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 in ambito bancario e finanziario.

Codice documento: MO_REMBAN

OID: 1.3.76.21.1.50.110

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 22/02/2021

Versione: 07

Intesa
An IBM Company

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

Revisioni

Versione n°: 07	***Data Revisione: 22/02/2021***
Descrizione modifiche:	Inserimento par. *F.4 - Certificati di firma digitale in particolari ambiti chiusi di utenti* Inserimento par. *I.6 - Autenticazione con tecniche grafometriche*
Motivazioni:	Aggiornamenti
Versione n°: 06	***Data Revisione: 13/01/2021***
Descrizione modifiche:	Precisazione circa l'operatività della RA del QTSP nella fase di identificazione del Richiedente. I.3.2, I.4: inserita funzionalità di OTP via SMS Inserimento par I.5.*Autenticazione con Notifica Push su App Mobile Banking* Aggiornamento riferimenti Help Desk (B.3)
Motivazioni:	Aggiornamenti
Versione n°: 05	***Data Revisione: 17/06/2020***
Descrizione modifiche:	Aggiornamento definizioni e riferimenti normativi Aggiornamento layout grafico e logo societario Inserimento procedure di video identificazione Puntualizzazione sulla sincronizzazione dei server di validazione temporale
Motivazioni:	Aggiornamenti normativi Aggiornamento servizi offerti
Versione n°: 04	***Data Revisione: 01/07/2019***
Descrizione modifiche:	Variazione dati societari e logo Aggiornamento definizioni e riferimenti normativi Aggiornamento layout grafico Inserimento procedura di firma per il *Cliente Prospect* (I.3.3)
Motivazioni:	Aggiornamenti normativi: Regolamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 (GDPR) Variazioni organizzative del TSP Nuova procedura per acquisizione cliente
Versione n°: 03	***Data Revisione: 13/06/2012***
Descrizione modifiche:	Estensione del manuale all'ambito finanziario (Istituti di Pagamento) oltreché bancario
Motivazioni:	Aggiornamento
Versione n°: 02	***Data Revisione: 02/04/2012***
Descrizione modifiche:	B.4.2. - Introdotto sistema di riconoscimento dell'identità del Titolare (Adeguata verifica) senza la presenza fisica del medesimo. C.5. - Introdotte modalità del sistema di riconoscimento dell'identità del Titolare (Adeguata verifica). F.1.3. - Inserito limite d'uso standard. G. - Inserita modalità di comunicazione e-mail delle conferme operative.
Motivazioni:	Aggiornamento
Versione n°: 01	***Data Revisione: 01/11/2011***
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*.
Comunicazione AgID 0016101 del 07-06-2016	"agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016", avente per oggetto "Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti". Nel seguito indicato anche solo come *Com. AgID 7/6/2016.*
D.lgs. 231/07 n.231	DECRETO LEGISLATIVO 21 novembre 2007, n. 231 Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

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 *Richiesta di certificazione*	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione.
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
CPS - CP	*CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico* del QTSP INTESA: documento costituisce il Practice Statement del QTSP e descrive le regole e le procedure operative per l'emissione dei certificati qualificati di firma elettronica e di sigillo elettronico, come definiti nel Regolamento (UE) 910/2014 (eIDAS). E' pubblicato sul sito dell'Agenzia e dal QTSP all'URL: *https://www.intesa.it/e-trustcom/*

A. Introduzione

Il presente documento costituisce il Manuale Operativo per il servizio di firma elettronica qualificata (firma digitale) digitale remota in ambito bancario e finanziario (nel seguito, *Manuale Operativo* o anche solo *MO*) del QTSP In.Te.S.A. S.p.A.

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 di Pagamento* (o anche solo *Banca / Istituto*).

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

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

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

A.1. Proprietà intellettuale

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

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

A.2. Validità

Quanto descritto in questo documento si applica al QTSP INTESA (cioè alle sue infrastrutture logistiche e tecniche, nonché al suo personale), ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata, anche avvalendosi delle marche temporali qualificate emesse dal QTSP INTESA, e alla Banca / Istituto di pagamento in qualità di Local Registration Authority

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

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

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle relative regole che disciplinano l'emissione di certificati qualificati da parte del QTSP INTESA.

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

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. ***07***, rilasciata il ***22/02/2021***, del ***Manuale Operativo per le procedure di firma digitale qualificata remota in ambito bancario e finanziario***, emesso in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è **1.3.76.21.1.50.110**.

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	*marketing@intesa.it*
Indirizzo (URL) registro dei certificati	*ldap://x500.e-trustcom.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21.1*

B.3. Responsabilità del Manuale Operativo

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

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

- un recapito di posta elettronica: *marketing@intesa.it*
- un recapito telefonico: +39 011.192.16.111
- un servizio di Help Desk 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, 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 paragrafo *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 delle funzioni di Registration Authority alla Banca / Istituto che avranno acquisito il servizio.

