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 remota nell'ambito dei servizi di CABEL Industry S.p.A.

Codice documento: MO_CB

OID: 1.3.76.21.1.50.2

Redazione: Antonio Raia

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

Data emissione: 5/01/2023

Versione: 03

Revisioni

Versione n°: 03	***Data revisione: 5 gennaio 2023***
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti normativi e tecnici par. *B.4*: aggiornamento par. *C.5*: aggiornamento par. *D.1*: aggiornamento par. *D.2*: aggiornamento par. F: aggiornamento par. *G*: aggiornamento Aggiornamento layout e correzione refusi
Motivazioni:	Variazione proprietà, direzione e coordinamento del QTSP Aggiornamento servizi Aggiornamenti normativi e Tecnici
Versione n°: 02	***Data revisione: 27 giugno 2016***
Descrizione modifiche:	Aggiornamento dati societari e logo Formattazione documento
Motivazioni:	Variazione dati societari e logo
Versione n°: 01	***Data revisione: 20 gennaio 2015***
Descrizione modifiche:	Nessuna
Motivazioni:	Prima emissione

Sommario

Riferimenti di legge

Testo Unico - DPR 445/00 e ss.mm.ii.	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*.
CAD - DLGS 82/05 e ss.mm.ii.	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 ss.mm.ii.	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 ss.mm.ii.	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS.*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	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.*
DETERMINAZIONE N. 147/2019 e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel 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 Qualificato*. 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 QTSP (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/Utente Richiesta di certificazione	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione.
SCA	PSD2 Strong Customer Authentication
Titolare	La Persona Fisica cui il certificato qualificato di firma è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma digitale.
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.
Giornale di Controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il QTSP, tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza (DPCM 22/02/2013, Art. 36)
RACI (Tabella)	RACI - Responsible, Accountable, Consulted, Informed Matrice di assegnazione delle responsabilità (in un processo)

A. Introduzione

Il presente documento costituisce il Manuale Operativo del QTSP INTESA per la procedura di Firma Digitale Remota nell'ambito dei servizi forniti da *CABEL Industry S.p.A. - Sede Legale Via Cherubini 99 - 50053 Empoli (FI); Tel. 0571/020.000 Web: www.cabel.it; - Codice fiscale e N. Iscrizione al Registro delle Imprese di Firenze 04780250488 R.E.A. FI 485272 – Partita IVA 04780250488.*

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 Decreto Legislativo 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.

Questo documento descrive le regole e le procedure operative del *QTSP In.Te.S.A. S.p.A.* (nel seguito, *QTSP INTESA, Certificatore* ovvero anche solo *INTESA*) per l'emissione dei certificati qualificati, la generazione e la verifica della firma elettronica qualificata e le procedure del servizio di validazione temporale in conformità con la vigente normativa quando questa è gestita all'interno di progetti bancari o finanziari.

In questa tipologia di progetti, le entità bancarie o finanziarie, erogatrici dei servizi di home banking e delle applicazioni di sportello, fungeranno anche da *Local Registration Authority* (nel seguito, *LRA*) per conto del QTSP INTESA. Nel seguito, tali entità bancarie o finanziarie verranno richiamate con il termine di *Banca* o *Istituto di Pagamento* (o anche solo *Banca / Istituto*).

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dal QTSP INTESA ovvero dalla stessa Banca / Istituto che, in virtù di specifico accordo con il QTSP INTESA, è autorizzata a svolgere la funzione di Local Registration Authority.

Si sottolinea che tutti i processi di sottoscrizione di documenti oggetto del presente Manuale Operativo saranno implementati esclusivamente all'interno di applicazioni bancarie o finanziarie.

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS) e con la Determinazione AgID 147/2019.

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, nonché 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, anche avvalendosi delle marche temporali qualificate emesse dal QTSP INTESA, e alla Banca / Istituto di pagamento in qualità di Local Registration Authority.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5, comma 4 del DPCM, in cui si dispone che 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 elettroniche 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 validazione temporale elettronica;
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 che disciplinano l'emissione di certificati qualificati da parte del QTSP INTESA.

Le suddette regole e procedure scaturiscono dall'ottemperanza alle attuali normative di riferimento la cui osservanza permette ad INTESA di essere inserita nell'elenco dei certificatori accreditati (EU Trusted List).

