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 elettronica qualificata remota nell'ambito dei servizi di CSE – Consorzio Servizi Bancari.

Codice documento: MO_CSE

OID: 1.3.76.21.1.50.14

Redazione: Antonio Raia

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

Data emissione: 11/05/2022

Versione: 02

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

Revisioni

Versione n°: 02	***Data Revisione: 11/05/2022***
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti normativi e tecnici Aggiornamento par. *F. Modalità di identificazione e registrazione degli utenti*
Motivazioni:	Variazione proprietà, direzione e coordinamento Aggiornamenti normativi Aggiornamento definizione limite d'uso e modalità di identificazione
Versione n°: 01	***Data Revisione: 04/02/2021***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

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.
Cliente *Cliente Prospect*	È il Cliente (o potenziale cliente, detto Prospect) della Banca / Istituto finanziario.
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
CDG – Codice Direzione Generale	E' il codice assegnato al Cliente della Banca / Istituto.

A. Introduzione

Il presente documento costituisce il Manuale Operativo del QTSP INTESA per il servizio di firma elettronica qualificata remota, nell'ambito delle soluzioni proposte da CSE – Consorzio Servizi Bancari Soc. Cons. a r.l. – sede legale Via Emilia, 272, 40068 – San Lazzaro di Savena (BO), Partita IVA 00501021208 (nel seguito, anche solo *CSE*) ai propri Istituti clienti.

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.

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* (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.

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 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 per la firma elettronica 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 è la versione n. ***02***, rilasciata in data ***11/05/2022***, del ***Manuale Operativo per le procedure di firma elettronica qualificata remota nell'ambito dei servizi di CSE – Consorzio Servizi Bancari***, emesso in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.50.14***.

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.

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 certificata (PEC)	*INTESA@pec.trustedmail.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, il QTSP INTESA ha predisposto i seguenti strumenti:

- un recapito di posta elettronica *uff_RA@intesa.it*
- un recapito telefonico: *+39.011.19216.111*
- 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 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.

B.4.1. Certification Authority (CA)

INTESA, operando in ottemperanza a quanto previsto dal DPCM, dal 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. Local Registration Authority (LRA)

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

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.

In particolare, la Banca / Istituto, nel rispetto della normativa antiriciclaggio, potrà identificare il Titolare (*adeguata verifica*) anche se questi non si presenterà fisicamente in un'agenzia.

In questo caso la Banca / Istituto dovrà comunque:

- accertare l'identità tramite documenti, dati o informazioni supplementari quali atti pubblici, scritture private autenticate, certificati utilizzati per la generazione di una firma elettronica qualificata associata a documenti informatici ovvero attraverso dichiarazione dell'Autorità Consolare Italiana;
- applicare misure supplementari per la verifica dei documenti forniti quali, ad esempio, certificazione di conferma di un ente creditizio o finanziario soggetto alla direttiva;
- utilizzare la documentazione provante che il rapporto di provvista provenga da un conto intestato al cliente.

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 i propri clienti ovvero per i propri dipendenti.

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. la chiusura del rapporto bancario).

Inoltre, limitatamente al caso di certificati emessi per persone aderenti alla propria organizzazione (dipendenti, collaboratori o affiliati), dà consenso all'inserimento nel Certificato Qualificato dell'indicazione dell'Organizzazione e di eventuali poteri di rappresentanza.

Per quanto riguarda invece i certificati emessi ai clienti bancari, tali certificati non prevedranno i poteri di rappresentanza e non conterranno l'indicazione del Terzo Interessato al loro interno.

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) 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 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.

Secondo quanto stabilito dall'Art.14 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

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;
- indica un sistema di verifica della firma elettronica, di cui all'Art.10 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.

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato qualificato per i servizi descritti nel presente Manuale Operativo è un cliente della Banca o dell'Istituto, che operano da Registration Authority.

Il Titolare riceverà un certificato qualificato per la Firma Elettronica Qualificata Remota, con cui poter sottoscrivere contratti e documenti relativi a prodotti e/o servizi offerti dalla Banca / Istituto, nelle modalità descritte al par. *I. 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;
- 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 o l'Istituto.

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

- verifica che il Cliente sia in possesso di tutti i requisiti necessari e autorizza il Cliente 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.2.1*.

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

A titolo esemplificativo, ma non esaustivo, si riportano le seguenti circostanze:

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

La richiesta di revoca o sospensione da parte del Terzo Interessato 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

Il QTSP INTESA, per esigenze connesse alla fornitura del servizio, potrà avvalersi su tutto il territorio nazionale di ulteriori soggetti (nel seguito 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 mediante specifico *Contratto di Mandato*, sottoscritto da entrambe le parti.

In particolare, le RA 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 Art.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 il 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.

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 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.2.1*.

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 o Istituto ai propri Clienti: le Tariffe per l'emissione, rinnovo, revoca e sospensione del certificato qualificato saranno indicate nei contratti stipulati tra Cliente e Banca / Istituto.

F. Modalità di identificazione e registrazione 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 anche 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 è ancora in corso di validità, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al QTSP attraverso la Banca/Istituto gli eventuali cambiamenti relativi ai propri dati di registrazione (par. *F.2*).