La LRA si impegna a svolgere le seguenti attività:

- Identificazione del Titolare;
- Registrazione del Titolare.

La Banca / Istituto, nell'esercizio della funzione di Registration Authority, dovrà vigilare affinché l'attività di riconoscimento 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.

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) 2016/679 (GDPR)
- Regolamento (UE) 910/2014 (eIDAS)

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 di Pagamento, 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 di pagamento.

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.1.1*.

La Banca / Istituto, come Terzo Interessato, quindi, potrà indicare al QTSP eventuali limitazioni d'uso del certificato, eventuali poteri di rappresentanza e dovrà comunicare qualsiasi variazione delle stesse.
A titolo esemplificativo si riportano le seguenti circostanze:

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

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

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

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

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

In particolare, le 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.

C.5.1. Identificazione del Titolare

Il servizio di identificazione potrà essere gestito in quattro modalità differenti, di seguito descritte:

- *Canonica*: il Richiedente viene identificato presso una filiale della Banca o dell'Istituto di Pagamento.
- *On demand*: all'apertura di un nuovo conto corrente, il Richiedente potrà chiedere di essere contattato da un *Personal Financial Adviser* che, fissatogli un appuntamento, supporterà il Cliente in tutte le procedure inerenti all'apertura di un Conto Corrente. In questa fase il Cliente verrà guidato (dopo essere stato identificato e registrato) anche nella richiesta di un certificato di firma elettronica qualificata.
- *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 ai fini di legge potrà:
  - utilizzare una procedura SEPA (o SDD - SEPA Direct Debit);
  - disporre un bonifico dal conto corrente già aperto presso la Banca di cui prima.
- *Video identificazione da remoto*: nella modalità "*con operatore*" ovvero, in alternativa, "*self + welcome call*", più ampiamente descritte al par. *F.2*.

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

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.1.1* ovvero *F.4.1*.

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 inviata ad AgID apposita dichiarazione di stipula.

E. Tariffe

Il Servizio viene fornito dalla Banca o Istituto di pagamento 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

F.1. Identificazione degli utenti

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

La suddetta operazione può essere demandata alla 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.

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;
- Indirizzo di residenza;
- Domicilio presso il quale saranno inviate le comunicazioni cartacee;
- Numero di telefono cellulare;
- Indirizzo di posta elettronica;
- Tipo e numero del documento d'identità esibito;
- Autorità che ha rilasciato il documento e data e luogo del rilascio e di scadenza.

Al termine di questa fase di registrazione, al Titolare potrà essere rilasciato in comodato d'uso un dispositivo One Time Password dotato di display e in grado di generare codici numerici monouso (chiamati nel seguito *codici OTP* o semplicemente *OTP*).

In alternativa ad un token OTP fisico, la Banca o l'Istituto di Pagamento potranno indicare ai Titolari come attivare un sistema di autenticazione software per dispositivi mobili (qualora il Titolare ne disponesse di uno e scegliesse questa modalità come preferibile per comodità d'uso rispetto all'impiego di un Token fisico). Tale sistema software permetterà la generazione di una One Time Password sul dispositivo mobile del Titolare e potrà essere pertanto utilizzato come strumento di autenticazione ai sistemi di firma remota.

Oltre all'OTP, saranno forniti al Titolare tutte le informazioni necessarie e un *Personal Identification Number* (*PIN*) che possano garantirgli un accesso sicuro al servizio di firma remota resogli disponibile dalla Banca / Istituto.

Lo stesso PIN potrà essere utilizzato come *codice di emergenza* (in caso, ad esempio, di smarrimento e/o perdita del Token OTP o del mobile) per *sospendere con urgenza* il certificato qualificato a lui intestato (par. *H.4*).

Il PIN potrà essere successivamente modificato o aggiornato dal Titolare usufruendo dei servizi che la Banca o l'Istituto di Pagamento gli avranno messo a disposizione.

In questa fase vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

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

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

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

F.1.1. Limiti d'uso

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

La formula standard è la seguente:

> *"L'utilizzo del certificato e' limitato ai rapporti con Nome Banca / Istituto."*
>
> *"This certificate may only be used in dealings with Nome Banca / Istituto."*

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

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

F.1.2. Titoli e abilitazioni professionali

Nel caso in cui sia richiesta l'indicazione, nel certificato qualificato, di abilitazioni professionali (es. l'appartenenza ad un ordine professionale), il richiedente deve produrre idonea documentazione a dimostrazione dell'effettiva sussistenza di tali abilitazioni professionali o documentazione equivalente.

Copia di tale documentazione viene conservata per 20 (venti) anni.

La documentazione atta a supportare la richiesta d'inserimento di titoli o abilitazioni professionali all'interno del certificato qualificato non potrà essere antecedente a 10 (dieci) giorni dalla data di presentazione della richiesta di emissione del suddetto certificato.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative ad abilitazioni professionali.

