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

Manuale Operativo
per le procedure di firma elettronica qualificata remota nell'ambito dei servizi di BPER BANCA e delle società del Gruppo BPER

Codice documento: MO_BPER

OID: 1.3.76.21.1.50.3

Redazione: Antonio Raia

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

Data emissione: 25/05/2022

Versione: 05

Intesa

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

Revisioni

Versione n°: 05	***Data Revisione: 25/05/2022***
Descrizione modifiche:	Aggiornamento titolo del documento Par. F.4 e G.2.3: aggiornamento limitazioni d'uso par. I.4: aggiornamento codice emergenza par. O: aggiornamento descrittivo par. P: aggiornamento descrittivo
Motivazioni:	Aggiornamenti per estensione del manuale alle società del Gruppo BPER Banca Aggiornamenti e correzione refusi
Versione n°: 04	***Data Revisione: 7/03/2022***
Descrizione modifiche:	Aggiornamento titolo par. B.4.2: aggiornamento par. B.4.3: aggiornamento par. C.4: aggiornamento par. C.5: aggiornamento par. F.1: aggiornamento par. F.4: aggiornamenti par. G.2.2 e G.2.3: aggiornamenti par. P: aggiornamento descrittivo
Motivazioni:	Aggiornamenti limitazioni d'uso Aggiornamenti Correzione refusi
Versione n°: 03	***03*** ***Data Revisione: 31/12/2021***
Descrizione modifiche:	Aggiornamento dati societari e logo del QTSP In.Te.S.A. S.p.A. Aggiornamento riferimenti normativi e tecnici par. C.5 aggiornamento par. D.1 aggiornamento par. D.2 aggiornamento par. K.2.1 aggiornamento
Motivazioni:	Variazione proprietà, direzione e coordinamento Aggiornamenti normativi
Versione n°: 02	***Data Revisione: 15/02/2017***
Descrizione modifiche:	par. A.1. da: *Banca popolare dell'Emilia-Romagna Soc. coop - Sede Legale Via San Carlo, 8/20 - 41121 Modena; Web: www.bper.it;* Codice Fiscale, Partita IVA e iscrizione nel Registro Imprese di Modena (di seguito anche solo BPER o *Banca*) a: *BPER Banca S.p.A. - Sede Legale Via San Carlo, 8/20 - 41121 Modena; Web: www.bper.it;* Codice Fiscale, Partita IVA e iscrizione nel Registro Imprese di Modena: 01153230360 (di seguito anche solo BPER o *Banca*).
Motivazioni:	Variazione ragione sociale
Versione n°: 01	***Data Revisione: 24/11/2016***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

Riferimenti Normativi & Acronimi

Riferimenti di legge

Testo Unico - DPR 445/00 e ss.mm.ii.	Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445. *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*. Nel seguito indicato anche solo come *TU*.
CAD - DLGS 82/05 e ss.mm.ii.	Decreto Legislativo 7 marzo 2005, n. 82 - "*Codice dell'amministrazione Digitale"*. Nel seguito indicato anche solo come *CAD*.
DPCM 22/02/2013 Nuove Regole Tecniche e ss.mm.ii.	Decreto Del Presidente Del Consiglio Dei Ministri 22 febbraio 2013 *"Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20 comma 3, 24 comma 4, 28 comma 3, 32 comma 3 lettera b), 35 comma 2, 36 comma 2, e 71" (del CAD, n.d.r.).* Nel seguito indicato anche solo come *DPCM* oppure *Decreto*.
Regolamento (UE)N. 910/2014 (eIDAS)	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS.*
DLGS 196/03 e ss.mm.ii.	Decreto Legislativo n.196 del 30 giugno 2003 "*Codice in materia di protezione dei dati personali"*. (G.U. n.174 del 29 luglio 2003, suppl. ord.). Nel seguito indicato anche solo come *DLGS 196/03*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation	REGOLAMENTO (UE) 2016/679 del Parlamento Europeo e Del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati). Nel seguito indicato anche solo come *GDPR.*
DETERMINAZIONE N. 147/2019 e ss.mm.ii.	Linee guida contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate". Nel seguito indicato anche solo come *DETERMINAZIONE* ovvero *LLGG*
D.lgs. 231/07 e ss.mm.ii.	DECRETO LEGISLATIVO 21 novembre 2007, n. 231 Attuazione della direttiva 2005/60/CE concernente la prevenzione dell'utilizzo del sistema finanziario a scopo di riciclaggio dei proventi di attività criminose e di finanziamento del terrorismo nonché della direttiva 2006/70/CE che ne reca misure di esecuzione.

