust Technologies rende disponibile a titolari, sottoscrittori, a chi fa affidamento sulle informazioni contenute nei certificati, fornitori e altre terze parti istruzioni chiare per la segnalazione di accertata o sospetta compromissione della chiave privata, uso improprio del certificato o altri tipi di frode, compromissione, uso improprio o comportamenti inappropriati relativi ai certificati. La CA TI Trust Technologies accetta, riconosce e dà riscontro alle segnalazioni di problemi ai certificati su base 24x7.

4.13 Key escrow e key recovery

Nell'ambito del servizio erogato dalla CA TI Trust Technologies in base a questo CPS, il *key escrow* delle chiavi non è previsto.

Il ripristino della chiave (*key recovery*) di certificazione è previsto, in caso di cancellazione involontaria o guasto o sostituzione del dispositivo HSM. Al fine di consentire il key recovery, la CA TI Trust Technologies mantiene una copia di backup della chiave di CA (vedere il paragrafo 6.8).

5 MISURE DI SICUREZZA FISICA ED OPERATIVA

L'infrastruttura tecnologica, le procedure operative, le misure di sicurezza fisica e logica ed il personale preposto all'erogazione del servizio descritto in questo CPS sono gli stessi utilizzati nell'ambito del servizio TI Trust Technologies di emissione e gestione dei certificati qualificati per firma digitale a norma di legge.

5.1 Sicurezza fisica

Il Centro Servizi di TI Trust Technologies è ubicato presso il Data Center Telecom Italia di Pomezia, con sede in Via Pontina km 29,100.

Le misure di sicurezza, implementate per la protezione fisica dei siti e dei locali che ospitano le piattaforme tecnologiche utilizzate per l'erogazione dei servizi di certificazione digitale, si articolano su vari livelli.

Il primo livello di protezione è costituito dal confine di proprietà del sito che ospita il Data Center / Centro servizi ed impedisce l'accesso a soggetti e/o automezzi non autorizzati. La delimitazione fisica perimetrale sia che si riferisca a siti già esistenti sia che si tratti di nuove realizzazioni deve possedere idonei requisiti costruttivi quali altezza, spessore, materiali utilizzati, etc., ed essere integrata con sistemi attivi antintrusione, i cui principi di funzionamento offrano la massima affidabilità.

L'integrazione di protezioni attive e passive deve garantire la rilevazione attendibile degli eventi anomali (tentativi di intrusione, manomissioni, etc.) da parte del personale di Vigilanza. Tale funzione può essere soddisfatta da un sistema di videosorveglianza gestito dalla Vigilanza, che deve operare in un locale presso il quale saranno accentrati tutti i telecomandi di sicurezza e le segnalazioni di allarme.

Misure di sicurezza fisica per il primo livello di protezione sono:

- Protezione Perimetrale Esterna (mura, recinzioni, sistemi elettronici);
- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione, il controllo del perimetro è effettuato con impianti a raggi infrarossi;
- Sbarre / Cancelli esterni, la cui apertura è a cura del personale di Vigilanza;
- Controllo Accessi pedonali e carrai: un presidio di Vigilanza, che supervisiona i transiti, identifica i visitatori ed eventualmente autorizza l'accesso all'interno del sito;
- Illuminazione;
- Vigilanza h24x7;
- Edifici dedicati.

Il secondo livello di protezione implementato, coincidente con il perimetro che delimita l'area o le aree dedicate agli ambienti valutabili di considerevole rilevanza strategica e le aree uffici, tutela l'accesso ai siti stessi. Misure di sicurezza fisica per il secondo livello di protezione sono:

- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione;
- Controllo Accessi tramite badge (di prossimità) e/o con riconoscimento biometrico;
- Illuminazione, Bussole, Tornelli, Vetri antisfondamento, grate;
- Vigilanza h24x7;
- Frazionamento delle aree.

L'accesso ai siti è possibile solo attraverso un ingresso esterno regolamentato da sistemi di tornelli ad accesso singolo a lettura badge. Il controllo accessi riferito agli edifici che costituiscono le sedi di TI Trust Technologies avviene secondo quanto previsto dalle procedure di accesso ai siti di Telecom Italia.

Il terzo livello di protezione protegge le aree critiche che includono gli asset a maggior valore strategico e che costituiscono il core business aziendale. Sono considerate aree critiche, ad esempio:

- le Sale TLC, ambienti dedicati ad ospitare switch, router e firewall
- le Sale Sistemi, che ospitano i sistemi della CA
- le Cage, "spazi chiusi" completamente dedicati ai sistemi - realizzate all'interno di sale sistemi - compartimentate per mezzo di una gabbia metallica, al fine di offrire un alto livello di sicurezza dei sistemi.

Misure di sicurezza fisica per il terzo livello di protezione sono:

- Videosorveglianza analogica e digitale: un sistema di videosorveglianza a circuito chiuso (TVCC) con video registrazione;
- Controllo Accessi tramite badge (di prossimità) e/o con riconoscimento biometrico;
- Illuminazione;
- Bussole, Cage;
- Armadi blindati, Camere di sicurezza (Lamperz).

I Data Center dove opera TI Trust Technologies sono conformi alle direttive del Gruppo TIM:

- hanno pareti esterne realizzate in cemento armato, con sale apparati delimitate da tramezzi realizzati con materiale da costruzione conforme alle norme antincendio;

- la Sala Sistemi di TI Trust Technologies a Pomezia, è dotata di un impianto di videocitofono utilizzato per mettere in comunicazione le persone che non fanno parte dell'organizzazione del Centro con il personale all'interno della sala stessa che è così in grado di vedere e riconoscere l'interlocutore esterno. È inoltre collegata mediante videocitofono con la Guardiola per le eventuali comunicazioni di servizio;
- tutti i supporti contenenti software di produzione e dei dati, audit, archivio o informazioni di backup vengono memorizzati all'interno di strutture con adeguati controlli di accesso fisici e logici volti a limitare l'accesso al personale autorizzato e proteggere tali supporti da danni accidentali (ad esempio, acqua, fuoco ed emissioni elettromagnetiche);
- i rilievi strumentali effettuati presso il Data Center, allo scopo di valutare i livelli di emissione del campo elettrico e magnetico prodotto dagli impianti ivi esistenti, permettono di evidenziare il rispetto dei limiti di esposizione, dei valori di attenzione e degli obiettivi di qualità previsti dal DPCM 8 luglio 2003. Si evidenzia che secondo quanto previsto dalla normativa sono presi come riferimento, per la valutazione dell'esposizione professionale del personale che opera nel Data Center, i limiti più cautelativi previsti per la popolazione;
- in tutti i locali protetti sono installati sensori volumetrici che rilevano i tentativi di passaggio nelle zone immediatamente sottostanti il sensore stesso e/o possibili mascheramenti. Questi sensori sono attivati dal personale della guardiania nell'orario di chiusura del Centro;
- l'energia elettrica è fornita da un sistema a doppia cabina di distribuzione, che implementa un meccanismo di ridondanza per garantire la continuità: i punti di allaccio alla rete sono serviti da una doppia alimentazione con possibilità di isolamento e manutenzione di tutti i componenti. Tutti i quadri che forniscono la corrente elettrica alle apparecchiature delle piattaforme di erogazione sono alimentati da gruppi di continuità;
- la continuità elettrica è garantita da gruppi statici di continuità, connessi in parallelo con modulo centrale di distribuzione e batterie con autonomia di molte ore. Tale impianto è asservito ad un sistema di gruppi elettrogeni di soccorso, di cui uno cabinato esterno, alimentati, all'occorrenza, tramite un deposito di combustibile costituito da serbatoi di gasolio di grande capacità;
- tutti gli ambienti sono dotati di rilevatori antifumo e sistemi antincendio con attivazione degli impianti di spegnimento automatico degli incendi a saturazione di ambiente. Tutte le segnalazioni dell'impianto antincendio sono tempestivamente riportate sia al presidio interno di manutenzione sia al presidio di security, in modo che il personale addetto possa avvertire in tempi contenuti i soggetti individuati nello specifico piano di sfollamento della sede.

