Registro O.I.D.

QTSP TI Trust Technologies

COMPLEMENTO AL CPS

VERSIONI DEL DOCUMENTO		
Revisione	Descrizione delle modifiche	Emissione
00	Prima emissione	01/08/2018

Indice degli argomenti

1 INTRODUZIONE

Telecom Italia Trust Technologies S.r.l. (nel seguito **TI Trust Technologies**, TI.TT o TSP, v. anche par. **Errore. L'origine riferimento non è stata trovata.**) 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 il registro degli OID (Object Identifier) che identificano le tipologie di certificato gestiti da TI.TT.

TI Trust Technologies rende disponibile la versioni aggiornata del documento al seguente indirizzo:
https://www.trusttechnologies.it/download/documentazione

1.2 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
LDAP	**Lightweight Directory Access Protocol**: protocollo utilizzato per la gestione degli accessi al registro dei certificati e l'effettuazione di operazioni di prelievo di certificati e liste di revoca e sospensione.
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.

1.3 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

2 QTSP "TI Trust Technologies S.R.L."

L'OID per l'organizzazione "**TI Trust Technologies S.R.L**." è

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

Il TSP definisce ed organizza i suoi OID per certificati e documenti che fanno riferimento al [CPS] in conformità al ***Regolamento eIDAS*** e al *Codice dell'Amministrazione Digitale (**CAD**)*.

La tabella seguente indica gli OID che identificano le categorie di oggetti gestiti nei propri servizi da TI.TT.

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
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
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
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, come illustrato nei paragrafi seguenti.

2.1.1 O.I.D. Certificati Qualificati per servizi di firma remota

La seguente tabella elenca gli OID dei certificati qualificati di firma elettronica utilizzati nell'ambito dei servizi di firma remota:

OID	*Descrizione*
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	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.

2.1.2 O.I.D. Certificati Qualificati su smart card/token

La seguente tabella elenca gli OID dei certificati qualificati distribuiti attraverso smart card/token

OID	*Descrizione*
1.3.76.33.1.1.1	Certificate Policy per i *Certificati Qualificati* per chiavi private custodite su smart card/token, emessi in conformità alla normativa italiana sulla Firma Digitale.