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

Manuale Operativo
per le procedure di firma digitale remota nell'ambito dei servizi di Gruppo TELEPASS.

Codice documento: MO_TPASS

OID: 1.3.76.21.1.50.7

Redazione: Antonio Raia

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

Data emissione: 12/12/2022

Versione: 03

Revisioni

Versione n°: 03	***Data Revisione: 12/12/2022***
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti normativi e tecnici par. *D.2*: aggiornamento par. *F.1*: aggiornamento par. *Q*: aggiornamento
Motivazioni:	Variazione proprietà, direzione e coordinamento Aggiornamenti normativi
Versione n°: 02	***Data Revisione: 16/01/2020***
Descrizione modifiche:	Estensione alle società del gruppo Modifica limitazione d'uso del certificato Aggiornamento riferimenti normativi
Motivazioni:	Estensione manuale operativo alle società del gruppo Telepass Aggiornamenti normativi
Versione n°: 01	***Data Revisione: 07/03/2017***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

Riferimenti di legge

Testo Unico - DPR 445/00 e successive modificazioni e integrazioni	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. "Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa". Nel seguito indicato anche solo come *TU*.
DLGS 196/03 – Codice della Privacy e successive modificazioni e integrazioni	Decreto Legislativo 30 giugno 2003, n. 196. "*Codice in materia di protezione dei dati personali*", modificato e integrato dal DLGS 101/2018. Nel seguito indicato anche solo come *DLGS 196/03*
CAD - DLGS 82/05 e successive modificazioni e integrazioni	Decreto Legislativo 7 marzo 2005, n. 82. "Codice dell'amministrazione Digitale". Nel seguito indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e successive modificazioni e integrazioni	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 "Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, n.d.r.). Nel seguito indicato anche solo come *DPCM*.
Regolamento (UE) N. 910/2014 (eIDAS) e successive modificazioni e integrazioni	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS* (electronic IDentification, Authentication and trust Services).
Regolamento (UE) N. 2016/679 (GDPR) e successive modificazioni e integrazioni	REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Nel seguito indicato anche solo come *GDPR* (General Data Protection Regulation).
DETERMINAZIONE N. 147/2019 e successive modificazioni e integrazioni	Linee guida contenenti le "*Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate*". Nel seguito indicato anche solo come *DETERMINAZIONE*.

Definizioni e acronimi

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP Qualified Trust Service Provider. Certificatore Accreditato	*Prestatore di Servizi Fiduciari Qualificati*. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A.
Servizio Fiduciario Qualificato	Servizio elettronico fornito da un QTSP e consistente negli elementi di cui all'Art.3, punto 16) e 17) del Reg. UE 910/2014 (eIDAS). Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta i servizi qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime.
Certificato Qualificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Reg. UE 910/2014 (eIDAS)

Chiave Privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave Pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale sul documento informatico.
CRL	Lista dei Certificati Revocati, Certificate Revocation List, un elenco che riporta i certificati revocati o sospesi, non più considerati validi dal Certificatore che li ha emessi.
OCSP	Online Certificate Status Protocol: servizio di verifica dello stato di validità del Certificato, secondo il protocollo OCSP.
Documento informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FEQ - Firma Elettronica Qualificata FD - Firma Digitale	Firma elettronica creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
Firma Remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal certificatore accreditato, che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
HSM - Hardware Security Module	Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014. Anche detti Dispositivi di Firma.
Qualified Electronic Time Stamp (Marca Temporale)	*Validazione Temporale Elettronica Qualificata* Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi dati esistevano in quel momento. Risponde ai requisiti dell'Art.42 del Reg. eIDAS
CA - Certification Authority	Autorità che emette i certificati per la firma elettronica.
RA - Registration Authority	*Autorità di Registrazione*: entità che, su incarico del QTSP, ha la responsabilità di registrare e verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al QTSP per emettere il Certificato Qualificato.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Richiedente	La Persona Fisica che richiede il Certificato.
Titolare	La Persona Fisica cui il certificato qualificato è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma elettronica qualificata o digitale.
Cliente Cliente Prospect	É il Cliente (o potenziale cliente, detto Prospect) della società del Gruppo.
Terzo Interessato	La persona fisica o giuridica il cui consenso è necessario per il rilascio al Titolare del Certificato Qualificato Ha il diritto/dovere di richiedere la revoca o sospensione del certificato nel caso risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
TSA - Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.