5.2 Sicurezza delle procedure

TI Trust Technologies definisce e mantiene un Piano della Sicurezza che analizza gli asset e descrive le misure tecniche ed organizzative atte a garantire un adeguato livello di sicurezza delle operazioni.

Tutte le procedure operative standard sono documentate e comprese nel Sistema integrato di Gestione della Qualità e della Sicurezza delle Informazioni di TI Trust Technologies, certificato secondo la norma ISO 9001:2008 e la norma ISO 27001:2013.

5.3 Sicurezza del personale

Il personale addetto al servizio ha una pluriennale esperienza nel campo della definizione, sviluppo e gestione di servizi di PKI ed ha ricevuto una adeguata formazione sulle procedure e gli strumenti da utilizzare nelle varie fasi operative.

5.4 Logging degli eventi

I principali eventi relativi alla gestione del ciclo di vita dei certificati, incluse le richieste di certificazione, sospensione o revoca, etc. sono registrati in forma cartacea od elettronica. Sono inoltre registrati anche altri eventi quali: gli accessi logici al sistema di gestione del certificato, le operazioni svolte dal personale della CA TI Trust Technologies, l'entrata e l'uscita di visitatori nei locali in cui si svolge l'attività di certificazione, etc.

Di ogni evento viene registrata la tipologia, la data e l'ora di occorrenza e, se disponibili, altre informazioni utili ad individuare gli attori coinvolti nell'evento e l'esito delle operazioni.

In nessun caso viene registrata nei log la chiave privata della CA TI Trust Technologies in alcuna forma (in chiaro o cifrata).

L'insieme delle registrazioni costituisce l'Audit log (per la CA TI Trust Technologies si parla anche di Giornale di Controllo): i file che lo compongono vengono trasferiti – con le modalità previste per ogni tipologia di log – tutti i giorni su supporto permanente, con garanzia di integrità ed inalterabilità del dato.

5.5 Archiviazione dei dati

La CA conserva tutte le informazioni relative ai processi di emissione e gestione dei certificati, come le seguenti:

- le richieste di emissione (possono essere anche in formato cartaceo),
- la documentazione fornita dai richiedenti (può essere anche in formato cartaceo),

- le Certificate Request fornite dai richiedenti,
- i dati anagrafici dei richiedenti e degli utilizzatori finali (ove siano soggetti diversi),
- le richieste di revoca o sospensione,
- tutti i certificati emessi,
- gli audit log, per un periodo non inferiore a 20 anni.

Una copia di sicurezza (backup) dei dati, delle applicazioni, del giornale di controllo e di ogni altro file necessario al completo ripristino del servizio viene effettuata quotidianamente.

I documenti cartacei vengono mantenuti, sempre per un periodo non inferiore a 20 anni, in appositi archivi all'interno dei locali della CA TI Trust Technologies.

5.6 Key Compromise e Disaster Recovery

Per "key compromise" s'intende la violazione di una o più condizioni vincolanti per l'erogazione del servizio di CA; per "disastro" s'intende un evento dannoso le cui conseguenze determinano l'indisponibilità del servizio in condizioni ordinarie.

A seguito di situazioni di compromissione della chiave privata della CA TI Trust Technologies è prevista apposita procedura finalizzata al ripristino (recovery) dei servizi di certificazione, procedura che è indirizzata all'interno del Piano di Continuità Operativa (il Business Continuity Plan) di TI Trust Technologies.

Il ripristino da compromissione o disastro avviene in ogni caso nelle seguenti situazioni:

- guasti di una o più delle apparecchiature usate per erogare i servizi di certificazione;
- compromissione (es. rivelazione a terzi non autorizzati, perdita, ecc.) di una o più chiavi private di certificazione.

La procedura di ripristino a seguito di disastro prevede una distinzione dei Servizi in funzione del valore di RTO (Recovery Time Objective) da rispettare e dello SLA previsto. La distinzione è puramente basata sulla necessità di attivare per primi, e nel minor tempo possibile, i *servizi "essenziali"* che la normativa considera continuativi (ad esempio la *Pubblicazione CRL*) rispetto agli altri.

5.7 Cessazione della CA TI Trust Technologies

In ogni caso in cui se ne dovesse presentare la necessità, la CA TI Trust Technologies procede alla cessazione dei servizi di CA secondo quanto di seguito descritto:

1) TI Trust Technologies comunica con un **anticipo di almeno 90 giorni** la propria determinazione a cessare i servizi di CA all'organismo di vigilanza preposto, ai clienti ed agli utilizzatori.
2) Ove TI Trust Technologies abbia individuato soggetti sostitutivi, nella sua comunicazione indicherà il prestatore di servizi fiduciari qualificato sostitutivo, il depositario di tutte le informazioni, dati, documenti, archivi, audit trails di competenza TI Trust Technologies, della relativa documentazione ed il periodo in cui tale soggetto manterrà evidenza delle operazioni [11], [12].
3) Ove TI Trust Technologies non indichi un prestatore di servizi fiduciari qualificato sostitutivo:
    a. procede alla revoca di tutti i certificati attivi al momento della cessazione della propria attività, generando una CRL finale raggiungibile all'URL originale e mantenuta disponibile per i tempi disposti dalla normativa vigente;
    b. provvede a riversare nel proprio sistema di Conservazione la documentazione e l'evidenza delle operazioni, dove provvederà a mantenerle disponibili nei termini previsti a far data dalle cessazione;
    c. assicura la definizione dei rapporti pendenti con altri eventuali soggetti coinvolti nell'ambito dei servizi;
    d. distrugge in modo da renderle irrecuperabili le chiavi private delle CA e dei Titolari di QSCD custodito dal QTSP.
4) TI Trust Technologies procede alla dismissione delle infrastrutture HW e SW dei servizi, conformemente alle proprie policy.

[11] Il trasferimento si configurerà come cessione di contratto da parte di TI Trust Technologies verso l'operatore sostitutivo per assicurare la continuità dei servizi di CA verso clienti ed utilizzatori. Le Condizioni di utilizzo dei servizi riconoscono comunque in questo caso al Cliente ed al Titolare la facoltà esercitare il recesso.

[12] In caso di eventuale avvio di procedure concursuali a carico di TI Trust Technologies ed in considerazione della loro lunga durata, nel caso in cui si verificassero circostanze tali da impedire a TI Trust Technologies di garantire tutti gli adempimenti connessi ai servizi di CA, TI Trust Technologies procederà alla loro cessazione con trasferimento dei contratti ad un operatore sostitutivo.

5.8 Sostituzione delle chiavi di Certificazione

La CA TI Trust Technologies provvede alla generazione di nuove chiavi almeno nei seguenti casi:

- Approssimarsi della scadenza della validità del certificato di CA,
- Necessità di utilizzare chiavi ed algoritmi più robusti per far fronte all'evoluzione tecnologica degli elaboratori.

Per quanto concerne la sostituzione per scadenza, le attività vengono effettuate in modo da consentire ai Titolari di continuare ad utilizzare i propri certificati di sottoscrizione senza discontinuità.

Tipicamente i certificati di sottoscrizione hanno durata massima di 3 anni, quindi le chiavi di certificazione vengono sostituite al massimo 3+1 anni prima della scadenza del relativo certificato in modo da poter gestire correttamente lo stato di tutti certificati non ancora scaduti.

Come previsto normativamente, ogni volta che vengono create nuove chiavi di certificazione la CA TI Trust Technologies aggiorna il presente documento e lo notifica all'AgID.

6 MISURE DI SICUREZZA TECNICA

L'infrastruttura tecnologica, le procedure operative, le misure di sicurezza fisica e logica ed il personale preposto all'erogazione del servizio descritto in questo CPS sono gli stessi utilizzati nell'ambito del servizio TI Trust Technologies di emissione e gestione dei certificati qualificati di firma e sigillo come disciplinati dal [Regolamento eIDAS] .

6.1 Generazione delle chiavi

6.1.1 Chiavi della CA TI Trust Technologies

La coppia di chiavi usata dalla CA TI Trust Technologies per firmare i certificati e le CRL è generata all'interno di un dispositivo crittografico che è almeno certificato FIPS 140-2 Level 3 o superiore, in un ambiente fisicamente sicuro.