INTESA, in caso di autocertificazione, il QTSP INTESA non assume alcuna responsabilità, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, Art.13), per l'eventuale inserimento nel certificato di informazioni autocertificate dal Titolare.

F.1.3. Poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di poteri di rappresentanza (e.g. l'appartenenza ad un'organizzazione e la carica ivi ricoperta, l'abilitazione ad operare in nome e per conto di un Cliente, etc.), il richiedente deve produrre idonea documentazione a dimostrazione della effettiva sussistenza di tali poteri di rappresentanza.

Per la rappresentanza di persone fisiche, il richiedente dovrà produrre una copia autentica della delega o procura notarile sottoscritta dalla persona rappresentata, insieme all'attestazione di consenso di quest'ultima all'inserimento del ruolo nel certificato.

Nel caso in cui sia richiesta l'indicazione nel certificato di un ruolo relativo alla rappresentanza di organizzazioni o enti di diritto privato, il Titolare dovrà presentare documentazione atta a comprovare il ruolo di cui si chiede l'inserimento nel certificato e una dichiarazione dell'organizzazione o dell'ente di appartenenza, mediante la quale l'ente o l'organizzazione autorizza il QTSP all'inserimento dello specifico ruolo nel certificato. Quest'ultimo documento non dovrà essere antecedente 20 (venti) giorni rispetto alla data di richiesta di emissione del certificato qualificato.

L'inserimento nel certificato qualificato d'informazioni relative all'esercizio di funzioni pubbliche o poteri di rappresentanza in enti od organizzazioni di diritto pubblico sarà subordinato a specifici accordi con gli enti stessi. Sulla base di tali accordi sarà possibile specificare il ruolo ricoperto dal Titolare all'interno dell'ente o organizzazione pubblica.

La documentazione prodotta sarà conservata per un periodo di 20 (venti) anni.

INTESA non è responsabile dei danni derivanti dall'uso improprio di un certificato qualificato con informazioni relative a poteri di rappresentanza.

F.1.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno Pseudonimo in alternativa ai propri dati reali.

Le informazioni relative alla reale identità dell'utente saranno conservate per 20 (venti) anni decorrenti dall'emissione del certificato.

F.2. 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 tramite webcam, in modalità assistita con operatore ovvero, in alternativa, 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.2.1. Video identificazione con operatore

Questa modalità prevede un'interazione tra richiedente e operatore completamente «online» e assistita, favorendo l'esperienza d'uso ed agevolando tutti coloro meno consoni all'uso delle tecnologie.

A fronte della conferma da parte dell'operatore di avvenuta identificazione, il video viene cifrato e inviato in Conservazione a Norma.

Il servizio di identificazione potrà essere gestito, remotamente, come segue:

- Il Richiedente, in possesso di un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante, si connette al sito della Registration Authority (RA) dove sono riportate tutte le istruzioni necessarie per eseguire i passi successivi e dove sono indicati i documenti necessari per l'identificazione.
- Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di RA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.
- Il Richiedente compila sul sito della RA una richiesta di certificato digitale compilando un form in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione.
- Compilato tale form, viene richiesto al Richiedente di prendere visione del presente *Manuale Operativo*, che dovrà essere aperto in lettura. Lo stesso Manuale Operativo sarà anche agevolmente scaricabile dal sito stesso.
- Fra le operazioni che necessariamente il Richiedente dovrà svolgere vi è anche la scelta del consenso privacy.
- Il Richiedente, sempre grazie alle funzionalità esposte sul sito, una volta presa visione del Manuale Operativo e dato il consenso, dovrà inviare alla RA una copia scannerizzata dei documenti di identità (carta d'identità, passaporto, tesserino sanitario nazionale). L'invio preventivo di tali documenti conferma la volontà del Richiedente di completare la procedura di identificazione finalizzata all'emissione di un certificato qualificato utilizzabile esclusivamente nell'ambito dei servizi di firma qualificata forniti dal TSP.