Definizioni & Acronimi

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP - Qualified Trust Service Provider. Certificatore Accreditato	*Prestatore di Servizi Fiduciari Qualificato*. Persona fisica o giuridica che presta uno o più servizi fiduciari qualificati. Già *Certificatore Accreditato*, ai sensi del CAD. Nel presente documento è il QTSP In.Te.S.A. S.p.A.
Servizio Fiduciario Qualificato	Servizio elettronico fornito da un QTSP e consistente negli elementi di cui all'Art.3, punto 16) e 17) del Reg. UE 910/2014 (eIDAS). Nel Presente documento è il QTSP In.Te.S.A. S.p.A. che presta i servizi qualificati di firma elettronica e di validazione temporale elettronica e altri servizi connessi con queste ultime.
Certificato Qualificato di firma elettronica	Attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona. È rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I del Reg. UE 910/2014 (eIDAS)

CPS	Certification Practice Statement - Una dichiarazione delle prassi seguite da un Certificatore / TSP nell'emettere e gestire certificati.
CRL	Certificate Revocation List - Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore / TSP che li ha emessi.
Doc. Informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Doc. Analogico	Documento analogico: rappresentazione non informatica di atti, fatti o dati giuridicamente rilevanti.
FEA	Firma elettronica Avanzata – ex Art.26 Reg. UE 910/2014 (eIDAS), la FEA soddisfa i segg. requisiti: a) è connessa unicamente al firmatario; b) è idonea a identificare il firmatario; c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Firma elettronica creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
Firma automatica	Particolare procedura informatica di firma elettronica qualificata o di firma digitale eseguita previa autorizzazione del sottoscrittore che mantiene il controllo esclusivo delle proprie chiavi di firma, in assenza di presidio puntuale e continuo da parte di questo
HSM - Hardware Security Module	Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014. Anche detti *Dispositivi di Firma*.
OID	Object Identifier - Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PKI	Public Key Infrastructure - Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
CA	Certification Authority: Entità della PKI che rilascia i certificati
RA - Registration Authority *LRA – Local RA*	*Autorità di Registrazione*: entità che, su incarico del QTSP, ha la responsabilità di registrare e verificare le informazioni (in particolare modo l'identità del Titolare) necessarie al QTSP per emettere il Certificato Qualificato. *Local Registration Autority (LRA)*: il QTSP INTESA può demandare lo svolgimento di alcune funzioni del proprio Ufficio di RA ad entità esterne (Local RA) tramite opportuno contratto di mandato. In tale contratto, sottoscritto da entrambe le parti, saranno definite le attività in carico alla LRA esterne e riportati gli obblighi delle parti. Nell'ambito del presente manuale potranno assumere la qualifica di LRA BPER Banca ovvero le singole Banche appartenenti al Gruppo BPER.
Qualified Electronic Time Stamp (Marca Temporale)	*Validazione Temporale Elettronica Qualificata* Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi dati esistevano in quel momento. Risponde ai requisiti dell'Art.42 del Reg. eIDAS
Terzo interessato (subscriber)	Il Terzo Interessato è la Persona Giuridica che richiede o autorizza l'emissione del certificato qualificato. Ha l'obbligo di richiedere la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali il certificato è stato rilasciato. (ETSI 319 401-1: "*subscriber: legal or natural person bound by agreement with a trust service provider to any subscriber obligations*").
Richiedente Richiesta di certificazione	La Persona Fisica che richiede il Certificato, cioè che inoltra al QTSP una richiesta di certificazione.
Titolare (subject)	La Persona Fisica cui il certificato qualificato di firma è rilasciato e che è autorizzato ad usarlo al fine di apporre la propria firma digitale. (ETSI 319 411-1: "*subject: entity identified in a certificate as the holder of the private key associated with the public key given in the Certificate*")

TSA – Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
Giornale di Controllo	Insieme delle registrazioni effettuate anche automaticamente dai dispositivi installati presso il QTSP, tenuto in modo da garantire l'autenticità delle annotazioni e consentire la ricostruzione, con la necessaria accuratezza, di tutti gli eventi rilevanti ai fini della sicurezza (DPCM 22/02/2013, Art. 36

A. Introduzione

A.1. Proprietà intellettuale

Questo documento è il Manuale Operativo per la procedura di Firma Digitale Remota nell'ambito dei servizi offerti *da BPER Banca S.p.A. – Sede Legale Via San Carlo, 8/20 – 41121 Modena; Web:* www.bper.it*;* Codice Fiscale, Partita IVA e iscrizione nel Registro Imprese di Modena: 01153230360 (di seguito anche solo BPER) e dalle società del Gruppo BPER (di seguito singolarmente definite *Banca*).

