In.Te.S.A. S.p.A.

Qualified Trust Service Provider

Manuale Operativo del QTSP In.Te.S.A. S.p.A.

per le procedure di firma digitale remota nell'ambito dei servizi del Banco BPM S.p.A.

Codice documento: MO_BP

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 17/07/2019

Versione: 05

Firmato da:
ANTONIO RAIA
Organizzazione: IN.TE.S.A. S.p.A./05262890014

VERSIONI

Versione n°: 05		**Data Revisione:**	**17/07/2019**
Descrizione modifiche:	Aggiornamento definizioni e riferimenti normativi Inserimento processi par. G e par. H		
Motivazioni:	Aggiornamenti normativi e descrittivi Nuove modalità di emissione certificati		
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 7.4.2018: 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* 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 del ***Banco BPM S.p.A.*** (di seguito anche solo *Banco BPM*) nell'ambito dei servizi dallo stesso offerti.

Il contenuto di questo Manuale Operativo è conforme a quanto stabilito dalle regole tecniche contenute nel Decreto del Presidente del Consiglio dei Ministri del 22 Febbraio 2013 (di seguito *DPCM*) e dal D. lgs 7 marzo 2005, n. 82, recante il "*Codice dell'Amministrazione Digitale*" come successivamente modificato e integrato (di seguito "*CAD*") 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.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti identificati dallo stesso Banco BPM che, in virtù di specifico accordo con il Certificatore, è autorizzato a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare la procedura di Firma Digitale Remota di documenti, atti, contratti, ordini, relativi a prodotti e servizi prestati o distribuiti da BANCO BPM.

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 INTESA (alle sue infrastrutture logistiche e tecniche nonché al suo personale), ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali qualificate emesse da INTESA, a Banco BPM in qualità di Registration Authority

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 c.4 DPCM 22/06/2013, in cui si dispone che le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;
b) chiavi di certificazione, destinate alla generazione e verifica delle firme apposte ai certificati qualificati, alle informazioni sullo stato di validità del certificato ovvero alla sottoscrizione dei certificati relativi a chiavi di 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 successive modificazioni e integrazioni	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 successive modificazioni e integrazioni	Decreto Legislativo 7 Marzo 2005, n. 82. "*Codice dell'amministrazione Digitale*". Nel seguito indicato anche solo come *CAD*.
DELIBERAZIONE CNIPA n. 45 e successive modificazioni e integrazioni	Deliberazione CNIPA 21 Maggio 2009, n. 45. *"Regole per il riconoscimento e la verifica del documento informatico"*. Nel seguito indicato anche solo come *DELIBERAZIONE*
DPCM 22/02/2013 *Nuove Regole Tecniche* e successive modificazioni e integrazioni	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, ndr).* Nel seguito indicato anche solo come *DPCM*
Regolamento (UE) N. 910/2014 (eIDAS) e successive modificazioni e integrazioni	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)

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
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 servizi qualificati di firma elettronica e di validazione temporale e altri servizi connessi con queste ultime.
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
Firma Digitale	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.

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 Certificatore, ha la responsabilità di registrare o verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al Certificatore per emettere il Certificato Qualificato.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Richiedente	Il Cliente del 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.
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 che disciplinano l'emissione di certificati qualificati da parte del certificatore accreditato 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.**05** del *Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per le procedure di firma remota nell'ambito dei servizi del Banco BPM,* rilasciato in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è **1.3.76.21.1.3.1.180**.

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

- all'indirizzo Internet del QTSP, *http://e-trustcom.intesa.it/DOCS/mo_BancoBPM.pdf*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*
- nell'ambito del sito istituzionale della Banca, *www.bancobpm.it*
- nell'ambito del sito commerciale della Banca, *www.bancobpmspa.com* e *www.webank.it*.