Pertanto, al fine di adempiere alle normative menzionate, risulterà necessario il coinvolgimento di più entità che saranno meglio identificate nel proseguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.***03*** del *Manuale Operativo per le procedure di firma elettronica qualificata remota nell'ambito dei servizi di Cabel Industry S.p.A.*, emesso in conformità con l'Art.40 del DPCM.

L'object identifier (OID) di questo documento è ***1.3.76.21.1.50.2***.

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 della Banca / Istituto.

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

Lo stesso manuale operativo viene pubblicato e aggiornato in simultanea anche sul sito di Cabel.

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

Il QTSP (*Prestatore di Servizi Fiduciari Qualificato*) 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 del QTSP 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 Help Desk *www.hda.intesa.it*
  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 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.

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*.

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

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

Le figure sopra elencate sono tutte appartenenti all'organizzazione del QTSP INTESA.

B.4.2. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (firma elettronica qualificata remota nell'ambito delle applicazioni bancarie e finanziarie), il QTSP demanda lo svolgimento di alcune funzioni di Registration Authority alla Banca / Istituto che avrà acquisito il servizio fornito da Cabel.

La Banca / Istituto, nell'esercizio della funzione di Local Registration Authority (LRA) si impegna a svolgere le seguenti attività:

- Identificazione del Titolare.
- Registrazione del Titolare.

La Banca/Istituto dovrà vigilare affinché l'attività di identificazione si svolga nel rispetto della normativa vigente e di quanto previsto nel presente Manuale Operativo.

B.4.3. Terzo Interessato

Nell'ambito del presente manuale, la Banca/Istituto riveste il ruolo di Terzo interessato, in qualità di committente del servizio del QTSP INTESA per persone aderenti alla propria organizzazione (dipendenti, collaboratori o affiliati).

In quest'ottica, la Banca/Istituto definisce l'opportuna limitazione di utilizzo per i certificati emessi e utilizzati nell'ambito dei servizi di firma elettronica qualificata e richiede la revoca dei medesimi quando non ne sussistono più le condizioni che ne hanno determinato l'emissione (ad es. dimissioni).

Inoltre, dà consenso all'inserimento nel Certificato Qualificato dell'indicazione dell'Organizzazione e di eventuali poteri di rappresentanza.

Gli obblighi del Terzo Interessato sono riportati al par. *C.4*.

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 dal:

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

- Regolamento (UE) 2016/679 (GDPR).

In particolare, il QTSP:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- 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 sicuro per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'Art.29 del Reg eIDAS;
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'Art.32 del CAD;
- informa i richiedenti, in modo esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza 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);
- secondo quanto stabilito dall'Art.14 del DPCM, fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali;
- 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).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato qualificato per i servizi descritti nel presente Manuale Operativo è un soggetto appartenente all'organizzazione della Banca/Istituto che opera da Registration Authority.

Il Titolare riceverà un certificato qualificato per la Firma Elettronica Qualificata Remota, con cui poter sottoscrivere atti e documenti nell'ambito dei servizi della Banca/Istituto nelle modalità descritte al paragrafo *G - Modalità operative per la sottoscrizione di documenti*.

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo 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;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (Art.5, comma 5, del DPCM);
- fare immediata denuncia alle Autorità competenti e alla Banca / Istituto, in caso di perdita o furto dei codici e/o dei dispositivi indicati per accedere alle proprie chiavi di firma; la Banca / Istituto provvederanno all'immediata revoca del certificato;
- 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.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, nei servizi descritti dal presente Manuale Operativo, è la Banca/Istituto.

Pertanto, la Banca / Istituto, nella veste di Terzo Interessato:

- verifica che il richiedente sia in possesso di tutti i requisiti necessari e autorizza il richiedente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota;
- svolge un'attività di supporto al Titolare;
- indica al QTSP eventuali ulteriori limitazioni d'utilizzo del Certificato Qualificato per la Firma Digitale oltre a quelle previste al par. *F.1.1*.

La Banca / Istituto, come Terzo Interessato, quindi, potrà indicare al QTSP eventuali limitazioni d'uso del certificato, eventuali poteri di rappresentanza e dovrà comunicare qualsiasi variazione delle stesse.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza.

