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

Manuale Operativo
per le procedure di firma digitale remota
nell'ambito dei servizi di FinecoBank S.p.A.

Codice documento: MO_FNC

OID: 1.3.76.21.1.3.1.160

Redazione: Antonio Raia

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

Data emissione: 21/07/2022

Versione: 07

Digitally signed by ANTONIO RAIA
Date: 2022.09.19 10:25:19 CEST

Revisioni

Versione n°: 07	***Data revisione: 21 luglio 2022***
Descrizione modifiche:	*F.5.1: a*ggiornamento limite d'uso *Q:* Aggiornamento descrittivo
Motivazioni:	Aggiornamenti
Versione n°: 06	***Data revisione: 31 dicembre 2021***
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti tecnici
Motivazioni:	Variazione proprietà, direzione e coordinamento Aggiornamenti normativi
Versione n°: 05	***Data revisione: 13 marzo 2020***
Descrizione modifiche:	Aggiornamento ragione sociale FinecoBank S.p.A. e logo F.3: nuovo paragrafo F.4: nuovo paragrafo Aggiornamento riferimenti di legge e definizioni Aggiornamento layout e logo del QTSP
Motivazioni:	Variazione statuto societario Aggiunta descrizione della modalità di autenticazione "Mobile Code" Aggiunta descrizione della modalità di autenticazione "Password Vocale" Aggiornamenti normativi Nuovo logo del QTSP In.Te.S.A. S.p.A.
Versione n°: 04	***Data revisione: 13 giugno 2017***
Descrizione modifiche:	A.1: aggiornato il Capitale Sociale C.5: aggiunta limitazione alle modalità di identificazione
Motivazioni:	Variazione Capitale Sociale FinecoBank S.p.A. Specificazione modalità di riconoscimento
Versione n°: 03	***Data revisione: 9 febbraio 2017***
Descrizione modifiche:	Variazione procedura di rilascio del certificato Variazione riferimenti normativi – verifica conformità
Motivazioni:	Aggiornamenti servizi Aggiornamenti normativi: Reg. (UE) 910/2014 (eIDAS) - Dlgs 26/8/2016, n. 179
Versione n°: 02	***Data revisione: 17 marzo 2014***
Descrizione modifiche:	Aggiornamento agli Obblighi delle Registration Authority esterne Aggiornamento riferimenti al DPCM 22 febbraio 2013 Introduzione dell'utilizzo di Applicazioni per dispositivi mobili Aggiornato il Codice documento (MO-FNC)
Motivazioni:	Aggiornamento
Versione n°: 01	***Data revisione: 07 novembre 2012***
Descrizione modifiche:	Nessuna
Motivazioni:	Prima emissione

Sommario

Revisioni **2**
Sommario **3**
Riferimenti di legge **5**
Definizioni e acronimi **5**
A. Introduzione **7**
A.1. Proprietà intellettuale 7
A.2. Il Manuale Operativo 7
A.3. Validità 7
B. Generalità **7**
B.1. Dati identificativi della versione del Manuale Operativo 8
B.2. Dati identificativi del QTSP – Qualified Trust Service Provider 8
B.3. Responsabilità del Manuale Operativo 8
B.4. Entità coinvolte nei processi 9
B.4.1. Certification Authority (CA) 9
B.4.2. Registration Authority (RA) 9
C. Obblighi **9**
C.1. Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP) 9
C.2. Obblighi del Titolare 10
C.3. Obblighi degli utilizzatori dei certificati 11
C.4. Obblighi del Terzo Interessato 11
C.5. Obblighi delle Registration Authority esterne 11
D. Responsabilità e limitazioni agli indennizzi **12**
D.1. Responsabilità del QTSP INTESA - Limitazione agli indennizzi 12
D.2. Assicurazione 12
E. .Tariffe **13**
F. Modalità di identificazione e registrazione degli utenti per il rilascio del Certificato Qualificato **13**
F.1. Identificazione degli utenti 13
F.2. SMS PIN 13
F.3. Mobile Code 14
F.4. Password Vocale 15
F.5. Certificato Qualificato per la firma digitale 15
F.5.1. Limitazioni d'uso 15
G. Generazione delle chiavi di Certificazione, di Validazione Temporale e di sottoscrizione **16**
G.1. Generazione delle chiavi di certificazione 16
G.2. Generazione delle chiavi del sistema di validazione temporale 16
G.3. Generazione delle chiavi di sottoscrizione 16
H. Modalità di emissione dei certificati **16**
H.1. Procedura di emissione dei Certificati di certificazione 16
H.2. Procedura di emissione dei Certificati di sottoscrizione 17
H.3. Informazioni contenute nei certificati 17
H.4. Codice di Emergenza 17
I. Modalità operative per la sottoscrizione di documenti **17**
I.1. Rilascio del Certificato Qualificato 18
I.2. Processo di firma 18
J. Modalità operative per la verifica della firma **19**
K. Modalità di revoca e sospensione dei certificati **19**
K.1. Revoca dei certificati 19
K.1.1. Revoca su richiesta del Titolare 19
K.1.2. Revoca su richiesta del Terzo Interessato 19
K.1.3. Revoca su iniziativa del QTSP 19