A. Introduzione

Questo documento è il Manuale Operativo per la procedura di Firma Digitale Remota nell'ambito dei servizi offerti da *TELEPASS S.P.A.* - Società per azioni Capitale Sociale € 26.000.000,00 interamente versato Codice Fiscale e n. di iscrizione al Registro delle Imprese di Roma 09771701001 REA-ROMA n. 1188554 - P.IVA 09771701001 - Sede Legale: Via A. Bergamini, 50 - 00159 Roma (di seguito anche solo *TELEPASS*) e dalle società del *Gruppo Telepass*.

Il Manuale Operativo descrive le procedure e relative regole utilizzate dal *Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A.* (di seguito anche solo *QTSP INTESA, Certificatore* o *INTESA*) per l'emissione dei Certificati Qualificati, la generazione e la verifica della firma elettronica qualificata nell'ambito dei servizi offerti dalle società del Gruppo Telepass.

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

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme vigenti e future che regolano la fattispecie concreta.

Per quanto non espressamente previsto nel presente Manuale Operativo, si fa riferimento alle norme tempo per tempo vigenti.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dalle Local Registration Authority (LRA), ovverosia dalla stessa TELEPASS o società del Gruppo Telepass (di seguito congiuntamente intesi come "**Gruppo Telepass**"), la quale, in virtù di specifico accordo con il QTSP INTESA, è autorizzata a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare la procedura di Firma Digitale Remota di documenti esclusivamente nell'ambito dei servizi offerti dalle piattaforme del Gruppo Telepass.

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS).

A.1. Proprietà intellettuale

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

Quanto qui descritto per l'espletamento delle attività di QTSP è coperto da diritti sulla proprietà intellettuale.

A.2. Validità

Quanto descritto in questo documento si applica al QTSP INTESA, cioè alle sue infrastrutture logistiche e tecniche e al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata relativa a tali certificati, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 del DPCM, al comma 4. Ai fini del suddetto decreto, le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle relative regole utilizzate dal QTSP INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei prestatori di servizi fiduciari qualificati.

Pertanto, in funzione delle normative menzionate, vengono coinvolte più entità che saranno meglio identificate nel prosieguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.***03***, rilasciata in conformità con l'Art.40 del DPCM, del *Manuale Operativo del QTSP In.Te.S.A. S.p.A. per le procedure di firma digitale remota nell'ambito dei servizi offerti da Telepass S.p.A., da società appartenenti al Gruppo Telepass, ovvero da terze società partner, purché offerti tramite le piattaforme di titolarità di Telepass S.p.A. o di società del Gruppo Telepass*.

L'object identifier (OID) di questo documento è ***1.3.76.21.1.50.7***.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica:

- all'indirizzo Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*
- nell'ambito del sito istituzionale del Gruppo Telepass.

Nota: la pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire solo previa autorizzazione dell'Agenzia per l'Italia Digitale.

B.2. Dati identificativi del QTSP – Qualified Trust Service Provider

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

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289** **10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**N. Iscrizione 1692/87**
N. di Partita I.V.A.	**05262890014**
N. di telefono (centralino)	**+39.011.19216.111**
Sito Internet	***www.intesa.it***
Indirizzo di posta elettronica	***marketing@intesa.it***
Indirizzo (URL) registro dei certificati	***ldap://x500.e-trustcom.intesa.it***
ISO Object Identifier (OID)	**1.3.76.21**

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art.40 comma 3 lett. c) del DPCM, è della Certification Authority INTESA, che ne cura la stesura e la pubblicazione.

Allo scopo di raccogliere eventuali osservazioni e richieste di chiarimenti, INTESA ha predisposto i seguenti strumenti:

- un recapito di posta elettronica: *marketing@intesa.it*
- un recapito telefonico: +39 011.192.16.111
- un servizio di HelpDesk per le chiamate dall'Italia 800.80.50.93
  per le chiamate dall'estero +39 02. 39.30.90.66

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal QTSP espletando, per la parte di loro competenza, le attività a loro attribuite.