F.1. Identificazione del Titolare

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

- *Canonica*: il Richiedente viene identificato *de visu in presenza*, presso una filiale della Banca o dell'Istituto ai sensi della normativa antiriciclaggio.
  Tale modalità di identificazione può essere anche svolta al di fuori della filiale Bancaria, previo appuntamento in presenza tra il richiedente del certificato e l'operatore della Banca o Istituto opportunamente formato e qualificato per tale operatività.
  In tali casistiche l'identificazione avviene sotto la piena responsabilità della Banca/istituto e per finalità collegate alla norma antiriciclaggio. Il certificato viene emesso successivamente sulla base dell'identificazione effettuata dalla Banca/Istituto.
- *On line*: se il Richiedente sceglie la modalità di adesione diretta ed è già titolare di un conto corrente presso una Banca sul territorio nazionale, per essere riconosciuto, sempre ai fini dell'antiriciclaggio, in linea a quanto previsto dalla normativa antiriciclaggio vigente potrà:
  - utilizzare una procedura SEPA Credit Transfer (SCT);
  - disporre un bonifico dal conto corrente già aperto presso la Banca di cui prima.
  Il cliente così riconosciuto dalla Banca/Istituto di destinazione ai sensi della normativa antiriciclaggio potrà richiedere un certificato qualificato basato sull'identificazione certa effettuata dalla Banca/Istituto di destinazione.
- Video identificazione da remoto: "self + welcome call", più ampiamente descritta al par. *F.3*.
- Identificazione *tramite identità digitali* notificate ai sensi del Regolamento eIDAS con livello pari a *substantial*, più ampiamente descritta al par. *F.4*.

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.

F.2. Registrazione dei soggetti richiedenti la certificazione

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

Questa operazione viene eseguita mediante un'applicazione software direttamente richiamabile dagli applicativi della Banca o dell'Istituto.

Fra i dati di registrazione necessari per l'esecuzione del servizio oggetto del presente documento ricordiamo:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Numero di telefono cellulare;
- Indirizzo e-mail.

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

- 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 relativa alla registrazione dei Titolari è conservata per 20 (venti) anni.

F.2.1. 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:

> *"Il presente certificato e' utilizzabile esclusivamente per la sottoscrizione di documenti mediante Firma Digitale Remota."*
>
> *"This certificate may only be used in Remote Digital Signature."*

Eventuali specifici limiti d'uso potranno essere concordati con CSE o con la Banca / Istituto.

Qualora il certificato sia utilizzato in procedure di firma automatica, questo dovrà essere specificato nella limitazione d'uso mediante la seguente asserzione (DPCM, Art. 5, comma 2):

> *"Il presente certificato e' valido solo per firme elettroniche qualificate apposte con procedura automatica."*
>
> *"This certificate may only be used for unattended/automatic qualified electronic signatures."*

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

F.3. Identificazione degli utenti da remoto (video identificazione)

Nel rispetto delle normative vigenti, il riconoscimento del Titolare può essere eseguito attraverso una procedura di identificazione remota in modalità video self.

Il servizio consente al cliente di collegarsi nel momento a lui più comodo senza necessariamente doversi spostare dal luogo in cui si trova per eseguire tale procedura.

F.3.1. Video identificazione in modalità self & welcome call

Il processo prevede che l'utente, in fase di identificazione, venga guidato dal sistema ad eseguire una serie di passi all'interno di una sessione video registrata.

In questa fase, prima dell'avvio della sessione di identificazione, all'interno del portale di vendita della Banca/Istituto, l'utente:

- inserisce i propri dati anagrafici;
- inserisce i recapiti e-mail e cellulare che vengono opportunamente verificati dalla Banca/Istituto;
- carica il proprio documento d'identità e tessera sanitaria per acquisizione (dati anagrafici e foto)
- prende visione e accetta, con una firma tramite OTP SMS, il documento della Banca/Istituto, completo di tutti i dati dell'utente, con il quale autorizza a fornire ad INTESA i dati necessari per avviare l'identificazione, nonché il modulo di richiesta di emissione del certificato;
- prende visione e accetta, con una firma tramite OTP SMS, il documento di richiesta del servizio della Banca/Istituto (Contratto Banca), completo di tutti i dati dell'utente, sul quale verrà apposta la firma automatica one-shot non appena sarà conclusa positivamente l'identificazione self & welcome call senza interruzioni della sessione medesima.

All'utente viene reso disponibile il link per accedere al portale INTESA per effettuare la registrazione del video selfie, dove sarà quindi richiesto di:

- riprendere il proprio volto tramite un video selfie (per confronto biometrico), eseguendo contestualmente alcune azioni casuali guidate del volto per verifica del liveness. Lo stream sarà successivamente analizzato utilizzando algoritmi di riconoscimento facciale per rilevare i movimenti del viso.

Il processo di verifica potrà avvenire in automatico, attraverso un algoritmo di *Face Recognition*, per match biometrico tra foto del documento di identità e ripresa del volto (tramite alcuni fotogrammi).