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

C.5. Obblighi delle Local Registration Authority (LRA)

Il QTSP INTESA, per esigenze connesse alla fornitura del servizio, potrà avvalersi 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.

Il QTSP In.Te.S.A. S.p.A. può demandare lo svolgimento della funzione di Registration Authority alla Banca o all'Istituto di pagamento mediante specifico *Contratto di Mandato*, sottoscritto da entrambe le parti.

In particolare, le LRA esterne espletano le seguenti attività:

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

Nel contratto di mandato sono esplicitati gli obblighi cui si deve attenere la Banca/Istituto cui i QTSP INTESA assegna l'incarico di LRA e sui quali il QTSP ha l'obbligo di vigilare.

In particolare, si richiede alla LRA di:

- vigilare affinché l'attività di identificazione posta in essere si svolga nel rispetto della normativa vigente (CAD, DPCM, Reg. eIDAS e normativa in materia di Antiriciclaggio);
- rendere possibile il tracciamento dell'operatore di LRA che ha effettuato l'identificazione del Titolare;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il GDPR;
- rendere disponibile ad INTESA il materiale raccolto nella fase di identificazione e registrazione;
- conservare in modo sicuro la documentazione raccolta nella fase di identificazione e registrazione, quindi inviarla all'Ufficio RA del QTSP INTESA su richiesta della QTSP stessa;
- consentire l'accesso presso i propri locali di personale del QTSP, ovvero di terzi dallo stesso incaricati, per adempiere agli obblighi di ispezione (audit); tale accesso deve essere consentito anche agli auditor incaricati dall'Organismo di Vigilanza (AgID);
- segnalare senza indugio al QTSP INTESA, per tramite dell'Ufficio RA (*uff_ra@intesa.it*) ovvero dei propri riferimenti INTESA, ogni evento o incidente inerente i punti indicati precedentemente, nonché tutte le violazioni della sicurezza o le perdite di integrità che abbiano un impatto significativo sui servizi oggetto del presente 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 ogni successiva modificazione e integrazione) 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 del 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 Certificatore 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.1.1*.

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 certificatore accreditato. Si ricorda, in particolare, di conservare con la dovuta diligenza i dispositivi OTP e i 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

Il Servizio viene fornito dalla Banca/Istituto ai soggetti appartenenti alla propria organizzazione: le tariffe per l'emissione, il rinnovo, la revoca e la sospensione dei certificati possono essere eventualmente indicate nei contratti stipulati fra la LRA e 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.

La suddetta operazione può essere svolta dalla Banca/Istituto che, in qualità di LRA e in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio, identificherà e registrerà il Titolare.

Per i successivi rinnovi, se effettuati quando il certificato qualificato già rilasciato è in corso di validità, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al QTSP attraverso la Banca/Istituto solo gli eventuali cambiamenti relativi ai propri dati di registrazione.

Il servizio di identificazione potrà essere gestito, dalla Banca / Istituto ovvero dal QTSP, in modalità:

- *Canonica*: il Richiedente viene identificato *de visu in presenza*, presso una filiale della Banca o dell'Istituto da parte di un operatore formato ai sensi della normativa antiriciclaggio.

Attraverso le procedure di cui sopra, il QTSP INTESA, anche per tramite della LRA Banca / Istituto, entrerà in possesso di tutte le informazioni previste dalla legge, in totale sicurezza e nel pieno rispetto della privacy.

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 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.

Dopo che il Titolare è stato identificato, l'operatore della Banca / Istituto comunica a Cabel l'avvenuto riconoscimento e, quest'ultima, provvede alla predisposizione e consegna di un dispositivo OTP fisico che, unitamente al Codice Utente e la Password personale, già in possesso del Titolare, consentirà a quest'ultimo di accedere all'area riservata del portale, al fine di garantire un accesso sicuro ai servizi di firma remota forniti da Cabel.

Nel caso in cui il Titolare sia già in possesso delle credenziali sopraindicate, l'attività post riconoscimento si ricondurrà all'associazione, con standard bancari, di tali credenziali al certificato appena emesso.

Preventivamente al rilascio di un certificato qualificato, il Titolare dovrà inoltre:

- prendere visione del Manuale Operativo del QTSP INTESA;
- autorizzare il trattamento dei propri dati personali per le finalità legate all'emissione di un certificato qualificato per la firma elettronica.