6.1.2 Chiavi dei Subscriber

La generazione delle chiavi dei Titolari avviene secondo modalità che garantiscono livelli di sicurezza analoghi a quelli previsti per la generazione di chiavi della CA TI Trust Technologies. I dispositivi di firma sono custoditi all'interno di appositi locali protetti.

Le chiavi sono generate internamente al dispositivo sicuro di firma dalla CA TI Trust Technologies o dal Titolare e sono attribuite ognuna ad un unico Titolare.

I dispositivi sicuri di firma utilizzati per le chiavi di sottoscrizione sono smartcard o dispositivi analoghi in grado di conservare in modo protetto la chiave privata e di generare al proprio interno le firme digitali, secondo la definizione indicata nella normativa vigente.

6.2 Distribuzione della chiave pubblica

6.2.1 Chiavi della CA TI Trust Technologies

La chiave pubblica della CA TI Trust Technologies è distribuita attraverso un link pubblico la cui URL è contenuta internamente ai Certificati digitali nell'estensione *AuthorityInformationAccess*.

6.2.2 Chiavi dei Richiedenti

La chiave pubblica del Richiedente viene fornita alla CA TI Trust Technologies sotto forma di Certificate Signing Request (CSR) conforme allo standard PKCS#10 [RFC2986].

6.3 Lunghezza delle chiavi

6.3.1 Chiavi della CA TI Trust Technologies

Per firmare i certificati dei clienti e le CRL la CA TI Trust Technologies utilizza chiavi con un modulo lungo 4096 bit.

6.3.2 Chiavi dei Richiedenti

Le chiavi dei Richiedenti devono avere lunghezza di (almeno) 2048 bit.

6.4 Parametri di generazione e qualità delle chiavi

6.4.1 Chiavi della CA TI Trust Technologies

La CA TI Trust Technologies usa una coppia di chiavi crittografiche a 4096 bit generate con algoritmo RSA, con esponente pubblico pari a 65537.

6.4.2 Chiavi dei Titolari

Di norma, il titolare del certificato usa una coppia di chiavi crittografiche a 2048 bit generate con algoritmo RSA.

6.5 Key usage (estensione X.509 v3)

Il certificato include l'estensione *KeyUsage* con gli opportuni valori che indicano lo scopo della chiave privata.

Per il certificato di CA TI Trust Technologies:

- Firma certificato,
- Firma CRL.

Per il certificato qualificato (firma e sigillo):

- Non Ripudio

Ulteriori dettagli sulla struttura dei certificati sono indicati al capitolo 7.

6.6 Protezione della chiave privata

Le coppie di chiavi usate dalle CA TI Trust Technologies per firmare i certificati e le CRL sono generate e conservate all'interno di un HSM (Hardware Security Module) di alta qualità.

Le coppie di chiavi di sottoscrizione dei titolari sono generate e conservate all'interno dispositivi sicuri di firma.

Tutti i dispositivi utilizzati sono dotati di adeguata certificazione di sicurezza (cfr. 6.7).

6.7 Standard di sicurezza dei moduli crittografici

Gli HSM (Hardware Security Module) utilizzati per le chiavi di certificazione (CA) e per il servizio di OCSP sono dotati di livello minimo di sicurezza secondo la norma FIPS 140-2 Level 4 e Common Criteria EAL 4+.

Analogamente i dispositivi sicuri di firma utilizzati per la custodia delle chiavi di sottoscrizione dei Titolari sono stati accertati sulla base dei requisiti di sicurezza definiti secondo la norma dell'articolo 3, paragrafo 4, della direttiva 1999/93/CE (SSCD, Secure Signature Creation Device).

I suddetti dispositivi sono validi per la creazione di una firma elettronica qualificata a norma del regolamento 910-2014 (eiDAS, che li definisce QSCD, Qualified Signature Creation Device).

La CA TI Trust Technologies, nell'ambito delle *ispezioni periodiche interne* (cfr. 8), verifica con periodicità almeno annuale la conformità normativa dei moduli crittografici utilizzati, prestando particolare attenzione ad eventuali scadenze delle Attestazioni di Conformità dei dispositivi ed individuando per tempo, qualora necessario, soluzioni alternative sulla base dei prodotti disponibili sul mercato.

6.8 Backup e ripristino della chiave privata

6.8.1 Backup e ripristino della chiave privata di Certificazione

Allo scopo di garantire la continuità del servizio, la CA TI Trust Technologies effettua una copia di backup delle chiavi della CA; la copia di backup viene conservata in luogo sicuro e distinto da quello in cui si trova la copia operativa (all'interno dello HSM).

Per le chiavi di CA è prevista una procedura specifica per la copia in sicurezza delle stesse, esclusivamente per motivi di ripristino in caso di guasto o aggiornamento o sostituzione del dispositivo HSM.

6.8.2 Backup e ripristino della chiave privata di Sottoscrizione su dispositivo QSCD custodito dal QTSP

Allo scopo di garantire la continuità dei servizi di firma basati su dispositivo QSCD custodito dalla CA TI Trust Technologies, viene effettuato il backup delle chiavi di sottoscrizione dei titolari utilizzando le funzionalità di sicurezza del dispositivo HSM che le custodisce.

Queste funzionalità garantiscono che:

- le chiavi private risultino sempre opportunamente cifrate con lo stesso livello di sicurezza delle chiavi originali;
- i relativi titolari ne mantengano il controllo esclusivo.

Gli HSM impiegati per l'utilizzo delle chiavi private sono sempre nel numero minimo necessario ad assicurare la continuità del servizio.

6.9 Compromissione della chiave privata

Se la chiave privata della CA TI Trust Technologies è compromessa (o si presume possa esserlo), sarà immediatamente revocato il Certificato corrispondente. Saranno prese misure aggiuntive tra cui la revoca di tutti i certificati di utente finale (cfr. paragrafo 5.6).

6.10 Distruzione della chiave privata

Ove necessario, la CA TI Trust Technologies provvede alla distruzione della chiave privata di CA in modo da garantire ragionevolmente che non vi siano resti residui della chiave che potrebbero portare alla ricostruzione della stessa.

A questo scopo la CA TI Trust Technologies si avvale delle funzionalità messe a disposizione dagli stessi *device* crittografici e altri mezzi adeguati per assicurare la completa distruzione delle chiavi private della CA.

Quando eseguita, l'attività di distruzione della chiave di CA viene registrata (log e/o verbale).

6.11 Dati di attivazione

La CA TI Trust Technologies memorizza e archivia in modo sicuro i dati di attivazione associati con la propria chiave privata.

Le operazioni della CA TI Trust Technologies sono svolte esclusivamente dal personale addetto alla gestione operativa del servizio, sotto la responsabilità del Responsabile della Certificazione.

6.12 Requisiti di sicurezza degli elaboratori

I sistemi operativi usati dalla CA TI Trust Technologies per la gestione dei certificati sono dotati di livello di sicurezza adeguata e segue le procedure di *hardening* definite a livello di Gruppo TIM.

I sistemi operativi sono configurati in modo tale da richiedere sempre l'identificazione dell'utente mediante username e password oppure, nel caso dei sistemi più critici, mediante smartcard e relativo PIN.

Gli eventi di accesso ai sistemi sono loggati, come descritto nella sezione 5.4.

6.13 Sicurezza di rete

L'accesso agli host on-line della CA TI Trust Technologies è protetto da firewall di alta qualità che garantiscono un adeguato filtraggio delle connessioni. Prima dei firewall, una batteria di router che implementano opportune ACL (Access Control List) costituisce un'ulteriore barriera di protezione.

Sui server del servizio di certificazione, tutte le porte di comunicazione non necessarie sono disattivate. Sono attivi esclusivamente quegli agenti che supportano i protocolli e le funzioni necessarie per il funzionamento del servizio.

Per irrobustire il filtraggio delle comunicazioni tutto il sistema di certificazione è suddiviso in un'area esterna, una interna ed una DMZ.

La CA TI Trust Technologies svolge almeno annualmente un *assessment* di sicurezza per verificare l'eventuale presenza di vulnerabilità di rete (Vulnerability Assessment), avvalendosi di specialisti indipendenti (Security Operation Center di TIM).