K.1.4. Revoca dei certificati relativi alle chiavi di certificazione 19
K.2. Sospensione dei certificati 20
K.2.1. Sospensione su richiesta del Titolare 20
K.2.2. Sospensione su richiesta del Terzo Interessato 20
K.2.3. Sospensione su iniziativa del QTSP 20
L. Modalità di sostituzione delle chiavi 20
L.1. Sostituzione dei certificati qualificati e delle chiavi del Titolare 20
L.1. Sostituzione delle chiavi del QTSP 20
L.1.1. Sostituzione in emergenza delle chiavi di certificazione 20
L.1.2. Sostituzione pianificata delle chiavi di certificazione 21
L.1.3. Chiavi del sistema di validazione temporale (TSA) 21
M. Registro dei certificati 21
M.1. Modalità di gestione del Registro dei certificati 21
M.2. Accesso logico al Registro dei certificati 21
M.3. Accesso fisico ai locali dei sistemi preposti al registro dei certificati 21
N. Modalità di protezione dei dati personali 21
O. .Procedura di gestione della copie di sicurezza 21
P. Procedura di gestione degli eventi catastrofici 22
Q. Modalità per l'apposizione e la definizione del riferimento temporale 22
Q.1. Modalità di richiesta e verifica marche temporali 23
R. Lead Time e Tabella Raci per il rilascio dei certificati 23
R.1. Lead Time di processo 23
R.2. Tabella RACI 24
S. Riferimenti Tecnici 24

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*.
Normativa Privacy	Comprende il Regolamento UE 2016/679 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 ("GDPR"); il Codice in materia di protezione dei dati personali, recante disposizioni per l'adeguamento dell'ordinamento nazionale al GDPR (D.Lgs. 196/2003), i provvedimenti, le linee guida e le opinioni del Garante per la protezione dei dati personali, del Comitato Europeo per la Protezione dei Dati (ex Gruppo di lavoro articolo 29) e di ogni altra autorità competente; le Parti agiscono in qualità di titolari autonomi del trattamento di dati personali che ciascuna di esse raccoglie in ragione delle proprie funzioni istituzionali e delle obbligazioni contrattuali. Nel seguito, sarà indicato solo come *Normativa Privacy*
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* (electronic IDentification, Authentication and trust Services).
DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE *e ss.mm.ii.*	DECISIONE DI ESECUZIONE (UE) 2015/1506 DELLA COMMISSIONE dell'8 settembre 2015 che stabilisce le specifiche relative ai formati delle firme elettroniche avanzate e dei sigilli avanzati che gli organismi del settore pubblico devono riconoscere, di cui all'articolo 27, paragrafo 5, e all'articolo 37, paragrafo 5, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (Testo rilevante ai fini del SEE). Nel seguito indicato anche solo come *DECISIONE (UE) 2015/1506*.
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* ovvero *Raccomandazioni AgID*.

Definizioni e acronimi

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP *Qualified Trust Service Provider.* *Certificatore Accreditato*	*Prestatore di Servizi Fiduciari Qualificati*. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A.
Servizio Fiduciario Qualificato	Servizio elettronico fornito da un QTSP e consistente negli elementi di cui all'art. 3, punto 16) e 17) del Reg. UE 910/2014 (eIDAS). Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta i servizi qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime.

Certificato Qualificato di firma elettronica (firma digitale)	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 QTSP / 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, 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 QTSP / Certificatore, contenente tutti i Certificati emessi.
Richiedente	La Persona Fisica che richiede il Certificato.
Titolare	La Persona Fisica cui il Certificato Qualificato è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma elettronica qualificata o digitale.
Cliente *Cliente Prospect*	É il Cliente (o potenziale Cliente, detto Prospect) della Banca.
Terzo Interessato	La persona fisica o giuridica il cui consenso è necessario per il rilascio al Titolare del Certificato Qualificato Ha il diritto/dovere di richiedere la revoca o sospensione del certificato nel caso risultano modificati i requisiti in base ai quali lo stesso è stato rilasciato
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
TSA - Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
RACI (Tabella)	RACI - Responsible, Accountable, Consulted, Informed Matrice di assegnazione delle responsabilità (in un processo)

A. Introduzione

Questo documento è il *Manuale Operativo per la procedura di firma digitale remota nell'ambito dei Servizi forniti da FinecoBank S.p.A.* (di seguito anche solo *Fineco* o *Banca*), con Sede Sociale in Piazza Durante 11, 20131 Milano - Direzione Generale in via Rivoluzione d'Ottobre, 16, 42123 Reggio Emilia Banca iscritta all'Albo delle Banche e Capogruppo del Gruppo Bancario FinecoBank – Albo dei Gruppi Bancari cod. 3015 - P.IVA 12962340159 - Codice Fiscale e n. iscr. R.I. Milano-Monza-Brianza-Lodi 01392970404 - R.E.A. n. 1598155 - Aderente al Fondo Nazionale di Garanzia e al Fondo Interbancario di Tutela dei depositi.

