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 offerte dalla società Ineo S.r.l.

Codice documento: MO_LS

OID: 1.3.76.21.1.50.15

Redazione: Antonio Raia

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

Data emissione: 08/05/2023

Versione: 02

Revisioni

Versione n°: 02	***Data Revisione: 08/05/2023***
Descrizione modifiche:	Variazione ragione sociale: Ineo Srl. Inserimento OID specifico per casi di gruppi chiusi di utenti. Estensione della possibilità di utilizzo di soluzioni di Conservazione a Norma accreditate per l'archiviazione delle evidenze audio/video. Inserimento delle modalità di identificazione per emissione dei successivi certificati one-shot. Inserimento della possibilità di utilizzo di soluzioni di firma di terze parti che hanno già integrato i certificati qualificati di Intesa. Aggiornamento descrittivo par. *Q - Modalità per l'apposizione e la definizione del riferimento temporale* Correzione refusi
Motivazioni:	Aggiornamento documento
Versione n°: 01	***Data Revisione: 13/10/2022***
Descrizione modifiche:	nessuna
Motivazioni:	primo rilascio

Sommario

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.*
Regolamento (UE)N. 910/2014 (eIDAS) e ss.mm.ii.	Regolamento (UE) n. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2104, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE. Nel seguito indicato anche solo come *Reg. eIDAS.*
Regolamento (UE) N. 2016/679 GDPR - General Data Protection Regulation e ss.mm.ii.	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.*

Definizioni e acronimi

AgID	*Agenzia per l'Italia Digitale* (già CNIPA e DigitPA) - *www.agid.gov.it*. Organismo di Sorveglianza ai sensi del Reg. UE 910/2014 (eIDAS). Nel seguito anche solo *Agenzia*.
QTSP *Qualified Trust Service Provider.* *Certificatore Accreditato*	*Prestatore di Servizi Fiduciari 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)
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.
Cointeressato e Cofirmatario	Soggetto giuridico che rappresenta la controparte nei documenti sottoscritti di cui al par. *F.1.3*

OCSP	Online Certificate Status Protocol: servizio di verifica dello stato di validità del Certificato, secondo il protocollo OCSP.
Documento informatico	Il documento elettronico che contiene la rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti
FEQ - Firma Elettronica Qualificata *FD - Firma Digitale*	Firma elettronica creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche. Coincide, in Italia, con la *Firma Digitale* definita nel CAD, Art.1, comma1, punto s): Firma elettronica qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al Titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità' di un documento informatico o di un insieme di documenti informatici.
Firma Remota	Particolare procedura di firma elettronica qualificata o di firma digitale, generata su HSM custodito e gestito, sotto la responsabilità, dal QTSP (certificatore accreditato), che consente di garantire il controllo esclusivo delle chiavi private da parte dei titolari delle stesse.
HSM - Hardware Security Module	Dispositivi per la creazione della firma elettronica qualificata, se conformi ai requisiti di cui all'Allegato II del Reg. (UE) 910/2014. Anche detti *Dispositivi di Firma*.
Qualified Electronic Time Stamp *(Marca Temporale)*	*Validazione Temporale Elettronica Qualificata* Dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi dati esistevano in quel momento. Risponde ai requisiti dell'Art.42 del Reg. eIDAS
CA - Certification Authority	Autorità che emette i certificati per la firma elettronica.
RA - Registration Authority *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
Registro dei Certificati	La combinazione di uno o più archivi informatici, tenuto dal Certificatore, contenente tutti i Certificati emessi.
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")
Terzo Interessato *(subscriber)*	Il Terzo Interessato è la persona o 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".
Cliente *Cliente Prospect*	È il Cliente (o potenziale cliente, detto Prospect) della Società.
Riferimento Temporale	Informazione contenente la data e l'ora, che viene associata ad uno o più documenti informatici.
TSA - Time Stamping Authority	Autorità che rilascia le validazioni temporali elettroniche.
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

Il presente documento costituisce il Manuale Operativo per il servizio di firma elettronica qualificata (firma digitale) remota (nel seguito, *Manuale Operativo* o anche solo *MO*) del QTSP In.Te.S.A. S.p.A. nell'ambito dei servizi offerti dalla società *Ineo S.r.l., sede legale Via Paolo di Dono, 149 – 00142 Roma, PIVA 11010851001*.