Il Manuale Operativo descrive le procedure e relative regole utilizzate dal Certificatore Accreditato In.Te.S.A. S.p.A. (di seguito anche solo *Certificatore* o *INTESA*) per l'emissione dei Certificati Qualificati, la generazione e la verifica della firma elettronica qualificata nell'ambito dei servizi offerti dalla Banca.

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 anche solo *Decreto*) e dal Decreto Legislativo 7 marzo 2005, n. 82, recante il "Codice dell'Amministrazione Digitale" come successivamente modificato e integrato (di seguito anche solo *CAD*) e in particolare:

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

Le attività descritte sono svolte in conformità con il Regolamento (UE) 910/2014 (eIDAS).

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme tempo per tempo vigenti.

In questo contesto, i Titolari di un Certificato Qualificato sono solo i soggetti riconosciuti dalla Registration Authority ovvero dalla stessa Banca, la quale, in virtù di specifico accordo con il Certificatore, è autorizzata a svolgere la funzione di Registration Authority.

Il processo prevede che il Titolare possa avviare la procedura di Firma Remota di documenti nell'ambito dei servizi offerti dalla Banca.

Nota: **il presente documento integra e sostituisce il "Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A.** ***per le procedure di firma remota nell'ambito dei servizi di Banco di Sardegna*****", ver.01, OID 1.3.76.21.1.50.5. Le procedure e le misure di sicurezza descritte in tale Manuale Operativo sono interamente riportate e descritte nel presente documento.**

A.2. Validità

Quanto descritto in questo documento si applica al Certificatore, 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 da INTESA.

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

a) chiavi di sottoscrizione, destinate alla generazione e verifica delle firme apposte o associate ai documenti;

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

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e delle relative regole utilizzate dal certificatore accreditato INTESA per l'emissione di certificati qualificati.

Tale impianto di regole e procedure scaturisce dall'ottemperanza alle attuali normative in merito la cui osservanza permette ad INTESA di essere inserita nell'elenco dei certificatori accreditati.

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

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n. **05** del ***Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per le procedure di firma elettronica qualificata remota nell'ambito dei servizi offerti da BPER BANCA e dalle società del Gruppo BPER***, forniti dalla Banca ovvero da terze società anche non appartenenti al Gruppo BPER Banca, rilasciato il **25/05/2022**, in conformità con l'Art.40 del Decreto.

L'object identifier (OID) di questo documento è ***1.3.76.21.1.50.3.***

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

- all'indirizzo Internet del QTSP, *https://www.intesa.it/e-trustcom/*
- all'indirizzo Internet dell'Agenzia per l'Italia Digitale, *www.agid.gov.it*
- nell'ambito del sito istituzionale della Banca.

La pubblicazione di versioni aggiornate del presente Manuale Operativo potrà avvenire solo successivamente al loro inoltro all'Agenzia per l'Italia Digitale.

B.2. Dati identificativi del Certificatore

Il Certificatore, ai sensi dell'Art.29 del CAD, è la società INTESA S.p.A., di cui di seguito sono riportati i dati identificativi.

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

B.3. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art. 40 comma 3 lett. c) del Decreto, è della Certification Authority INTESA, che ne cura la stesura, la pubblicazione, l'aggiornamento e ogni eventuale revisione, in accordo e in collaborazione con BPER in qualità di società capogruppo del Gruppo BPER.

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

- un recapito di posta elettronica: *marketing@intesa.it*
- un recapito telefonico: +39 011.192.16.111
- un servizio di Help Desk per le chiamate dall'Italia: 800.80.50.93
  per le chiamate dall'estero: +39 02.39.30.90.66

B.4. Entità coinvolte nei processi

All'interno della struttura del 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 con quanto previsto dal Decreto 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 nel paragrafo precedente.

Il personale responsabile delle attività di certificazione, in conformità con l'Art. 38 del Decreto, 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.4.2. Local Registration Authority (LRA)

Per la particolare tipologia di servizio offerto (Firma Digitale Remota nell'ambito delle applicazioni di firma descritte in questo Manuale Operativo), il Certificatore ha rilasciato mandato a svolgere le funzioni di Local Registration Authority (LRA) alla Banca.

In particolare, la LRA si impegna a svolgere 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.

In particolare, la Banca, nel rispetto della normativa antiriciclaggio, così come previsto dal D.lgs. 231/07 e ss.mm.ii., nonché dalle Disposizioni in materia di adeguata verifica della clientela per il contrasto del riciclaggio e del finanziamento del terrorismo, potrà identificare il Titolare e verificarne con certezza l'identità (vedi contenuti degli obblighi di *adeguata verifica*) anche se questi non si presenterà fisicamente in un'agenzia.