- Completata la fase di inserimento dati e invio (upload) dei documenti necessari per l'identificazione, il Richiedente potrà continuare la sessione attivando appena possibile il collegamento via webcam oppure fissare un successivo appuntamento con gli operatori di RA per completare in un momento successivo a lui più comodo la procedura.
- Gli operatori di RA, sulla base dei documenti ricevuti, possono eseguire ulteriori controlli utilizzando specifiche banche dati, come SCIPAFI (il Sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento: attualmente quelle dell'Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei Trasporti, INPS e INAIL), oppure altre banche dati private (ad es. CRIF, Cerved, ecc.) in grado di erogare servizi di verifica dati e documenti d'identità.
- Durante la sessione on-line (via webcam), l'operatore di RA domanda al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi, verificando che nella foto del documento sia riconoscibile il Richiedente. Inoltre, chiede al soggetto di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del richiedente.
- L'intera sessione viene registrata in modalità audio e video (sia lato Richiedente che lato operatore) e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.
- La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa distinguibile del documento di riconoscimento inquadrato). L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione. L'operatore deve essere libero di rifiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.
- Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie per permettergli successivamente di utilizzare il certificato qualificato che sta per essergli emesso e di firmare digitalmente.
- In particolare, vengono date tutte le informazioni necessarie per utilizzare successivamente, nel momento della firma, uno strumento di autenticazione implementato per funzionare su mobile e/o smartphone in alternativa a token OTP fisici che risultano inadeguati per le modalità di erogazione della firma digitale previste dal presente manuale operativo.
- Si precisa che il QTSP INTESA, in ottemperanza con quanto previsto dall'Art.35, comma5 del CAD, prevede l'impiego di dispositivi di autenticazione che abbiano ottenuto una valutazione positiva di conformità da parte di AGID.
- L'impiego di dispositivi quali mobile e/o smartphone richiede che gli stessi vengano censiti in un'anagrafica gestita e mantenuta dal Provider: questa operazione di censimento viene eseguita durante la sessione gestita con webcam. Al termine, l'operatore di RA chiama il Richiedente al numero telefonico appena censito. Solo se il Richiedente risponde in diretta webcam e visto dall'operatore, la procedura di identificazione potrà dirsi effettivamente conclusa.
- Al termine del processo, il certificato di firma viene emesso dalla Certification Authority e al Richiedente, ora Titolare di certificato, viene anche associato un identificativo univoco presso il QTSP.

Dopo che il Titolare è stato identificato, l'operatore provvederà anche alla consegna di un Codice Utente e di un Personal Identification Number (PIN), tramite i quali sarà possibile accedere all'area riservata del portale, al fine di garantire un accesso sicuro ai servizi di firma remota.

Il PIN fornito inizialmente potrà essere successivamente modificato/aggiornato dal Titolare usufruendo dei servizi resi disponibili dal Provider.

Lo stesso PIN potrà essere utilizzato dal Titolare come codice di emergenza (in caso, ad esempio, di smarrimento e/o perdita del mobile) per sospendere il certificato digitale a lui intestato.

Durante il collegamento, vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

La documentazione precedentemente citata, relativa alla registrazione dei Titolari, viene conservata dal QTSP INTESA per 20 (venti) anni.

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

F.2.2. Video identificazione in modalità self & welcome call

In alternativa al video riconoscimento descritto al paragrafo precedente, una possibile modalità di video identificazione è rappresentata dalla 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.

Al richiedente sarà richiesto di:

- Mostrare in webcam il proprio documento d'identità per acquisizione (dati anagrafici e foto).
- Verifica dell'indirizzo di posta elettronica e del numero di cellulare tramite OTP e/o Magic Link.
- Riprendere il proprio volto (per confronto biometrico).
- Eseguire azioni casuali (per verifica *liveness*).

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 caso di esito positivo, il video sarà accettato dal sistema, altrimenti si inviterà l'utente ad effettuare la video identificazione con operatore e il video sarà cancellato.

Successivamente, un operatore autorizzato verificherà i video accettati dal sistema e 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.
- In modalità "*unattended*" per il Cliente; vengono quindi eseguite 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;
  - confronto tra i dati inseriti nel portale e quelli riportati nei documenti d'identità caricati.
- 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 inseriti nel form di registrazione.

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/Richiedente.

F.3. Registrazione degli utenti richiedenti la certificazione

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

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

F.4. Certificati di firma digitale in particolari ambiti chiusi di utenti

È possibile l'emissione di un certificato qualificato di firma elettronica prima che sia conclusa l'identificazione del Titolare solamente nel caso sussistano particolari circostanze riconducibili a limitati utilizzi della firma digitale in contesti chiusi di utenti che non consentono alle firme digitali generate di produrre alcun effetto giuridico qualora la verifica dell'identità del titolare del certificato non termini con esito positivo.

Questa possibilità è stata confermata dall'Agenzia con la comunicazione alle CA del 7 giugno 2016, "*agid.AOO-AgID.REGISTRO UFFICIALE(U).0016101.07-06-2016*", avente per oggetto "*Richiesta di chiarimenti in merito all'utilizzo della firma digitale in particolari ambiti chiusi di utenti*".

Tipico è il caso in cui l'oggetto della sottoscrizione è un atto per cui sia prescritta la sottoscrizione di due o più parti, senza le quali è giuridicamente *imperfetto*, privo quindi di qualunque effetto giuridico (ad es. la richiesta di adesione a specifici servizi, quali carte di credito, conti deposito, etc..).