6.14 Riferimento temporale

La sincronizzazione temporale dei sistemi della CA TI Trust Technologies rispetto alla scala di Tempo Universale Coordinato (UTC), è garantita dall'utilizzo di due orologi di qualità con NTP server incorporato che mantengono allineati i server della piattaforma.

In particolare vengono utilizzati sistemi[13] che permettono:

- la rilevazione satellitare GPS (Global Position System)
- la rilevazione del segnale DCF77, il trasmettitore di frequenza campione e di segnale orario situato in Germania, a Mainflingen.

[13] Time Server Meinberg©:
- "*LANTIME M300/PZF: DCF Time Server with integrated DCF77 radio clock*";
- "*LANTIME M300/GPS : NTP Time Server with integrated GPS radio clock*".

Personale espressamente autorizzato da TI Trust Technologies, provvede a monitorare e garantire il buon funzionamento del sistema di sincronizzazione temporale.

Ulteriori meccanismi di controllo consentono il monitoraggio continuo delle fonti di riferimento temporale, verificando lo stato dei server della piattaforma della CA TI Trust Technologies. Mediante tali dispositivi di monitoraggio, infatti, è possibile richiedere, tramite protocollo SMNP, il riferimento temporale all'elemento di rete monitorato (server), confrontando i dati ricevuti con una terza parte esterna, lo IEN “Galileo Ferraris”.

La rilevazione di qualsiasi anomalia che possa modificare la sincronizzazione dei sistemi, in modo da renderla incompatibile con i requisiti previsti dalla norma, viene registrata e successivamente risolta dal personale autorizzato da TI Trust Technologies.

7 PROFILO DEI CERTIFICATI E DELLE CRL

7.1 Profilo dei certificati

I certificati della CA TI Trust Technologies sono conformi allo standard internazionale ISO/IEC 9594-8:2005 [X.509 versione 3] e alla specifica pubblica [RFC5280]. Inoltre recepiscono i requisiti definiti dal [Regolamento eIDAS] e dallo standard ETSI EN 319 412-1.

La CA TI Trust Technologies emittente compila i campi issuer e subject di ciascun certificato rilasciato dopo l'adozione dei requisiti di cui sopra in conformità con quanto indicato nella Certificate Policy.

Con il rilascio del certificato, la CA TI Trust Technologies dichiara di aver seguito la procedura descritta nella sua CPS per provare che, alla data di emissione del certificato, tutte le informazioni relative al subject erano accurate.

7.1.1 Profilo dei certificati di certificazione

7.1.1.1 Certificato della CA TI Trust Technologies

Il certificato della CA TI Trust Technologies ha il seguente profilo.

Campo	Valore	Commenti
Version	<versione del certificato codificato> =V3	
Serial Number	1	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	20 anni Dal 02/12/2013 16:04:01 GMT Al 27/11/2033 16:04:01 GMT	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) =TI Trust Technologies CA	
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		

Organization Name	subject:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
commonName	subject:commonName (2.5.4.3) =TI Trust Technologies CA	
Organizational Unit	subject:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Country Name	subject:countryName (2.5.4.6) =IT	
Subject Public Key Information	2048-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	
Signature Value	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
Basic Constraints	critico: cA = TRUE pathLenConstraint (opzionale)= 0	
Authority Key Identifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	
Subject Key Identifier	extensions:subjectKeyIdentifier (2.5.29.14) =38 AD 7E D5 E5 62 41 23 FB 83 1A 8B 5D CE 19 6F BF 24 1F 0E	hash della chiave pubblica del Subject
Key Usage	critico: Firma certificati, Firma CRL, Firma CRL offline	
Certificate Policies (OID)	[1]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://ca.tipki.it/TTCA/CPS	
CRL Distribution Points (CDP)	[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/TTCA/CRL	

7.1.1.2 Certificato della CA per il Cliente Ministero dell'Interno

Il certificato della CA ha il seguente profilo:

Campo	**Valore**	**Commenti**
Version	<versione del certificato codificato> =V3	
Serial Number	1	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	

Validity Period	20 anni Dal 02/12/2013 16:46:41 GMT Al 27/11/2033 16:46:41 GMT	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) =TI Trust Technologies per il Ministero dell'Interno CA	
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		
Organization Name	subject:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
commonName	subject:commonName (2.5.4.3) = TI Trust Technologies per il Ministero dell'Interno CA	
Organizational Unit	subject:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Country Name	subject:countryName (2.5.4.6) =IT	
Subject Public Key Information	2048-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	
Signature Value	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
Basic Constraints	critico: cA = TRUE pathLenConstraint (opzionale)= 0	
Authority Key Identifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	
Subject Key Identifier	extensions:subjectKeyIdentifier (2.5.29.14) = 47 2D 74 B9 01 CE 60 FA 35 07 F1 4E 57 3D 99 B9 AD B1 0B 76	hash della chiave pubblica del Subject
Key Usage	critico: Firma certificati, Firma CRL, Firma CRL offline	

Certificate Policies (OID)	[1]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://ca.tipki.it/TTCA/CPS	
CRL Distribution Points (CDP)	[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/MDITTCA/CRL	

7.1.1.3 Certificato della CA 1, TI Trust Technologies

Il certificato della CA, denominata TI Trust Technologies CA 1, ha il seguente profilo:

Campo	Valore	Commenti
Version	<versione del certificato codificato> =V3	
Serial Number	1	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	20 anni Dal 12/05/2015 13:46:20 GMT Al 12/05/2035 13:46:20 GMT	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) =TI Trust Technologies CA 1	
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		
Organization Name	subject:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
commonName	subject:commonName (2.5.4.3) =TI Trust Technologies CA 1	
Organizational Unit	subject:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Country Name	subject:countryName (2.5.4.6) =IT	

Subject Public Key Information	4096-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	
Signature Value	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
Basic Constraints	critico: cA = TRUE pathLenConstraint (opzionale)= 0	
Authority Key Identifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	
Subject Key Identifier	extensions:subjectKeyIdentifier (2.5.29.14) =F3 17 66 EB 48 88 FB EB 5C 97 E3 28 09 75 67 CF 4A 84 AC 0E	hash della chiave pubblica del Subject
Key Usage	critico: Firma certificati, Firma CRL, Firma CRL offline	
Certificate Policies (OID)	[1]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://ca.tipki.it/TTCA/CPS	
CRL Distribution Points (CDP)	[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/TTCA1/CRL	

7.1.1.4 Certificato della CA 2, TI Trust Technologies

Il certificato della CA, denominata TI Trust Technologies CA 2, ha il seguente profilo:

Campo	**Valore**	**Commenti**
Version	<versione del certificato codificato> =V3	
Serial Number	1	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	20 anni Dal 12/05/2015 13:54:48 GMT Al 12/05/2035 13:54:48 GMT	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) =TI Trust Technologies CA 2	
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	

Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		
Organization Name	subject:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
commonName	subject:commonName (2.5.4.3) =TI Trust Technologies CA 2	
Organizational Unit	subject:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Country Name	subject:countryName (2.5.4.6) =IT	
Subject Public Key Information	4096-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	
Signature Value	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
Basic Constraints	critico: cA = TRUE pathLenConstraint (opzionale)= 0	
Authority Key Identifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave= A5 93 C5 9B 92 F1 11 71 AC 36 2E B8 FA 22 B1 99 24 7D 0A 43	
Subject Key Identifier	extensions:subjectKeyIdentifier (2.5.29.14) = A5 93 C5 9B 92 F1 11 71 AC 36 2E B8 FA 22 B1 99 24 7D 0A 43	hash della chiave pubblica del Subject
Key Usage	critico: Firma certificati, Firma CRL, Firma CRL offline	
Certificate Policies (OID)	[1]Criterio certificato: Identificatore criterio= 1.3.76.33.1.1.1 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: http://ca.tipki.it/TTCA/CPS	
CRL Distribution Points (CDP)	[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/TTCA1/CRL	