In questo caso la Banca dovrà comunque:

- accertare l'identità tramite documenti, dati o informazioni supplementari quali atti pubblici, scritture private autenticate, certificati utilizzati per la generazione di una firma elettronica qualificata associata a documenti informatici ovvero attraverso dichiarazione dell'Autorità Consolare Italiana;
- applicare misure supplementari per la verifica dei documenti forniti quali, ad esempio, certificazione di conferma di un ente creditizio o finanziario soggetto alla direttiva;
- utilizzare la documentazione provante che il rapporto di provvista provenga da un conto intestato al cliente;

- verifica del numero di cellulare e dell'indirizzo e-mail.

Gli obblighi della LRA sono riportati al par. *C.4*.

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 ovvero per i propri dipendenti.

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).

Inoltre, limitatamente al caso di certificati emessi per persone aderenti alla propria organizzazione (dipendenti, collaboratori o affiliati), da consenso all'inserimento nel Certificato Qualificato dell'indicazione dell'Organizzazione e di eventuali poteri di rappresentanza.

Per quanto riguarda invece i certificati emessi ai clienti bancari, tali certificati non prevedranno i poteri di rappresentanza e non conterranno l'indicazione del Terzo Interessato al loro interno.

Gli obblighi del Terzo Interessato sono riportati al par. *C.5*.

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

Nello svolgimento della propria 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.
- Decreto Legislativo 30 giugno 2003, n.196, e successive modificazioni, recante codice in materia di protezione dei dati personali.
- REGOLAMENTO (UE) 2016/679 – GDPR (RGPD regolamento generale sulla protezione dei dati)
- Regolamento (UE) 910/2014 (eIDAS)

In particolare, il Certificatore Accreditato:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel Decreto;
- 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 Decreto;
- 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 (DLGS 196/03 - 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 queste 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 Decreto, 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 (Art.42 del Decreto);
- garantisce l'interoperabilità del prodotto di verifica, di cui all'Art.14 del Decreto, 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 Decreto), e la rende accessibile per via telematica (Art.42, comma 3 del Decreto).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo potrà ricevere un certificato qualificato di firma per sottoscrivere atti e documenti nell'ambito dei servizi di firma remota offerti dalla Banca.

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- mettere a disposizione del Certificatore, tramite la Banca, eventuali variazioni alle informazioni fornite all'atto della registrazione, avvenute durante il periodo di validità del certificato digitale: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (Art.5, comma 5, del Decreto);
- revocare immediatamente il certificato digitale in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma;
- revocare o sospendere il certificato digitale secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

Coloro che intendano 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;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e la loro validità;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori;
- 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.

Gli obblighi sopra descritti sono automaticamente espletati dai Software di Verifica conformi alle normative vigenti (Art. 14 del Decreto) ed implementati nei servizi offerti dal Certificatore sul portale della Banca.

C.4. Obblighi della Registration Authority esterna

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

Ai sensi del presente Manuale Operativo, il QTSP INTESA demanda lo svolgimento della funzione di Local Registration Authority alla Banca mediante specifico *Contratto di Mandato*, sottoscritto da entrambe le parti.

In particolare, in qualità di LRA, la Banca è tenuta a espletare 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 dell'Art. 8 e dell'Art. 10, comma 2, del Decreto.

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere la Banca cui il QTSP INTESA assegna l'incarico di LRA.

In particolare, si richiede alla LRA di:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente (normativa in materia Antiriciclaggio, CAD, DPCM, Reg. eIDAS);
- rendere possibile il tracciamento dell'operatore di LRA che ha effettuato l'identificazione del Titolare;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il GDPR;
- rendere disponibile per il Certificatore 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.

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

C.5. Obblighi del Terzo Interessato

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

La Banca, nella veste di Terzo Interessato:

- verifica che il Cliente sia in possesso di tutti i requisiti necessari e autorizza il Cliente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota;
- svolge un'attività di supporto al Titolare;
- indica al QTSP eventuali ulteriori limitazioni d'utilizzo del Certificato Qualificato per la Firma Digitale (vedi par. *F.4*).

La Banca, come Terzo Interessato, quindi, potrà indicare al QTSP eventuali limitazioni d'uso del certificato, eventuali poteri di rappresentanza e dovrà comunicare qualsiasi variazione delle stesse.

Il Terzo Interessato provvederà all'inoltro delle richieste di revoca o sospensione nei casi e nelle modalità previste dal presente Manuale Operativo.

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente inoltrata alla CA quando vengano meno i requisiti in base ai quali al Titolare era stato rilasciato un certificato qualificato per la firma elettronica; a titolo esemplificativo, ma non esaustivo, si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza;
- cessazione del rapporto bancario (chiusura conto).

