BPCE
EQUIPMENT SOLUTIONS

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 offerti da BPCE Equipment Finance Italia S.p.A.

Codice documento: MO_BPCE-EFI

OID: 1.3.76.21.1.50.11

Redazione: Antonio Raia

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

Data emissione: 19/06/2025

Versione: 02

Intesa

Revisioni

Versione n°: 02	***Data Revisione: 19/06/2025***
Descrizione modifiche:	Aggiornamenti per cambio ragione sociale LRA Aggiornamento Codice Documento Aggiornamenti e correzione refusi Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti normativi e tecnici Par. *F.3*: aggiornamento Par. *Q*: aggiornamento
Motivazioni:	Variazione Ragione Sociale LRA Aggiornamenti normativi e descrittivi
Versione n°: 01	***Data Revisione: 23/03/2020***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

Riferimenti Normativi & Acronimi

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* oppure *Decreto.*
Regolamento (UE)N. 910/2014 (eIDAS)	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.*
DLGS 196/03 e ss.mm.ii.	Decreto Legislativo n.196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali*". (G.U. n.174 del 29 luglio 2003, suppl. ord.). Nel seguito indicato anche solo come *DLGS 196/03*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation	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* ovvero *LLGG*
REGOLAMENTO (UE) 2024/1183	REGOLAMENTO (UE) 2024/1183 DEL PARLAMENTO EUROPEO E DEL CONSIGLIO dell'11 aprile 2024 che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale.

Definizioni e acronimi

Sono qui di seguito riportati i significati di acronimi e di termini specifici, fatti salvi quelli di uso comune.

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)
CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un QTSP (Certificatore) nell'emettere e gestire certificati e validazioni temporali.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal QTSP (Certificatore) che li ha emessi.
Doc. Informatico	Documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Doc. Analogico	Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA - Firma elettronica Avanzata	Firma elettronica Avanzata – ex art.26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	*Firma Elettronica Qualificata*: 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 propria responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
Firma automatica	Particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo.
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*.
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PKI *Public Key Infrastructure*	Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA *Certification Authority*	*Autorità di Certificazione*: entità della PKI che rilascia i certificati.
RA - Registration Authority *LRA – Local RA*	*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. *Local Registration Autority (LRA)*: il QTSP INTESA può demandare lo svolgimento di alcune funzioni del proprio Ufficio di RA ad entità esterne (Local RA) tramite opportuno contratto di mandato. In tale contratto, sottoscritto da entrambe le parti, saranno definite le attività in carico alla LRA esterne e riportati gli obblighi delle parti.
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
Terzo interessato (subscriber)	Il Terzo Interessato è la Persona Giuridica che richiede o autorizza l'emissione del certificato qualificato. Ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato. (ETSI 319 401-1: "*subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations*").

Richiedente *Richiesta di certificazione*	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione (cioè di emissione di un certificato qualificato).
Titolare *(subject)*	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. (ETSI 319 411-1: "*subject: entity identified in a certificate as the holder of the private key associated with the public key given in the Certificate*")
TSA – Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
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
BCPE	*BPCE Equipment Finance Italia S.p.A.* (già SG Leasing S.p.A.)

A. *Introduzione*

Il presente documento è il Manuale Operativo per le procedure di firma elettronica qualificata remota nell'ambito dei servizi offerti da *BPCE Equipment Finance Italia S.p.A.* – Codice Fiscale e Numero di iscrizione al Registro delle Imprese di Milano n. 06422900156 – R.E.A. di Milano al n. 1096118, Partita I.V.A. n. 06422900156 - iscritta all'Albo degli Intermediari Finanziari ex art.106 T.U.B. (c.d. "Albo Unico") al n. 31. Sede Legale: via Gattamelata 34, 20149 Milano. Nel seguito: anche solo BPCE.

Il contenuto di questo documento 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* (di seguito, anche solo *Reg. eIDAS*).

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

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

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dalla stessa BPCE anche per il tramite della propria rete distributiva, che, in virtù di specifico accordo con il QTSP INTESA, sono autorizzate a svolgere la funzione di Registration Authority.