Il processo, conforme alla comunicazione sopra menzionata, ha le seguenti restrizioni:

1) Il processo è riconducibile esclusivamente a sistemi di firma remota;
2) L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;
3) Nel certificato qualificato del Titolare sono presenti stringenti limiti d'uso afferenti il rapporto specifico tra Cliente e Banca / Istituto, Titolare e cointeressato e cofirmatario (par. *F.4.1*);
4) Con l'obiettivo di distinguere chiaramente questi certificati da quelli emessi con procedure più tradizionali, il certificato qualificato del Titolare contiene uno specifico OID (par.*F.4.2*);
5) L'applicazione di firma remota utilizzata limita gli oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario. I documenti oggetto della sottoscrizione devono essere giuridicamente imperfetti, cioè privi di effetto fino all'apposizione della firma del cointeressato e cofirmatario. A titolo di esempio, si citano i contratti per l'adesione ad un servizio;
6) Nel caso in cui la verifica dell'identità del Titolare avvenga per mezzo di un incontro fisico fra Titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del Certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario se diverso dal Certificatore;
7) Il cointeressato e cofirmatario può espletare la verifica dell'identità in vece del Certificatore, attraverso sessioni audio-video ovvero in applicazione della normativa afferente la verifica dell'identità di cui al *D.lgs. 231/2007*, ove applicabile. Qualora, nell'ambito della verifica ai sensi di tale D.lgs. sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;
8) All'apposizione della firma del Titolare non viene apposta la marca temporale: questa è apposta solo dopo la firma del cointeressato e cofirmatario che rende l'atto giuridicamente perfetto;
9) Fino all'apposizione della firma e della marca di cui al precedente punto 8, l'oggetto sottoscritto dal solo Titolare non è fornito ad alcuno e, qualora la verifica dell'identità del Titolare non avesse buon fine, il documento è distrutto conservando traccia degli eventi in appositi log.

F.4.1. Limite d'uso specifico

Per ottemperare al punto 3) del par. *F.4*, sarà definito un limite d'uso specifico per questa tipologia di certificati.

La formula standard è la seguente:

> *"Il presente Certificato Qualificato è valido solo per la sottoscrizione di documenti relativi all'adesione ai servizi di Nome servizio erogati da Nome Banca / Istituto ai propri Clienti."*
>
> *"This Qualified Certificate is valid only for electronic signatures affixed to documentation relating to Nome servizio provided by Nome Banca / Istituto to its Customers."*

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

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

F.4.2. OID specifico

Per ottemperare al punto 4), il certificato emesso sotto queste condizioni è distinguibile dagli altri certificati in quanto contiene, nel campo uno dei seguenti OID (ognuno definito in riferimento alla CA di root che ha emesso il certificato):

- ***1.3.76.21.1.3.1***.1.1
- ***1.3.76.21.1.5.1***.1.1
- ***1.3.76.21.10.2.1***.2.1

Per ulteriori approfondimenti sugli OID utilizzati dal QTSP, è disponibile il documento *CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico*, pubblicato all'URL *https://www.intesa.it/e-trustcom/*.

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 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 di certificato sarà immediatamente inviata dall'applicazione della Banca / Istituto alla 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 alla DETERMINAZIONE AgID N. 147/2019 (*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati*).

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale contengono almeno una limitazione d'uso (par. *F.1.1*, ovvero par. *F.4.1* per le tipologie di firma di cui al par. *F.4*).

H.4. Codice di Emergenza

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

Nelle applicazioni descritte dal presente Manuale Operativo, sarà considerato come codice di emergenza il PIN consegnato al Titolare all'atto della sua registrazione.

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi della Banca o dell'Istituto di Pagamento, 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 di Pagamento oppure direttamente allo sportello di una filiale della Banca o dell'Istituto di Pagamento.

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 due modalità di autenticazione diverse che, nel rispetto della normativa vigente, permettono ad un Titolare, una volta registrato, di procedere prima con la generazione delle chiavi di firma e richiesta di un certificato qualificato e poi di utilizzare le stesse per effettuare firme elettroniche qualificate.

A conferma dell'effettuazione delle operazioni di firma saranno inviati SMS. Qualora il Titolare disponga di uno smartphone abilitato alla lettura della corrispondenza, su richiesta del Titolare stesso, in alternativa, potranno essere inviati e-mail.

I.1. Autenticazione di tipo "Call Drop"

Questa modalità di autenticazione richiede all'utente, già precedentemente identificato, 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, in caso di verifica positiva, autorizzata l'operazione di firma elettronica qualificata.

Pertanto, quando il Titolare vorrà firmare un documento accedendo al portale della Banca / Istituto utilizzerà un'autenticazione a due fattori attraverso l'inserimento di un PIN (informazione che solo l'utente conosce) e un numero di telefono (dato dalla SIM, che solo l'utente possiede).

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, viene chiusa.

L'utente Titolare non riceve mai una risposta alla propria chiamata e pertanto non incorre in alcun costo telefonico.

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.

Vedremo nel seguito come questa autenticazione appena descritta sia altamente gradita quando il Titolare si trovi da operare in stazioni non presidiate (tipicamente collegandosi ai servizi della Banca o dell'Istituto di Pagamento con il proprio PC attraverso i servizi di home banking esposti dalla Banca o dell'Istituto di Pagamento stessi), ma, invece, sia poco praticabile quando il Titolare si trovi ad operare di fronte ad un operatore esterno, ad esempio in una stazione presidiata da un cassiere della Banca o dell'Istituto di Pagamento.