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 Certificatore

Il Certificatore, ai sensi dell'art.29 del CAD, 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**
N. di fax	**+39.011.19216.375**
Indirizzo di posta elettronica	**marketing@intesa.it**
Indirizzo (URL) registro dei certificati	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

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 Certificatore 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 della Certification Authority INTESA, che ne cura la stesura e la pubblicazione.

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

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

un recapito di posta elettronica:	*marketing@intesa.it*
un recapito telefonico:	+39 011.192.16.111
un recapito fax:	+39 011.192.16 375
un servizio di HelpDesk	per le chiamate dall'Italia 800.80.50.93
	per le chiamate dall'estero +39 02.871.193.396

B.4. Entità coinvolte nei processi

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

B.4.1. Certification Authority (Certificatore Accreditato)

INTESA, operando in ottemperanza a quanto previsto dal DPCM e dal CAD, espleta le attività di Certificatore Accreditato. Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per la firma digitale remota.

I dati identificativi del certificatore accreditato INTESA sono riportati al precedente paragrafo B.2.

B.4.2. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (Firma Digitale Remota nell'ambito delle applicazioni del Banco BPM descritte nel presente Manuale Operativo), Intesa in qualità di Certificatore ha demandato lo svolgimento delle funzioni di Registration Authority al Banco BPM tramite apposito atto di mandato.

Banco BPM si impegna a svolgere le seguenti attività:

- Identificazione del Titolare.

- Registrazione del Titolare.

Banco BPM nell'esercizio della funzione di Registration Authority, dovrà vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente.

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

Nello svolgimento della sua attività il Certificatore Accreditato opera in conformità con quanto disposto dal:

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

In particolare, il Certificatore Accreditato:

- 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 esplicito e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (GDPR);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo (di esclusiva pertinenza del Certificatore) 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 Certificatore;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;

- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

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

Inoltre, il Certificatore:

- 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;
- garantisce l'interoperabilità del prodotto di verifica, di cui all'art.10 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 come stabilito dall'Art.42, comma 3 del DPCM.

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo può essere un cliente (con rapporto bancario già aperto) o un cliente prospect di Banco BPM.

In entrambi i casi la Banca opera da Registration Authority.

Il Titolare potrà ricevere uno o più certificati qualificati per la Firma Digitale Remota al fine di sottoscrivere contratti, documenti e ordini relativi a prodotti e/o servizi prestati o distribuiti da Banco BPM.

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al Certificatore, tramite Banco BPM, eventuali variazioni alle informazioni fornite all'atto della registrazione: recapiti telefonici e indirizzo di posta elettronica;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- dare immediata comunicazione al Banco BPM, in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma, Banco BPM 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

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 regolamento 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 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 Certificatore 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 Banco BPM.

Pertanto, Banco BPM, nella sua veste di Terzo Interessato:

- verifica che il Cliente sia in possesso di tutti i requisiti necessari e autorizza il Cliente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota;
- svolge eventuale, attività di supporto al Titolare durante le operazioni di firma;
- indica al Certificatore eventuali ulteriori limitazioni d'utilizzo del Certificato Qualificato per la Firma Digitale oltre a quelle previste al paragrafo F.1.1.

C.5. Obblighi delle Registration Authority esterne

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

Il Certificatore In.Te.S.A. S.p.A. ha demandato lo svolgimento della funzione di Registration Authority al Banco BPM mediante la sottoscrizione, da entrambe le parti, di un Contratto di Mandato.

In particolare, le RA esterne espletano le seguenti attività:

- identificazione con certezza del richiedente la certificazione (in seguito Titolare del certificato);
- registrazione del richiedente / Titolare;
- presentazione della modulistica contrattuale in formato elettronico che il richiedente / Titolare deve sottoscrivere ai fini della formalizzazione della richiesta di certificazione verso il QTSP INTESA (contratto, modulo di richiesta e informativa ai sensi del GDPR);
- richiesta al Titolare di fornire codici che gli permetteranno di accedere alla propria chiave di firma nel rispetto degli Art.8 e 10 comma 2 del DPCM;
- invio della documentazione sottoscritta al QTSP INTESA.