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*") ed è conforme al *Regolamento UE 910/2014* (nel seguito, *Reg. eIDAS*).

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

Questo documento descrive le regole e le procedure operative del *QTSP In.Te.S.A. S.p.A.* (nel seguito, *QTSP INTESA, Certificatore* ovvero anche solo *INTESA*) per l'emissione dei certificati qualificati, la generazione e la verifica della firma elettronica qualificata e le procedure del servizio di validazione temporale in conformità con la vigente normativa nei progetti gestiti dalla società *Ineo S.r.l.*

Ineo è un'impresa che fornisce servizi assimilabili alla prevenzione sul piano amministrativo delle frodi e di digital onboarding con soluzioni proprietarie e in parte brevettate, e ha adottato e reso noto anche al Garante della Privacy, in data 13 marzo 2015, un codice di autodisciplina redatto con altre società antifrode e reperibile all'indirizzo *https://www.ineo.it/deontologico*.

In questa tipologia di progetti, la società Ineo fungerà anche da *Local Registration Authority* (nel seguito, anche solo *LRA*) per conto del QTSP INTESA, in virtù di specifico accordo tra le parti.

In questo contesto, i Titolari di un Certificato Qualificato saranno i soggetti identificati dalla società Ineo, nelle modalità che verranno descritte nel seguito.

Le attività descritte nel presente Manuale Operativo sono svolte in conformità con il Reg. UE 910/2014 (eIDAS) e con la Determinazione AgID 147/2019.

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A., che è Titolare di ogni relativo diritto intellettuale.

Quanto qui descritto per l'espletamento delle attività di QTSP è coperto da diritti sulla proprietà intellettuale.

A.2. Validità

Quanto descritto in questo documento si applica al QTSP INTESA (cioè 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, anche avvalendosi delle marche temporali qualificate emesse dal QTSP 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.

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 QTSP 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 prosieguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento è la versione n. ***02*** del ***Manuale Operativo per le procedure di firma elettronica qualificata remota offerte dalla società Ineo S.r.l.***, emesso in conformità con l'Art.40 del DPCM.

L'object identifier di questo documento è ***1.3.76.21.1.50.15***.

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*
- nel sito istituzionale della società Ineo S.r.l.

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

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

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

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

B.3. Responsabilità del Manuale Operativo

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

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 QTSP vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal QTSP espletando, per la parte di loro competenza, le attività a loro attribuite.

B.4.1.1. Certification Authority (CA)

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

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

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

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

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

B.4.2. Local Registration Authority (LRA)

Per la particolare tipologia di servizio offerto (firma elettronica qualificata remota) descritta nel presente Manuale Operativo, il QTSP INTESA ha demandato lo svolgimento delle funzioni di Registration Authority alla Società Ineo.

La LRA si impegna a svolgere le seguenti attività:

- Identificazione del Titolare;
- Registrazione del Titolare.

La società Ineo, nell'esercizio della funzione di Registration Authority, dovrà vigilare affinché l'attività di riconoscimento venga svolta dai suoi incaricati nel rispetto della normativa vigente e di quanto previsto nel presente Manuale Operativo.

In particolare, Ineo potrà identificare il Titolare anche se questi non si presenterà fisicamente negli uffici della società.

In questo caso Ineo dovrà comunque:

- accertare l'identità tramite documenti, dati o informazioni supplementari quali atti pubblici, scritture private autenticate, dichiarazione dell'Autorità Consolare Italiana, o tramite autenticazione SPID o CIE;
- applicare, a seconda delle modalità di riconoscimento attuate, misure supplementari per la verifica dei documenti forniti quali:
  - controllo tramite sistema Scipafi;
  - Face Matching: confronto tra la fotografia del volto del Richiedente presente sul documento di riconoscimento acquisito e una sua immagine live raccolta dall'operatore tramite il dispositivo in dotazione (attività eseguite solo dopo aver raccolto il consenso espresso da parte del Richiedente e nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.2 e Par 9.2.3);
  - riprese Video con interazione del Richiedente chiamato ad effettuare dei movimenti su richiesta;
- ulteriori controlli antifrode utili ad intercettare anche possibili tecniche di Deep Fake nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.2 e Par 9.2.3.