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore – Limitazione agli indennizzi

Conformemente a quanto previsto dal CAD, dal Decreto, dal GDPR e dal DLGS 196/03, INTESA è responsabile verso i Titolari per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal Decreto, dal GDPR, dal DLGS 196/03 e dal CAD e successive modificazioni e integrazioni (vedi *C.1 – Obblighi del Certificatore Accreditato*).

INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, art. 13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'Art.5 del Decreto, 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 indicata sul certificato stesso (par. *F.4*).

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

Per la particolarità del servizio oggetto di questo Manuale Operativo il Certificatore non indica delle tariffe per l'emissione, il primo rinnovo, la revoca e la sospensione dei certificati.

Queste saranno eventualmente indicate nei contratti che verranno stipulati fra la Banca e il Titolare.

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.

Questa operazione viene demandata alla Registration Authority del Certificatore ovvero alla Local Registration Authority, ed è svolta in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito.

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 Certificatore, attraverso la RA ovvero la Banca (LRA), 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, data e luogo del rilascio, data di scadenza.

Pertanto, la RA, ovvero la LRA, in ottemperanza con quanto previsto dalla vigente normativa e dalle normative interne, svolge tutte le operazioni necessarie all'identificazione e registrazione del richiedente.

Dopo che il Titolare è stato identificato, con una delle modalità nel seguito descritte (par. *F.1.1*, *F.1.2*, *F.1.3*), il numero di cellulare personale del richiedente verrà utilizzato dal QTSP per l'invio di codici numerici monouso (chiamati nel seguito codici OTP o semplicemente OTP) in grado di garantire un accesso sicuro al servizio di firma remota resogli disponibile dalla Banca.

Oltre all'OTP, nel caso in cui il Titolare faccia uso di certificati qualificati a lungo termine, la RA/LRA mette a disposizione del Titolare le funzionalità per impostare un Personal Identification Number (PIN) da utilizzare in abbinamento all'OTP quale secondo fattore di autenticazione.

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

Lo stesso PIN potrà essere utilizzato dal Titolare come *codice di emergenza* (par. *I.4*) per *sospendere con urgenza* il certificato qualificato in corso di validità a lui intestato (in caso, ad esempio, di smarrimento e/o indisponibilità dell'OTP).

Sul cellulare predefinito dal Titolare, o su di un indirizzo e-mail indicato dal cliente, potrebbero essere inviati specifici messaggi (SMS/e-mail) che possano avvisarlo relativamente alle operazioni eseguite attraverso l'impiego del certificato digitale (firma di un documento, ma anche sospensione, revoca o rinnovo del certificato digitale).

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

Solo attraverso l'uso congiunto di PIN e OTP sarà possibile sottoscrivere digitalmente documenti di vario genere nell'ambito dei servizi internet offerti dalla Banca.

Per il caso d'uso di certificati a lungo termine, vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

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

- prendere visione del Manuale Operativo del QTSP INTESA;

- autorizzare il trattamento dei propri dati personali per le finalità legate all'emissione di un certificato qualificato per la firma elettronica.

La documentazione relativa alla registrazione dei Titolari viene conservata dalla Registration Authority che ha effettuato l'identificazione per 20 (venti) anni.

F.1.1. Identificazione de visu in presenza del titolare

Per l'identificazione è richiesta la presenza fisica del Titolare.

Il soggetto che effettua l'identificazione verifica l'identità del Titolare tramite il riscontro con almeno un documento di riconoscimento, valido e non scaduto.

F.1.2. Identificazione tramite riconoscimento precedente

Il Certificatore si avvale del riconoscimento già effettuato da un Intermediario finanziario o da altro Soggetto Esercente Attività Finanziaria, che, ai sensi delle norme antiriciclaggio tempo per tempo vigenti, è obbligato al riconoscimento dei propri clienti.

Gli Intermediari e gli altri Soggetti Esercenti Attività Finanziaria acquisiscono i Dati in base alle procedure alle adottate secondo la normativa antiriciclaggio vigente alla data del riconoscimento al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale).

In questo caso, i dati identificativi del Titolare raccolti da quest'ultimo all'atto del riconoscimento vengono utilizzati direttamente per l'emissione dei certificati, previa accettazione da parte del Titolare delle condizioni contrattuali per il rilascio del certificato e degli strumenti per l'apposizione della firma nonché approvazione e conferma dei dati anagrafici registrati.

Nel caso in cui la richiesta sia per certificato a lungo termine, il Richiedete dovrà scegliere il PIN e il codice di emergenza che potrà utilizzare con il certificato che verrà rilasciato al termine del riconoscimento.

F.1.3. Identificazione de visu da remoto

Il servizio di identificazione a distanza è gestito dalla RA INTESA.

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

Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di RA interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.

L'intera sessione viene registrata in modalità audio e video (sia lato richiedente che lato operatore) e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.