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere Banco BPM al quale INTESA conferisce l'incarico di RA e sui quali il Certificatore ha l'obbligo di vigilare.

In particolare, si richiede a Banco BPM di:

- vigilare affinché l'attività di identificazione posta in essere si svolga nel rispetto della normativa vigente (CAD e successive modificazioni, DPCM, Reg. eIDAS e qualora si tratti di Cliente di Banco BPM anche della normativa in materia di Antiriciclaggio);
- di assicurare, nel caso di Prospect, di aver adottato tutte le misure di mitigazione del rischio al fine di consentire al Prospect, solo ed esclusivamente la sottoscrizione della richiesta di apertura dei rapporti, segnalando alla CA i casi in cui i processi di identificazione e adeguata verifica non si concludano correttamente nei tempi previsti, in modo da consentire la revoca del certificato;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il GDPR;
- rendere disponibile per il Certificatore il materiale raccolto nella fase di identificazione e registrazione.

Il personale di Banco BPM, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne al Banco BPM stesso, svolge tutte le operazioni necessarie volte all'identificazione e registrazione del Richiedente.

Il servizio di identificazione potrà essere gestito come segue:

- *tramite il personale di filiale di Banco BPM*, il Titolare al momento dell'apertura di un rapporto verrà identificato e registrato per mezzo i documenti d'identità forniti, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne al Banco BPM stesso. 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 di Banco BPM mediante tecniche di comunicazione a distanza.

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

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore – 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. paragrafo *C.1. Obblighi del Certificatore Accreditato*.

INTESA, fatto salvo 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, INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo esemplificativo: calamità naturali, disservizi e/o disfunzioni tecniche e logistiche al di fuori del proprio controllo, interventi dell'Autorità, rivolte o atti di guerra che colpiscano anche o solo i soggetti delle cui attività INTESA si avvale per la prestazione dei propri servizi di certificazione.

Il Certificatore 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 paragrafo *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 inviata ad AgID apposita dichiarazione di stipula.

E. Tariffe

Il Servizio viene fornito dal 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 Certificatore deve verificare con certezza l'identità del richiedente alla prima richiesta di emissione di certificato qualificato.

La suddetta operazione viene demandata a Banco BPM che, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio, identificherà e registrerà il Titolare.

Per i successivi rinnovi, se effettuati quando il certificato qualificato è ancora in corso di validità, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al Certificatore attraverso Banco BPM solo 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
- 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.

Il Prospect o il già Cliente, identificati da Banco BPM in ottemperanza con quanto previsto dalla vigente normativa che disciplina il rilascio dei certificati qualificati e dalle normative interne al Banco BPM stesso, potrà attivare la procedura di generazione del Certificato Qualificato per la Firma Digitale Remota presso la Filiale ovvero all'interno dell'Internet Banking (per i già Clienti), ovvero nell'ambiente di onboarding per i prospect.

F.1.1. Limiti d'uso

Nel Certificato Qualificato per la Firma Digitale, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti da Banco BPM , è inserito uno dei limiti d'uso di seguito riportati.

- **Per Banco BPM**

  "Questo certificato è utilizzabile solo per la sottoscrizione di documenti, atti, contratti, ordini, relativi a prodotti e servizi prestati o distribuiti da BANCO BPM nell'ambito:

  (i) del dominio informatico BANCO BPM, identificabile con le pagine web del sito della Banca raggiungibile all'url www.bancobpm.it;

  (ii) delle Agenzie/Filiali di BANCO BPM dislocate sul territorio nazionale.

  Il presente certificato è valido tre anni dall'emissione".

  "This certificate can be used only for the signing of documents, deeds, contracts, orders, relating to products and services provided or distributed by BANCO BPM in the context:

  (i) of the BANCO BPM IT domain, identifiable with the web pages of the Bank's website accessible to the URL www.bancobpm.it;

  (ii) BANCO BPM Agencies / Branches located throughout the country.