La documentazione precedente, relativa alla registrazione dei Titolari, viene conservata dalla LRA per 20 (venti) anni dalla scadenza del certificato.

Dopo il rilascio del certificato qualificato, per le successive operazioni di firma, l'utilizzo congiunto degli strumenti di autenticazione precedentemente definiti (Codice utente Banca, Password utente Banca e dispositivo OTP fisico) è richiesto dalla normativa vigente.

Solo attraverso l'uso congiunto di PIN e OTP sarà possibile sottoscrivere digitalmente documenti di vario genere.

F.1.1. Limiti d'uso

Nel Certificato Qualificato per la firma elettronica, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti dalla Banca / Istituto, è inserito sempre un limite d'uso, che deve essere riportato sia in lingua italiana, sia in lingua inglese.

La formula standard è la seguente:

> "*L'utilizzo del certificato e' limitato ai rapporti con Nome Banca / Istituto e con le aziende da essa rappresentate.*".
> "*This certificate may only be used in dealings with Nome Banca / Istituto and with the companies it represents.*".

Specifici limiti d'uso potranno essere concordati con la Banca o con l'Istituto.

INTESA non è responsabile dei danni derivanti dall'uso di un certificato qualificato che ecceda i limiti posti allo stesso o derivanti dal superamento di tale limite.

F.2. Identificazione eseguita da un Istituto Bancario/Finanziario

Intesa può delegare l'attività di identificazione certa ad un Istituto Bancario/Finanziario.

L'identificazione dovrà avvenire seguendo i requisiti di cui al Decreto Legislativo 21 novembre 2007, n. 231, come modificato dal D. Lgs. 25 maggio 2017, n. 90, dalla direttiva (UE) 2015/849 del Parlamento europeo e del Consiglio, del 20 maggio 2015, come modificata dalla Direttiva (UE) 2018/843, ovvero in applicazione della normativa afferente la verifica dell'identità ai sensi della Direttiva (UE) 2018/843, e ss.mm.ii., in aderenza alle relative implementazioni a livello dei singoli Stati Membri.

L'identificazione dovrà tenere conto, anche, degli Orientamenti congiunti delle Autorità di Vigilanza Europee, emanati ai sensi dell'art. 17 e dell'art. 18, par. 4, della direttiva (UE) 2015/849 sulle misure semplificate e rafforzate di adeguata verifica della clientela ed essere completata e perfezionata prima del rilascio del certificato qualificato.

F.3. Registrazione degli utenti richiedenti la certificazione

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi della Certification Authority.

Questa operazione potrà essere eseguita mediante un'applicazione software direttamente richiamabile dagli applicativi della Banca o dell'Istituto di Pagamento.

G. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi della Banca o dell'Istituto, rende disponibile ai Titolari quanto necessario a generare delle firme elettroniche qualificate conformemente 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, ma piuttosto delle funzionalità di firma richiamabili via internet o accedendo ai servizi forniti dalla LRA o da Cabel.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno assolutamente conformi a quanto previsto dal DPCM all'Art.3 comma 2 relativamente agli algoritmi utilizzati.

Inoltre, tali documenti come richiesto dall'Art.3 comma 3 dello stesso DPCM, non conterranno macro istruzioni o codici eseguibili, tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati.

A conferma dell'effettuazione delle operazioni di firma, verranno inviati degli SMS, qualora un Titolare possegga uno smartphone abilitato alla lettura della corrispondenza; su richiesta del Titolare stesso, in alternativa potranno essere inviate alla sua attenzione delle e-mail.

G.1. Autenticazione con Token OTP

Questa modalità di autenticazione prevede che all'utente, già precedentemente identificato, sia rilasciato un codice PIN di identificazione del certificato stesso e un dispositivo hardware di autenticazione (Token USB) per confermare la propria volontà di firmare un documento.

Pertanto, quando il Titolare vorrà firmare un documento accedendo al portale della Banca/Istituto, utilizzerà un'autenticazione a due fattori attraverso l'inserimento di un Codice Utente e Password Bancarie (informazione che solo l'utente conosce) associate ad un OTP (dato dal Token fisico che solo l'utente possiede).

G.1.1. Processo di Firma Remota

Entrato in possesso del proprio certificato qualificato il Titolare potrà procedere alla firma di un documento secondo le modalità di seguito descritte.