Il personale responsabile delle attività di certificazione, in conformità con l'Art.38 del DPCM, è articolato nelle figure seguenti tutte appartenenti all'organizzazione del QTSP:

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

B.4.1. Certification Authority (CA)

INTESA, operando in ottemperanza a quanto previsto dal DPCM, CAD e dal Reg. eIDAS, espleta le attività di Qualified Trust Service Provider. Tali attività includono i servizi fiduciari qualificati di creazione, verifica e convalida di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche (marche temporali).

I dati identificativi del QTSP INTESA sono riportati al precedente par. *B.2*.

B.4.2. Registration Authority (RA)

Per la particolare tipologia di servizio offerto (Firma Digitale Remota nell'ambito delle applicazioni di firma descritte in questo Manuale Operativo), il QTSP INTESA rilascia mandato a svolgere le funzioni di Local Registration Authority (LRA) alla società del Gruppo che opererà in tale ruolo.

In particolare, la LRA potrà svolgere le seguenti attività:

- Identificazione certa del Titolare.
- Registrazione del Titolare.

La società del Gruppo Telepass, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente.

C. Obblighi

C.1. Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)

Nello svolgimento della sua attività, il Prestatore di Servizi Fiduciari Qualificato (indicato anche come *Certificatore Accreditato*) opera in conformità con quanto disposto da:

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

In particolare, il QTSP:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
- si attiene alle regole tecniche specificate nel DPCM e ss.mm.ii.;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'Art.29 del Reg. eIDAS;
- rilascia e rende pubblico il certificato qualificato secondo quanto stabilito all'Art.32 del CAD, nel rispetto del GDPR e del DLGS 196/03;
- informa i richiedenti, in modo esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali;

- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza del QTSP) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

Inoltre, il QTSP:

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

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

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo potrà ricevere un certificato qualificato di firma digitale remota di atti e documenti nell'ambito dei servizi offerti dalle piattaforme del Gruppo Telepass.

Il Titolare è tenuto a conservare le informazioni necessarie all'utilizzo della chiave privata di firma in modo adeguato e ad adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri (CAD, Art.32, comma 1).

Il Titolare della chiave deve inoltre:

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

- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

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

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

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

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

Gli obblighi sopra descritti sono automaticamente espletati dai Software di Verifica conformi alle normative vigenti (Art. 14 del DPCM) e implementati nei servizi offerti dal QTSP INTESA sui portali del Gruppo Telepass.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato provvederà all'inoltro delle richieste di revoca o sospensione nei casi e nelle modalità previste dal presente Manuale Operativo e dalla normativa vigente.

C.5. Obblighi della Registration Authority esterna

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

In particolare, la LRA deve espletare le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- registrazione del Titolare;
- consegna al Titolare dei codici che gli permettano di accedere alla propria chiave di firma nel rispetto degli Artt. 8 e 10, comma 2, del DPCM.

Il QTSP INTESA ha rilasciato mandato a svolgere la funzione di Registration Authority (RA) alla società del Gruppo Telepass (LRA) mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere la Local RA cui INTESA assegna l'incarico di RA e sui quali il QTSP ha l'obbligo di vigilare; in particolare si richiede di:

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

La documentazione relativa alle attività di cui sopra e necessaria all'emissione del Certificato Qualificato viene conservata secondo gli obblighi di legge, per 20 (venti) anni.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

Il QTSP INTESA è responsabile verso i Titolari per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal GDPR, dal CAD e dal Reg. eIDAS (e loro ss.mm.ii.), come descritto al par. *C.1.Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)*.

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

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

Il QTSP INTESA non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma Digitale Remota in relazione alla limitazione d'uso come specificata al par. *F.1.3*.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal QTSP INTESA. Si ricorda, in particolare, di conservare con la dovuta diligenza dispositivi OTP e codici segreti indispensabili per accedere alle chiavi di firma.

D.2. Assicurazione

Il QTSP INTESA è beneficiario di contratti assicurativi per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è resa disponibile ad AgID apposita dichiarazione di stipula.