B.4.3. Terzo Interessato

Nell'ambito del presente manuale, la *Società cliente* di Ineo S.r.l. riveste il ruolo di *Terzo interessato*, in qualità di soggetto giuridico che fruisce dei certificati qualificati emessi dal QTSP INTESA a favore dei propri clienti ovvero per i propri dipendenti.

In quest'ottica, la Società 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 della Società, 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.4*.

C. Obblighi

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

Nello svolgimento della sua attività, il Prestatore di Servizi Fiduciari Qualificato (indicato anche come *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 QTSP:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel DPCM e ss.mm.ii.;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo per la generazione delle firme (HSM) abbia i requisiti di sicurezza previsti dall'Art.29 del Reg. eIDAS;
- rilascia e rende pubblico il certificato qualificato, 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 QTSP) assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il QTSP;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.
- fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali (Art.14 del DPCM)

Inoltre, il QTSP:

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

- 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;
- conduce periodicamente verifiche e ispezioni (audit) al fine di vigilare sulle attività delle LRA, riservandosi il diritto di interrompere il servizio qualora, a seguito dei predetti audit, emergesse che le attività di identificazione non venissero espletate in maniera idonea e conforme alle normative vigenti.

C.2. Obblighi del Titolare

Il Titolare riceverà un certificato qualificato per la Firma Elettronica Qualificata Remota, con cui poter sottoscrivere contratti e documenti relativi a prodotti e/o servizi, nelle modalità descritte al par. *I. Modalità operative per la sottoscrizione di documenti*.

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal QTSP, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al QTSP, anche per tramite della LRA, eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- fare immediata denuncia alle Autorità competenti e alla LRA, in caso di perdita o furto dei codici e/o dei dispositivi indicati per accedere alle proprie chiavi di firma; il QTSP provvederà all'immediata revoca del certificato;
- inoltrare eventuali richieste di revoca e di sospensione del certificato qualificato secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

Utilizzatore (*Relying Party*) è chiunque riceva un documento firmato digitalmente e, al fine di verificarne la validità, si avvalga del Certificato Qualificato utilizzato dal Titolare per firmare il documento stesso.

La verifica della firma digitale e la successiva estrazione degli oggetti firmati può essere effettuata con qualsiasi software in grado di elaborare file firmati in conformità al Reg. eIDAS.

Coloro che si avvalgono di un Certificato Qualificato per verificare la validità di un documento firmato digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato dagli standard vigenti al momento della sua emissione;
- verificare lo stato di validità del certificato mediante il protocollo OCSP o tramite l'accesso alle Liste di Revoca;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei QTSP;
- verificare l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare.

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, nei servizi descritti dal presente Manuale Operativo, è il soggetto giuridico che ha deciso di avvalersi dei servizi offerti da Ineo anche quale LRA. Nel presente documento è indicata anche solo come *Società*.

Pertanto, tale Società, nella veste di Terzo Interessato:

- verifica che il proprio cliente sia titolato ad avviare la procedura per richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota.
- svolge un'attività di supporto al Titolare
- indica al QTSP eventuali ulteriori limitazioni di utilizzo del Certificato Qualificato per la Firma Digitale oltre a quelle previste al par. *F.2.1*.

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

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 di clientela (es. chiusura del rapporto bancario)

La richiesta di revoca o sospensione da parte del Terzo Interessato pervenuta alla LRA 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.

C.5. Obblighi delle Registration Authority esterne (LRA)

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.

Per le attività descritte nel presente Manuale Operativo **il QTSP In.Te.S.A. S.p.A. demanda a Ineo S.r.l. lo svolgimento della funzione di Registration Authority mediante specifico *Contratto di Mandato*, sottoscritto da entrambe le parti.**

In particolare, la società Ineo, come RA esterna, dovrà espleta le seguenti attività:

- identificazione con certezza del richiedente la certificazione (in seguito Titolare del certificato);
- registrazione del richiedente / Titolare;
- verificare che al Titolare vengano consegnati dei dispositivi e/o codici che gli permetteranno di accedere alla propria chiave di firma nel rispetto degli Art.8 e 11 comma 2 del DPCM;
- invio della documentazione sottoscritta all'Ufficio RA del QTSP INTESA, salvo differenti accordi riportati sul contratto di mandato.