In modalità unattended per il richiedente, vengono quindi eseguite dal QTSP una serie di verifiche tra cui:

- controllo sui dati anagrafici;
- verifica di leggibilità delle foto dei documenti d'identità e confronto tra fotogrammi del Video Self e la foto sul documento di identità;
- verifica della liveness;
- verifica con fonte autoritativa (Scipafi).

In caso di esito positivo, il video sarà accettato dal sistema; altrimenti si inviterà l'utente a rivolgersi alla propria Banca e il video sarà cancellato.

Successivamente, in caso di esito positivo, un operatore del QTSP INTESA, opportunamente autorizzato, accederà ad un pannello di back-office in cui sono riepilogati gli esiti dei controlli di cui sopra. Nel caso in cui ogni esito sia positivo, l'operatore del QTSP INTESA, confermerà il riconoscimento solo dopo aver effettuato una procedura di *welcome call*, nella quale chiederà al titolare di confermare i suoi dati e la volontà di richiedere un certificato qualificato.

Il video sarà cifrato e memorizzato su sistemi del QTPS INTESA insieme alla registrazione della welcome call.

La procedura di welcome call, necessaria ai fini dell'identificazione certa del Titolare, si compone dei seguenti step:

- le informazioni raccolte dal Portale e dall'applicazione sono passate al backoffice e al Service Telefonico, per il completamento del riconoscimento;
- il Cliente è quindi chiamato dal Service Telefonico (Welcome Call) per una verifica incrociata dell'identità: saranno poste in questa fase al cliente una serie di domande per verificare la corrispondenza tra risposte fornite e i dati/documenti acquisiti dal sistema Self ID. Allo scopo di assicurare la conformità del procedimento a quanto disposto dalle normative vigenti che regolano la materia, la chiamata sarà registrata e conservata per il periodo previsto (20 anni). I campioni vocali potranno essere impiegati anche per una verifica a posteriori della corretta identificazione del Titolare.

F.4. Identità Elettroniche

F.4.1. Identificazione tramite SPID

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione SPID con credenziali di livello 2 o 3.

In tale processo di autenticazione, sono richiesti almeno i seguenti dati minimi:

- Nome
- Cognome
- Sesso
- Luogo di nascita
- Data di nascita
- Codice fiscale.

Il certificato qualificato rilasciato tramite identità digitale SPID conterrà l'***OID 1.3.76.16.5***, registrato a cura dell'Agenzia per l'Italia Digitale con la seguente descrizione: "*Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity*";

Eventuali certificati qualificati emessi a seguito di una richiesta sottoscritta con firma elettronica qualificata basata su tali certificati qualificati devono, a loro volta, contenere il suddetto OID.

Nella fattispecie il processo di identificazione con SPID prevede una procedura composta dai seguenti passaggi:

1) il prospect atterra su pagine del portale Banca/Istituto in cui effettua il data entry. In questa fase sono registrati i seguenti dati del richiedente:
   - Dati anagrafici: nome, cognome, codice fiscale, luogo e data di nascita;
   - Dati di contatto: e-mail e numero di cellulare;
   - Dati del documento di identità: Tipo, Numero, Ente Emittente e data di scadenza

- Residenza: Indirizzo, Comune, Provincia, Stato.

2) Dopo la raccolta dati le pagine Banca gestite da CSE mostrano all'utente due moduli informativi:
   a. (Modulo A), ovvero il modulo Banca/Istituto dove viene richiesta l'autorizzazione al passaggio dei dati al QTSP INTESA e viene fornita apposita informativa riguardo al fatto che all'utente sarà inviata una OTP SMS da inserire, nella pagina Banca, come manifestazione del consenso al passaggio dei dati al QTSP e accettazione di un processo di firma elettronica qualificata del Contratto Banca, attraverso un certificato qualificato per firma automatica.
      Tale modulo precisa che il certificato qualificato sarà emesso, e contestualmente utilizzato, al termine del processo di identificazione con SPID. Non prima.
   b. (Modulo B), ovvero il modulo del QTSP INTESA che include l'informativa privacy e la richiesta certificato (certificato one-shot con la limitazione d'uso relativa alla procedura automatica) disciplinato dal presente MO. Tale modulo serve a raccogliere anche il consenso dell'utente all'utilizzo del certificato di firma automatica da parte della CA, immediatamente dopo il completamento del riconoscimento.

   I due moduli sopracitati sono compilati con i dati inseriti dall'utente allo step 1.
   In questa fase viene raccolta la firma elettronica semplice dell'utente su entrambi i moduli, tramite l'invio e successivo inserimento di una OTP SMS.
3) Una volta raccolto il consenso dello step 2), le pagine Banca mostrano la copia del Contratto Banca, debitamente compilato.
   L'utente è quindi chiamato a visionarlo per confermarne l'esattezza e correttezza dei dati in esso contenuti.
   Tale oggetto rappresenta il documento informatico che sarà firmato con firma elettronica qualificata automatica al termine del processo di identificazione SPID.