Per gestire queste ultime situazioni, si è studiata una soluzione basata su una gestione dinamica dei numeri telefonici da chiamare per finalizzare il processo di autenticazione proprio in quelle che chiameremo stazioni presidiate.

I.2. Processo di Firma in stazioni non presidiate (Home banking)

Entrato in possesso dei necessari codici durante la fase di identificazione, il Titolare potrà in un momento successivo richiedere il proprio Certificato digitale e procedere poi alla firma di un documento secondo le modalità di seguito descritte.

1. Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione.
2. Seleziona e verifica il documento da firmare.
3. Inserisce il proprio codice PIN.
4. Appena validato il PIN, il Titolare, in un tempo configurato (non superiore al minuto primo) e utilizzando il cellulare precedentemente censito, deve, per confermare la propria intenzione di firmare il documento, immediatamente chiamare un numero telefonico che gli sarà nel frattempo comparso a video.
5. Il sistema, rilevando che il numero chiamante è proprio quello censito in precedenza e associato al Titolare, procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa.
6. Se, invece, è trascorso il tempo prefissato senza che il sistema abbia ricevuto una telefonata al numero indicato al punto 4, l'operazione viene considerata nulla e conclusa senza la sottoscrizione del documento.

Qualora i documenti da firmare fossero più di uno, il Titolare deve reiterare i passi dal 2 al 5 per ogni documento.

I.2.1. Processo di Firma in stazioni presidiate (Sportello bancario o finanziario)

Una volta ottenuto il certificato qualificato, il Titolare potrà procedere alla sottoscrizione di un documento.

Come detto in precedenza, presso uno sportello bancario o finanziario e di fronte ad un operatore il Titolare potrebbe trovarsi in difficoltà ad inserire codici personali e riservati quali ad esempio un PIN.

Si è perciò pensato anche ad una soluzione alternativa, che garantisca comunque il massimo della sicurezza:

1. L'utente si presenta allo sportello di una filiale della Banca / Istituto (stazione presidiata) e viene riconosciuto dal personale addetto (il cassiere, ad esempio) in modalità canonica.
2. Visionato il documento da firmare, il Titolare può avviare il processo di firma.
3. Viene a questo punto reso disponibile su di un video, visibile al Titolare, un numero telefonico (scelto casualmente all'interno di un copioso set di numeri disponibili) e contemporaneamente viene fatto partire un timer.
4. Il Titolare, in un tempo configurato non superiore al minuto primo, deve chiamare il numero che gli è apparso a video (utilizzando il proprio cellulare, censito in precedenza) per confermare la propria intenzione di sottoscrivere il documento.
5. Il sistema, a questo punto, se rileva la correttezza del chiamante, provvede ad eseguire la sottoscrizione del documento e ad inviare via SMS una conferma dell'operazione stessa.
6. Se, invece, è trascorso il tempo prefissato senza che il sistema abbia ricevuto una telefonata al numero indicato al punto 3, l'operazione viene annullata.

Qualora i documenti da firmare fossero più di uno, il Titolare deve reiterare i passi dal 2 al 5 per ogni documento.

I.3. Autenticazione di tipo OTP Mobile

In alternativa allo strumento di autenticazione *Call Drop*, è resa disponibile una seconda modalità di autenticazione denominata "*OTP Mobile*".

Per attivare questa modalità, il Titolare dovrà disporre di uno smartphone fra quelli specificati dalla Banca / Istituto come adeguati per tale servizio.

Eseguita questa verifica, in fase di identificazione presso lo sportello della Banca / Istituto dove è avvenuta la registrazione, al Titolare sarà comunicato un indirizzo internet specifico sul sito della Banca o dell'Istituto di Pagamento da cui scaricare sul suo smartphone un'applicazione definita di "*OTP Mobile*" e gli sarà consegnato un PIN.

Anche per questa seconda modalità di autenticazione descriviamo il processo di sottoscrizione a seconda che si svolga o meno in stazioni presidiate.

I.3.1. Processo di Firma in stazioni non presidiate (Home banking)

Entrato in possesso del proprio certificato qualificato, il Titolare potrà sottoscrivere un documento nei seguenti passi:

1. Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione.
2. Seleziona e verifica il documento da firmare.
3. Inserisce quindi il suo PIN.
4. Lancerà poi l'applicazione precedentemente scaricata sul suo smartphone ricevendone un OTP mobile da inserire successivamente al PIN.
5. Il sistema, rilevando la correttezza del PIN e dell'OTP mobile appena inseriti, procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa.

Qualora i documenti da firmare fossero più di uno, il Titolare deve reiterare i passi dal 2 al 5 per ogni documento.