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. Il Manuale Operativo

Il Manuale Operativo descrive le procedure e le relative regole utilizzate dal *Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A.* (di seguito anche solo *INTESA* o *QTSP INTESA*) per l'emissione dei Certificati Qualificati e la generazione e la verifica della firma elettronica qualificata nell'ambito dei servizi offerti da FinecoBank 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* (nel seguito, anche solo "*DPCM*") e dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "*Codice dell'Amministrazione Digitale*", come successivamente modificato e integrato (nel seguito, anche solo "*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 tempo per tempo vigenti.

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

Il processo prevede che il Titolare possa avviare la procedura di firma remota di documenti e/o contratti relativi a prodotti e servizi offerti dalla Banca.

A.3. Validità

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

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

- *chiavi di* sottoscrizione (o di *firma*), destinate alla generazione e verifica delle firme apposte o associate ai documenti;
- *chiavi di certificazione*, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
- *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 relative regole utilizzate dal QTSP INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito, la cui osservanza permette ad INTESA di essere inserita nell'elenco dei Prestatori di Servizi Fiduciari Qualificati (QTSP) ai sensi del Reg. eIDAS.

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

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n. ***07***, rilasciata in conformità con l'art. 40 del DPCM, del *Manuale Operativo per la procedura di firma digitale remota nell'ambito dei Servizi forniti da FinecoBank S.p.A.*

L'object identifier di questo documento è **1.3.76.21.1.3.1.160**.

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

- all'indirizzo Internet del QTSP, *www.intesa.it/e-trustcom/*
- all'indirizzo Internet di Fineco, *finecobank.com*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*

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

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

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

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

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'art. 40 comma 3 lett. c) del DPCM è del QTSP INTESA, che ne cura la stesura, la pubblicazione, l'aggiornamento e ogni eventuale revisione, in accordo e in collaborazione con la Banca.

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

- un recapito di posta elettronica: *marketing@intesa.it*
- un recapito telefonico: +39 011.192.16.111
- un servizio di HelpDesk: per le chiamate dall'Italia 800.805 093
per le chiamate dall'estero +39 39 02.39.30.90.66

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP INTESA 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 INTESA espletando, per la parte di loro competenza, le attività a loro attribuite.

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

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

B.4.1. Certification Authority (CA)

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

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

B.4.2. Registration Authority (RA)

Per la particolare tipologia di servizio offerto (firma digitale remota nell'ambito delle applicazioni della Banca descritte in questo Manuale Operativo), il QTSP INTESA ha rilasciato mandato a svolgere le funzioni di Local Registration Authority (LRA) a Fineco.

In particolare, la Banca svolge le seguenti attività:

- Identificazione certa del Richiedente / Titolare.
- Registrazione del Richiedente.

La Banca, nello svolgimento della funzione di Registration Authority, deve vigilare affinché l'attività di identificazione del Titolare si svolga nel rispetto della normativa vigente.

C. Obblighi

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

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

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

In particolare, il QTSP:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno a terzi;
- si attiene alle regole tecniche specificate nel DPCM e ss.mm.ii.;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'art. 29 del Reg. eIDAS;
- rilascia e rende pubblico il Certificato Qualificato secondo quanto stabilito all'art. 32 del CAD, nel rispetto della Normativa Privacy ;
- 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 secondo quanto stabilito dalla Normativa Privacy;
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del Certificato Qualificato in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al Certificato Qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza del QTSP) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

Inoltre, il QTSP:

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

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

C.2. Obblighi del Titolare

Il Titolare richiedente un Certificato Qualificato di firma digitale per i servizi descritti nel presente Manuale Operativo è un Cliente della Banca, la quale opera da Registration Authority.

In quanto tale potrà ricevere un Certificato Qualificato per la firma digitale remota per sottoscrivere contratti e documenti relativi a prodotti e /o servizi offerti dalla Banca.

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al QTSP, tramite la Banca, 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;

- dare immediata comunicazione alla Banca, in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma, la Banca provvederà all'immediato blocco degli stessi e dei canali di accesso ai servizi di firma digitale;
- 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 e il momento della sua emissione; 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 prestatori di servizi fiduciari qualificati (QTSP);
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del Prestatore di Servizi Fiduciari che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

Gli obblighi sopra descritti sono automaticamente espletati dai Software di Verifica conformi alle normative vigenti (art. 14 del DPCM).

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato nei servizi descritti dal presente Manuale Operativo è Fineco.