   In questa fase, onde raccogliere in modo inequivoco la volontà dell'utente di procedere alla sottoscrizione, nonché la sua conferma esplicita circa la correttezza dei contenuti riportati, viene inviata una seconda OTP SMS, che deve essere inserita nella stessa pagina Banca in cui l'utente ha visualizzato il contratto Banca.
4) Dopo la raccolta del consenso dell'utente di cui allo step precedente e la corretta verifica della seconda OTP SMS, all'utente viene reso disponibile il link per accedere al portale INTESA per effettuare l'identificazione SPID di Livello almeno 2.

   Il cliente, seguendo il link sopraindicato, atterra su pagine del QTSP INTESA che, in qualità di Service Provider Privato SPID, effettua l'identificazione del richiedente il certificato qualificato tramite lo SPID in suo possesso.

   In questa fase, il certificato qualificato rilasciato a seguito dell'identificazione SPID viene utilizzato dal QTSP per firmare un'informativa standard presente sul sistema di identificazione.

   Al termine del processo di identificazione, il QTSP INTESA, tramite canale protetto, informa il sistema Banca circa l'esito del riconoscimento e l'esito del controllo di congruità tra i dati anagrafici estratti da SPID e quelli sottoposti dal sistema Banca al termine dello step 3.

   I dati su cui vengono effettuati i controlli di corrispondenza sono: nome, cognome e codice fiscale.

Se l'esito ritornato dai controlli di identità effettuati dal sistema del QTSP INTESA è positivo e se la coerenza tra i dati passati dal sistema Banca (nome, cognome e codice fiscale) e i dati raccolti dal sistema SPID è confermata, il portale Banca, senza alcuna interruzione del flusso, richiede il rilascio di un secondo certificato qualificato one-shot per firma automatica e procede alla sottoscrizione del Contratto Banca visualizzato dal richiedente allo step 3) e accettato da questo tramite la seconda OTP SMS.

F.4.2. Identificazione tramite CIE (Carta di Identità Elettronica)

Ai sensi dell'art. 24, comma 1, lett. b) del Reg. eIDAS, Il QTSP INTESA può ottemperare alla verifica dell'identità del richiedente un certificato qualificato attraverso un processo di autenticazione CIE.

In questo caso il Richiedente, previo inserimento del PIN, effettua l'autenticazione sul portale del Certificatore o del CIE ID Server. Il sistema, dopo aver completato l'autenticazione, verifica le informazioni anagrafiche inserite nel certificato digitale della CIE e le associa a quelle relative al certificato di sottoscrizione oggetto di richiesta.

Nella fattispecie, il processo di identificazione con CIE prevede una procedura composta dai seguenti passaggi:

1) il prospect atterra su pagine del portale Banca/Istituto, in cui effettua il data entry.
   In questa fase sono registrati i seguenti dati del richiedente:
   - Dati anagrafici: nome, cognome, codice fiscale, luogo e data di nascita;
   - Dati di contatto: e-mail e numero di cellulare;
   - Dati del documento di identità: Tipo, Numero, Ente Emittente e data di scadenza
   - Residenza: Indirizzo, Comune, Provincia, Stato.
2) Dopo la raccolta dati, le pagine Banca gestite da CSE mostrano all'utente due moduli informativi:
   a. (Modulo A), ovvero il modulo Banca/Istituto dove viene richiesta l'autorizzazione al passaggio dei dati al QTSP INTESA e viene fornita apposita informativa riguardo al fatto che all'utente sarà inviata una OTP SMS da inserire, nella pagina Banca, come manifestazione del consenso al passaggio dei dati al QTSP e accettazione di un processo di firma elettronica qualificata del Contratto Banca, attraverso un certificato qualificato per firma automatica.
      Tale modulo precisa che il certificato qualificato sarà emesso, e contestualmente utilizzato, al termine del processo di identificazione con CIE. Non prima.
   b. (Modulo B), ovvero il modulo del QTSP INTESA che include l'informativa privacy e la richiesta del certificato (certificato one-shot con la limitazione d'uso relativa alla procedura automatica) disciplinato dal presente MO.
      Tale modulo serve a raccogliere anche il consenso dell'utente all'utilizzo del certificato di firma automatica da parte della CA, immediatamente dopo il completamento del riconoscimento.

   I due moduli sopracitati sono compilati con i dati inseriti dall'utente allo step 1.
   In questa fase viene raccolta la firma elettronica semplice dell'utente su entrambi i moduli tramite l'invio e successivo inserimento di una OTP SMS.
3) Una volta raccolto il consenso dello step 2), le pagine Banca mostrano la copia del Contratto Banca, debitamente compilato.
   L'utente è quindi chiamato a visionarlo per confermarne l'esattezza e correttezza dei dati in esso contenuti.
   Tale oggetto rappresenta il documento informatico che sarà firmato con firma elettronica qualificata automatica al termine del processo di identificazione CIE.

   In questa fase, onde raccogliere in modo inequivoco la volontà dell'utente di procedere alla sottoscrizione, nonché la sua conferma esplicita circa la correttezza dei contenuti riportati, viene inviata una seconda OTP SMS, che deve essere inserita nella stessa pagina Banca in cui l'utente ha visualizzato il contratto Banca.
4) Dopo la raccolta del consenso dell'utente allo step precedente e la corretta verifica della seconda OTP SMS, al cliente viene reso disponibile un link al portale INTESA per effettuare l'identificazione CIE.