7.1.1.5 Certificato della CA eIDAS, TI Trust Technologies

Il certificato della CA, denominata TI Trust Technologies eIDAS CA, ha il seguente profilo:

Campo	Valore	Commenti
Version	<versione del certificato codificato> =V3	
Serial Number	1	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	20 anni Dal 01/08/2018 12:04:00 GMT Al 01/08/2038 12:04:00 GMT	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) =TI Trust Technologies eIDAS CA	
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Qualified Trust Service Provider	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Organization Identifier	subject:organizationIdentifier (2.5.4.97) = VATIT-04599340967	
Subject Distinguished Name		
Organization Name	subject:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
commonName	subject:commonName (2.5.4.3) =TI Trust Technologies eIDAS CA	
Organizational Unit	subject:organizationalUnitName (2.5.4.11) = Qualified Trust Service Provider	
Country Name	subject:countryName (2.5.4.6) =IT	
Organization Identifier	subject:organizationIdentifier (2.5.4.97) = VATIT-04599340967	
Key & Signature Properties		

Subject Public Key Information	4096-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	
Signature Value	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
Basic Constraints	critico: cA = TRUE pathLenConstraint (opzionale)= 0	
Subject Key Identifier	extensions:subjectKeyIdentifier (2.5.29.14) = 34 70 93 37 e4 99 d4 79 0b 9e 2d 5d cd 47 52 8a f1 41 4b 87	hash della chiave pubblica del Subject
Key Usage	critico: Firma certificati, Firma CRL, Firma CRL offline	
Certificate Policies (OID)	[1]Criterio certificato: Identificatore criterio=2.5.29.32.0 [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: https://www.trusttechnologies.it/download/documentazione	

7.1.2 Profilo dei certificati qualificati

7.1.2.1 Certificato Qualificato persona fisica su dispositivo QSCD

Il certificato qualificato persona fisica su dispositivo QSCD (Policy ID: 0.4.0.194112.1.2) viene emesso col seguente profilo:

Campo	**Valore**	**Commenti**
Version	<versione del certificato codificato> =V3	
Serial Number	<numero intero univoco>	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	Fino a 36 mesi, espressi in formato UTC	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) = subjectDistinguishedName della CA	In base alla CA emittente l'attributo può assumere rispettivamente uno dei seguenti valori: *- TI Trust Technologies CA* *- TI Trust Technologies CA 1* *- TI Trust Technologies CA 2* *- TI Trust Technologies eIDAS CA* *- TI Trust Technologies per il Ministero dell'Interno CA*

Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		
Organization Name (opzionale)	subject:organizationName (2.5.4.10)	Se presente, questo campo contiene la denominazione dell'organizzazione alla quale appartiene titolare del certificato.
Organization Identifier (opzionale)	subject:organizationIdentifier (2.5.4.97)	Se presente, questo campo contiene la Partita IVA o il Codice Fiscale dell'organizzazione alla quale appartiene titolare del certificato.
GivenName	subject:GivenName (2.5.4.42)	Questo campo contiene il nome di battesimo del titolare del certificato.
SurName	subject:SurName (2.5.4.4)	Questo campo contiene il cognome del titolare del certificato.
commonName	subject:commonName (2.5.4.3)	Questo campo contiene la combinazione dei valori degli attibuti SurName e GivenName separati dal carattere spazio.
serialNumber	subject:serialNumber (2.5.4.5) =<TIN|PAS|IDC|...><COUNTRY_CODE>- <CODICE IDENTIFICATIVO TITOLARE>	Contiene il codice fiscale del titolare indicato con il prefisso TIN, come prescritto dalla norma EN 319412-1 (es. TINIT-CCCNNN64T30H501H). Esclusivamente nel caso in cui al titolare non sia stato assegnato un codice fiscale dall'autorità italiana vengono utilizzati analoghi codici di identificazione come prescritto da [ETSI EN 319 412-1] e [Det. 189/2017].
dnQualifier	subject:dnQualifier (2.5.4.46)	Questo campo contiene il codice identificativo del titolare presso il QTSP.
Country Name	subject:countryName (2.5.4.6)	Questo campo contiene il codice paese a due lettere in formato ISO 3166 dello Stato in cui: - È residente il Titolare - (se valorizzata) è registrata l'organizzazione alla quale appartiene il titolare del certificato.

Subject Public Key Information	2048-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	Chiave pubblica RSA da 2048 bit
Signature	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
AuthorityKeyIdentifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica dell'Issuer). L'estensione non è marcata critica.
SubjectKeyIdentifier	extensions:subjectKeyIdentifier (2.5.29.14)	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica del Subject). L'estensione non è marcata critica
KeyUsage	Non Repudiation	
CertificatePolicies (OID)	certificatePolicies:policyQualifiers:policyQualifierId certificatePolicies:policyIdentifier *<0.4.0.194112.1.2>* [2]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.1.10 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=User notice Definizione: Testo avviso=<Testo di eventuale limitazione di utilizzo del certificato> [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: https://www.trusttechnologies.it/download/documentazione [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	Questa estensione può contenere uno o più *policyIdentifier*, anche privati, che identificano le policy e le procedure utilizzate dalla CA.

AuthorityInformationAccess	<indirizzo del server OCSP> *authorityInfoAccess:* *accessDescription:accessMethod*, specifica il tipo e il formato delle informazioni sull'emittente indicato in *accessDescription:accessLocation*. *id-ad-ocsp (1.3.6.1.5.5.7.48.1)* *id-ad-caIssuers (1.3.6.1.5.5.7.48.2)* *accessDescription:accessLocation*, contiene l'URL che indica posizione e protocollo per accedere al OCSP Responder del QTSP. =[1]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.tipki.it [2]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://ca.tipki.it/<Identificativo CA>/CERT	<Identificativo CA> all'interno della URL di accesso al certificato CA varia in funzione della CA emittente e può assumere uno dei seguenti valori: • TTCA (se *cn=TI Trust Technologies CA*) • TTCA1 (se *cn=TI Trust Technologies CA1)* • TTCA2 (se *cn=TI Trust Technologies CA2)* • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)* • MDITTCA (se *cn=TI Trust Technologies per il Ministero dell'Interno CA*)
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> =[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/<Identificativo CA>/<CDPn>	<Identificativo CA> all'interno della URL di accesso al certificato CA variain funzione della CA emttente epuò assumere uno dei seguenti valori: • TTCA (se *cn=TI Trust Technologies CA*) • TTCA1 (se *cn=TI Trust Technologies CA1)* • TTCA2 (se *cn=TI Trust Technologies CA2)* • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)* • MDITTCA (se *cn=TI Trust Technologies per il Ministero dell'Interno CA*) <CDPn> assume valori variabili in base al contesto e rappresenta il suffisso che completa la url per accedere allo specifico frammento di CRL che gestisce il certificato in oggetto. La url esatta è contenuta nei singoli certificati.
QCStatement	esi4-qcStatement-1	Questa estensione dichiara che il certificato è un certificate qualificato in EU ed è stato emesso in accord con la Direttiva 1999/93/EC [i.3] oppure con l'Annex I, III o IV del Regolamento (EU) No 910/2014, in base a quello in vigore al momento dell'emissione del certificato.
	esi4-qcStatement-3 QcEuRetentionPeriod = 20 (anni)	
	esi4-qcStatement-4	Questa estensione dichiara che la chiave private relative al certificate risiede in un dispositivo Qualified

		Signature/Seal Creation Device (QSCD), in accord con il regolamento (EU) No 910/2014 [i.8] o inun dipsositivo sicuro di firma (SSCD) così come definito nella Direttiva 1999/93/EC
	esi4-qcStatement-5 PdsLocation URL=https://www.trusttechnologies.it/download/disclosure-statement-qc	Contiene la URL dove è disponibile il PKI Disclosure Statements (PDS) realizzato in conformità all'Annex A del documento ETSI EN 319 411-1
	esi4-qcStatement-6 = id-etsi-qct-esign	Indica che il certificato è per firma elettroniche così come definite in Regulation (EU) No 910/2014

La CA si riserva di inserire nel certificato ulteriori informazioni e/o ulteriori estensioni purché nel rispetto della specifica pubblica [RFC5280] e salvaguardando la funzionalità del certificato per l'uso previsto.