Pertanto, la Banca deve verificare che il Cliente sia in possesso di tutti i requisiti necessari e, quindi, autorizza il Cliente stesso a richiedere il rilascio del Certificato Qualificato per la firma digitale remota.

La Banca, nella sua veste di Terzo Interessato, svolge un'attività di supporto al Titolare; in particolare sarà la Banca ad indicare al QTSP INTESA:

- eventuali ulteriori limitazioni d'uso del Certificato Qualificato per la firma digitale, oltre a quelle previste al par. *F.5.1*;
- informazioni specifiche relative al Titolare, quali a titolo esemplificativo, ma non esaustivo, eventuali poteri di rappresentanza del Titolare.

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente inoltrata quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato il Certificato Qualificato.

C.5. Obblighi delle Registration Authority esterne

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

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

Il QTSP INTESA ha rilasciato mandato a svolgere la funzione di Registration Authority a Fineco mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

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

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

Il personale della Banca, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa, ovvero in conformità ad analoghe procedure adottate secondo la normativa antiriciclaggio vigente al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale Operativo), svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

La documentazione relativa alle attività di cui sopra, necessaria all'emissione del Certificato Qualificato, viene conservata dalla Banca, secondo gli obblighi di legge, per 20 (venti) anni dall'eventuale scioglimento di tale rapporto.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP INTESA - 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, dalla Normativa Privacy, dal CAD, dal Reg. eIDAS (e ogni loro ss.mm.ii.) e da tutta la pertinente normativa di riferimento, come disciplinato al par. *C.1 - Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)*.

Il QTSP INTESA, *fatto salvo i casi di dolo o colpa* (ai sensi del 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.5.1*.

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 QTSP INTESA. Si ricorda, in particolare, di conservare con la dovuta diligenza dispositivi OTP e codici segreti indispensabili per accedere alle chiavi di firma.

D.2. Assicurazione

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

Di tale contratto è inviata ad AgID apposita dichiarazione di stipula.

E. .Tariffe

Il Servizio di firma digitale è senza oneri per il Titolare e non è pertanto soggetto a tariffazione.

F. Modalità di identificazione e registrazione degli utenti per il rilascio del Certificato Qualificato

F.1. Identificazione degli utenti

Il QTSP INTESA deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di un Certificato Qualificato per la firma digitale.

Questa operazione viene demandata alla Banca che, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio, identificherà e registrerà il Titolare.

Il servizio di identificazione potrà essere gestito in due modalità:

1. ***Modalità tramite Personal Financial Advisor*** - Il Titolare potrà chiedere di essere contattato da un Personal Financial Advisor che, fissatogli un appuntamento, lo supporterà in tutte le procedure inerenti l'apertura di un Conto Corrente, tra le quali l'identificazione ai sensi della vigente normativa antiriciclaggio**. NB**: questa modalità di identificazione è limitata al mercato italiano.
2. ***Modalità diretta on line*** - Il Titolare richiede l'apertura di un Conto Corrente in modalità diretta on-line. In questo caso la Banca effettua l'identificazione secondo le modalità previste dalla normativa antiriciclaggio vigente.

Per i successivi rinnovi, qualora effettuati prima che il Certificato Qualificato (precedentemente rilasciato) sia scaduto, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al QTSP INTESA, attraverso la Banca, solo gli eventuali cambiamenti relativi ai propri dati di registrazione.

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

- nome e cognome;
- data di nascita;
- comune o stato estero di nascita;
- codice fiscale;
- indirizzo di residenza;
- domicilio presso il quale saranno inviate le comunicazioni cartacee;
- numero di telefono cellulare;
- indirizzo di posta elettronica;
- tipo e numero del documento d'identità esibito;
- autorità che ha rilasciato il documento, luogo del rilascio, data di emissione e di scadenza.

Per l'accesso ai servizi offerti da Fineco, la stessa consegna ai propri clienti un *Codice Utente* e un *Codice di attivazione*, tramite i quali sarà possibile impostare la Password necessaria per accedere all'area riservata del sito *finecobank.com*, e un *PIN - Personal Identification Number* (composto da 8 caratteri numerici), che garantiscano un accesso sicuro ai servizi dispositivi e al servizio di firma digitale remota fornito dalla Banca stessa.

Queste credenziali potranno essere successivamente modificate/aggiornate dal Titolare usufruendo dei servizi resi disponibili dalla Banca.

F.2. SMS PIN

Per le successive operazioni (rilascio del Certificato Qualificato contestualmente alla prima procedura di firma digitale), invece di far uso dei più tradizionali strumenti OTP (One time Password) basati su token fisici, il Cliente potrà disporre di un servizio alternativo denominato ***SMS PIN***.

Tale servizio fornisce ai Clienti che vi abbiano aderito tramite la procedura di attivazione un alto livello di sicurezza e consiste nella generazione e nell'invio di un messaggio SMS sul telefono cellulare del Cliente. Questo messaggio SMS PIN è praticamente un codice OTP "*usa e getta*", da utilizzarsi in aggiunta al PIN dispositivo standard per la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dalla Banca.