La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa distinguibile del documento di riconoscimento inquadrato). L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione.

- *Il Richiedente:*

1. si connette al sito della Banca, dove sono riportate tutte le istruzioni necessarie per eseguire la procedura di riconoscimento e dove sono indicati i documenti necessari per l'identificazione;
2. compila, sul sito della Banca, una richiesta di certificato digitale compilando un form in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione;
3. prende visione del presente *Manuale Operativo*, che dovrà essere aperto in lettura. Lo stesso Manuale Operativo sarà anche disponibile al download dal sito stesso;
4. autorizza il consenso al trattamento dei dati personali;
5. esegue, tramite l'apposita funzione del sito, l'upload della copia scansionata dei documenti di identità (carta d'identità, passaporto, tesserino sanitario nazionale). L'invio preventivo di tali

documenti conferma la volontà del Richiedente di completare la procedura di identificazione finalizzata all'emissione di un certificato qualificato utilizzabile esclusivamente nell'ambito dei servizi di firma qualificata forniti dal Certificatore;

6. nel caso in cui la richiesta sia per certificato a lungo termine, in questa fase la piattaforma di video riconoscimento permette la scelta, da parte del Richiedente, del PIN e del codice di emergenza che potrà utilizzare con il certificato che verrà rilasciato al termine del riconoscimento;
7. Decide, eseguiti gli step precedenti, se continuare la sessione attivando appena possibile il collegamento via webcam oppure se continuare fissando un successivo appuntamento con gli operatori di RA, per completare in un momento successivo a lui più comodo la procedura;

- *L'operatore di RA:*

1. esegue controlli sui documenti ricevuti;
2. domanda, durante la sessione on-line (via webcam), al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati e controlla che i documenti siano gli stessi, verificando che nella foto del documento sia riconoscibile il Richiedente.

L'operatore deve essere libero di rifiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.

Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie per permettergli di utilizzare il certificato qualificato che sta per essergli emesso e di firmare digitalmente.

La documentazione precedentemente citata, relativa alla registrazione dei Titolari, viene conservata dal Certificatore per 20 (venti) anni dalla scadenza del certificato.

Al termine del processo, il certificato qualificato viene emesso dalla Certification Authority e al Titolare viene associato un identificativo univoco presso il Certificatore.

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

F.2. Titoli e abilitazioni professionali

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

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

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

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

F.3. Poteri di rappresentanza

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

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

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

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

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

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

F.4. Limitazioni d'uso

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

"*Il presente certificato è valido solo per firme apposte per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da BPER Banca*."
"This *certificate may only be used for the signature of documents and/or contracts concerning products and/or services offered by BPER Banca*."

Oppure:

"*Il presente certificato è valido solo per firme apposte per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da Banco di Sardegna.*"
"This *certificate may only be used for the signature of documents and/or contracts concerning products and/or services offered by Banco di Sardegna.*"

Oppure:

"*L'utilizzo del certificato è limitato ai rapporti con le società del Gruppo BPER o con le società da cui hanno ricevuto delega per offrire servizi per la stipula dei contratti*."
"*The* use *of the certificate is limited to relations with BPER Group companies or with the companies from which they have been delegated to offer the service to conclude contracts.*"

Nel caso di Certificato Qualificato per la Firma Digitale apposta con *procedura automatica*, è previsto un limite d'uso specifico (vedi par. *G.2.3*).

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

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

G. Modalità operative per la sottoscrizione di documenti

Il Certificatore, attraverso i servizi della Banca, rende disponibile ai Titolari quanto necessario a generare delle firme elettroniche qualificate conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia del servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer, ma piuttosto delle funzionalità di firma richiamabili via internet o accedendo ai servizi offerti dalla Banca.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno assolutamente conformi a quanto previsto dal DPCM all'Art.3 comma 2 relativamente agli algoritmi utilizzati.

Inoltre, tali documenti, come richiesto dall'Art.3 comma 3 del 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.

G.1. Autenticazione di tipo invio codice di sicurezza a mezzo SMS

L'autenticazione attraverso il codice OTP è realizzata con l'invio a mezzo SMS di un codice randomico generato dal sistema verso il cellulare indicato dal Titolare e verificato in fase di registrazione.

G.2. Processo di Firma

G.2.1. Firma Remota

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

1. Il Titolare si connette all'applicazione di firma attraverso i suoi codici personali;
2. Visiona il documento da firmare;
3. Inserisce quindi il suo PIN;
4. Esegue il click su "richiedi codice OTP";
5. Il sistema invia a mezzo SMS un codice randomico di 6 cifre e attende la digitazione da parte del firmatario nell'apposito campo;
6. Rilevando la correttezza del PIN e della digitazione del codice appena inseriti, procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa;
7. Qualora i documenti da firmare fossero più di uno, si applicherà quanto previsto al par. G.2.3.