Nel Contratto di Mandato sono esplicitati gli obblighi cui si deve attenere la società Ineo, cui il QTSP INTESA ha assegnato l'incarico di LRA, e sui quali il QTSP ha l'obbligo di vigilare.

In particolare, si richiede alla LRA di:

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

C.5.1. Identificazione del Titolare

Il servizio di identificazione può essere gestito con le seguenti modalità:

- ***Riconoscimento de visu (in presenza)*** - Ineo, in qualità di Local RA, tramite personale proprio o di terzi appositamente autorizzati dal QTSP, verifica con certezza, *de visu in presenza*, l'identità del richiedente alla prima richiesta di emissione di certificato qualificato di firma.

- ***Riconoscimento de visu (da remoto)*** - Il richiedente, al fine di procedere all'identificazione finalizzata al rilascio di un certificato qualificato di firma, può richiedere un'identificazione da remoto. A tal fine, il Richiedente dovrà preventivamente registrarsi sulla piattaforma online gestita da Ineo, dove potrà anche prenotare una sessione di video identificazione, al termine della quale potrà essere emesso un certificato qualificato
- ***Riconoscimento stand alone (con supervisione offline)*** - per mezzo di un'applicazione sviluppata ad hoc da Ineo, il richiedente potrà gestire in "quasi" totale autonomia la fase di identificazione e richiesta del certificato di firma digitale. L'identificazione viene, in questo caso, realizzata sfruttando un'apposita piattaforma tecnologica che è in grado di coadiuvare e rendere maggiormente sicura e affidabile l'attività del richiedente.
- ***Identificazione a distanza tramite firma elettronica qualificata*** - basata sul riconoscimento effettuato da altro Prestatore di Servizi Fiduciari Qualificato eIDAS.
- ***Riconoscimento basato sull'utilizzo di altro mezzo d'identificazione elettronica*** notificato ai sensi del Regolamento europeo 910/2014- eIDAS.

Le sopra citate modalità sono descritte più dettagliatamente al par. *F.1. Identificazione degli utenti*.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del QTSP – Limitazione agli indennizzi

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

INTESA, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, Art.13), non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'Art.5 del DPCM, e in particolare dal mancato rispetto da parte del Titolare e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e/o dalla mancata osservanza da parte degli stessi della normativa vigente.

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

Il QTSP INTESA non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al par. *F.2.1*.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal certificatore accreditato. Si ricorda, in particolare, di conservare con la dovuta diligenza i dispositivi OTP e i codici segreti indispensabili per accedere alle chiavi di firma.

D.2. Assicurazione

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

Di tali contratti è resa disponibile ad AgID apposita dichiarazione di stipula.

E. Tariffe

Le Tariffe per l'emissione, rinnovo, revoca e sospensione del certificato qualificato saranno indicate nei contratti stipulati tra Ineo e le imprese che si avvalgono dei servizi descritti nel presente manuale operativo.

F. Modalità di identificazione e registrazione degli utenti

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

La suddetta operazione può essere demandata a Ineo che, in qualità di LRA e in ottemperanza con quanto previsto dalla vigente normativa anche in materia di Antiriciclaggio laddove applicabile, 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 QTSP attraverso Ineo gli eventuali cambiamenti relativi ai propri dati di registrazione.

Al termine di questa fase di registrazione, al Titolare potrà essere rilasciato in comodato d'uso un dispositivo One Time Password dotato di display e in grado di generare codici numerici monouso (chiamati nel seguito *codici OTP* o semplicemente *OTP*).

In alternativa ad un token OTP fisico, la società che ha deciso di avvalersi dei servizi di Ineo potrà indicare ai Titolari come attivare un sistema di autenticazione software per dispositivi mobili (qualora il Titolare ne disponesse di uno e scegliesse questa modalità come preferibile per comodità d'uso rispetto all'impiego di un Token fisico). Tale sistema software permetterà la generazione di una One Time Password sul dispositivo mobile del Titolare e potrà essere pertanto utilizzato come strumento di autenticazione ai sistemi di firma remota.