Il messaggio SMS, oltre al codice OTP, contiene elementi distintivi della specifica operazione richiesta dal Cliente; in particolare, ricordiamo che:

- ogni codice SMS PIN generato è associato ad una singola operazione richiesta dal Cliente e non è in alcun modo riutilizzabile;
- l'attivazione del Servizio è consentita esclusivamente ai clienti il cui numero di cellulare presente in Anagrafe Generale risulti "certificato";
- l'attivazione del Servizio è indispensabile per poter ottenere il Certificato Qualificato di firma digitale.

Sempre in questa fase, saranno fornite al Titolare ulteriori informazioni e un codice di emergenza, grazie al quale l'utente, in qualsiasi momento, potrà sospendere il Certificato Qualificato a lui intestato. Nelle applicazioni descritte dal presente Manuale Operativo sarà considerato come codice di emergenza il codice SMS PIN descritto in precedenza.

Per certificare il numero di cellulare, il Cliente deve accedere all'area riservata del sito *finecobank.com* mediante inserimento del codice utente e della password e quindi:

- accedere alla sezione "*Gestione Contatti*";
- inserire in apposita maschera il numero di cellulare che si vuole certificare convalidando l'operazione tramite PIN dispositivo;
- attendere la ricezione al numero di cellulare inserito di un SMS contenente il codice di controllo (viene inviata anche un'e-mail informativa);
- confermare l'operazione inserendo sul sito il codice di controllo ricevuto.

A conferma dell'avvenuta certificazione, viene inviata un e-mail al Cliente e un SMS al numero di cellulare appena attivato.

In caso di modifica del numero di cellulare, il servizio sarà trasferito automaticamente sul nuovo recapito telefonico in seguito all'avvenuta certificazione dello stesso. Fino a tale momento, il servizio continuerà ad essere attivo sul precedente numero.

Per garantire la massima sicurezza, in caso di un eventuale cambio del numero di cellulare, saranno inviati due SMS, di cui uno al vecchio numero e uno al nuovo, e sarà verificato il possesso di entrambi i numeri da parte del Cliente.

F.3. Mobile Code

A seguito dell'entrata in vigore della Normativa Europea PSD2, è stato implementato un servizio gratuito dall'App Fineco che eleva gli standard di sicurezza in tema di Strong Customer Authentication, denominato *Mobile Code*.

Utilizzando il Mobile Code si può evitare il doppio inserimento di *PIN dispositivo + SMS PIN*; in alternativa, è possibile l'utilizzo della *Password Vocale + PIN Dispositivo* (cfr. par. *F.4*).

Per attivare il servizio è necessario scaricare l'ultima versione dell'App Fineco e seguire la procedura guidata che consentirà di creare il Mobile Code personale.

Per attivare il Mobile Code verrà chiesto di:

- impostare un codice personale di 7 cifre (il Mobile Code), che dovrà essere memorizzato;
- confermare l'operazione con il *PIN dispositivo* (il PIN dispositivo è il codice composto da 8 cifre che viene utilizzato, sia dal sito Fineco che da App, per confermare le operazioni dispositive, quali ad esempio: bonifici, giroconti, ricariche cellulari);
- inserire il codice OTP che sarà inviato via SMS sul numero di cellulare certificato.

IMPORTANTE! Al termine del processo di attivazione, il Cliente potrà decidere di associare il codice impostato (Mobile Code) al riconoscimento biometrico (*TouchID*, *Fingerprint* o *FaceID*). In questo modo sarà possibile confermare le disposizioni per cui è richiesto il Mobile Code, con riconoscimento facciale (*FaceID*) o con l'impronta digitale (*TouchID*, *Fingerprint*) in modo più semplice, veloce e sicuro.

In caso di mancata associazione al riconoscimento biometrico, il Cliente dovrà digitare il codice impostato di 7 cifre per confermare ogni operazione che necessita del Mobile Code.

Il Mobile Code potrà essere attivato in qualsiasi momento dalle *Impostazioni* dell'App Fineco alla voce "*Mobile Code > Associa"*.

F.4. Password Vocale

Sempre in tema di Strong Customer Authentication, un'ulteriore possibilità di autenticazione, in alternativa al *Mobile Code* o al *PIN dispositivo + SMS PIN*, può essere l'utilizzo di *Password Vocale + PIN Dispositivo*.

Come attivare la *Password Vocale* dall'Area Riservata del sito Fineco:

- Rilasciare il *consenso al trattamento dei propri dati biometrici* e inserire il PIN Dispositivo per prenotare un contatto.
- Successivamente si riceve una chiamata dal numero 02.2899.2899.
  Attenzione! Per poter essere messo in contatto con l'operatore si dovrà rispondere alla chiamata pronunciando la parola "*Pronto*". Nel caso in cui non venga pronunciata alcuna parola, la chiamata rimarrà muta e dopo dieci secondi sarà disconnessa.
- Durante l'attivazione sarà chiesto di ripetere da tre a cinque volte la frase «*La mia banca riconosce il suono della mia voce*». Questo permetterà di registrare il timbro della voce.