  This certificate is valid for three years from issue.".

- **Per Webank :**

  "Questo certificato è utilizzabile solo per la sottoscrizione di documenti, atti, contratti, ordini, relativi a prodotti e servizi prestati o distribuiti da BANCO BPM nell'ambito:

  (i) del dominio informatico BANCO BPM, identificabile con le pagine web del sito della Banca raggiungibile all'url www.webank.it.

  Il presente certificato è valido tre anni dall'emissione".

" This certificate can be used only for the signing of documents, deeds, contracts, orders, relating to products and services provided or distributed by BANCO BPM in the context:

(i) of the BANCO BPM IT domain, identifiable with the web pages of the Bank's website accessible to the URL www.webank.it.

This certificate is valid for three years from issue.".

G. Procedure di rilascio del Certificato Qualificato per la Firma Digitale Remota

G.1. Rilascio in Filiale

Il processo per il rilascio del certificato qualificato per la firma digitale remota (FDR) presso la filiale è sintetizzato nei punti seguenti:

1. Il Cliente, già identificato da un operatore di Banco BPM nelle modalità prescritte dalla vigente normativa, richiede il rilascio di un certificato qualificato per la firma digitale remota (FDR).
2. Prima di procedere, l'operatore di filiale verifica con certezza la piena disponibilità di un dispositivo mobile da parte del Cliente.
   Questa verifica viene effettuata da Banco BPM richiedendo al Cliente di dare evidenza di un codice OTP che nel frattempo gli sarà stato inviato (da Banco BPM) sul numero del dispositivo mobile indicato in filiale all'operatore.
3. Viene quindi presentata al Cliente, su un tablet, la documentazione di richiesta del certificato obbligatoria del QTSP INTESA, di cui il Cliente sarà tenuto a sottoscrivere la presa visione.
4. Il Cliente che intende procedere potrà, a questo punto, firmare elettronicamente la richiesta del certificato, spuntando i check box del documento contrattuale della QTSP INTESA.
5. Dopo che il Cliente ha completato il check di approvazione per tutti i punti presentati a video, si può procedere all'emissione del certificato qualificato.
   Al momento della generazione del certificato è indispensabile che venga inserito un PIN/Password , il quale sarà poi richiesto ad ogni utilizzo del certificato di firma
6. Dopo che il certificato qualificato è stato generato, a conclusione della procedura il QTSP INTESA invia al Cliente un sms di notifica dell'avvenuta generazione del certificato di FDR

Al termine della procedura verrà messa a disposizione dell'utente copia della documentazione firmata.

G.2. Rilascio tramite Internet Banking (per i clienti)

Il processo per il rilascio della firma digitale remota (FDR) può essere gestito dal Cliente anche all'interno dell'applicazione di Internet Banking.

Il processo è compatibile con i principali browser (Chrome, Firefox, Edge, Safari) e sui dispositivi mobile più recenti della famiglia Android e Apple e segue la seguente procedura:

1. Il Cliente, una volta acceduto all'internet Banking del Banco BPM, richiede il rilascio di un certificato qualificato per la firma digitale remota (FDR).
2. Al Cliente è presentato il riepilogo dei dati personali utili ai fini del rilascio del certificato (par. F.1)
3. Viene presentata al Cliente la documentazione di richiesta del certificato del QTSP INTESA, di cui il Cliente sarà tenuto a sottoscrivere la presa visione spuntando i check box del documento apponendo una firma elettronica mediante l'inserimento di un OTP ricevuto via sms dal QTSP INTESA.
4. Se l'OTP fornito dal QTSP INTESA è riscontrato positivamente, il processo di firma viene concluso e Banco BPM riceve un responso sull'esito del processo (in caso contrario dovrà essere richiesto un nuovo OTP).