   Il cliente, seguendo il link sopraindicato, atterra su pagine del QTSP INTESA che, in qualità di Service Provider Privato CIE, effettua l'identificazione del richiedente il certificato qualificato, tramite la CIE in suo possesso.

   In questa fase, il certificato qualificato rilasciato a seguito dell'identificazione CIE viene utilizzato dal QTSP per firmare un'informativa standard presente sul sistema di identificazione.

Al termine del processo di identificazione il QTSP INTESA, tramite canale protetto, informa il sistema Banca circa l'esito del riconoscimento e l'esito del controllo di congruità tra i dati anagrafici estratti dal sistema "Entra con CIE" e quelli sottoposti dal sistema Banca al termine dello step 3.

I dati su cui vengono effettuati i controlli di corrispondenza sono: nome, cognome e codice fiscale.

Se l'esito ritornato dai controlli di identità effettuati dal sistema del QTSP INTESA è positivo, e se la coerenza tra i dati passati dal sistema Banca (nome, cognome e codice fiscale) e i dati raccolti dal sistema "Entra con CIE" è confermata, il portale Banca, senza alcuna interruzione del flusso, richiede il rilascio di un secondo certificato qualificato one shot per firma automatica e procede alla sottoscrizione del Contratto Banca visualizzato dal richiedente allo step 3) e da questi accettato tramite la seconda OTP SMS.

F.5. Identificazione tramite credenziali utilizzate per l'emissione di un precedente certificato one-shot

In questa modalità, il Certificatore si basa sull'identificazione già effettuata durante l'emissione di un precedente certificato one-shot.
Il certificato one-shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso nell'ambito della stessa sessione o processo di firma in cui è stato rilasciato il precedente certificato one-shot.

Il Richiedente, in possesso dell'e-mail e del numero di cellulare certificati dal Certificatore nel corso del rilascio del precedente certificato one shot, può richiedere il rilascio del nuovo certificato one-shot solo dopo aver ricevuto, sull'e-mail e sul cellulare certificati, i nuovi codici One-Time, che dovranno essere verificati dal Richiedente per l'emissione e per l'utilizzo del nuovo certificato, purché ciò avvenga all'interno della stessa sessione o processo di firma.

Nel caso in cui il certificato one-shot sia utilizzabile nell'ambito di procedure di firma automatica, in virtù della specifica procedura di firma utilizzata, e limitatamente alle casistiche di identificazione attraverso identità digitali notificate ai sensi del Regolamento eIDAS con livello pari a *substantial* di cui al par. *F.4*, è possibile utilizzare l'identificazione e la raccolta del consenso effettuate a monte del processo, il quale non dovrà subire interruzioni.

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 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 di certificazione 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 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 in una delle modalità descritte al par. *I. 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.

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.

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).

H.2. Procedura di emissione dei Certificati di sottoscrizione

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

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel par. *G.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 gestita dalla Certification Authority del QTSP.

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

H.3. Informazioni contenute nei certificati di sottoscrizione

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 elettronica è conforme al Regolamento eIDAS e agli obblighi previsti dalla 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 una limitazione d'uso (par. *F.2.1*).

H.3.1. Certificati con validità temporale limitata ("one shot")

Per alcuni processi, tipicamente legati all'onboarding di clienti prospect, il QTSP INTESA offre un servizio di firma elettronica qualificata remota, generata su HSM, conforme alla normativa, mediante l'utilizzo di un certificato qualificato a validità temporale limitata: 15 (quindici) minuti dall'emissione o come altrimenti concordato con la LRA / Terzo Interessato.

Tali certificati, oltre a prevedere dei forti vincoli in termini temporali, sono anche caratterizzati da vincoli applicativi che ne limitano l'adozione ai soli documenti proposti dalla LRA e da limiti d'uso (par *F.2.1*) che ne circoscrivono la validità legale ai fini della sottoscrizione dei documenti sopracitati.

Per l'apposizione della firma in modalità remota tramite questi certificati, è possibile utilizzare applicazioni di tipo on-line della Banca e funzionanti mediante i servizi erogati dal Certificatore o dalla LRA. In quest'ultimo caso il Certificatore provvede ad assicurarsi che il sistema gestito dalla LRA garantisca la conoscenza esclusiva del dato per la creazione della firma da parte del Titolare grazie ad opportuni requisiti di sicurezza.

Il Certificatore mette a disposizione web services per permettere l'integrazione con le applicazioni richiedenti i servizi di firma. Si intende che i documenti oggetto di firma siano normalmente formati da dette applicazioni in dipendenza dalle specifiche necessità.

La richiesta di firma proveniente dall'utente, vista la breve durata dei certificati one shot, nonché i forti vincoli applicativi e d'uso, viene autenticata attraverso la componente delle credenziali nota al Titolare di tipo OTP SMS, che sono inserite a monte della procedura, seguendo le modalità operative descritte ai par. *F.3.1* e *F.4*.

H.4. Codice di Emergenza

Il Certificatore garantisce, nel caso di certificati triennali, 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 *CDG* (*Codice Direzione Generale*).

