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 dedicati alle imprese da Banco BPM S.p.A.

Codice documento: MO_BP-IMP

OID: 1.3.76.21.1.3.1.181

Redazione: Antonio Raia

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

Data emissione: 10/01/2023

Versione: 05

Firmato da:
Antonio Raia
Organizzazione: IN.TE.S.A. - INIZIATIVE TELEMATICHE PER I SERVIZI APPLICATIVI S.P.A./05262890014

Revisioni

Versione n°: 05	***Data Revisione: 10/01/2023***
Descrizione modifiche:	Aggiornamento Titolo Aggiornamento OID Introduzione utilizzo firma per mezzo dell'uso dell'App per il Mobile Banking Aggiunta sezione autenticazione biometrica Variazione dati societari e logo Aggiornamento riferimenti tecnici Aggiornamento definizioni e riferimenti normativi
Motivazioni:	Aggiornamenti normativi e descrittivi Spin-off dal Manuale Banco BPM ver. 04
Versione n°: 04	***Data Revisione: 01/06/2017***
Descrizione modifiche:	Variazione dati societari e logo Aggiornamento definizioni e riferimenti normativi Inserimento processo par.G.2.
Motivazioni:	Aggiornamenti normativi: Regolamento (UE) 910/2014 (eIDAS), D.Lgs.179/2016 Variazioni organizzative Certificatore Variazioni operative
Versione n°: 03	***Data Revisione: 03/04/2015***
Descrizione modifiche:	Estensione della firma digitale remota ai prodotti telematici per le aziende
Motivazioni:	Aggiornamento
Versione n°: 02	***Data Revisione: 13/01/2015***
Descrizione modifiche:	Aggiornamento riferimenti al DPCM 22 febbraio 2013 Aggiornamento Limitazione d'uso
Motivazioni:	Aggiornamento
Versione n°: 01	***Data Revisione: 20/09/2013***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

A. Introduzione

A.1. Proprietà intellettuale

Il presente documento è il Manuale Operativo per la procedura di firma digitale remota del Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A. nell'ambito dei servizi forniti da *Banco BPM S.p.A. Capogruppo del Gruppo Bancario BANCO BPM - Sede Legale: Piazza F. Meda, 4 - 20121 Milano Tel. 02/77001 Sede Amministrativa: Piazza Nogara, 2 - 37121 Verona - Tel. 045/8675111 www.bancobpm.it Capitale Sociale al 7.4.2022: euro 7.100.000.000 int. vers. - ABI 05034 - Codice Fiscale e Iscrizione al Registro delle Imprese di Milano n. 09722490969 - Rappresentante del Gruppo IVA Banco BPM Partita IVA 10537050964 - Aderente al Fondo Interbancario di Tutela dei Depositi e al Fondo Nazionale di Garanzia - Iscritto all'Albo delle Banche della Banca d'Italia e all'Albo dei Gruppi Bancari - Imposta di bollo assolta in* modo *virtuale, ove dovuta, Aut. Ag. delle Entrate Ufficio di Milano 5 - n. 3358 del 10/01/2017.*

Il Manuale Operativo descrive le procedure e le relative regole attuate dal Prestatore di Servizi Fiduciari Qualificati In.Te.S.A. S.p.A. (di seguito anche solo *QTSP INTESA, QTSP* o *Certificatore*) per l'emissione dei Certificati Qualificati, ai sensi del Reg. UE 910/2014, nella generazione e verifica della firma elettronica qualificata del Cliente ***Banco BPM S.p.A.*** (di seguito anche solo *Banco BPM* o *Banca*) nell'ambito dei servizi dallo stesso offerti alla propria clientela.

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, *DPCM*)e dal D. lgs 7 marzo 2005, n. 82, recante il "*Codice dell'Amministrazione Digitale*" come successivamente modificato e integrato (nel seguito, *CAD*) e conforme al Reg. UE 910/2014 (nel seguito, *Reg. eIDAS*); in particolare:

- CAD - capo II, Sez. II, che disciplina le firme elettroniche e i certificatori,
- CAD - capo VII, che prevede le modalità con le quali vengono dettate le regole tecniche previste dal Codice.