Si sottolinea pertanto che tutti i processi di sottoscrizione di documenti oggetto del presente Manuale Operativo saranno implementati esclusivamente all'interno della applicazione di titolarità di BPCE.

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 INTESA è coperto da diritti sulla proprietà intellettuale.

A.2. Validità

Quanto descritto in questo documento si applica ad INTESA, alle relative infrastrutture logistiche e tecniche, nonché al 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 da INTESA, e BPCE nella sua qualità di LRA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'art.5 del DPCM, che, al comma 4, distingue le chiavi e i correlati servizi 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;
d) chiavi dedicate alla sottoscrizione delle informazioni sullo stato di validità dei certificati (OCSP);
e) chiavi destinate alla sottoscrizione del separato certificato di attributo.

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 di 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 costituisce la versione n. ***02***, 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 BPCE Equipment Finance Italia S.p.A.***

L'*object identifier* di questo documento è ***1.3.76.21.1.50.11***.

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

- all'indirizzo Internet del QTSP, *www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*
- nell'ambito del sito istituzionale di BPCE, *www.equipmentsolutions.groupebpce.com*

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 (Certificatore Accreditato)

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*
Sito Internet	*www.intesa.it*
Indirizzo di posta elettronica	*intesa@pec.trustedmail.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21*

B.3. Responsabilità del Manuale Operativo

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

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

un recapito di posta elettronica	*uff_RA@intesa.it*
un servizio di Help Desk	*www.hda.intesa.it*
per le chiamate dall'Italia	*800.80.50.93*
per le chiamate dall'estero	*+39 02.39.30.90.66*

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP 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 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).

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 di 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 LRA a BPCE Equipment Finance Italia S.p.A.

BPCE si impegna a svolgere le seguenti attività:

- Identificazione del Titolare;
- Registrazione del Titolare.

BPCE, nell'esercizio della funzione di LRA, dovrà vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente e di quanto previsto nel presente Manuale Operativo

In particolare, nel rispetto delle disposizioni previste dal D.Lgs. 231/2007 ss.mm.ii e dal Provvedimento della Banca di Italia in materia di adeguata verifica della clientela, BPCE potrà identificare il Titolare in assenza della presenza fisica dello stesso mediante tecniche di identificazione a distanza, secondo quanto previsto dalla normativa antiriciclaggio tempo per tempo applicabile.

In ogni caso, BPCE si impegna a conformare le suddette tecniche di identificazione altresì alle previsioni del CAD e del Reg. eIDAS e ad eventuali aggiornamenti di tale normativa, concordando con INTESA le modifiche operative da attuare.

Fatti salvi eventuali periodi transitori di adeguamento normativamente previsti ovvero pattuiti tra INTESA e BPCE, qualora BPCE, al termine dei suddetti periodi, non risulti conforme alle previsioni normative sopra menzionate (CAD e Reg. eIDAS), INTESA si riserva il diritto di interrompere il servizio, previa comunicazione senza indebito ritardo a BPCE.

B.4.3. Altre entità

B.4.3.1. Titolare del certificato qualificato

Persona fisica o giuridica cui è attribuita la firma elettronica, che ha accesso ai dispositivi per la creazione della firma elettronica.

È il soggetto intestatario del certificato.

B.4.3.2. Terzo interessato

Il Terzo Interessato è la persona fisica o giuridica (impresa, associazione di categoria, ente, ecc.) che richiede o autorizza l'emissione del certificato qualificato. Ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato.

B.4.3.3. Utilizzatore (Relying Party)

L'Utilizzatore è colui che, verificando il documento elettronico, utilizza i certificati (e le eventuali marche temporali) emesse dal QTSP INTESA.

C. Obblighi

Nel seguito sono riportati gli obblighi cui devono sottostare i partecipanti alla PKI (par. *B.4 - Entità coinvolte nei processi*).