Oltre all'OTP, saranno forniti al Titolare tutte le informazioni necessarie e un *Personal Identification Number* (*PIN*) che possano garantirgli un accesso sicuro al servizio di firma remota resogli disponibile dal QTSP Intesa.

Lo stesso PIN potrà essere utilizzato come *codice di emergenza* (in caso, ad esempio, di smarrimento e/o perdita del Token OTP o del mobile) per *sospendere con urgenza* il certificato qualificato a lui intestato (par. *H.3.1*).

Il PIN potrà essere successivamente modificato o aggiornato dal Titolare usufruendo dei servizi che Ineo gli avrà messo a disposizione direttamente nella sua stessa piattaforma attraverso l'area riservata dedicata.

In questa fase vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in 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 è conservata per 20 (venti) anni.

F.1. Identificazione degli utenti

Sono di seguito descritte le modalità di identificazione previste nell'ambito di quanto riportato nel presente MO ai fini del rilascio di un certificato qualificato di firma elettronica.

F.1.1. Identificazione de visu – in presenza

L'identificazione certa viene supportata da un'apposita APP mobile sviluppata da Ineo che è in grado di coadiuvare e rendere maggiormente sicura e affidabile l'attività di identificazione in presenza svolta dall'operatore di LRA (nel seguito, *APP Ineo*).

L'operatore di LRA sarà preventivamente identificato con certezza e incaricato da Ineo attraverso una procedura scritta che sarà da questi controfirmata (vedi Allegato 2 su abilitazione APP Ineo)

L'APP Ineo verifica che il telefono non sia in modalità root durante la installazione o durante l'avviamento e il funzionamento.

Nello specifico:

- l'operatore, dotato di smartphone o tablet appositamente configurato e dotato dell'APP Ineo, si autentica tramite proprio PIN;
- seguendo le istruzioni fornite dall'APP Ineo, l'Operatore identifica il cliente mediante un documento di riconoscimento in corso di validità e ne acquisisce copia informatica tramite la fotocamera del dispositivo in dotazione;
- con le stesse modalità prende visione e acquisisce copia della tessera sanitaria;

- l'operatore raccoglie i seguenti dati del Richiedente:
  - ente richiedente;
  - cognome e nome;
  - data e luogo di nascita;
  - codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano);
  - nazione di residenza;
  - numero di telefono (mobile);
  - indirizzo di posta elettronica;
  - eventuale indirizzo PEC;
- l'APP, tramite le informazioni raccolte dal dispositivo utilizzato, memorizza luogo e ora dell'incontro con il richiedente, se previsto nel rapporto commerciale/convenzionale[1] tra l'erogatore del servizio (soggetto obbligato) per il quale si sta richiedendo la Firma, ad esempio nel caso di un finanziamento, la Banca o l'operatore LRA, ad esempio l'agente e Ineo.

Qualora il documento di riconoscimento presentato dal Richiedente sia una Carta d'Identità Elettronica di ultima generazione (cd. CIE 3.0), l'APP Ineo permette anche la lettura, tramite tecnologia NFC, del certificato digitale contenuto nella CIE.

L'APP Ineo, elaborando le operazioni raccolte, rende disponibili al Richiedente, per una sua sottoscrizione, i seguenti documenti:

- il contratto di servizio;
- il documento Modulo Richiesta Certificato Digitale;
- il documento Presa visione del Manuale Operativo INTESA;
- il documento Dichiarazione di autorizzazione al trattamento dei dati personali, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del Regolamento UE 679/2016.

I documenti vengono resi disponibili al richiedente, tramite l'operatore che li sottoporrà al Richiedente, o anche direttamente attraverso l'accesso alla sua area riservata; tale accesso potrà avvenire tramite l'invio di un link protetto da credenziale nota solo all'operatore e il Richiedente, o in alternativa, tramite la generazione di un QR code sull'APP Ineo che il Titolare inquadra con il proprio smartphone confermando anche il contatto fisico con l'operatore.

La documentazione così predisposta viene visionata dal Richiedente che procede alla sua sottoscrizione mediante OTP comunicato tramite SMS al numero di cellulare dichiarato dal Richiedente stesso.