Se la *Password Vocale* non fosse stata attivata in fase di attivazione dei codici, è possibile seguire la stessa procedura riportata sopra accedendo dalla propria *Area Riservata* del sito Fineco, sezione "*Gestione Conto > I tuoi codici Fineco > Password Vocale*".

Ricordiamo che è possibile attivare il servizio solo se il numero di cellulare è certificato. Per certificare il cellulare accedere alla sezione "*Gestione Conto > I tuoi contatti*" e seguire le istruzioni.

F.5. Certificato Qualificato per la firma digitale

Il Certificato Qualificato per la firma digitale sarà rilasciato, previa richiesta al QTSP INTESA, al Cliente in possesso di *cellulare certificato* e identificato dalla Banca in ottemperanza con quanto previsto dalla vigente normativa, anche in materia di Antiriciclaggio, e dalle normative interne alla Banca stessa, solo contestualmente all'avvio della prima procedura di firma digitale sul sito della Banca (par. *I*).

Nell'ambito della documentazione contrattuale inerente all'apertura del conto corrente Fineco, la Banca fornisce al Cliente adeguata informativa, concernente gli aspetti normativi e di privacy derivanti dall'emissione del Certificato Qualificato, nonché le specifiche per la richiesta del medesimo al QTSP INTESA.

F.5.1. Limitazioni d'uso

Nel Certificato Qualificato per la firma digitale emesso nell'ambito dei servizi di Fineco descritti nel presente Manuale è inserito il seguente limite d'uso:

"*Il presente certificato e' utilizzabile per la sottoscrizione di disposizioni e/o documenti e/o contratti relativi a prodotti e/o servizi di FinecoBank S.p.A. e/o di terzi, offerti da FinecoBank tramite il sito internet e/o l'App Fineco. Puo' essere altresi' utilizzato per la sottoscrizione di contratti di agenzia o di accordi di collaborazione con FinecoBank, nonche' di patti ad essi accessori."*.

"*This certificate may be used for digital signature of provisions and/or documents and/or contracts concerning products and/or services of FinecoBank S.p.A. and/or of third parties, provided by FinecoBank through the website and/or Fineco's App. It may be used also for signature of agency contracts or cooperation agreements with FinecoBank, as well as their ancillary agreements.*".

Nota: Ulteriori specifici limiti d'uso potranno essere concordati con la Banca.

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

G.1. Generazione delle chiavi di certificazione

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

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma (HSM) del sistema di generazione dei certificati, con i quali si firmano i certificati dei Titolari, e di 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. Per maggior sicurezza, tali chiavi sono suddivise 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 secondo quanto stabilito dall'art. 49 del DPCM.

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

G.3. Generazione delle chiavi di sottoscrizione

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

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato Qualificato di firma digitale ad esse associato autenticandosi al sistema fornitogli dalla Banca in una delle modalità precedentemente descritte.

Il PIN e l'OTP (generata secondo le modalità descritte) costituiscono l'insieme di dati di cui il Titolare deve avere, in modo esclusivo, la conoscenza e il possesso ai sensi dell'art. 8, comma 5, lett. d) del DPCM. Questi stessi dati gli saranno richiesti tutte le volte che voglia sottoscrivere un documento, secondo quanto richiesto dall'art. 35 comma 2 del CAD.

Lo stesso sistema di autenticazione permetterà al Titolare di conservare, in modo esclusivo, il controllo delle proprie chiavi di firma, ai sensi dell'art. 7 comma 3 lett. d) del DPCM.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è di almeno 2048 bit) vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa 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 al par. *G.1*, sono generati i certificati delle chiavi pubbliche, conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

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

H.2. Procedura di emissione dei Certificati di sottoscrizione

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

Generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione della Banca 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

I certificati emessi dal QTSP INTESA nell'ambito del presente manuale sono certificati qualificati ai sensi del Regolamento (UE) 910/2014 (eIDAS) e, pertanto, ne è garantita la loro interoperabilità e il riconoscimento a livello comunitario. I certificati sono inoltre conformi a quanto indicato dalla Determinazione AgID N. 147/2019 (*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati*).

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

- numero di serie;
- ragione o denominazione sociale del QTSP (*issuer*);
- codice identificativo unico del Titolare presso il QTSP;
- nome, cognome, codice fiscale del Titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Il Certificato Qualificato definisce con certezza il QTSP che lo ha emesso (*issuer*) e contiene tutti i dati necessari per la verifica della firma digitale.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale Operativo conterranno sempre una limitazione d'uso (par. *F.5.1*).

H.4. Codice di Emergenza

Il QTSP garantisce un codice di emergenza da utilizzarsi per richiedere la sospensione del Certificato (DPCM, art. 21).