C.1. Obblighi del QTSP INTESA

Nello svolgimento della sua attività, INTESA opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche (CAD)
- Decreto Presidente del Consiglio dei Ministri 22 febbraio 2013 (DPCM)
- Decreto Legislativo 30 giugno 2003, n.196, e successive modificazioni, recante codice in materia di protezione dei dati personali
- Regolamento (UE) 2016/679 - GDPR (RGPD - Regolamento Generale sulla Protezione dei Dati)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il QTSP INTESA:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM e sue ss.mm.ii.;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione di firme e/o sigilli (HSM) abbia i requisiti di sicurezza previsti del Reg. eIDAS (artt. 29 e 39);
- identifica con certezza il richiedente la certificazione (futuro Titolare del certificato);
- 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;
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni, in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza del QTSP) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;

- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione;

Inoltre, il QTSP:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati ai sensi dell'art.42 del DPCM;
- 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.

C.2. Obblighi del Titolare

Il Titolare al quale è stato attribuito un certificato qualificato per i servizi per i servizi fiduciari del QTSP INTESA descritti nel presente Manuale Operativo è un Firmatario che intende sottoscrivere, in nome e per conto proprio o del Cliente, un contratto con BPCE, che opera da LRA.

Il Titolare, con il certificato qualificato per la Firma Elettronica Qualificata Remota, può sottoscrivere contratti e documenti unicamente relativi a prodotti e/o servizi offerti da BPCE Equipment Finance Italia S.p.A.

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 di firma 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 INTESA, anche per tramite della LRA, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (art.5, comma 5, del DPCM);
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente Manuale Operativo;
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma.

C.3. Obblighi degli utilizzatori dei certificati

L'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 BPCE.

Pertanto, BPCE, nella veste di Terzo Interessato:

- verifica che il Firmatario sia in possesso di tutti i requisiti necessari e autorizza il medesimo a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota.
- svolge un'attività di supporto al Titolare nell'ambito dei normali servizi di assistenza cliente all'impiego degli strumenti forniti;
- indica al QTSP INTESA eventuali ulteriori limitazioni d'utilizzo del Certificato Qualificato per la Firma Digitale oltre a quelle previste al par. *F.1.2*.

BPCE, come Terzo Interessato, quindi, potrà indicare a INTESA 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 dovrà essere immediatamente comunicata al QTSP 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

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

Ai sensi del presente Manuale Operativo, il QTSP INTESA demanda lo svolgimento della funzione di Local Registration Authority a BPCE Equipment Finance Italia S.p.A. mediante specifico *Contratto di Mandato*, sottoscritto da entrambe le parti.

In particolare, BPCE, nella sua qualità di LRA, è tenuta ad espletare le seguenti attività:

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

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere BPCE e sui quali INTESA 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);
- 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.

Il servizio di identificazione ai sensi del CAD potrà essere svolto dal personale di BPCE e/o della sua rete distributiva.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

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, come descritto al par. *C.1. Obblighi del QTSP INTESA*.

Il 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.

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*.

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.

D.2. Responsabilità finanziaria - copertura assicurativa

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

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

E. Tariffe

Il Servizio viene fornito da BPCE ai propri Clienti e le tariffe per l'emissione, rinnovo, revoca e sospensione del certificato qualificato saranno indicate nei contratti stipulati tra il Cliente e BPCE.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

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

La suddetta operazione viene demandata a BPCE che, in qualità di LRA, identificherà il Titolare e ne registrerà i dati (par. *C.5*).

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 ad INTESA, per il tramite di BPCE, 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 (se diverso dalla residenza);
- 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.

La LRA, in ottemperanza con quanto previsto dalla vigente normativa, svolge tutte le operazioni necessarie all'identificazione e registrazione del richiedente.

F.2. Accesso e Firma

Ai fini del rilascio del certificato qualificato di firma digitale e per l'apposizione della stessa, BPCE fornisce ai propri clienti l'accesso al sito di firma digitale.

Il link per la registrazione al suddetto sito di firma digitale viene fornito da BPCE, e nel sito stesso il Titolare può impostare la Password necessaria per accedere alla propria area riservata. Per l'accesso al sito, viene inviato un OTP SMS come elemento rafforzativo per garantire un accesso sicuro al servizio di firma remota fornito da BPCE.