5. Se l'OTP non pervenisse al Cliente via SMS, il Cliente può richiedere che l'operazione venga reiterata fino ad un massimo di tre tentativi.
   Falliti tali tentativi, l'OTP potrà essere inviato all'email fornita in precedenza durante la fase di registrazione, a condizione che l'email risulti essere stata precedentemente certificata (a condizione cioè che sia stata già verificata la piena disponibilità dell'email da parte del Cliente).
6. Completato positivamente il check di approvazione per tutti i punti presentati a video, si può procedere all'emissione del certificato qualificato.
   Al momento della generazione del certificato è indispensabile che venga inserito un PIN/Password, il quale sarà poi richiesto ad ogni utilizzo del certificato di firma

Al termine della procedura verrà messa a disposizione dell'utente copia della documentazione firmata

G.3. Rilascio nell'ambiente di OnBoarding (per i clienti prospect)

Il processo per il rilascio della firma digitale remota (FDR) può essere gestito anche da un Cliente Prospect durante le attività di OnBoarding.

Il processo è compatibile con i principali browser (Chrome, Firefox, Edge, Safari) e sui dispositivi mobile più recenti della famiglia Android e Apple e si articola come segue:

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

In entrambi i casi il Cliente Prospect verrà comunque informato da Banco BPM sull'esito delle verifiche e sull'eventuale revoca del certificato.

H. Modalità operative per la sottoscrizione di documenti

Il Certificatore, attraverso i servizi di Banco BPM, 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 da Banco BPM attraverso l'area web riservata o mediante le opportune applicazioni di filiale. Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno conformi a quanto previsto dal DPCM, all'Art.4 comma 2, relativamente agli algoritmi utilizzati.

I documenti sottoscritti con tale applicazione di firma, come richiesto dall'Art.4 comma 3 dello stesso DPCM, non conterranno macroistruzioni o codici eseguibili tali ad attivare funzionalità che possano, all'insaputa del sottoscrittore, modificare atti, fatti e dati nei documenti stessi rappresentati.

Inoltre, tali documenti saranno sempre disponibili, per il sottoscrittore, all'interno di specifica sezione dell'area Riservata del sito internet.

H.1. Processo di Firma

Dopo aver richiesto il proprio Certificato digitale, il Titolare potrà poi procedere alla firma di un documento sia in filiale che nell'Internet banking secondo le modalità di seguito descritte.

H.1.1. Filiale:

Le modalità di firma presso la Filiale saranno le seguenti:

1. Il Titolare del Certificato Qualificato per la Firma Digitale potrà richiedere la sottoscrizione di documenti, atti, contratti, ordini, relativi a prodotti e servizi prestati o distribuiti da BANCO BPM.
2. Il Titolare prende visione del documento da firmare digitalmente e di eventuale ulteriore documentazione informativa utilizzando il display della tavoletta installata presso la postazione dell'operatore di Banco BPM.
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 un cellulare precedentemente registrato per ricevere le comunicazioni di Banco BPM, di un opportuno SMS confermerà l'avvenuta sottoscrizione.

Qualora i documenti da firmare fossero più di uno, con PDF separati, il Titolare, per ogni documento, può reiterare i passi dal 2 al 4.

H.1.2. Internet Banking

Modalità quasi del tutto analoghe andranno seguite per la firma sull'Internet Banking; in questo caso:

1. Il Titolare del Certificato Qualificato per la Firma Digitale, accedendo all'area Riservata del sito di Internet Banking di Banco BPM, richiede la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dal Banco BPM stesso.
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 generato dai dispositivi di sicurezza in uso.
4. La ricezione, su di un cellulare precedentemente registrato per ricevere le comunicazioni di Banco BPM, di un opportuno SMS confermerà l'avvenuta sottoscrizione.

Qualora i documenti da firmare fossero più di uno, con PDF separati, il Titolare, per ogni documento, può reiterare i passi dal 2 al 4.