E. Tariffe

Per la particolarità del servizio oggetto di questo Manuale Operativo, il QTSP INTESA non indica delle tariffe per l'emissione, il primo rinnovo, la revoca e la sospensione dei certificati.

Queste verranno eventualmente indicate nei contratti che verranno stipulati fra TELEPASS e il Titolare.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

Il QTSP deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

Questa operazione viene demandata alla Local Registration Authority (società del Gruppo Telepass), ed è svolta in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito.

Ai fini dell'identificazione certa dei clienti (comprendendo pertanto anche la fase di verifica dell'identità), la LRA acquisisce tutti i dati propedeutici all'espletamento degli obblighi di Adeguata Verifica della clientela ed effettua l'identificazione certa del richiedente ai sensi del D.Lgs 231/2007 e ss.mm.ii. (per i servizi per i quali è richiesta).

Per i servizi per cui non è richiesta l'aderenza normativa al D.Lgs 231/2007 (ad esempio Toll Payment – Telepedaggio Telepass Family), la verifica dell'identità viene condotta dallo stesso personale adottato per

le verifiche AML, utilizzando le stesse procedure AML, ma che, rispetto a quelle regolarmente adottate per servizi o prodotti AML, non prevedono la verifica dello stato di PEP (Persona Politicamente Esposta).

Fra i **dati di registrazione** necessari all'avviamento del servizio ricordiamo:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Indirizzo di residenza;
- Domicilio presso il quale saranno inviate le eventuali comunicazioni cartacee;
- Numero di telefono cellulare;
- Indirizzo di posta elettronica;
- Tipo e numero del documento d'identità esibito;
- Autorità che ha rilasciato il documento, data e luogo del rilascio, data di scadenza.

La documentazione relativa alla registrazione dei Titolari viene conservata dalla LRA che ha effettuato l'identificazione per il periodo necessario ad assolvere le finalità contrattuali, gli obblighi di legge e garantire l'eventuale difesa dei diritti in giudizi nel rispetto degli obblighi normativi tempo per tempo vigenti

F.1.1. Identificazione tramite identificazione precedente

Il QTSP INTESA si avvale dell'identificazione già effettuata da un *Intermediario finanziario* o da altro *Soggetto Esercente Attività Finanziaria*, che, ai sensi delle norme antiriciclaggio tempo per tempo vigenti, è obbligato all'identificazione dei propri clienti.

Tale modalità di identificazione presuppone che il Titolare abbia un rapporto già in essere con il Soggetto di cui sopra.

Gli Intermediari e gli altri Soggetti Esercenti Attività Finanziaria acquisiscono i dati in base alle procedure adottate secondo la normativa antiriciclaggio vigente al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale Operativo).

I dati identificativi del Titolare raccolti all'atto della registrazione sono quindi utilizzati per l'emissione del certificato "one-shot" a lui intestato, previa sua conferma dei dati anagrafici e accettazione delle condizioni contrattuali per il rilascio del certificato e delle modalità operative per l'apposizione della firma digitale.

F.1.2. Identificazione tramite meccanismi di riconoscimento biometrico

L'identificazione può essere effettuata dalla LRA anche mediante soluzioni tecnologiche di riconoscimento biometrico, per le quali la LRA si avvale di un provider esterno specializzato, e che prevedono la verifica di corrispondenza tra a) i dati biometrici del volto del richiedente rappresentato sul documento di identità fornito dal richiedente stesso e b) i dati biometrici del volto del richiedente presente nelle immagini video (cd. Selfie dinamico o video-selfie) acquisite dal richiedente.

Tale processo è subordinato a rilascio da parte del richiedente di uno specifico consenso privacy al trattamento dei dati biometrici da parte della LRA e si articola nelle seguenti fasi:

- L'Utente, in fase di adesione ai prodotti/servizi del Gruppo, dovrà scattare la foto fronte/retro di un suo documento di identità valido e procedere al caricamento in App/sito della LRA, cui copia sarà fornita ai sistemi del provider prescelto;
- L'Utente provvederà, su App e/o sito della LRA, ad effettuare il cd. selfie dinamico o video-selfie del suo volto secondo quanto verrà richiesto in maniera dinamica e randomica (es. Al richiedente viene richiesto di scattare una foto con delle pose del viso e/o dello sguardo secondo indicazioni di volta in volta suggerite dallo strumento integrato nell'App/sito, oppure viene richiesto di leggere ad alta voce delle cifre visualizzate, in maniera dinamica, sul display.)