L'utente titolare del certificato qualificato di firma remota può sottoscrivere i documenti tramite un processo che prevede i seguenti controlli prima dell'applicazione della firma:

a. L'utente deve effettuare un login a dominio Bancario.
   Questo step consente di esercitare un primo fattore di autenticazione di tipo *SYK* (*Something You Know*) e avere la garanzia che la richiesta di firma possa essere istanziata solo da postazioni di lavoro attestate in contesti Bancari e coperte da stringenti policy di sicurezza tipiche di tali ambiti (antivirus, filtri applicativi, filtri admin, etc.)
b. L'utente si logga, con un'altra utenza applicativa, all'applicazione web della Banca in cui sono resi disponibili i documenti da firmare.
   Questo step consente di esercitare un secondo fattore di autenticazione di tipo SYK e di ereditare le policy di sicurezza applicate all'applicazione web in cui opera l'utente.
   L'applicazione è quella Bancaria tramite la quale l'utente svolge il day-by-day lavorativo.
c. L'utente è chiamato ad inserire un codice OTP valido generato dalla chiavetta OTP.

Qualora i documenti da firmare fossero più di uno, il Titolare per ogni documento deve reiterare lo step c).

G.2. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF; tale formato di sottoscrizione è considerato infatti di facile utilizzo nell'ambito delle applicazioni di firma remota.

Infatti, la verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software Acrobat Reader scaricabile gratuitamente dal sito *www.adobe.com/it*.

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

H.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile 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 per 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 solamente 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.

H.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 di certificazione è conforme alla normativa tempo per tempo vigente.

H.3. Generazione delle chiavi di sottoscrizione

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

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato facendone richiesta alla LRA.

Successivamente, il Titolare, effettuando il primo accesso della sessione di lavoro al sistema LRA ed effettuando un secondo login all'applicativo per lo svolgimento delle proprie mansioni, potrà confermare la corretta consegna del dispositivo OTP necessario all'utilizzo delle chiavi di sottoscrizione, attraverso una prima autenticazione OTP associata alla propria utenza applicativa.

Le modalità sono descritte al par. *G. Modalità operative per la sottoscrizione di documenti*.

Le coppie di chiavi di sottoscrizione sono create su dispositivi di firma sicuri (HSM - Hardware Security Module), conformi alle specifiche di cui all'*Allegato II* del Reg. eIDAS.

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

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta al par. *H.3*, 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.

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

I.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. *H.3*, è generata 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 PKCS#10 di certificato sarà immediatamente inviata dall'applicazione della Banca / Istituto alla Certification Authority del QTSP, anche per il tramite di servizi securizzati esposti dalla CA.

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

I.3. Informazioni contenute nei certificati

I certificati del QTSP INTESA, emessi 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 Certificatore che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

Ogni Certificato Qualificato per la Firma Digitale contiene 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*).

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale contengono almeno una limitazione d'uso (par. *F.1.1*).

I.4. Codice di Emergenza

Il Certificatore garantisce in conformità con quanto previsto dall'Art.21 del DPCM un codice di emergenza da utilizzarsi per richiedere la ***sospensione urgente*** del Certificato.

Nelle applicazioni descritte dal presente Manuale Operativo, sarà considerato come codice di emergenza il codice OTP definito in precedenza.

J. 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.

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

La lista CRL è disponibile anche sul registro dei certificati (par. *L*).

Nei casi in cui la revoca ovvero la sospensione avvengano su iniziativa del Certificatore o del Terzo Interessato (artt. 23, 25, 27 e 29 del DPCM), il Certificatore 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).

J.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.

J.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca o dell'Istituto oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto.

Il QTSP, avvertito dalla Banca / Istituto, provvederà all'immediata revoca del certificato.

J.1.2. Revoca su richiesta del Terzo Interessato

La Banca o l'Istituto, in qualità di Terzo Interessato, possono richiedere la revoca del certificato.