7.1.2.2 Certificato Qualificato persona fisica su dispositivo remoto QSCD

Il certificato qualificato persona fisica su dispositivo remoto QSCD (Policy ID: 0.4.0.194112.1.2) viene emesso col seguente profilo:

Campo	Valore	Commenti
Version	<versione del certificato codificato> =V3	
Serial Number	<numero intero univoco>	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	Fino a 36 mesi, espressi in formato UTC	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) = <commonName della CA>	In base alla CA emittente può assumere rispettivamente uno dei seguenti valori: *- TI Trust Technologies CA* *- TI Trust Technologies CA 1* *- TI Trust Technologies CA 2* *- TI Trust Technologies eIDAS CA*
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		

Organization Name (opzionale)	subject:organizationName (2.5.4.10)	Se presente, questo campo contiene la denominazione dell'organizzazione alla quale appartiene titolare del certificato.
Organization Identifier (opzionale)	subject:organizationIdentifier (2.5.4.97)	Se presente, questo campo contiene la Partita IVA o il Codice Fiscale dell'organizzazione alla quale appartiene titolare del certificato.
GivenName	subject:GivenName (2.5.4.42)	Questo campo contiene il nome di battesimo del titolare del certificato.
SurName	subject:SurName (2.5.4.4)	Questo campo contiene il cognome del titolare del certificato.
commonName	subject:commonName (2.5.4.3)	Questo campo contiene la combinazione dei valori degli attibuti SurName e GivenName separati dal carattere spazio.
serialNumber	subject:serialNumber (2.5.4.5) ==<TIN|PAS|IDC|...><COUNTRY CODE>-<CODICE IDENTIFICATIVO TITOLARE>	Contiene il codice fiscale del titolare indicato con il prefisso TIN, come prescritto dalla norma EN 319412-1 (es. TINIT-CCCNNN64T30H501H). Esclusivamente nel caso in cui al titolare non sia stato assegnato un codice fiscale dall'autorità italiana vengono utilizzati analoghi codici di identificazione come prescritto da [ETSI EN 319 412-1] e [Det. 189/2017].
dnQualifier	subject:dnQualifier (2.5.4.46)	Questo campo contiene il codice identificativo del titolare presso il QTSP.
Country Name	subject:countryName (2.5.4.6)	Questo campo contiene il codice paese a due lettere in formato ISO 3166 dello Stato in cui: - È residente il Titolare - (se valorizzata) è registrata l'organizzazione alla quale appartiene il titolare del certificato.
Subject Public Key Information	2048-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	Chiave pubblica RSA da 2048 bit
Signature	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
AuthorityKeyIdentifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica dell'Issuer). L'estensione non è marcata critica.

SubjectKeyIdentifier	extensions:subjectKeyIdentifier (2.5.29.14)	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica del Subject). L'estensione non è marcata critica
KeyUsage	Non Repudiation	
CertificatePolicies (OID)	certificatePolicies:policyQualifiers:policyQualifierId [1]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.n [1,1]Informazioni sulla definizione del criterio: ID definizione criterio=User notice Definizione: Testo avviso=<Testo di eventuale limitazione di utilizzo del certificato> [1,2]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: https://www.trusttechnologies.it/download/documentazione [2]Criterio certificato: Identificatore criterio=*0.4.0.194112.1.2* [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	Questa estensione può contenere uno o più *policyIdentifier*, anche privati, che identificano le policy e le procedure utilizzate dalla CA. Sul primo O.I.D. n può assumere può assumere uno dei valori descritti nel paragrafo 4.5.3
Subject Alternative Name (opzionale)	subjectAltName:Other Name: Telephone number (1.3.6.1.4.1.1466.115.121.1.50) = <numero di cellulare>	Questa estensione viene valorizzata esclusivamente nell'ambito dei servizi di firma remota con autenticazione del titolare tramite telefono cellulare. Se presente contiene quindi la codifica UTF8 del numero di cellulare utilizzabile dal titolare con il proprio certificato.

AuthorityInformationAccess	<indirizzo del server OCSP> *authorityInfoAccess:* *accessDescription:accessMethod*, specifica il tipo e il formato delle informazioni sull'emittente indicato in *accessDescription:accessLocation*. *id-ad-ocsp (1.3.6.1.5.5.7.48.1)* *id-ad-caIssuers (1.3.6.1.5.5.7.48.2)* *accessDescription:accessLocation*, contiene l'URL che indica posizione e protocollo per accedere al OCSP Responder del QTSP. =[1]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.tipki.it [2]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://ca.tipki.it/<Identificativo CA>/CERT	<Identificativo CA> all'interno della URL di accesso al certificato CA variain funzione della CA emttente epuò assumere uno dei seguenti valori: • TTCA (se *cn=TI Trust Technologies CA*) • TTCA1 (se *cn=TI Trust Technologies CA1)* • TTCA2 (se *cn=TI Trust Technologies CA2)* • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)*
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> =[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/<Identificativo CA>/<CDPn>	<Identificativo CA> all'interno della URL di accesso al certificato CA variain funzione della CA emttente epuò assumere uno dei seguenti valori: • TTCA (se *cn=TI Trust Technologies CA*) • TTCA1 (se *cn=TI Trust Technologies CA1)* • TTCA2 (se *cn=TI Trust Technologies CA2)* • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)* <CDPn> assume valori variabili in base al contesto e rappresenta il suffisso che completa la url per accedere allo specifico frammento di CRL che gestisce il certificato in oggetto. La url esatta è contenuta nei singoli certificati.
QCStatement	esi4-qcStatement-1	Questa estensione dichiara che il certificato è un certificate qualificato in EU ed è stato emesso in accord con la Direttiva 1999/93/EC [i.3] oppure con l'Annex I, III o IV del Regolamento (EU) No 910/2014, in base a quello in vigore al momento dell'emissione del certificato.
	esi4-qcStatement-3 QcEuRetentionPeriod = 20 (anni)	

	esi4-qcStatement-4	Questa estensione dichiara che la chiave private relative al certificate risiede in un dispositivo Qualified Signature/Seal Creation Device (QSCD), in accord con il regolamento (EU) No 910/2014 [i.8] o inun dipsositivo sicuro di firma (SSCD) così come definito nella Direttiva 1999/93/EC
	esi4-qcStatement-5 PdsLocation URL=https://www.trusttechnologies.it/download/disclosure-statement-qc	Contiene la URL dove è disponibile il PKI Disclosure Statements (PDS) realizzato in conformità all'Annex A del documento ETSI EN 319 411-1
	esi4-qcStatement-6 = id-etsi-qct-esign	Indica che il certificato è per firma elettroniche così come definite in Regulation (EU) No 910/2014

La CA si riserva di inserire nel certificato ulteriori informazioni e/o ulteriori estensioni purché nel rispetto della specifica pubblica [RFC5280] e salvaguardando la funzionalità del certificato per l'uso previsto.