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

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi della Banca, rende disponibile ai Titolari un'applicazione di firma digitale conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia del servizio non richiede che l'applicazione di firma sia installata sul proprio personal computer; la funzionalità di firma sarà resa disponibile accedendo ai servizi offerti dalla Banca attraverso l'area protetta del sito *finecobank.com* o delle Applicazioni per dispositivi mobili (utilizzate su Smartphone e Tablet con sistema operativo Apple IOS, Android e Windows Phone 8). Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno conformi a quanto previsto dal DPCM all'art. 4 comma 2 relativamente agli algoritmi utilizzati.

I documenti sottoscritti con tale applicazione di firma, 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.

Inoltre, tali documenti saranno sempre disponibili, per il sottoscrittore, all'interno di specifica sezione dell'area protetta del sito *finecobank.com*.

I.1. Rilascio del Certificato Qualificato

Come descritto al par. *F*, nel caso il Cliente non sia ancora Titolare di un Certificato Qualificato per la firma digitale nell'ambito dei servizi di FinecoBank, contestualmente all'avvio della prima procedura di firma sul sito della Banca, il Cliente richiederà al QTSP INTESA, per il tramite di Fineco, l'emissione del proprio Certificato.

In tal caso, il Cliente, dopo aver preso visione del Manuale Operativo, dell'Informativa sul servizio e dell'informativa privacy fornita da INTESA, invia la richiesta di certificazione mediante apposizione di un *flag* su di uno specifico disclaimer, che lo rende pienamente cosciente di tutti gli aspetti normativi e di privacy derivanti dall'utilizzo del Certificato Qualificato; accettato in tal modo il disclaimer, Fineco inoltrerà, per conto del Cliente, la richiesta di emissione del certificato alla CA INTESA.

Il presente Manuale Operativo, nonché il disclaimer, saranno sempre disponibili per la visualizzazione nell'area riservata del sito della Banca.

I.2. Processo di firma

Entrato in possesso dei necessari codici durante la fase di identificazione, il Cliente potrà attivare la procedura di firma di un documento secondo le modalità sotto descritte.

1. Il Titolare del Certificato Qualificato per la firma digitale, accedendo all'area riservata del sito *finecobank.com* o delle Applicazioni per dispositivi mobili (utilizzate su Smartphone e Tablet con sistema operativo *Apple IOS*, *Android* e *Windows Phone 8*), mediante inserimento del codice utente e della password in un'apposita sezione, richiede la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dalla Banca stessa.
2. Prende visione del\i documento\i da firmare digitalmente e di eventuale ulteriore documentazione informativa.
3. Avvia il processo di firma, accettando la sottoscrizione del\i contratto\i mediante l'inserimento del PIN dispositivo.
4. Attende la ricezione sul cellulare del messaggio contenente l'SMS PIN.
5. Conferma *online* l'operazione digitando il codice ricevuto. Il Cliente può procedere alla conferma dell'operazione immediatamente ovvero in un momento successivo (ma comunque entro il termine di validità dell'SMS PIN) accedendo ad un'apposita sezione che conterrà i documenti ancora "*Da confermare*" e inserendo l'SMS PIN ricevuto sul cellulare. È anche possibile confermare l'operazione inoltrando l'SMS ricevuto ad apposito numero, senza cancellare il testo del messaggio originale.
6. A fronte del corretto inserimento dell'SMS PIN viene inviato un SMS a conferma dell'avvenuta operazione.
7. In caso di mancata ricezione del codice SMS PIN, il Cliente può: chiedere un nuovo invio dell'SMS PIN cliccando sul link "*Non hai ricevuto l'SMS?*", presente nell'area in cui è richiesto l'inserimento del codice. Sono consentite 3 richieste di nuovo invio.
8. In alternativa all'utilizzo del *PIN dispositivo + SMS Pin*, il Cliente potrà utilizzare il *Mobile Code*, qualora sia stato preventivamente attivato (par. *F.3*), oppure *Password Vocale + PIN Dispositivo* (par. *F.4*).
   NOTA: la Banca si riserva la piena facoltà di decidere, tempo per tempo, la modalità di autenticazione connessa alla richiesta del Certificato Qualificato di firma digitale, anche in virtù dell'evoluzione delle normative di riferimento.
9. Una volta trascorso il tempo prefissato senza che il sistema abbia ricevuto una conferma come indicato al punto 5, l'operazione viene considerata nulla e conclusa senza la sottoscrizione del\i documento\i.

J. Modalità operative per la verifica della firma

I documenti sottoscritti con le modalità indicate in precedenza saranno esclusivamente in formato *PDF* (*firma elettronica PDF*, DECISIONE (UE) 2015/1506, art. 1) e, pertanto, potranno essere verificati utilizzando il software *Adobe Acrobat Reader DC*, scaricabile gratuitamente dal sito *www.adobe.com*.