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso ovvero all'indirizzo di residenza, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

J.1.3. Revoca su iniziativa del Certificatore

Il Certificatore che intende revocare il Certificato Qualificato, salvo casi di motivata urgenza, ne dà preventiva comunicazione via e-mail o PEC alla Banca / Istituto (Terzo interessato) e contemporaneamente sarà data comunicazione al Titolare all'indirizzo e-mail indicato in fase di richiesta del Certificato della Firma Digitale ovvero all'indirizzo di residenza, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

J.1.4. Revoca dei certificati relativi a chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- cessazione dell'attività.

il Certificatore procede con la revoca dei certificati di certificazione corrispondenti e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione.

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

J.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al par. *J.1*.

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba effettivamente essere revocato (ad esempio nei casi in cui si tema lo smarrimento o furto del Token OTP, oppure si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

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

In assenza di comunicazioni da parte del Titolare, il certificato verrà automaticamente revocato dopo un periodo di sospensione di 90 (novanta) giorni o comunque entro la data di scadenza del certificato stesso.

La data di decorrenza della revoca coinciderà, in ogni caso, con la data di decorrenza della sospensione.

J.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione del certificato accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca o dell'Istituto oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto.

Il Certificatore procede alla sospensione che verrà comunicata al Titolare utilizzando specifiche funzioni rese disponibili all'interno dei servizi della Banca o dell'Istituto.

Successivamente il Titolare potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre dalla Banca / Istituto.

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione indicato in fase di richiesta e la data di revoca coinciderà con la data di decorrenza della sospensione.

J.2.2. Sospensione su richiesta del Terzo Interessato

La Banca o l'Istituto di Pagamento, in qualità di Terzo Interessato, potranno richiedere la sospensione del certificato.

Il Certificatore, accertata la correttezza della richiesta, sospenderà tempestivamente il certificato e ne darà notizia della sospensione ai Titolari interessati tramite posta elettronica o con comunicazione attraverso i servizi esposti dalla Banca o dall'Istituto.

J.2.3. Sospensione su iniziativa del Certificatore

Il Certificatore salvo i casi di motivata urgenza potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo e-mail fornito in fase di registrazione ovvero all'indirizzo di residenza, specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

Una comunicazione analoga verrà inviata dal Certificatore anche al Terzo Interessato.

K. Modalità di sostituzione delle chiavi

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

I certificati qualificati di firma elettronica emessi dal Certificatore nell'ambito del contesto descritto nel presente Manuale Operativo hanno validità di 36 (trentasei) mesi dalla data di emissione.

Al termine dei tre anni si renderà necessaria la generazione di una nuova coppia di chiavi di sottoscrizione e contestualmente l'emissione di un nuovo certificato.

In questo caso la procedura seguita per l'emissione del nuovo certificato sarà simile a quella indicata in fase di primo rilascio, al netto della fase di identificazione del Titolare che non dovrà essere ripetuta se la procedura è effettuata prima della scadenza del certificato.

K.2. Sostituzione delle chiavi del Certificatore

K.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. *O*.

K.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 Certificatore procederà in base a quanto stabilito dall'Art.30 del DPCM.

K.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.

L. Registro dei certificati

L.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.
- 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 Certificatore 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.

Nella copia LDAP accessibile dagli non sono disponibili i certificati di sottoscrizione

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

L.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 può quindi registrare i certificati emessi e le CRL.

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

L.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 per 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.

M. Modalità di riservatezza dei dati personali

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

N. Procedura di gestione delle 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. *L*.
- 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.

O. Procedura di gestione degli eventi catastrofici

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

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

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

Per poter fare fronte alla gestione dell'emergenza è prevista la replica off-site dei dati e l'intervento entro 24 ore del personale addetto.

P. 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).

P.1. Modalità di richiesta e verifica delle marche temporali

Il Certificatore 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.

La verifica della marca temporale apposta è contestuale alla verifica della firma.

Q. 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.

Lead Time di Processo

Soggetto	Richiesta	Ente Coinvolto	Azione Ente Coinvolto	Ente Coinvolto	Azione Ente Coinvolto
Utente, Richiedente, Titolare Certificato	*Richiesta di Emissione del Certificato vs. LRA*	*Banca / Istituto (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/Sospensione del Certificato vs. RA o LRA*	*INTESA (acting as) Registration Authority (RA) o Banca (acting as) LRA*	*Emette ordine di Revoca/Sospensione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Revoca/Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*INTESA (acting as) Registration Authority (RA) o Banca (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.

Tabella RACI

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

R. 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 -------