- A valle dell'acquisizione delle immagini e dei dati come sopra descritto, in back end le applicazioni del provider individuato provvederanno a verificare che i dati e le informazioni fornite dall'utente coincidano con i dati identificativi indicati dallo stesso in fase di registrazione e che anche il volto rappresentato nel cd. Selfie dinamico coincida con quello riportato sul documento di identità. Tali controlli saranno effettuati sia tramite metodi automatici di riconoscimento facciale sia attraverso verifiche da parte di operatori di back office del Gruppo Telepass.
  Si precisa che gli operatori del Gruppo Telepass sono sempre coinvolti ai fini della verifica dei risultati dei controlli sulle immagini e sui video effettuati dal provider individuato. Nel caso in cui dalle verifiche dovessero emergere difformità e/ o anomalie (quali a titolo esemplificativo documento di identità non leggibile, foto non chiaramente visualizzabile) si provvederà a ricontattare l'utente tramite contatto telefonico e/o e-mail per invitarlo a seguire nuovamente le fasi sopra descritte.
- All'esito positivo dei controlli su descritti, utili alla corretta identificazione dell'Utente, la LRA provvederà ad effettuare gli ulteriori controlli necessari al completamento del processo di adeguata verifica della clientela richiesto dalla normativa antiriciclaggio, laddove la stessa sia applicabile per i servizi richiesti dall'Utente, espletando tutti gli obblighi in osservanza delle disposizioni previste dalla vigente normativa Antiriciclaggio e Contrasto al Finanziamento del Terrorismo.

La procedura descritta garantisce, altresì, la cifratura del canale di comunicazione mediante il quale vengono acquisiti i video e le immagini attraverso l'adozione di meccanismi standard, applicativi e protocolli aggiornati: in particolare si utilizza per le comunicazioni una crittografia TLS almeno 1.2 e a 256 bit sempre e per tutte le operazioni e sul dispositivo di ogni richiedente.

F.1.3. Limitazioni d'uso

Nel Certificato Qualificato per la Firma Digitale Remota, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti dalle piattaforme del Gruppo Telepass, è inserito il seguente limite d'uso:

"*Il presente certificato è valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti o promossi tramite le piattaforme del Gruppo Telepass.*"

"*This certificate may only be used for unattended/automatic digital signature for the signature of documents and/or contracts concerning products and/or services offered or promoted through the Telepass Group web portals.*".

Nota: Ulteriori specifici limiti d'uso potranno essere concordati con Gruppo Telepass.

G. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione

G.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile dei Servizi di Certificazione, come previsto dal DPCM all'Art.7

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

Il tutto avviene in modalità dual control ad evitare operazioni illecite.

Le operazioni successive alla generazione delle coppie di chiavi di certificazione sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto attraverso le chiavi contenute in tali dispositivi di autorizzazione di cui sopra.

Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "*n di m*", in modo che solo la concomitante presenza di almeno *n* di *m* parti della chiave permettano di operare con gli opportuni privilegi. Pertanto, esse vengono custodite in apposite casseforti distinte.

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

G.2. Generazione delle chiavi del sistema di validazione temporale

La generazione delle chiavi di validazione temporale avviene in conformità a quanto stabilito dall'Art.49 del DPCM.

La lunghezza delle chiavi del sistema di validazione temporale è conforme alla normativa tempo per tempo vigente.

G.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del QTSP, è possibile procedere alla generazione delle chiavi di sottoscrizione.

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato dopo essersi autenticato tramite il portale o le piattaforme di titolarità del Gruppo Telepass.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è conforme alla normativa tempo per tempo vigente) vengono create su dispositivi sicuri, Hardware Security Module (HSM), conformi a quanto previsto dalla normativa vigente.

Una volta completata il processo di apposizione della firma sul documento da sottoscrivere, le chiavi del Titolare sono eliminate dal dispositivo HSM.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel par. *G.1*, sono generati i certificati delle chiavi pubbliche, conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia per l'Italia Digitale attraverso il sistema di comunicazione di cui all'Art.12, comma 1, del DPCM.