I.3.2. Processo di Firma in stazioni presidiate (Sportello bancario o finanziario)

Anche in questo caso si è studiata una soluzione che non richieda al Titolare di inserire davanti al personale della Banca o dell'Istituto di Pagamento codici riservati che possano essere 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 di Pagamento (stazione presidiata) e viene riconosciuto dal personale addetto (il cassiere, ad esempio) in modalità canonica.
2. Al momento della firma viene attivato di fronte all'utente uno specifico monitor dotato di webcam.
3. Il Titolare, una volta verificato su tale monitor il documento da firmare e deciso di procedere con l'operazione di sottoscrizione, lancia dal proprio smartphone la generazione di un OTP che viene visualizzata anche in formato di codice a barre.

4. Il Titolare può a questo punto, posizionando il proprio smartphone verso la webcam, permettere la lettura dell'OTP generata al passo 3 e avviare la procedura di sottoscrizione vera e propria.
5. Il sistema una volta firmato il documento provvede a darne immediata notifica attraverso l'invio di un SMS al Titolare stesso.

Qualora i documenti da firmare fossero più di uno, il Titolare deve reiterare i passi dal 2 al 5 per ogni documento.

Rimanendo nel caso di un processo di firma che avvenga in una stazione presidiata da un operatore banca, il Titolare potrà ricevere il codice OTP anche via SMS sul proprio dispositivo mobile (precedentemente censito secondo le procedure previste dall'istituto bancario). Inoltre, se la postazione presidiata è dotata di un tablet in grado di recepire attraverso una tastiera virtuale l'inserimento dell'OTP, il Titolare, una volta ricevuto lo stesso, potrà digitarlo alla presenza dell'operatore sul tablet stesso, confermando così la volontà di procedere con la firma del documento.

I.3.3. Processo di Firma per i clienti Prospect

Il processo per il rilascio del Certificato qualificato di firma remota può essere gestito anche da un Cliente Prospect durante le attività di Onboarding (acquisizione del Cliente).

Il processo è compatibile con i principali browser (Chrome, Firefox, Edge, Safari) e con i dispositivi mobile più recenti della famiglia Android e Apple.

Si articola come segue:

1. All'avvio del processo si richiede al Cliente Prospect l'inserimento dei propri dati personali al fine di permettere una successiva identificazione certa, previa sottoscrizione dell'informativa sulla privacy del QTSP INTESA.
2. La Banca Istituto procede con l'invio di un SMS il cui testo contiene un OTP (One Time Password) con validità temporanea: è richiesto al Cliente Prospect di inputare tale codice, al fine di verificare la reale disponibilità del dispositivo mobile indicato in fase di inserimento dati.
3. Completata la verifica di cui al punto precedente, il Cliente Prospect procede quindi a trasmettere i documenti di identità alla Banca Istituto: i dati anagrafici verranno inseriti dal Prospect o acquisiti dai documenti mediante un sistema di OCR.
4. Completata la fase di registrazione, la Banca invierà al Cliente Prospect la documentazione contrattuale che il Cliente Prospect potrà firmare con un certificato qualificato di firma digitale remota (FDR) emesso dal QTSP INTESA.
5. Al Cliente Prospect, analogamente alla procedura descritta per l'internet banking, verrà presentata la documentazione di richiesta del certificato del QTSP INTESA.
6. La presa visione della stessa dovrà essere obbligatoriamente sottoscritta spuntando i check box del documento e apponendo una firma elettronica mediante l'inserimento di un OTP ricevuto via sms dal QTSP INTESA.
7. Se l'OTP fornito dal QTSP INTESA sarà verificato positivamente, si potrà procedere con l'emissione di un certificato qualificato, in caso contrario dovrà essere richiesto un nuovo OTP.
8. Al momento della generazione del certificato è indispensabile, comunque, che venga inserito un PIN, il quale sarà poi richiesto ad ogni utilizzo del certificato di firma.
9. Il certificato appena emesso potrà essere, comunque, utilizzato solo per sottoscrivere la proposta contrattuale e nessun altro documento finché la Banca non abbia completato le necessarie verifiche propedeutiche all'apertura di un conto corrente.
10. Se le verifiche della Banca avranno successo e il conto corrente viene attivato, il Cliente Prospect potrà utilizzare il certificato emesso, nel rispetto delle sue limitazioni d'uso, nei rapporti con la Banca.
    Se, invece, la Banca dovesse decidere di non dare seguito alla richiesta di apertura di un conto corrente, lo stesso certificato verrebbe revocato inibendone un suo ulteriore utilizzo.
11. In entrambi i casi di cui al punto precedente, il Cliente Prospect verrà comunque informato sull'esito delle verifiche e sull'eventuale revoca del certificato.

I.4. Autenticazione con Token OTP

Infine, può essere utilizzata un'autenticazione legata all'utilizzo di Token OTP fisici (molto diffusi nel mondo bancario e finanziario).

L'utilizzo di questo Token OTP fisico è oggi previsto solo per accessi in stazioni non presidiate (tipicamente una postazione remota di home banking).