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

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS).

A.2. Validità

Quanto descritto in questo documento si applica al QTSP, 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 cui sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali emesse dal QTSP 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 del sopracitato decreto, le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

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

A.3. 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*.
DETERMINAZIONE AgID 121/2019	Determinazione 121/2019 e s.m.i. *"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.*
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)	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*
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)
PSD2	Direttiva (UE) 2015/2366 del Parlamento Europeo e del Consiglio del 25 novembre 2015 relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE
RD SCA RTS	Regolamento Delegato (UE) 2018/389 della Commissione del 27 novembre 2017 che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri.
LLGG AgID 2021	Linee Guida AgID sulla formazione, gestione e conservazione dei documenti informatici, maggio 2021

A.4. 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*.
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).
QTSP	Qualified Trust Service Provider – Prestatore di Servizi Fiduciari Qualificati. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*. Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta servizi fiduciari qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime
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).

Chiave Privata	L'elemento della coppia di chiavi asimmetriche, utilizzato dal Titolare, mediante il quale si appone la firma digitale sul documento informatico.
Chiave Pubblica	L'elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale sul documento informatico.
CRL	Lista dei Certificati Revocati, Certificate Revocation List, un elenco che riporta i certificati revocati o sospesi, non più considerati validi dal Certificatore che li ha emessi.
OCSP	Online Certificate Status Protocol: servizio di verifica dello stato di validità del Certificato, secondo il protocollo OCSP.
Documento informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s).
Firma Remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
HSM	Hardware Security Module, dispositivi per la creazione della firma digitale dedicati alla sicurezza crittografica e alla gestione delle chiavi, in grado di garantire un elevato livello di protezione.
Marca Temporale	Validazione Temporale Elettronica Qualificata: il Riferimento Temporale che consente la validazione temporale.
Registration Authority	Autorità di Registrazione: lo stesso Banco BPM che, su incarico del QTSP, ha la responsabilità di registrare o verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al QTSP per emettere il Certificato Qualificato. La Registration Authority assume automaticamente il ruolo di Cointeressato e Cofirmatario nel caso in cui adotti la procedura di firma in ambiti chiusi di utenti.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal QTSP, contenente tutti i Certificati emessi.
Richiedente	Il Cliente di Banco BPM o altro soggetto che può non essere cliente della Banca, ma comunque riconosciuto con i medesimi criteri., che richiede il Certificato.
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
SCA	Strong Customer Authentication ai sensi del RD SCA RTS
Titolare	Il Cliente del Banco BPM, o soggetto autorizzato, cui il certificato digitale è rilasciato e che è autorizzato ad usarlo al fine di apporre la firma digitale.
TSA	Time Stamping Authority, autorità che rilascia le marche temporali.

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle 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 al QTSP INTESA di essere inserita nell'elenco dei Prestatori di Servizi Fiduciari Qualificati (QTSP).

Pertanto, in funzione delle normative menzionate, vengono coinvolte 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. ***05*** del *Manuale Operativo del Prestatore di Servizi Fiduciari Qualificato (QTSP) In.Te.S.A. S.p.A. per le procedure di firma remota nell'ambito dei servizi dedicati alle imprese da Banco BPM* (prima denominato "*Manuale Operativo del Certificatore Accreditato In.Te.S.A. per le procedure di firma remota nell'ambito dei servizi del Banco BPM*"), rilasciata in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.3.1.181***.

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

- all'indirizzo Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*
- nell'ambito del sito commerciale della Banca, *www.bancobpm.it* (all'interno dell'area riservata di ciascun cliente).

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

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

Il QTSP (*Prestatore di Servizi Fiduciari Qualificato*), ai sensi del Reg. eIDAS, è la società In.Te.S.A. S.p.A., di cui di seguito sono riportati i dati identificativi.