G.2.2. Firma con certificato One-Shot

Il Certificatore offre un servizio di Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato "one shot", cioè una particolare tipologia di certificato per la quale è prevista una validità temporale limitata.

Essa è generata su di un HSM custodito e gestito sotto la responsabilità del Certificatore accreditato.

Il Titolare attiva la procedura di firma mediante i sistemi di autenticazione previsti nel Manuale Operativo del Certificatore Accreditato IN.TE.S.A. S.p.A.

Nel seguito è descritto l'elenco degli step che vengono eseguiti per l'apposizione della firma:

1. Il Titolare riceve un'e-mail all'indirizzo di posta registrato al momento della identificazione.
2. L'email contiene un invitation (URL) che redirige l'utente all'interno di un portale in cui viene mostrato il documento ovvero il set di documenti costituenti una specifica pratica che devono essere visionati, prima di poter procedere alla sottoscrizione degli stessi;
3. Una volta che l'utente, preso atto del contenuto del/i documento/i, attiva la funzione di richiesta certificato per la firma, viene quindi inviato un OTP/SMS al numero registrato in fase di identificazione. Solo quando l'utente avrà inserito il codice OTP all'interno della maschera mostrata dal portale, il processo di firma viene attivato. Il certificato è caratterizzato da una durata temporale molto limitata, che verrà utilizzato per apporre la firma elettronica qualificata esclusivamente sul set di documenti precedentemente visionati ed approvati dall'utente nelle maschere.

Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale del Certificatore (par. *P*).

G.2.3. Firma con procedure automatiche

Il Certificatore offre un servizio di generazione automatica delle firme digitali, da utilizzarsi per la gestione dell'apposizione di più firme digitali su uno o più documenti, anche nell'ambito della firma con certificato di validità temporale limitata di cui al precedente par. *G.2.2*, a fronte della verifica di un singolo token OTP.

Operativamente, il processo avviene, analogamente a quanto descritto al par. *G.2.1*, nel seguente modo:

1. Il Titolare si connette all'applicazione di firma attraverso i suoi codici personali;
2. Visiona i documenti da firmare;
3. Appone un flag su ogni documento (inteso come ogni campo firma) dichiara di prender visione dei documenti, accanto ai quali viene apposto il relativo flag;
4. Inserisce quindi il suo PIN;

5. Esegue il click su "richiedi codice OTP";
6. Il sistema invia a mezzo SMS un codice randomico di 6 cifre e ne attende la digitazione da parte del firmatario nell'apposito campo;
7. Rilevando la correttezza del PIN e della digitazione del codice appena inseriti, procede nell'operazione di firma di tutti i documenti di cui il Titolare ha precedentemente preso visione e visualizza la conferma del successo dell'operazione stessa.

Anche in questo caso i certificati di sottoscrizione generati dal Certificatore risiedono, con le rispettive chiavi private, su di un dispositivo di firma di tipo Hardware Security Module (HSM). Il servizio è conforme a quanto stabilito dalla normativa (DPCM, Art.5, comma 2 e 3) e il formato delle firme elettroniche generate è conforme alla normativa vigente.

A ciascuna firma è associata una marca temporale generata dal servizio di validazione temporale, descritto al par. *P – Modalità per l'apposizione e la definizione del riferimento temporale*.

Per quanto riguarda i certificati qualificati di firma automatica, sarà inserito il seguente limite d'uso:

"*Il presente certificato è valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da BPER Banca.*"
"*This certificate may only be used for unattended/automatic digital signature for the signature of documents and/or contracts concerning products and/or services offered by BPER Banca*."

Oppure:

"Il presente certificato è valido solo per firme apposte con procedura automatica per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti dal Banco di Sardegna."

"This certificate may only be used for unattended/automatic digital signature for the signature of documents and/or contracts concerning products and/or services offered by da Banco di Sardegna.".

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

G.3. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF; tale formato di sottoscrizione è considerato infatti di facile utilizzo nell'ambito delle applicazioni di firma remota.

Infatti, la verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC* scaricabile gratuitamente dal sito *www.adobe.com/it*.

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

H.1. Generazione delle chiavi di certificazione

La generazione delle chiavi di Certificazione all'interno dei dispositivi di firma custoditi nei locali del TSP avviene in presenza del *Responsabile dei servizi di certificazione* (Art.7, comma 1 del Decreto)

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

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

Le operazioni successive alla generazione delle coppie di chiavi di certificazione sono possibili solamente attraverso particolari dispositivi di autorizzazione (token usb): l'accesso privilegiato agli HSM è eseguibile soltanto attraverso le chiavi contenute in tali dispositivi di autorizzazione di cui sopra. Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "*n di m*", in modo che solo la concomitante presenza di almeno *n* di *m* parti della chiave permettano di operare con gli opportuni privilegi. Pertanto, esse vengono custodite in apposite casseforti distinte.