K. Modalità di revoca e sospensione dei certificati

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

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

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

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

K.1. Revoca dei certificati

Un Certificato Qualificato di firma digitale 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 del proprio Certificato Qualificato di firma accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca oppure mettendosi in contatto diretto con il Servizio Clienti della Banca.

Il QTSP, avvertito dalla Banca, provvederà alla immediata revoca del certificato.

K.1.2. Revoca su richiesta del Terzo Interessato

La Banca in qualità di Terzo Interessato può richiedere la revoca del certificato.

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso.

K.1.3. Revoca su iniziativa del QTSP

Il QTSP, salvo i casi di motivata urgenza, potrà revocare un Certificato Qualificato di firma, dandone preventiva comunicazione al Titolare all'indirizzo di posta elettronica (eventualmente PEC) comunicato in fase di registrazione, specificando i motivi della revoca e data e ora a partire dalle quali tale revoca sarà efficace.

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

K.1.4. Revoca dei certificati relativi alle chiavi di certificazione

Nei casi di:

- compromissione della chiave di certificazione,
- guasto del dispositivo di firma (HSM),
- cessazione dell'attività,

il QTSP procederà con la revoca dei certificati di certificazione (par. *H.1*) e dei certificati di sottoscrizione firmati con la chiave di certificazione relativa.

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

K.2. Sospensione dei certificati

Circa le modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al 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.

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli artt. 23, 24 e 25 (QTSP, 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 oppure mettendosi in contatto diretto con il Servizio Clienti della Banca.

Il QTSP avvertito dalla Banca provvederà alla immediata sospensione del certificato.

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

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione.

K.2.2. Sospensione su richiesta del Terzo Interessato

La Banca in qualità di Terzo Interessato potrà richiedere la sospensione del certificato.

Il QTSP, accertata la correttezza della richiesta, sospenderà immediatamente il certificato e darà notizia della sospensione ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso.

K.2.3. Sospensione su iniziativa del QTSP

Il QTSP salvo i casi di motivata urgenza potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo di posta certificata comunicato in fase di registrazione specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

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

L. Modalità di sostituzione delle chiavi

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

Per i servizi oggetto di questo manuale, i certificati digitali emessi dal QTSP INTESA hanno una validità di 12 (dodici) mesi dalla data di emissione.

Tali certificati verranno tacitamente rinnovati per altri due anni.

Al termine dei tre anni si renderà invece necessaria una procedura del tutto simile a quella seguita per l'emissione di un nuovo certificato (primo rilascio).

L.1. Sostituzione delle chiavi del QTSP

L.1.1. Sostituzione in emergenza delle chiavi di certificazione

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

L.1.2. Sostituzione pianificata delle chiavi di certificazione

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

L.1.3. Chiavi del sistema di validazione temporale (TSA)

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

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

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

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

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

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

M.2. Accesso logico al Registro dei certificati

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

L'accesso è possibile all'indirizzo ***ldap://x500.e-trustcom.intesa.it*** secondo il protocollo LDAP.

Il QTSP INTESA consente l'accesso alle CRL anche via Internet 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 presenti almeno nel numero ritenuto adeguato 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 tecniche e organizzative sono adeguate e garantiscono che il trattamento dei dati personali sia effettuato in conformità alla Normativa Privacy.

O. .Procedura di gestione della copie di sicurezza

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

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *L.1*.

- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e 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 TSP (DPCM, art. 36).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (DPCM, art. 49 comma 1).
- 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 (DPCM, art. 52).

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

P. Procedura di gestione degli eventi catastrofici

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

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

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

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

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

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

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

Tutte le macchine del QTSP INTESA sono sincronizzate al riferimento temporale fornito dall'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata mediante il protocollo *NTP* (*Network Time Protocol*). L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi, a loro volta, sono sincronizzati alla scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

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

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

Q.1. Modalità di richiesta e verifica marche temporali

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

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

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

R.1. Lead Time di processo

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 (acting as) Local RA*	*Emette ordine di pubblicazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Certificazione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Revoca del Certificato vs. RA o LRA*	*INTESA (acting as) Registration Authority (RA) o Banca (acting as) LRA*	*Emette ordine di revoca del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Revoca*
Utente, Richiedente, Titolare Certificato	*Richiesta di Sospensione del Certificato vs. RA o LRA*	*INTESA (acting as) Registration Authority (RA) o Banca (acting as) LRA*	*Emette ordine di sospensione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Sospensione*
Utente, Richiedente, Titolare Certificato	*Richiesta di Riattivazione del Certificato vs. RA o LRA*	*INTESA (acting as) Registration Authority (RA) o Banca (acting as) LRA*	*Emette ordine di riattivazione del Certificato vs CA previa verifica identità*	*Certification Authority*	*Evasione Richiesta di Riattivazione*

R.2. Tabella RACI

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

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

S. Riferimenti Tecnici

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

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