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 inserirà il PIN e il codice OTP che avrà nel frattempo generato e visualizzato sul display del Token.

Facendo sempre riferimento ai servizi di Home Banking, il Titolare oltre, al Token OTP fisico, potrà utilizzare anche OTP via SMS, Mobile Token e strumenti con analoghe caratteristiche.

La password generata dallo strumento di strong authentication potrà essere utilizzata unitamente al codice di identificazione personale (PIN) quale strumento di autenticazione per sottoscrivere digitalmente, nell'ambito del servizio di Home Banking, documenti, disposizioni o contratti relativi a prodotti o servizi erogati dalla Banca o Istituto finanziario.

I.5. Autenticazione con Notifica Push su App Mobile Banking

Le Banche e gli Istituti finanziari si stanno dotando sempre di più frequentemente di ulteriori innovativi strumenti tecnologici per permettere la firma di documenti, disposizioni o contratti relativi a prodotti o servizi erogati che fanno uso di App emesse dallo stesso istituto.

Il processo di attivazione dell'App Mobile Banking prevede, a garanzia della sicurezza, che:

- il Cliente possa utilizzare in modalità dispositiva la propria App Mobile Banking solo previa attivazione della stessa su un solo dispositivo Mobile;
- l'utilizzo dell'App Mobile Banking per la sottoscrizione possa essere effettuato da ciascun Cliente su di un solo dispositivo Mobile; pertanto, nel caso in cui il Cliente decidesse di attivare l'App Mobile Banking in modalità dispositiva su uno Smartphone differente rispetto a quello precedentemente utilizzato, prima di poter effettuare una nuova attivazione, sarà necessario completare la disattivazione dell'App sul precedente dispositivo Mobile;
- l'attivazione dell'App Mobile Banking prevede una verifica incrociata dei recapiti del Cliente (numero di telefono e indirizzo e-mail) e richiede una *Strong Authentication* finale.

Dovendo procedere con una firma digitale in questa modalità, il Titolare dovrà, prima di procedere, accedere all'app precedentemente installata.

Il processo di Login all'interno dell'App Mobile Banking richiederà una verifica incrociata di alcune informazioni, che consentono l'identificazione univoca del Cliente:

- Codice Adesione
- Codice PIN di accesso al Servizio Internet Banking oppure Fingerprint / Riconoscimento del volto/Iride (cioè il codice di accesso numerico / biometrico che dovrà essere necessariamente inserito dal Cliente ad ogni Login).
- Codice OTP: è un codice OTP (Mobile Token) che viene generato automaticamente dall'App in fase di Login (si specifica infatti che l'App, una volta attivata su un dispositivo Mobile, è in grado di generare Codici Token di Sicurezza).

L'App invierà queste tre informazioni ai Sistemi Banca per opportune verifiche, autorizzando pertanto la Login del Cliente solo nel caso in cui l'esito di tali verifiche sia positivo.

Se lo Smartphone del Cliente supporta la tecnologia per il riconoscimento dell'impronta digitale, del volto o dell'iride, questi potrà utilizzare la modalità denominata "FingerPrint/FaceId o Riconoscimento del volto" sia per identificarsi in sede di accesso al Servizio di Banca Multicanale tramite Applicazione Mobile Banking, sia per autorizzare operazioni/processi previsti per tale modalità.

Il Titolare, grazie a questi strumenti di autenticazione, dopo aver visionato il documento potrà procedere alla firma dello stesso confermando la propria volontà utilizzando le tecniche sopra descritte.

I.6. Autenticazione con tecniche grafometriche

Il processo è previsto presso le stazioni presidiate (sportello bancario o finanziario)

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 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.

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 non raggiungimento dello score desiderato può essere dovuto a errori anche banali, ma immediatamente rilevati dal sistema (mancanza di una lettera, omissione di vocali accentate, etc.).

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 di Pagamento oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto di Pagamento.

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 di pagamento, 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 di Pagamento oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto di Pagamento.

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

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

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 di Pagamento, in qualità di Terzo Interessato, potranno richiedere la sospensione del certificato.

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

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 hanno validità di 36 (trentasei) mesi dalla data di emissione.

Al termine sopracitato, 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.

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 alla sezione *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.

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

M.2. Accesso logico al Registro dei certificati

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

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

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

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

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

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

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

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

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 server dedicati ai servizi di marcatura temporale hanno inoltre un controllo software tra l'orario della macchina e un cospicuo numero di server NTP distribuiti a livello planetario: l'utilità di controllo, installata su ognuno dei server utilizzati dal QTSP INTESA nell'ambito della validazione temporale, periodicamente verifica l'allineamento del clock di sistema questi NTP Server di riferimento Se l'allineamento temporale non risulta conforme alle specifiche tecniche di riferimento tempo per tempo vigenti, il servizio di marcatura temporale erogato dallo specifico server che risultasse disallineato viene arrestato.

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).

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 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - 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 V2.1.0 - 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-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - 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 V2.1.1 - 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
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)

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