Successivamente all'autenticazione al sito firma digitale, all'atto della firma digitale del contratto, ovvero di altra documentazione con BPCE, il Firmatario riceverà, al numero di cellulare indicato, un SMS OTP "usa e getta" necessario per il rilascio del certificato qualificato, in maniera contestuale alle operazioni di firma della documentazione contrattuale.

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.

Inoltre, collegandosi al portale di firma digitale di BPCE preventivamente alla richiesta di rilascio di un certificato qualificato, il Titolare dovrà:

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

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

Si precisa che il QTSP INTESA, in ottemperanza con il CAD (art.35, comma 5), prevede esclusivamente l'impiego di dispositivi di autenticazione che abbiano ottenuto una valutazione positiva da parte di AgID.

F.3. Identificazione da remoto (web ID)

Il servizio di identificazione a distanza (WEB ID) è gestito direttamente da INTESA e prevalentemente applicabile alle figure dei garanti del Cliente.

Requisito necessario è la disponibilità di utilizzare un device (PC, tablet, smartphone) con una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante.

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 INTESA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.

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.

Più in dettaglio:

- Il Richiedente:

- si connette al sito dedicato di BPCE, dove sono riportate tutte le istruzioni necessarie per eseguire la procedura di riconoscimento e dove sono indicati i documenti necessari per l'identificazione;
- compila, sul sito di BPCE, una richiesta di certificato digitale compilando un *form* in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione;
- prende visione del presente *Manuale Operativo*, che dovrà essere aperto in lettura. Lo stesso Manuale Operativo sarà anche disponibile al *download* dal sito stesso;
- autorizza il consenso al trattamento dei dati personali;
- esegue, tramite l'apposita funzione del sito, l'upload della copia scansionata 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 QTSP INTESA;
- decide, eseguiti gli step precedenti, se continuare la sessione attivando appena possibile il collegamento via webcam oppure se continuare fissando un successivo appuntamento con gli operatori di RA, per completare in un momento successivo a lui più comodo la procedura.

- L'operatore di RA:

- esegue controlli sui documenti ricevuti;
- laddove il processo di preregistrazione lo preveda nei passaggi precedenti alla sessione on-line, nel corso della sessione stessa, (via webcam), l'operatore domanda al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi. Laddove invece il processo di preregistrazione non preveda l'invio preliminare dei documenti, gli stessi vengono acquisiti durate la sessione di videoriconoscimento e l'operatore verifica che i documenti presentati dal Richiedente siano autentici, validi e che nella foto sia chiaramente riconoscibile il Richiedente.

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 di utilizzare il certificato qualificato che sta per essergli emesso e di firmare digitalmente.

La documentazione precedentemente citata, relativa alla registrazione dei Titolari, viene conservata dal QTSP INTESA per 20 (venti) anni dalla scadenza del certificato. Al termine del processo, il certificato digitale viene emesso dalla Certification Authority e al Titolare viene associato un identificativo univoco presso il Certificatore.

F.4. Registrazione degli utenti richiedenti la certificazione

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi del QTSP INTESA.

Questa operazione potrà essere eseguita mediante un'applicazione software direttamente richiamabile dagli applicativi di BPCE.

F.5. Limiti d'uso

Nel Certificato Qualificato per la firma digitale remota, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti da BPCE, è inserito il seguente limite d'uso:

L'utilizzo del certificato è limitato ai rapporti con BPCE Equipment Finance Italia S.P.A.

This certificate may only be used in dealings with BPCE Equipment Finance Italia S.P.A.

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

Il QTSP 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.

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

G.1. Generazione delle chiavi di certificazione

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

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e i certificati 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 del Certificatore sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto attraverso le chiavi contenute in tali dispositivi di autorizzazione di cui sopra. Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "*n di m*", in modo che solo la concomitante presenza di almeno *n* di *m* parti della chiave permettano di operare con gli opportuni privilegi. Pertanto, esse vengono custodite in apposite casseforti distinte.

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

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

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

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

G.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del 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 secondo quanto descritto al par. *H.2. Procedura di emissione dei Certificati di sottoscrizione*.

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 (*QSCD – Qualified Signature Creation Device*).