H.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.33 del DPCM.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta al par. *G.3*, è possibile generare una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione del portale o delle piattaforme di titolarità del Gruppo Telepass alla Certification Authority del QTSP.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.18, comma 4).

H.2.1. Informazioni contenute nei certificati

I certificati emessi dal QTSP INTESA nell'ambito del presente manuale, sono certificati qualificati ai sensi del Regolamento (UE) 910/2014 (eIDAS) e, pertanto, ne è garantita la loro interoperabilità e riconoscimento a livello comunitario.

Il Certificato Qualificato definisce con certezza il QTSP che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

Ogni Certificato Qualificato per la firma elettronica emesso dal QTSP INTESA è conforme al Regolamento eIDAS e alla DETERMINAZIONE AgID N. 147/2019 (*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati*).

Ogni Certificato Qualificato per la Firma Digitale contiene, a titolo esemplificativo, ma non esaustivo, le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del QTSP;
- codice identificativo unico del Titolare presso il QTSP;
- nome, cognome, codice fiscale del Titolare;

- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale Operativo conterranno sempre una limitazione d'uso (par. *F.1.3*).

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi disponibili sui portali del Gruppo Telepass, rende disponibile ai Titolari quanto necessario a generare delle Firme Digitali conformi a quanto previsto dalla normativa vigente.

La particolare, tipologia del servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer. La funzionalità di Firma Digitale è richiamabile via internet accedendo ai servizi offerti dai portali del Gruppo.

I documenti sottoscritti non conterranno macroistruzioni o codici eseguibili tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati (DPCM, art. 4 comma 3).

I.1. Firma con certificato One-Shot

Il QTSP INTESA fornisce un servizio di Firma Digitale Remota, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato "one-shot", cioè una particolare tipologia di certificato per la quale è prevista una validità temporale limitata all'apposizione della prima firma.

Per richiedere l'emissione di tale tipologia di certificato e la successiva firma elettronica qualificata, il Titolare:

- si connette al portale o alle piattaforme di titolarità del Gruppo Telepass; prende visione, oltre che del presente documento, di un'informativa contenente una descrizione del processo che verrà messo in atto per l'emissione del certificato e la firma del documento;
- si autentica tramite la verifica di un codice OTP ricevuto sul numero di cellulare precedentemente indicato;
- visualizza il documento in modalità digitale;
- richiede l'emissione del certificato "one-shot" e la firma del documento;

L'emissione e la firma potranno avvenire solo dopo che siano state espletate le procedure di adeguata verifica che garantiscono l'identificazione certa (par. *F.1*).

Una volta identificato il Titolare, conformemente a quanto specificato dall'informativa di processo visionata dal Titolare, la CA provvede a:

- Generare il certificato qualificato one-shot su di un HSM custodito e gestito sotto la responsabilità del QTSP INTESA;
- firmare il documento in modalità automatica, utilizzando il certificato "one-shot" appena emesso;
- conformemente alla normativa, è apposta la marca temporale generata dal servizio di validazione temporale del QTSP, descritto al par. *Q*;
- al termine della firma, le chiavi di sottoscrizione sono cancellate dall'HSM, rendendo così inutilizzabile il certificato per ulteriori sottoscrizioni.

J. Modalità operative per la verifica della firma

I documenti sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF.

Tale formato di sottoscrizione è di facile utilizzo nell'ambito delle applicazioni di firma digitale remota, in quanto la verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC* scaricabile gratuitamente dal sito www.adobe.com.

K. Modalità di revoca e sospensione dei certificati

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

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

La lista CRL è disponibile anche sul registro dei certificati.

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

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

K.1. Revoca dei certificati

Un certificato può essere revocato su richiesta del Titolare, del Terzo Interessato o della Certification Authority (cioè il QTSP).

Il certificato revocato non può essere in alcun modo riattivato.

K.1.1. Revoca dei certificati di sottoscrizione

Data la natura del servizio, la revoca del certificato non si rende necessaria, in quanto le chiavi di sottoscrizione sono cancellate dal dispositivo di firma dopo l'utilizzo.