I. 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 firme elettroniche qualificate conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia di servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer, ma piuttosto delle funzionalità di firma richiamabili o accedendo al servizio di home banking della Banca o dell'Istituto oppure direttamente allo sportello di una filiale della Banca o dell'Istituto.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno assolutamente conformi a quanto previsto dal DPCM all'Art.4 comma 2 relativamente agli algoritmi utilizzati.

Tali documenti, inoltre, come richiesto dall'Art.4 comma 3 dello stesso DPCM, 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.

Vengono di seguito descritte le modalità di autenticazione diverse che, nel rispetto della normativa vigente, permettono ad un Titolare, una volta registrato, di procedere all'utilizzo delle chiavi di firma, e relativo certificato qualificato triennale, per effettuare firme elettroniche qualificate.

Ai fini di una corretta e completa interpretazione dei successivi paragrafi, si precisa che, nei casi di rilascio di certificati triennali, il sistema applicativo CSE in uso da parte della Banca/Istituto effettua tutte le operazioni necessarie al rilascio del certificato ed all'assegnazione sicura e certa delle credenziali per il suo utilizzo al titolare del certificato qualificato.

Tra queste rientrano almeno le seguenti:

1. recupero dell'anagrafica cliente dall'archivio Banca con garanzia, secondo standard di livello bancario, di autenticità e immodificabilità dei dati acquisiti;
2. associazione di un PIN all'anagrafica cliente, generato in ambiente sicuro, attraverso regole di derivazione basate su algoritmi crittografici in grado di garantire l'associazione univoca tra dati personali e quantità di sicurezza del titolare del certificato, nonché la riconducibilità certa al legittimo titolare.

Le misure sopraindicate permettono di non mantenere "*at rest*" alcuna quantità di sicurezza personale associata al titolare del certificato qualificato e di derivarle in real time solo al momento dell'effettivo utilizzo del certificato qualificato, partendo da informazioni personali dell'utente ma, soprattutto, da dati riservati (quali OTP inviate sul numero personale, oppure credenziali per il login bancario, oppure credenziali di tipo grafometrico), quest'ultimi noti ovvero disponibili esclusivamente al titolare stesso.

I.1. Processo di Firma in stazioni presidiate (Sportello bancario o finanziario)

I.1.1. Autenticazione con tecniche grafometriche

Per poter accedere alle proprie chiavi di firma, il Titolare dovrà autenticarsi apponendo una firma di tipo grafometrico su di un dispositivo tablet. I parametri grafometrici rilevati in questa fase verranno confrontati con quelli raccolti durante la fase di enrollment bancario (in presenza) e, se considerati sufficientemente "attendibili" (con percentuale di riconoscimento uguale o superiore almeno al 80%), potranno permettere lo sblocco delle chiavi di firma.

Tale percentuale è giustificata dal fatto che le operazioni di firma avvengono esclusivamente in postazioni presidiate da operatori della Banca / Istituto e che, congiuntamente alla verifica della firma, vengono tracciate informazioni quali: un riferimento temporale del momento in cui l'operazione è avvenuta, il codice dell'operatore che ha assistito il Titolare al momento della firma e il numero della postazione dove la firma è stata verificata. Inoltre, in considerazione del fatto che il Titolare era stato anche identificato in maniera canonica dal personale di filiale, è possibile garantire un riconoscimento certo dello stesso.

In questo caso, il Titolare, precedentemente identificato, al momento della firma si troverà presso una filiale (o fuori sede) al cospetto del personale della società stessa che lo avrà nuovamente riconosciuto.

Dopo che questo nuovo riconoscimento sarà stato effettuato ed una volta che il titolare abbia potuto esaminare il/i documento/i da firmare, egli potrà avviare tale procedura apponendo una firma su di un dispositivo tablet (in modo analogo a come aveva firmato nella fase di enrollment precedentemente descritta).

Il sistema è in grado di rilevare alcune fra le caratteristiche grafometriche più salienti della firma appena apposta e confrontarle con il profilo precedentemente archiviato.

Uno score determinerà quanto la firma apposta per ultima si discosta dal profilo registrato per quell'utente, se lo score di riconoscimento sarà considerato sufficientemente alto (>=80%) e in considerazione che il Titolare è stato nuovamente identificato dal personale della Banca / Istituto, il processo di firma potrà essere avviato.

Qualora invece il confronto fra la firma appena apposta ed il profilo registrato non dovesse raggiungere lo score desiderato, nonostante l'identificazione appena effettuata, verrà richiesto all'utente di apporre con maggiore attenzione una nuova firma. Questo perché probabilmente il mancato raggiungimento dello score desiderato può essere dovuto a errori anche lievi, ma immediatamente rilevati dal sistema: mancanza di una lettera, omissione di vocali accentate, etc...

I.1.2. Autenticazione con OTP via SMS

Onde tutelare al massimo la sicurezza dell'utente, la soluzione implementata evita di richiedere al Titolare l'inserimento di codici statici davanti al personale della Banca o dell'Istituto.

Questa misura evita il rischio che i codici riservati possano essere eventualmente poi riutilizzati in maniera fraudolenta ai suoi danni.