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

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

La generazione delle chiavi di validazione temporale avviene secondo quanto stabilito dall'Art.49 del Decreto.

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

H.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 autenticandosi al sistema fornitogli dalla Banca.

Il PIN 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 Decreto; 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 Decreto.

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.

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel par. *H.1*, vengono generati i certificati delle chiavi pubbliche conformemente con quanto disposto dal Decreto, 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 (AgID) attraverso il sistema di comunicazione di cui all'Art.16, comma 1, del DPCM.

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

I.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.33 del Decreto.

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta al par. *H.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 (Decreto, Art. 18, comma 4).

I.3. Informazioni contenute nei certificati

I certificati INTESA sono conformi a quanto indicato nel Regolamento eIDAS. In seguito a ciò è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani ed europei.

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 conterranno sempre una limitazione d'uso.

I.4. Codice di Emergenza

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

Nelle applicazioni descritte dal presente Manuale Operativo potrà essere considerato come codice di emergenza, in aggiunta al codice OTP definito in precedenza, anche il PIN scelto dal Titolare all'atto della sua registrazione.

J. Modalità di revoca e sospensione dei certificati

J.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista CRL (Art.22 Decreto).

Il profilo delle CRL/CSL è conforme con lo standard RFC 3280.

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita e ad ogni revoca o sospensione. La lista 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 Decreto), 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, Decreto).

J.1.1.1. 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 all'immediata revoca del certificato.

J.1.1.2. Revoca su richiesta del Terzo Interessato

Anche il Terzo Interessato (cfr. par. *B.4.3*) può richiedere la revoca del certificato.

In caso di estinzione di un contratto che lega un 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.

J.1.1.3. Revoca su iniziativa del Certificatore

Il Certificatore che intende revocare il Certificato Qualificato ne dà preventiva comunicazione alla Banca (all'indirizzo di PEC - 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 la Banca, inviando una comunicazione all'indirizzo di Posta Elettronica Certificata.

J.1.1.4. Revoca dei certificati relativi a chiavi di certificazione

Il Certificatore procede con la revoca dei certificati di certificazione e dei certificati di sottoscrizione firmati con la stessa chiave di certificazione nei casi di:

1. compromissione della chiave di certificazione,
2. guasto del dispositivo di firma (HSM),
3. cessazione dell'attività.

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

J.2. Sospensione dei certificati

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

In assenza di comunicazioni ulteriori, il certificato sarà automaticamente revocato dopo il periodo di sospensione indicato (non superiore ai 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.

J.2.1.1. 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 dalla Banca.

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

J.2.1.2. Sospensione su richiesta del Terzo Interessato

Come per la revoca un Terzo Interessato potrà richiedere anche la sospensione di un certificato digitale emesso per dei Titolari da lui rappresentati.

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.

J.2.1.3. 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, eventualmente, anche al Terzo Interessato.

K. Modalità di sostituzione delle chiavi

K.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.

K.2. Sostituzione delle chiavi del Certificatore

K.2.1.1. Sostituzione pianificata delle chiavi di certificazione

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

K.2.1.2. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) o di disastro presso la sede centrale è trattato al par. *O*.

K.2.1.3. Sostituzione pianificata delle chiavi del sistema di validazione temporale

In conformità con quanto indicato all'Art.49, comma 2, del Decreto, ai fini di limitare il numero di marche temporali generate con la medesima coppia di chiavi di marcatura 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.

L'operazione è svolta in presenza del *Responsabile del Servizio*.

K.2.1.4. Sostituzione in emergenza delle chiavi del sistema di validazione temporale

Il procedimento utilizzato in caso di guasto del dispositivo di firma (HSM) o di disastro presso la sede centrale è descritto al par. *O*.

L. Registro dei certificati

L.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 (Decreto Art.42, comma 1).
6. 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 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.

L.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/CSL.

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.

L.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.

M. Modalità di protezione della riservatezza

Le misure di sicurezza per la protezione dei dati personali sono conformi alle misure previste dal GDPR e DLGS 196/03 e successive modificazioni e integrazioni.

N. Procedura di gestione della copie di sicurezza

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

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *L*.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del Certificatore (Art.36 del Decreto).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del Decreto).
- 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 Decreto).

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

O. 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.

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

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

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

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

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

P.1. Modalità di richiesta e verifica marche temporali

Il Certificatore appone una marca temporale 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.

Q. 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 -------