7.1.2.3 Certificato Qualificato persona giuridica su dispositivo remoto QSCD

Il certificato qualificato persona giuridica su dispositivo remoto QSCD (Policy ID: 0.4.0.194112.1.3) viene emesso col seguente profilo:

Campo	Valore	Commenti
Version	<versione del certificato codificato> =V3	
Serial Number	<numero intero univoco>	
Issuer Signature Algorithm	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	
Validity Period	Fino a 36 mesi, espressi in formato UTC	
Issuer Distinguished Name		
Common Name	issuer:commonName (2.5.4.3) = <commonName della CA>	In base alla CA emittente può assumere rispettivamente uno dei seguenti valori: *- TI Trust Technologies eIDAS CA*
Organizational Unit	issuer:organizationalUnitName (2.5.4.11) =Servizi di certificazione	
Organization Name	issuer:organizationName (2.5.4.10) =Telecom Italia Trust Technologies S.r.l.	
Country Name	issuer:countryName (2.5.4.6) =IT	
Subject Distinguished Name		

Organization Name	subject:organizationName (2.5.4.10)	Questo campo contiene la denominazione dell'organizzazione alla quale appartiene titolare del certificato.
Organization Identifier	subject:organizationIdentifier (2.5.4.97)	Contiene il la Partita IVA (VAT) o il numero di Iscrizione al Registro delle Imprese (NTR), come prescritto dalla norma EN 319412-1 (es. VATIT-04599340967).
commonName	subject:commonName (2.5.4.3)	Questo campo contiene il nome dell'organizzazione.
serialNumber	subject:serialNumber (2.5.4.5) ==<VAT|NTR><COUNTRY CODE>-<CODICE IDENTIFICATIVO ORGANIZZAZIONE>	Contiene il la Partita IVA (VAT) o il numero di Iscrizione al Registro delle Imprese (NTR), come prescritto dalla norma EN 319412-1 (es. VATIT-04599340967). Come previsto in [Det. 121/2019], nel caso di organizzazioni italiane non dotate né di partita IVA né di NTR, ma solamente del codice fiscale, è possibile utilizzare il prefisso "CF:IT" (esempio: CF:IT-97735020584).
dnQualifier	subject:dnQualifier (2.5.4.46)	Questo campo contiene il codice identificativo del titolare presso il QTSP.
Country Name	subject:countryName (2.5.4.6)	- Questo campo contiene il codice paese a due lettere in formato ISO 3166 dello Stato che ha rilasciato il codice identificativo della Persona Giuridica
Subject Public Key Information	2048-bit RSA key modulus, RSAEncryption (1.2.840.113549.1.1.1)	Chiave pubblica RSA da 2048 bit
Signature	sha256RSAWithRSAEncryption (1.2.840.113549.1.1.11)	Firma della CA
Estensione	**Valore**	**Commenti**
AuthorityKeyIdentifier	extensions:authorityKeyIdentifier (2.5.29.35) =ID chiave	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica dell'Issuer). L'estensione non è marcata critica.
SubjectKeyIdentifier	extensions:subjectKeyIdentifier (2.5.29.14)	Contiene il campo *keyIdentifier* (valorizzato con l'hash della chiave pubblica del Subject). L'estensione non è marcata critica
KeyUsage	Non Repudiation	
CertificatePolicies (OID)	certificatePolicies:policyQualifiers:policyQualifi	Questa estensione può contenere uno

	erId certificatePolicies:policyIdentifier *<0.4.0.194112.1.3>* [2]Criterio certificato: Identificatore criterio=1.3.76.33.1.1.1.21 [2,1]Informazioni sulla definizione del criterio: ID definizione criterio=User notice Definizione: Testo avviso=<Testo di eventuale limitazione di utilizzo del certificato> [2,2]Informazioni sulla definizione del criterio: ID definizione criterio=CPS Definizione: https://www.trusttechnologies.it/download/documentazione [3]Criterio certificato: Identificatore criterio=1.3.76.16.6	o più *policyIdentifier*, anche privati, che identificano le policy e le procedure utilizzate dalla CA.
AuthorityInformationAccess	<indirizzo del server OCSP> *authorityInfoAccess:* *accessDescription:accessMethod*, specifica il tipo e il formato delle informazioni sull'emittente indicato in *accessDescription:accessLocation*. *id-ad-ocsp (1.3.6.1.5.5.7.48.1)* *id-ad-caIssuers (1.3.6.1.5.5.7.48.2)* *accessDescription:accessLocation*, contiene l'URL che indica posizione e protocollo per accedere al OCSP Responder del QTSP. =[1]Accesso alle informazioni sull'autorità Metodo di accesso=Protocollo di stato del certificato online (1.3.6.1.5.5.7.48.1) Nome alternativo: URL=http://ocsp.tipki.it [2]Accesso alle informazioni sull'autorità Metodo di accesso=Autorità emittente il certificato (1.3.6.1.5.5.7.48.2) Nome alternativo: URL=http://ca.tipki.it/<Identificativo CA>/CERT	<Identificativo CA> all'interno della URL di accesso al certificato CA variain funzione della CA emttente epuò assumere uno dei seguenti valori: • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)*
CRLDistributionPoints (CDP)	<indirizzo HTTP per accedere alla CRL> =[1]Punto di distribuzione CRL Nome punto distribuzione: Nome completo: URL=http://ca.tipki.it/<Identificativo CA>/<CDPn>	<Identificativo CA> all'interno della URL di accesso al certificato CA variain funzione della CA emttente epuò assumere uno dei seguenti valori: • TTEFQCA (se *cn=TI Trust Technologies eIDAS CA)* <CDPn> assume valori variabili in base al contesto e rappresenta il suffisso che completa la url per accedere allo specifico frammento di CRL che gestisce il certificato in oggetto. La url esatta è contenuta nei singoli certificati.

QCStatement	esi4-qcStatement-1	Questa estensione dichiara che il certificato è un certificate qualificato in EU ed è stato emesso in accord con la Direttiva 1999/93/EC [i.3] oppure con l'Annex I, III o IV del Regolamento (EU) No 910/2014, in base a quello in vigore al momento dell'emissione del certificato.
	esi4-qcStatement-3 QcEuRetentionPeriod = 20 (anni)	
	esi4-qcStatement-4	Questa estensione dichiara che la chiave private relative al certificate risiede in un dispositivo Qualified Signature/Seal Creation Device (QSCD), in accord con il regolamento (EU) No 910/2014 [i.8] o inun dipsositivo sicuro di firma (SSCD) così come definito nella Direttiva 1999/93/EC
	esi4-qcStatement-5 PdsLocation URL=https://www.trusttechnologies.it/download/disclosure-statement-qc	Contiene la URL dove è disponibile il PKI Disclosure Statements (PDS) realizzato in conformità all'Annex A del documento ETSI EN 319 411-1
	esi4-qcStatement-6 = id-etsi-qct-eseal	Indica che il certificato è per sigilli così come definiti in Regulation (EU) No 910/2014

La CA TI Trust Technologies si riserva di inserire nel certificato ulteriori informazioni e/o ulteriori estensioni purché nel rispetto della specifica pubblica [RFC5280] e salvaguardando la funzionalità del certificato per l'uso previsto.

7.2 Profilo della CRL

Le CRL sono conformi allo standard internazionale ISO/IEC 9594-8:2005 [X.509 versione 2] e alla specifica pubblica [RFC5280].

Oltre ai dati obbligatori, le CRL contengono:

- il campo *nextUpdate* (data prevista per la prossima emissione della CRL)
- l'estensione *CRLNumber* (numero progressivo della CRL)
- l'estensione *Authority Key Identifier*
- l'estensione *Issuing Distribution Point* (punto di distribuzione della CRL)
- l'estensione *ExpiredCertOnCRL*

7.3 Profilo dell'OCSP

L'OCSP è conforme alla specifica pubblica [RFC6960].

La CA TI Trust Technologies mantiene traccia del profilo OCSP in un documento tecnico indipendente, reso disponibile, su richiesta, a propria discrezione.

8 VERIFICHE DI CONFORMITÀ

Il business di riferimento per TI Trust Technologies è costituito dalla *fornitura di prodotti e servizi collegati alle tecnologie di crittografia a chiave pubblica* (PKI - Public Key Infrastructure).

I servizi erogati prevedono il rispetto di precisi obblighi normativi imposti dalla normativa nazionale ed internazionale.

Le disposizioni normative attribuiscono alla figura della Certification Authority la responsabilità di adottare i requisiti tecnici, organizzativi e societari, nonché di sicurezza previsti dalla norma di riferimento per lo svolgimento dell'attività e di rispettare le prescrizioni previste dalla normativa vigente e di verificarne l'efficacia. A tal fine, TI Trust Technologies effettua verifiche ed ispeziioni periodiche e programmate circa la propria conformità alle suddette prescrizioni.

8.1 Argomenti coperti dalle verifiche

L'ispezione è finalizzata a verificare la conformità del servizio CA di TI Trust Technologies alle norme di legge, dal punto di vista tecnico ed organizzativo. L'ispezione segue delle Linee Guida basate sulla norma europea [ETSI TS 101 456] ("*Policy requirements for certification authority issuing qualified certificates*").