Entrato in possesso del proprio certificato qualificato, il Titolare potrà sottoscrivere un documento come segue:

1. L'utente si presenta allo sportello di una filiale bancaria o dell'Istituto (stazione presidiata) oppure incontra fisicamente, fuori dai locali della Banca/Istituto, personale di quest'ultima opportunamente autorizzato e viene riconosciuto dall'addetto (ad esempio il cassiere o il promotore) in modalità canonica.
2. Al momento della firma, viene inviato un messaggio SMS all'utente, riportante un codice OTP di validità temporalmente limitata. L'SMS è inviato sul dispositivo mobile del Titolare, precedentemente censito e certificato secondo le procedure previste dalla Banca / Istituto.
3. Il Titolare (Utente), una volta ricevuto l'SMS, digita il codice OTP nell'apposito campo.
4. Rilevando la correttezza della digitazione del codice appena inserito, il sistema procede nell'operazione di firma.

La visualizzazione del contenuto dei documenti da firmare e la digitazione dell'OTP possono avvenire, alternativamente, su un dispositivo tablet collegato alla postazione in uso da parte dell'operatore della Banca (o dell'Istituto) oppure direttamente tramite monitor e tastiera di tale postazione.

I.2. Processo di Firma in stazioni non presidiate (Internet Banking)

Entrato in possesso dei necessari codici durante la fase di identificazione, il Titolare, accede tramite credenziale bancaria doppio fattore, nell'area riservata dell'internet banking e può, in un momento successivo, richiedere il proprio certificato digitale (o utilizzare quello già emesso) e procedere alla firma di un documento secondo le modalità di seguito descritte:

1. Il Titolare si connette all'area riservata attraverso i suoi codici personali per l'accesso all'applicazione e con credenziali doppio fattore bancarie.
2. Seleziona e verifica il documento (o i documenti di una stessa pratica) da firmare.
3. Conferma la volontà di apporre la firma con lo strumento di autenticazione della Banca / Istituto (token fisico, Secure Call, token mobile con notifica push).
4. Il sistema, a fronte dell'esito positivo dello step 3, procede all'invio di una OTP via SMS al n. cellulare del Titolare.
5. Il Titolare digita in mappa l'OTP ricevuta e, qualora corretta, il sistema procede allo sblocco del certificato di firma e all'apposizione della firma digitale sul documento.

La stessa procedura può essere utilizzata per emettere in real time il certificato qualificato laddove l'utente loggato in area riservata risulti non esserne equipaggiato.

In tali casi, naturalmente, l'utente, prima di poter ottenere il certificato qualificato e procedere alla firma, viene informato sulle condizioni e termini di utilizzo del certificato, viene invitato alla lettura del presente Manuale Operativo e viene infine raccolto il suo consenso esplicito a procedere al rilascio tramite OTP SMS su numero certificato dalla Banca.

I.2.1. Autenticazione con Token fisico + OTP via SMS

Tale modalità di autenticazione è legata all'utilizzo di Token OTP fisici (ancora diffusi nel mondo bancario e finanziario).

Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione e, per avviare la procedura di firma, dovrà prima autenticarsi digitando l'OTP generata dal token fisico e visualizzata sul relativo display poi inserire una seconda OTP ricevuta via SMS.

I.2.2. Autenticazione di tipo "Secure Call" + OTP via SMS

Questa modalità di autenticazione richiede all'utente, già precedentemente identificato, e autenticato tramite SCA nei confronti del portale della Banca/Istituto, di effettuare con il proprio telefono cellulare (dallo stesso numero fornito in fase di identificazione) una chiamata ad un numero telefonico specifico, fornito nell'ambito del servizio, al fine di confermare la propria volontà di firmare un documento.

Al ricevimento della suddetta telefonata, ne viene verificata la provenienza dal numero di telefono (*Call Identifier*) preventivamente associato all'utente in fase di registrazione e viene richiesto allo stesso di digitare, sul "tastierino" del device, il codice proposto sul front-end. In caso di verifica positiva del numero chiamante e del codice digitato, sarà richiesto all'utente di inserire in mappa l'OTP ricevuta via SMS, per sbloccare la firma remota.

Questo tipo di autenticazione viene anche detta "*Call Drop*", in quanto quando il Titolare chiama per essere autenticato: non viene attivata nessuna conversazione e la telefonata, dopo qualche secondo, e dopo l'inserimento del codice mostrato a schermo, viene chiusa.

Tra i vantaggi di questa tecnica vi sono l'estrema economicità e praticità, in quanto non è richiesto l'uso di alcun dispositivo fisico di autenticazione, ed è molto facile da usare.

I.2.3. Autenticazione con Token Mobile con notifica push + OTP via SMS

Le Banche e gli Istituti finanziari si stanno dotando sempre di più frequentemente di ulteriori innovativi strumenti tecnologici per permettere l'autenticazione forte in area riservata.