In ogni modo, il Titolare può richiedere la revoca del proprio Certificato, utilizzando i canali di comunicazione definiti con la Local RA (Gruppo Telepass) o contattando direttamente il QTSP.

Il QTSP provvederà all'immediata revoca del certificato e Titolare sarà avvisato dell'avvenuta revoca.

K.1.2. Revoca dei certificati relativi a chiavi di certificazione

Il QTSP procede con la revoca dei certificati di certificazione e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione nei casi di:

- compromissione della chiave di certificazione;
- guasto del dispositivo di firma (HSM) delle chiavi di Certificazione, nel caso sia compromessa la sicurezza delle chiavi ivi contenute;
- cessazione dell'attività.

Entro 24 ore, il QTSP notificherà la revoca all'Agenzia per l'Italia Digitale e ai Titolari.

K.2. Sospensione dei certificati

Il servizio oggetto di questo manuale non prevede la sospensione del certificato del Titolare, in quanto il certificato emesso all'atto della firma ha validità temporale limitata e le chiavi sono cancellate subito dopo la sottoscrizione.

L. Modalità di sostituzione delle chiavi

L.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare

Per i servizi oggetto di questo manuale, i certificati digitali emessi dal QTSP INTESA hanno una validità limitata legata all'utilizzo del certificato stesso e non ne è prevista la sostituzione alla scadenza. Le chiavi del Titolare sono cancellate dal dispositivo di firma immediatamente dopo la sottoscrizione.

L.2. Sostituzione delle chiavi del Certificatore

L.2.1. Sostituzione in emergenza delle chiavi di certificazione

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) contenente le chiavi di certificazione (CA e TSCA) o di disastro presso la sede centrale è trattato al par. *P - Procedura di gestione degli eventi catastrofici*.

L.2.2. Sostituzione pianificata delle chiavi di certificazione

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

L.2.3. Chiavi del sistema di validazione temporale (TSA)

In conformità con quanto indicato all'Art.49, comma 2, del DPCM, ai fini di limitare il numero di marche temporali generate con la medesima coppia di chiavi di validazione temporale, queste sono sostituite entro 90 (novanta) giorni dalla data della loro emissione. Contestualmente, un certificato è emesso relativamente alla nuova coppia di chiavi (senza revocare il precedente, relativo alla coppia di chiavi sostituita).

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

- I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
- I certificati delle chiavi di certificazione (CA e TSCA).
- I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
- Certificati per le chiavi di firma dell'Agenzia per l'Italia Digitale (DPCM Art.42, comma 1).
- Le liste di revoca e sospensione (CRL).

Le operazioni che coinvolgono il registro dei certificati vengono svolte soltanto dalle persone a ciò autorizzate, presenti in quantità adeguata a impedire azioni illecite da parte di un limitato numero di addetti.

Il QTSP mantiene una copia di riferimento del registro dei certificati inaccessibile dall'esterno; questa aggiorna in tempo reale la copia operativa, accessibile da parte degli utenti con protocollo LDAP.

La verifica di rispondenza tra copia di riferimento e copia operativa è fatta sistematicamente.

M.2. Accesso logico al Registro dei certificati

La copia di riferimento è collocata all'interno di una rete dedicata protetta da adeguati dispositivi, per cui non è accessibile ad altri che dal server di emissione dei certificati, che vi registra i certificati emessi e le CRL.

L'accesso sulle copie operative è possibile all'indirizzo ***ldap://x500.e-trustcom.intesa.it*** (protocollo LDAP).

Il QTSP INTESA consente anche l'accesso alle CRL attraverso il protocollo http, all'URL indicato nel campo CDP (CRL Distribution Point) del certificato.

M.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo se in modalità dual control ad evitare azioni illecite.

Gli addetti alla gestione dei sistemi, alla gestione della rete, alla manutenzione, ecc., possono accedere al locale ove il sistema è installato e, per gli addetti specifici, operarvi solo in presenza di addetti abilitati alla gestione del registro dei certificati secondo le modalità precedentemente esplicitate per gli operatori abilitati.

N. Modalità di protezione dei dati personali

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure previste dal Regolamento Europeo 679/2016 (GDPR), dal DLGS 196/03 e loro successive modificazioni e integrazioni.