H.2. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF in conformità all'Art.21 comma 8 e 15 della Deliberazione CNIPA n. 45 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.

La suddetta operazione è preceduta dall'inizializzazione dei dispositivi di firma per il sistema di generazione dei certificati con i quali si firmano i certificati dei Titolari e quelli del sistema di validazione temporale.

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

Le operazioni successive alla generazione delle coppie di chiavi del Certificatore sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto 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 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 di 2048 bit.

I.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 di 2048 bit.

I.3. Generazione delle chiavi di sottoscrizione

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

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato in una delle modalità precedentemente descritte al par. G. Procedure di rilascio del Certificato Qualificato per la Firma Digitale Remota.

Le coppie di chiavi di sottoscrizione sono create su dispositivi di firma sicuri (HSM – Hardware Security Module), conformi alle specifiche di cui all'Allegato II del Reg. eIDAS.

La lunghezza delle chiavi di sottoscrizione è di almeno 2048 bit.

J. Modalità di emissione dei certificati

J.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo 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 Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei certificatori e lo pubblica nel proprio registro dei certificati. Il Certificatore deve poi mantenere copia della lista, sottoscritta da Agenzia per l'Italia Digitale, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.42, commi 1 e 3).

J.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 paragrafo *H.3*, è generata una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

Generate le chiavi la richiesta di certificato sarà immediatamente inviata dall'applicazione di Banco BPM al Certificatore.

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

J.2.1. Informazioni contenute nei certificati di sottoscrizione

I certificati 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 Digitale contiene, a titolo esemplificativo ma non esaustivo, le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del Certificatore;
- codice identificativo unico del Titolare presso il Certificatore;
- 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 uno dei limiti d'uso riportati al par. ***F.1.1***

J.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, il codice di emergenza sarà comunicato al Titolare in fase di richiesta di certificazione.

K. Modalità di revoca e sospensione dei certificati

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

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

La lista CRL è disponibile anche sul registro dei certificati.

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

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

In conformità al Reg. eIDAS, le informazioni sullo stato del certificato sono disponibili anche via protocollo OCSP.

K.1. Revoca dei certificati

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 Banco BPM.

Il Certificatore, avvertito da Banco BPM, provvederà alla immediata revoca del certificato.

K.1.2. Revoca su richiesta del Terzo Interessato

Banco BPM in qualità di Terzo Interessato può richiedere la revoca del certificato.

In caso di estinzione del contratto (di conto corrente) che lega il Titolare al Terzo Interessato, quest'ultimo potrà esercitare la richiesta di revoca con le modalità stabilite con il Certificatore. In questo caso il Certificatore non deve provvedere ad inviare alcuna comunicazione al Titolare.

Nel caso in cui Banco BPM richiedesse la revoca del certificato senza la simultanea interruzione del contratto in essere 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 o successivamente aggiornati e comunicati dal Titolare alla CA (cfr. C.2 - Obblighi del Titolare).

K.1.3. Revoca su iniziativa del Certificatore

Il Certificatore che intende revocare il Certificato Qualificato ne dà preventiva comunicazione via PEC con Banco BPM; 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.

Effettuata la revoca, il Certificatore avviserà 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,
- 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, ai Titolari e a Banco BPM

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 Banco BPM

Il Certificatore, avvertito da Banco BPM, provvederà alla immediata sospensione del certificato.

Successivamente il Titolare potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre da Banco BPM.

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

Banco BPM in qualità di Terzo Interessato potrà richiedere la sospensione del certificato.

Il Certificatore, 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 alla CA (par. *C.2 - Obblighi del Titolare*).

K.2.3. Sospensione su iniziativa del Certificatore

Il Certificatore, salvo i casi di motivata urgenza potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo e-mail fornito in fase di richiesta del certificato comunicato in fase di registrazione ovvero all'indirizzo di residenza, specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

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

L. Modalità di sostituzione delle chiavi

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

I certificati qualificati di firma elettronica emessi dal Certificatore nell'ambito del contesto descritto nel presente Manuale Operativo hanno validità di 36 (trentasei) mesi dalla data di emissione.