8.2 Frequenza

Al fine di adempiere agli obblighi di legge previsti in materia di gestione dei servizi della Certification Authority, le attività di verifiche interne vengono eseguite annualmente mediante ispezioni programmate. La frequenza annuale è ritenuta adeguata per assicurare il controllo della conformità del QTSP rispetto alle prescrizioni di riferimento.

TI Trust Technologies si sottopone almeno ogni due anni ad una verifica da parte di un organismo di valutazione della conformità, presentando nei tempi richiesti all'organismo di vigilanza il relativo rapporto di conformità.

8.3 Relazioni tra la CA TI Trust Technologies e gli ispettori esterni

Non esiste alcuna relazione tra la CA TI Trust Technologies e AgID che possa in alcun modo influenzare l'esito delle ispezioni a favore di TI Trust Technologies.

Il responsabile Audit di TI Trust Technologies è un dipendente che riporta direttamente alla Direzione ed è pertanto indipendente dalla struttura organizzativa preposta all'erogazione del servizio di CA.

8.4 Azioni conseguenti alle verifiche

I risultato delle ispezioni, siano esse effettuate internamente, da AgID o da un Ente Certificatore, sono condivise con la CA TI Trust Technologies attraverso un verbale di ispezione.

Il risultato dell'ispezione viene comunicato alla Direzione ed ai responsabili della struttura organizzativa preposta all'erogazione del servizio di CA.

TI Trust Technologies predispone un Piano di Adeguamento che consente di indicare le azioni correttive da realizzare per il ripristino del livello di compliance previsto quando, a seguito delle attività di verifica, siano emerse *non conformità*[14]. Il Piano di Adeguamento deve riportare per ciascuna delle non conformità individuate, le modalità, le responsabilità ed i tempi con i quali si intendono effettuare le azioni di miglioramento. La formalizzazione di un Piano di Adeguamento completo ed adeguato costituisce lo strumento che consente a TI Trust Technologies di programmare e di monitorare le azioni per la risoluzione delle non conformità riscontrate. Pertanto, è necessario che il Piano sia compilato applicando le seguenti linee guida:

- le azioni correttive devono essere descritte in modo specifico e con un livello di dettaglio sufficiente a consentire una valutazione della loro efficacia;
- per ciascuna azione deve essere chiaramente individuato il "responsabile dell'attuazione", nell'ambito della struttura organizzativa interessata. Qualora la realizzazione dell'azione sia di competenza di più funzioni aziendali, il "responsabile dell'attuazione" avrà il compito di richiedere l'intervento delle funzioni competenti e di verificarne la realizzazione;
- per ciascuna azione dovranno essere indicati i tempi di realizzazione. Tali tempi dovranno essere i più brevi possibile, in particolare per le misure che derivano da obblighi previsti dalla legge.

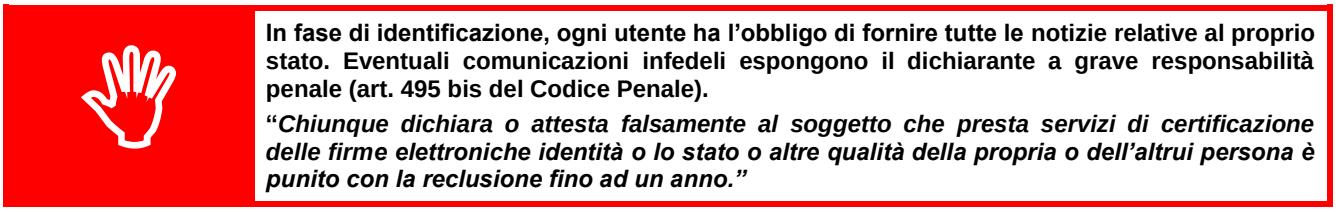
Il Piano di Adeguamento deve essere condiviso con il Responsabile dell'Audit che verifica la completezza e la correttezza dei dati riportati. L'attuazione dello stesso sarà oggetto di monitoraggio successivo da parte del Responsabile dell'Audit che dovrà verificare la conclusione di ciascuna azione.

9 ASPETTI OPERATIVI E LEGALI PER L'UTILIZZO DEI SERVIZI

I servizi erogati da TI Trust Technologies sono regolati dalle condizioni generali e specifiche per l'utilizzo dei servizi di certificazione che devono essere sottoscritte in fase di richiesta del servizio. Tali condizioni, pubblicate sul sito web

[14] *Non conformità*: esiti negativi ai controlli effettuati in Fase di Esecuzione.

https://www.trusttechnologies.it/download/legale-e-privacy/ sono sottoscritte con firma digitale, per accettazione, dal Rappresentante Legale di TI Trust Technologies.



9.1 Tariffe del servizio

In caso di vendita diretta del servizio al Cliente Finale, le tariffe sono pubblicate sullo store on line del sito web https://www.trusttechnologies.it.

Per i servizi di vendita indiretta le condizioni sono negoziate caso per caso, in base ai volumi richiesti e possono essere soggette a variazioni salva la facoltà di recesso epr il cliente.

9.2 Tutela della riservatezza e trattamento dei dati personali

TI Trust Technologies è titolare dei dati personali raccolti in fase di identificazione e registrazione dei soggetti che richiedono i certificati e si obbliga quindi a trattare tali dati con la massima riservatezza e nel rispetto di quanto previsto dalla [Normativa Privacy].

L'informativa privacy fornita al titolare ed è pubblicata sul sito web https://www.trusttechnologies.it/download/legale-e-privacy/

9.3 Diritti di proprietà intellettuale

L'utilizzo dei servizi non implica per nessuno dei partecipanti alcuna alterazione sui diritti di proprietà intellettuale di cui ciascuno è detentore.

9.4 Validità temporale del documento

Questo documento ha valore a partire dal momento della sua pubblicazione fino al momento della sua eventuale sostituzione con una nuova versione, come specificato nel cap. **2** .

Anche in caso di cessazione delle attività da parte di TI Trust Technlogies (cfr. **5.7**), il presente documento mantiene la sua applicabilità per tutte le operatività successive alla cessazione.

9.5 Modifiche

Eventuali modifche che TI Trust Technologies intende apportare al presente CPS che non influiscono sull'attuazione della CP o sull'accetabilità dei certificati, saranno effettuate senza nessuna informativa preventiva come definito nel cap.2.3 .

9.6 Risoluzione delle dispute

Qualsiasi controversia derivante dal presente CPS tra TI Trust Technologies ed i clienti del servizio è deferita al giudizio di un collegio arbitrale. La sede dell'arbitrato sarà Roma.

9.7 Legge applicabile

Questo CPS è soggetto alla legge italiana e come tale sarà interpretato ed eseguito. Per quanto non espressamente previsto nel presente CPS, valgono le norme vigenti.

Altri contratti in cui questo CPS è incorporato con riferimento possono contenere clausole distinte rispetto alla legge applicabile.

9.8 SLA, indicatori e misure di qualità

In questo paragrafo sono definiti gli indicatori atti a descrivere i livelli di qualità della fornitura.

Gli SLA (Service Level Agreement) riportati nel seguito sono validi per il servizio erogato da TITT con piattaforma allocata e gestita presso il centro servizi di Pomezia.

Gli SLA vengono calcolati sulla base delle segnalazioni degli utenti tracciate su trouble ticket aperti dai tecnici dell'Help Desk. In particolare, ogni segnalazione di guasto che perviene al numero verde gestito dall'Help Desk dà luogo all'apertura di un ticket la cui registrazione consente di effettuare un monitoraggio periodico per la verifica del rispetto degli SLA.

Servizio	SLA
Disponibilità dei SERVIZI	99,5% su base 4 mesi
Disponibilità Certificate Revocation List (CRL) ed OCSP	99,8% su base 4 mesi
Supporto di Help Desk telefonico	H24 7x7
Consegna del kit di firma (QSCD)	15 giorni dalla ricezione dell'ordine in presenza di tutte le informazioni ed i documenti necessarie per la produzione
Attivazione del servizio di firma su dispositivo QSCD remoto	Entro 15 gg (entro 7 giorni lavorativi se ordine da WEB) lavorativi dalla ricezione dell'ordine in presenza di tutte le informazioni ed i documenti necessarie per la produzione