Denominazione sociale	*In.Te.S.A. S.p.A.*
Indirizzo della sede legale	*Strada Pianezza, 289 - 10151 Torino*
Legale Rappresentante	*Amministratore Delegato*
Registro delle Imprese di Torino	*N. Iscrizione 1692/87*
N. di Partita I.V.A.	*05262890014*
N. di telefono (centralino)	*+39.011.19216.111*
Sito Internet	*www.intesa.it*
Indirizzo di posta elettronica certificata (PEC)	*INTESA@pec.trustedmail.intesa.it*
ISO Object Identifier (OID)	*1.3.76.21*

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

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

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

B.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.

Nel caso fosse necessario procedere con l'aggiornamento e ogni eventuale revisione del presente documento, il QTSP lo comunicherà senza ritardo a Banco BPM e in accordo con essa procederà alle modifiche.

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

- un recapito di posta elettronica: *uff_RA@intesa.it*
- un recapito telefonico: *+39.011.19216.111*
- un servizio di Help Desk: *www.hda.intesa.it*

per le chiamate dall'Italia	800.80.50.93
per le chiamate dall'estero	+39 02.39.30.90.66

B.4. Entità coinvolte nei processi

All'interno della struttura del QTSP sono 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)

Il QTSP INTESA, operando in ottemperanza con quanto previsto dal DPCM, dal CAD e dal Reg. eIDAS, espleta le attività di Prestatore di Servizi Fiduciari Qualificato (Qualified Trust Service Provider). Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per la firma digitale remota.

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

B.4.2. Local Registration Authority (LRA)

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 Registration Authority a Banco BPM. In particolare, la Banca svolge le seguenti attività:

- Identificazione del Titolare.
- Registrazione del Titolare.

La Banca, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente e di quanto previsto nel presente Manuale Operativo.

B.4.3. Terzo Interessato

Nell'ambito del presente manuale, la Banca riveste il ruolo di Terzo interessato, in qualità di committente del servizio del QTSP INTESA per i propri clienti.

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

Gli obblighi del Terzo Interessato sono riportati al par. ***Errore. L'origine riferimento non è stata trovata.***.

C. Obblighi

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

Nello svolgimento della sua attività il Prestatore di Servizi Fiduciari Qualificato (QTSP) opera in conformità con quanto disposto dal:

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche.
- Decreto Presidente del Consiglio dei Ministri 22 Febbraio 2013.
- Regolamento (UE) 2016/679 (GDPR)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il Prestatore di Servizi Fiduciari Qualificato (QTSP):

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche e i requisiti di sicurezza previsti dall'Art.35 del CAD e all'Art.11 del DPCM;
- 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 compiuto e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;

- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.
- secondo quanto stabilito dall'Art.14 del DPCM, il QTSP fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il QTSP:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati (Art.42 del DPCM);
- garantisce l'interoperabilità del prodotto di verifica, di cui all'art.14 del DPCM, ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative;
- 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 per la specifica finalità della verifica delle firme elettroniche qualificate e digitali (Art.42, comma 3 del DPCM).
- 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 digitale per i servizi descritti nel presente Manuale Operativo è un cliente della Banca che opera da Registration Authority.

In quanto tale, il Titolare potrà ricevere uno o più certificati qualificati per la Firma Digitale Remota per sottoscrivere contratti e documenti relativi a prodotti e /o servizi offerti dalla Banca.

Il Titolare del certificato di firma 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 del certificato 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 digitale secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

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 allo standard ISO 9594-8, e il momento della sua emissione;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e il momento della sua emissione;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori e su eventuali certificati derivanti da accordi di mutua certificazione tra il proprio Certificatore e quelli altrui;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, in base a quanto indicato nel Manuale Operativo del QTSP che ha emesso il certificato di colui che ha sottoscritto il documento informatico.

C.4. Obblighi del Terzo Interessato

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

Pertanto, la Banca deve verificare che il cliente sia in possesso di tutti i requisiti necessari e autorizza il cliente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota.

La Banca, nella sua veste di Terzo Interessato, svolge un'attività di supporto al Titolare; in particolare sarà la Banca ad indicare al QTSP eventuali ulteriori limitazioni d'uso del Certificato Qualificato per la Firma Digitale oltre a quelle previste al par. *F.1.1*.