La lunghezza delle chiavi di sottoscrizione 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 QTSP 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

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 *PKCS10*, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Quindi, generate le chiavi, la richiesta di certificato sarà immediatamente inviata dall'applicazione di BPCE alla Certification Authority di INTESA.

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

H.2.1. 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 Operativo contengono una limitazione d'uso (par. *F.5 Limiti d'uso*).

H.2.2. Codice di Emergenza

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

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

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i servizi di BPCE, 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 accedendo all'area riservata sul sito di BPCE. 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.

I.1. Processo di Firma Remota

A seguito dell'avvenuto riconoscimento, e dopo essere entrato in possesso del proprio certificato qualificato, il Titolare potrà sottoscrivere un documento nei seguenti passi:

1. Connettendosi all'applicazione attraverso i suoi codici personali per l'accesso alla stessa;
2. Selezionando e verificando il documento da firmare;
3. Inserendo un OTP (One Time Password) SMS da inserire successivamente al PIN a conferma dell'operazione di firma

Il sistema, rilevando la correttezza dell'OTP mobile appena inserito, 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 per ogni documento deve reiterare i passi sopra indicati.

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. L'URL della lista CRL è indicato sul certificato, nel campo *CDP - CRL Distribution Point*.

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

In fase di richiesta, dovranno essere specificate la data e l'ora a partire dalle quali il certificato risulterà dovrà risultare revocato o sospeso (art.24, comma 1, DPCM).

K.1. Revoca dei certificati

Un certificato può essere revocato su richiesta del Titolare, del Terzo Interessato o del QTSP INTESA.

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 di BPCE.

INTESA, avvertita da BPCE, 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

BPCE, in qualità di Terzo Interessato, può richiedere la revoca del certificato.

INTESA, 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 ad INTESA, anche per mezzo delle LRA (par. *C.2. Obblighi del Titolare*).

K.1.3. Revoca su iniziativa del QTSP

Il Certificatore Accreditato che intende revocare il Certificato Qualificato, salvo casi di motivata urgenza, ne dà preventiva comunicazione via e-mail o PEC a BPCE 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 QTSP 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 QTSP 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 **solamente** nel caso in cui si debba fare un supplemento di indagine per verificare se il certificato impattato debba essere revocato o no (ad esempio nei casi in cui si tema la compromissione della chiave privata o lo smarrimento / furto del Token OTP, oppure si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.). **Ogni altro motivo per l'utilizzo della sospensione è *deprecato***.

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

In caso di revoca di un certificato sospeso, 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 di BPCE oppure mettendosi in contatto diretto con il Servizio Clienti di BPCE.

Il QTSP procede alla sospensione che verrà comunicata al Titolare utilizzando specifiche funzioni rese disponibili all'interno dei servizi di BPCE.

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

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

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

K.2.3. Sospensione su iniziativa del QTSP

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.

L.2. Sostituzione delle chiavi del QTSP

L.2.1. Sostituzione in emergenza delle chiavi di certificazione

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

L.2.2. Sostituzione pianificata delle chiavi di certificazione

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

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

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

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

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

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

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

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

M.2. Accesso logico al Registro dei certificati

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

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

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

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

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

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

N. Modalità di protezione dei dati personali

Le misure di sicurezza per la protezione dei dati personali sono conformi a quanto previsto 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 di INTESA (art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (art.52 del DPCM).

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

P. Procedura di gestione degli eventi catastrofici

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

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

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

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

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

Tutte le macchine del QTSP INTESA sono sincronizzate con servizi di riferimento temporale dislocati su varie parti del pianeta, compreso il servizio 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*). 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.

Le validazioni temporali apposte 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.

Il formato della validazione temporale è conforme con quanto richiesto dal Regolamento eIDAS e, nello specifico, con la *ETSI-319.422*

Q.1. Controllo del sincronismo con l'ora campione

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).

In caso di blocco, una segnalazione è inviata al personale addetto, al fine di verificarne le cause e intervenire di conseguenza.

Q.2. 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*	*BPCE (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 BPCE (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 BPCE (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 BPCE (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 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 - 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 - 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 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 - 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 - 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 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles

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