O. Procedura di gestione della copie di sicurezza

Gli archivi informatici che sono oggetto di copie di sicurezza sono i seguenti:

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *M*.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonché le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del QTSP (Art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

La conservazione, per tutte le copie di sicurezza descritte, è conforme a quanto previsto dalle normative vigenti in materia.

P. Procedura di gestione degli eventi catastrofici

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

- gestione dell'emergenza: in questa fase è garantita la continuità di accesso alle CRL; la loro emissione può subire ritardi derivanti dalla necessità di attivare il server di backup della CA, situato nel sito di back up;
- gestione del transitorio: in questo periodo è assicurata l'emissione dei certificati e il ripristino di ulteriori soluzioni di disaster recovery;
- ritorno dell'esercizio a regime: nel medesimo sito originale o in un altro alternativo, ma definitivo.

Va premesso che la presenza di repliche della copia operativa del registro dei certificati distribuite in più punti consente comunque, in caso di interruzione di funzionamento di una delle sedi, di accedere al contenuto del registro dei certificati aggiornato fino al momento dell'interruzione.

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e HW, anche della situazione di emergenza.

In tutte le sedi interessate dalla gestione degli eventi catastrofici è depositata copia cartacea del piano di emergenza.

Q. Modalità per l'apposizione e la definizione del riferimento temporale

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

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata mediante il protocollo *NTP* (*Network Time Protocol*). L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi, a loro volta, sono sincronizzati alla

scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

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

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.41 del DPCM). I server dedicati ai servizi di marcatura temporale hanno, inoltre, un controllo software tra l'orario della macchina e un cospicuo numero di server NTP distribuiti a livello planetario: l'utilità di controllo, installata su ognuno dei server utilizzati dal QTSP INTESA nell'ambito della validazione temporale, periodicamente verifica l'allineamento del clock di sistema questi NTP Server di riferimento. Se l'allineamento temporale non risulta conforme alle specifiche tecniche di riferimento tempo per tempo vigenti, il servizio di marcatura temporale erogato dallo specifico server che risultasse disallineato viene arrestato. Alla data, è previsto il blocco del sistema di validazione temporale in caso di superamento di una soglia di tolleranza fissata a 1 (un) minuto secondo (in valore assoluto).

Q.1. Modalità di richiesta e verifica marche temporali

Il QTSP INTESA appone una marca temporale (validazione temporale elettronica qualificata, ai sensi del Reg. eIDAS) su tutti i documenti sottoscritti dal Titolare nell'ambito dei servizi descritti da questo Manuale Operativo.

L'apposizione di detta marca è un processo integrato con l'operazione di firma e non richiede nessuna attività specifica da parte del Titolare.

R. Lead Time e Tabella Raci per il rilascio dei certificati

Di seguito si riporta la Tabella relativa al "Lead Time di Processo" per la gestione delle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto	Richiesta	Ente Coinvolto	Azione Ente Coinvolto	Ente Coinvolto	Azione Ente Coinvolto
Utente, Richiedente, Titolare Certificato	*Richiesta di Emissione del Certificato vs. LRA*	*Società del Gruppo (acting as) Local RA*	*Emette ordine di pubblicazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Certificazione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Revoca del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Società del Gruppo (acting as) LRA*	*Emette ordine di revoca del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Revoca*
Utente, Richiedente, Titolare Certificato	*Richiesta di Sospensione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Società del Gruppo (acting as) LRA*	*Emette ordine di sospensione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*Intesa (acting as) Registration Authority (RA) o Società del Gruppo (acting as) LRA*	*Emette ordine di riattivazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Riattivazione*

Di seguito si riporta la Tabella RACI relativa alla individuazione delle responsabilità degli enti coinvolti nelle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

Soggetto Coinvolto	Responsible	Accountable	Consulted	Informed
Registration Authority	***X***			
Local Registration Authority	***X***			
Certification Authority		***X***		
Utente, Richiedente, Titolare del Certificato			***X***	***X***

S. Riferimenti Tecnici

ETSI-319.401	ETSI EN 319 401 v2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.4.4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.2.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.3.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

------- FINE DEL DOCUMENTO -------