Uno di questi strumenti è rappresentato dall'APP di notifica push (integrata nell'APP bancaria); essa prevede, a garanzia della sicurezza, che:

- il Cliente della Banca o dell'Istituto (utente/Titolare) possa utilizzare la propria App per l'autenticazione solo previa attivazione della stessa su di un dispositivo Mobile;
- l'attivazione iniziale dell'App avvenga previa digitazione di una OTP ricevuta via SMS ad uno dei recapiti telefonici certificati presso la Banca o l'Istituto.

Dovendo procedere con una firma digitale di un documento in area riservata dell'internet banking, tramite SCA, il Titolare dovrà, in primo luogo, autenticarsi tramite l'app di notifica push, inserendo il PIN scelto in fase di enrollment o con la modalità fingerprint, se impostata sullo smartphone.

Successivamente, il cliente riceverà una OTP via SMS, che dovrà inserire nel front-end. Se corretta, sarà sbloccato il suo certificato qualificato di firma.

I.2.4. Firma con certificati one-shot

Per alcuni processi, tipicamente legati all'onboarding di clienti prospect effettuato a distanza, si utilizzano certificati one-shot, caratterizzati da una durata di 15 (quindici) minuti.

Il loro sblocco avviene in modalità unattended da parte dei Titolari, ossia si tratta di firme automatiche rilasciate mediante l'adozione di un processo di identificazione e autorizzativo effettuato a monte del rilascio.

Nel corso di tale processo viene preventivamente raccolta la volontà esplicita dell'utente a firmare un determinato contratto Banca tramite firma automatica, viene effettuata l'identificazione certa dell'utente e viene quindi avviato il processo di firma automatica sul contratto precedentemente visualizzato ed approvato. La sessione è unica e comprende, senza interruzioni, le fasi di:

1) visualizzazione Contratto Banca/Istituto e raccolta esplicita del consenso tramite OTP/SMS;
2) identificazione del richiedente;
3) emissione certificato one-shot per firma automatica;
4) utilizzo del certificato one-shot di firma automatica per la sottoscrizione del Contratto Banca/Istituto di cui allo step 1).

Preventivamente, ciascun utente autorizza la Banca (o l'Istituto), confermando con OTP ricevuta via SMS, ad inoltrare al QTSP In.Te.S.A. la richiesta di emissione, a proprio nome, di un certificato di tale tipologia ed a utilizzarlo per apporre la propria firma digitale a completamento del processo di onboarding.

La firma del documento avverrà secondo le modalità di seguito descritte:

1. L'utente accede al sistema della Banca/Istituto.
2. Verifica il documento (o i documenti di una stessa pratica) da firmare.
3. Conferma la volontà di apporre la firma e il sistema procede all'invio di una OTP via SMS al n. cellulare dell'utente.
4. L'utente digita l'OTP ricevuta e, qualora corretta, il sistema procede ad indirizzare l'utente allo step di identificazione.
5. Al termine dell'identificazione il sistema procede nell'operazione di apposizione della firma digitale di tutti i documenti di cui il Titolare ha precedentemente preso visione.

Maggiori dettagli su tali modalità di utilizzo del certificato sono descritti ai par. *F.3.1* e *F.4*.

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 considerato infatti di facile utilizzo nell'ambito delle applicazioni bancarie o finanziarie.

La verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC*, applicazione in grado di verificare tutte le tipologie di firma elettronica qualificata in formato PDF prodotte nell'Unione Europea in conformità con il Regolamento eIDAS.

Acrobat Reader DC è scaricabile gratuitamente dal sito di Adobe, *www.adobe.com/it/*

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 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).

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 su richiesta del Titolare

Il Titolare può richiedere la revoca 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 QTSP, avvertito dalla Banca / Istituto, che nel frattempo avrà anche bloccato i codici di accesso del Titolare, provvederà alla immediata revoca del certificato.

K.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 o successivamente aggiornati e comunicati dal Titolare al QTSP, anche per mezzo delle LRA (par. *C.2. Obblighi del Titolare*).

K.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 utilizzando l'indirizzo e-mail fornito in fase di richiesta del certificato ovvero all'indirizzo di residenza, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

K.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.

K.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al precedente par. *K.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 / furto del Token OTP, o 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.

K.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.

Il Titolare successivamente potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre dalla Banca o dall'Istituto.

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

K.2.2. Sospensione su richiesta del Terzo Interessato

La Banca o l'Istituto, 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.

K.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 richiesta del certificato comunicato 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.

L. Modalità di sostituzione delle chiavi

L.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 sono di due tipologie:

a) **Long term**: durata di 36 (trentasei) mesi dalla data di emissione
b) **One shot**: durata limitata a 15 (quindici) minuti dall'emissione o come altrimenti concordato con la LRA / Terzo Interessato.

Al termine dei sopracitati periodi, nel caso si intenda procedere con il rinnovo del certificato, 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.

Nel caso di rinnovo di certificato one-shot, tenuta presente la sua validità temporale estremamente ridotta, vengono utilizzati i processi di rilascio e utilizzo descritti nei par. *F.3.1*, *F.4*, *F.5*.

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

L.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 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.

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* con protocollo LDAP.

Il Certificatore 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) e successive modificazioni e integrazioni.

O. 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. *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

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.

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

Il TSP 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 00specifico 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 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.

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*	*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 / Istituto (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 / Istituto (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 -------