C.5. Obblighi delle Registration Authority

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

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 Art.8 e 10 comma 2 del DPCM.

Il QTSP INTESA ha rilasciato mandato a svolgere la funzione di Registration Authority a Banco BPM 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 cui il QTSP assegna l'incarico di RA e sui quali il QTSP ha l'obbligo di vigilare; in particolare si richiede di:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente (CAD e successive modificazioni, DPCM e normativa in materia di Antiriciclaggio);
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il GDPR;
- rendere disponibile per il QTSP il materiale raccolto nella fase di identificazione e l'autorizzazione all'uso dei dati personali;
- 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), svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

Il servizio di identificazione potrà essere gestito come segue:

- tramite il personale di filiale della Banca, il Titolare al momento dell'apertura di un rapporto verrà identificato e registrato grazie ai documenti d'identità forniti, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa. Eseguite queste operazioni il Cliente potrà richiedere l'emissione di un certificato di firma qualificata.
- attraverso procedura di riconoscimento a distanza tramite altro intermediario qualora il Titolare fosse diventato cliente della Banca con modalità online.

La documentazione relativa alle attività di cui sopra e necessaria all'emissione del Certificato Qualificato viene conservata dal QTSP INTESA , secondo gli obblighi di legge, per 20 (venti) anni.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

Il QTSP INTESA è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal GDPR, dal CAD e dal Reg. eIDAS . Cfr. par. *C.1 - Obblighi del Prestatore di Servizi Fiduciari Qualificato (QTSP)*.

Il QTSP INTESA, fatti salvi i casi di dolo o colpa (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, il QTSP INTESA non potrà essere ritenuto 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 il QTSP si avvale per la prestazione dei propri servizi di certificazione.

Il QTSP non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al par. *F.1.1*.

D.2. Assicurazione

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

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

E. Tariffe

Il Servizio viene fornito da Banco BPM ai propri Clienti senza oneri e non è pertanto soggetto a tariffazione.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

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

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

Per i successivi rinnovi, se effettuati prima che il certificato qualificato già rilasciato non sia scaduto, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al QTSP 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 e data e luogo del rilascio.

Per l'accesso ai servizi offerti da Banco BPM, la stessa consegna ai propri clienti un Codice Utente e un Personal Identification Number (PIN), ovvero una Password, tramite i quali sarà possibile accedere all'area riservata della Banca al fine di garantire un accesso sicuro ai servizi dispositivi e al servizio di firma remota fornito dalla Banca stessa.

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

Inoltre, il Titolare, nell'ambito dei servizi offerti dalla Banca, potrà utilizzare dei codici numerici (One Time Password, di seguito OTP):

- generati da dispositivi token, resi disponibili dalla Banca, in grado di generare OTP;
- trasmessi tramite SMS dalla Banca sul cellulare predefinito del Titolare, utilizzabili una sola volta.

Sul cellulare predefinito dal Titolare, la Banca potrà inviare degli specifici SMS che possano avvisarlo relativamente alle operazioni eseguite attraverso l'impiego del certificato digitale (firma di un documento, ma anche emissione, revoca o rinnovo del certificato digitale stesso).

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

Solo attraverso l'uso congiunto di PIN/Password e OTP sarà possibile sottoscrivere digitalmente, nell'ambito dei servizi internet offerti dalla Banca, documenti e contratti relativi a prodotti o servizi offerti da Banco BPM.

Il cliente, identificato dalla Banca in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa, potrà attivare la procedura di generazione del Certificato Qualificato per la Firma Digitale all'interno dell'area riservata.

Una volta entrato in questa sezione dovrà, dopo aver preso visione del Manuale Operativo, inserire il PIN/Password.

In pochi secondi riceverà il certificato qualificato, la ricezione sul cellulare di uno specifico SMS gli confermerà l'avvenuta operazione.

Durante questa fase verrà anche generato l'identificativo univoco del Titolare presso il QTSP.