Al termine sopracitato, si renderà necessaria la generazione di una nuova coppia di chiavi di sottoscrizione e, contestualmente, l'emissione di un nuovo certificato.

In questo caso la procedura seguita per l'emissione del nuovo certificato sarà simile a quella indicata in fase di primo rilascio, al netto della fase di identificazione del Titolare che non dovrà essere ripetuta.

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 / TSCA) o di disastro presso la sede centrale è trattato alla sezione *O. 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 / TSCA), utilizzate dai sistemi di emissione dei certificati di sottoscrizione e dei certificati di TSA, il Certificatore procederà in base a quanto stabilito dall'art. 30 del DPCM.

L.3. Chiavi del sistema di validazione temporale (TSA)

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

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

1. I certificati delle chiavi di sottoscrizione e del sistema di validazione temporale.
2. I certificati delle chiavi di certificazione.
3. I certificati emessi a fronte di accordi di certificazione con altri.
4. I certificati emessi a seguito della sostituzione delle chiavi di certificazione.
5. Certificati per le chiavi di firma dell'Agenzia per l'Italia Digitale (DPCM Art.42, comma 1).
6. Le liste di revoca e sospensione (CRL).

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

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

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

M.2. Accesso logico al Registro dei certificati

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

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

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

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

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

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

N. Modalità di protezione dei dati personali

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure previste dal Regolamento Europeo 679/2016 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 alla sezione 0.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonchè 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 Certificatore (Art.36 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del DPCM).

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

P. Procedura di gestione degli eventi catastrofici

Il Responsabile della sicurezza gestisce un piano di gestione degli eventi catastrofici che prevede le seguenti fasi:

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

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

Per poter fare fronte alla gestione dell'emergenza è prevista la replica nel sito di backup del registro dei certificati, dei dati del sistema di emissione dei certificati e l'intervento entro 24 ore di personale atto ad attivare la funzionalità di emissione delle CRL/CSL. Di detto personale è curato l'addestramento, oltre che alla gestione del SW e HW, anche della situazione di emergenza. È previsto inoltre l'intervento, entro il medesimo lasso di tempo, dei depositari dei dispositivi di autorizzazione per il ripristino della chiave privata della CA ai fini di ricostruirla nel dispositivo di firma (HSM) del sito di backup.

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

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

Tutte le macchine del sistema di PKI del Certificatore sono sincronizzate con l'*I.N.RI.M. - Istituto Nazionale di Ricerca Metrologica* di Torino (già *Istituto Elettrotecnico Nazionale Galileo Ferraris*). Questa funzionalità è realizzata da un software specifico installato su ogni server che, mediante il protocollo NTP (Network Time Protocol), si collega al server remoto configurato.

Il Network Time Protocol (NTP) è uno dei metodi più accurati e flessibili per passare l'informazione di tempo e di data sulla rete Internet. Esso permette di mantenere sincronizzati tra loro computer collegati tramite reti locali, metropolitane o addirittura mondiali (Internet) utilizzando una struttura di tipo gerarchico a piramide.

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 sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la 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.

Il software installato presso il certificatore si collega al server remoto ad intervalli regolari di tempo e, dopo aver ottenuto l'ora corrente, provvede a correggere il clock della macchina locale mediante sofisticati algoritmi.

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

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.41 del DPCM).

Q.1. Modalità di richiesta e verifica marche temporali

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

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

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

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

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

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

S. Riferimenti Tecnici

ETSI-319.401	ETSI EN 319 401 v2.1.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.1.0 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.411-3	ETSI EN 319 411-3 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 3: Policy requirements for Certification Authorities issuing public key certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures
ETSI-319.412-2	ETSI EN 319 412-2 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.1.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
Rec ITU-R	Recommandation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)