F.1.1. Limiti d'uso

Nel Certificato Qualificato per la Firma Digitale, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti dalla Banca, è inserita il seguente limite d'uso:

> *"Questo certificato e' utilizzabile esclusivamente per la sottoscrizione di documenti, atti e/o contratti relativi a prodotti e servizi prestati o distribuiti da societa' del Gruppo BANCO BPM"*
>
> *"This certificate may be used only to sign documents, deeds and/or contracts*

concerning products and services placed or performed by the companies of the Group BANCO BPM"

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

G. Modalità operative per la sottoscrizione di documenti

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

La particolare tipologia del servizio non richiede che tale 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 Riservata. 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 macro istruzioni 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 Riservata.

G.1. Processo di Firma

Dopo aver richiesto il proprio Certificato digitale il Titolare potrà poi procedere alla firma di un documento secondo le modalità di seguito descritte.

1. Il Titolare del Certificato Qualificato per la Firma Digitale, accedendo all'area Riservata della Banca, ovvero accedendo all'area Riservata tramite la propria App per il Mobile Banking, richiede la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dalla Banca stessa.
2. Il Titolare prende visione del documento da firmare digitalmente e di eventuale ulteriore documentazione informativa
3. Il Titolare avvia il processo di firma accettando la sottoscrizione del contratto mediante l'inserimento del PIN/Password e dell'OTP.
4. La ricezione, su di un cellulare precedentemente registrato per ricevere le comunicazioni dalla Banca, di un opportuno SMS confermerà l'avvenuta sottoscrizione.

Tenuto presente che la Banca si è dotata anche di ulteriori e innovativi strumenti tecnologici per permettere l'operatività bancaria in perfetta aderenza alla normativa PSD2 e, che tali strumenti soddisfano gli elevati standard di sicurezza dettati dalle relative normative in ambito di standard tecnologici adottati tramite Regolamenti Delegati della Commissione Europea (RD SCA RTS), in alternativa all'utilizzo di meccanismi tradizionali, come PIN/Password e OTP, la firma di documenti può avvenire anche tramite l'uso dell'App per il Mobile Banking Banco BPM, sfruttando i meccanismi di strong authentication che la stessa mette a disposizione per autenticare l'utente nell'ambito delle operazioni bancarie.

In tal senso, l'utente che intende firmare all'interno dell'App di Mobile Banking di Banco BPM, in alternativa all'uso di PIN e OTP, potrà utilizzare il sistema di autenticazione biometrico messo a disposizione dall'App stessa.

Qualora i documenti da firmare fossero più di uno, con PDF separati, il Titolare, per ogni documento, può reiterare i passi dal 2 al 3.

In alternativa alla reiterazione degli step di visualizzazione e sblocco della firma, laddove i documenti da sottoscrivere siano più di uno o ci siano diversi punti firma sul medesimo documento, e siano gestibili nell'ambito di una singola sessione di firma, l'utente potrà prendere visione di tutti i documenti da firmare nell'ambito dello step 2 e, all'interno della sessione sopracitata, che non ha interruzioni, e tramite un singolo inserimento delle credenziali di sblocco del certificato di firma (siano queste PIN/Password e OTP oppure autenticazione biometrica PSD2 SCA compliant) potrà apporre la firma su tutti i punti firma di tutti i documenti visionati allo step 2.

H. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF e pertanto potranno essere verificati utilizzando il software Acrobat Reader DC scaricabile gratuitamente dal sito *www.adobe.com*.

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

I.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile di Certificazione, come previsto dal DPCM all'Art.7 ed è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

Il tutto avviene in modalità dual control ad evitare operazioni illecite.

Le operazioni successive alla generazione delle coppie di chiavi di certificazione sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è possibile solamente attraverso la chiave contenuta 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 due 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.

I.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 di validazione temporale è conforme alla normativa tempo per tempo vigente.

I.3. Generazione delle chiavi di sottoscrizione

Completata la fase di registrazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del QTSP, 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 autenticandosi al sistema fornitogli dalla Banca in una delle modalità precedentemente descritte.

Il PIN/Password e l'OTP (generata secondo le modalità precedentemente 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.8 comma 5 lett. d) del DPCM.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è conforme alla normativa tempo per tempo vigente) vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa vigente.

J. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta al par. *I.1*, vengono 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 QTSP genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dal dipartimento (qui e nel seguito per dipartimento s'intende il Dipartimento per l'Innovazione e le Tecnologie della Presidenza del Consiglio dei Ministri) per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il QTSP deve poi mantenere copia della lista, sottoscritta dal dipartimento, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

I.2. Procedura di emissione dei Certificati di sottoscrizione

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

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel par.*I.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 al Certificatore.

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

I.3. Informazioni contenute nei certificati

I certificati del QTSP INTESA, emessi nell'ambito del presente manuale, sono certificati qualificati ai sensi del Regolamento UE 910/2014 (eIDAS) e, pertanto, ne è garantita la loro interoperabilità e riconoscimento a livello comunitario.

Il Certificato Qualificato definisce con certezza il QTSP che lo ha emesso e contiene i dati necessari per la verifica della Firma Digitale.

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;
- 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.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale, contengono almeno il limite d'uso indicato al par. *F.1.1*.

I.4. Codice di Emergenza

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

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

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

La lista CRL è disponibile anche sul registro dei certificati.

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 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 certificato, che potrà essere inoltrata utilizzando i canali di comunicazione definiti con la Banca.

Il Certificatore, 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.

In caso di estinzione del contratto del prodotto telematico che lega il Titolare al Terzo Interessato, quest'ultimo potrà esercitare la richiesta di revoca con le modalità stabilite con il Certificatore.

Il Certificatore, 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 e inserirà il certificato nella lista di revoca, che sarà emessa il prima possibile.

K.1.3. Revoca su iniziativa del Certificatore

Il certificatore che intende revocare il Certificato Qualificato ne dà preventiva comunicazione al Banco BPM (all'indirizzo di posta elettronica certificata), e al Titolare all'indirizzo di corrispondenza o all'indirizzo e-mail indicato in fase di rilascio del Certificato della Firma Digitale, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

Effettuata la revoca, il Certificatore avviserà il Banco BPM, inviando una comunicazione all'indirizzo di Posta Elettronica Certificata.

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

Nei casi di:

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

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

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

K.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al 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. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

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

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

K.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione del certificato, che potrà essere inoltrata utilizzando i canali di comunicazione definiti con la Banca

Il Certificatore, avvertito dalla Banca, provvederà alla immediata sospensione del certificato.

Successivamente il Titolare 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 Certificatore, accertata la correttezza della richiesta, sospenderà immediatamente il certificato e ne 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 Certificatore

Il Certificatore 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 Certificatore anche al Terzo Interessato.

L. Modalità di sostituzione delle chiavi

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

I certificati digitali emessi dal Certificatore hanno validità di 36 (trentasei) mesi dalla data di emissione.

Al termine dei tre anni si renderà invece necessaria non solo l'emissione di un nuovo certificato ma anche la sostituzione delle chiavi precedentemente utilizzate dal Titolare.

In questo caso la procedura seguita per l'emissione di un nuovo certificato sarà del tutto simile a quella indicata in fase di primo rilascio.

L.2. Sostituzione delle chiavi del Certificatore

L.2.1. Sostituzione in emergenza delle chiavi di certificazione

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

L.2.2. Sostituzione pianificata delle chiavi di certificazione

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

L.2.3. Sostituzione pianificata delle chiavi del sistema di validazione temporale

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, il QTSP INTESA pubblica:

- I certificati delle chiavi di certificazione e del sistema di validazione temporale.
- 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.

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.

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

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

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

N. Modalità di protezione dei dati personali

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

O. Procedura di gestione delle copie di sicurezza

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

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. ***Errore. L'origine riferimento non è stata trovata.***.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonché le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del QTSP (Art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

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

P. Procedura di gestione degli eventi catastrofici

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

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

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

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

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

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

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

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

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

Di seguito si riporta la Tabella relativa al "Lead Time di Processo" per la gestione delle richieste di Emissione, Revoca, Sospensione e Riattivazione dei Certificati.

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

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

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 –