In alcuni contesti, come ad esempio quello bancario, l'attività d'identificazione viene svolta anche con finalità ulteriori (ad esempio quella richiesta dalla normativa Antiriciclaggio di cui al D.lgs. 231/2007 e ss.mm.ii.) e mediante specifiche e innovative misure tecniche che si aggiungono ai controlli standard (tipo Scipafi):

- Controllo antifrode sul documento e sui dati inseriti dall'Operatore.
- Face Matching, opzionale ed eventuale sulla base di quanto definito a monte dal Richiedente (ad esempio, Banca in caso di finanziamento), confronto tra la fotografia del volto del Richiedente presente sul documento di riconoscimento acquisito e una sua immagine live raccolta dall'operatore tramite il dispositivo in dotazione (attività eseguite solo dopo aver raccolto il consenso espresso da parte del Richiedente e nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.2 e Par 9.2.3).

Le misure indicate nell'elenco di cui sopra sono opzionali in quanto il riconoscimento avviene de-visu.

L'attività d'identificazione comporta la produzione di un apposito Report, il quale riporta le informazioni (dati identificativi, data, ora e luogo) relative all'incontro tra Operatore LRA e Richiedente, comprensivo del risultato, se eventualmente effettuate, delle analisi antifrode e antiriciclaggio. Al raggiungimento del risultato minimo atteso dai controlli previsti, l'Operatore, raccolte le sottoscrizioni elettroniche del Richiedente, invierà richiesta di emissione del certificato qualificato al QTSP.

[1] Per rapporto convenzionale/commerciale si intende il rapporto in essere tra Ineo e lo specifico soggetto obbligato a cui Ineo, in qualità di terzo rispetto al soggetto obbligato, offre servizi per l'assolvimento degli obblighi di AV ai sensi dell'Art 26 del 231.

Tali attività potranno svolgersi non solo presso un ufficio, ma anche presso la residenza/domicilio del Richiedente qualora questi chieda di essere contattato da un operatore di Ineo che, fissatogli un appuntamento, assisterà il Richiedente in tutte le procedure inerenti l'identificazione e quelle successive di richiesta di un certificato di firma elettronica qualificata.

F.1.2. Identificazione de visu – da remoto

Il Richiedente riceverà un magic link e accederà ad una area riservata della piattaforma web Ineo e nella quale potrà:

- decidere se avvalersi della autenticazione tramite SPID o per la identificazione (in quest'ultimo caso il Richiedente dovrà scaricare l'App Mobile e si procederà come previsto al par. *F.1.3.2*);
- inserire o validare i suoi dati personali (nel caso in cui i suoi dati siano forniti già alla società cliente di Ineo che li avrà raccolti prima della identificazione per cercare di accelerare poi tutti i passi successivi);
- caricare le immagini dei suoi documenti di identità;
- generare e inserire un OTP SMS
- prenotare la Video call in cui verrà effettuato il riconoscimento.

Alla data e all'ora fissata, il Richiedente accederà alla piattaforma tramite un link autogenerato con token di sicurezza integrato per un accesso univoco alla piattaforma.

Il sistema richiederà l'accesso al microfono e alla webcam del PC o dello smartphone in uso al Richiedente tramite il quale verrà effettuata la video call.

L'operatore, anche esso autenticato in modo sicuro alla piattaforma, avrà a disposizione un'apposita schermata che, oltre all'audio e al video del Richiedente, renderà disponibile un elenco guidato di tutti i passaggi che dovranno essere eseguiti ai fini del video-riconoscimento.

L'Operatore, preliminarmente, verificherà che il collegamento audio-video attivato rispetti le seguenti condizioni:

- le immagini video sono a colori e consentono una visualizzazione chiara del Richiedente in termini di luminosità, nitidezza, contrasto, fluidità delle immagini;
- l'audio è chiaramente udibile, privo di distorsioni o disturbi evidenti;

La sessione audio/video, che ha per oggetto le immagini video e l'audio del Richiedente e dell'Operatore, dovrà essere effettuata in ambienti privi di particolari elementi di disturbo.

Confermata l'adeguatezza del collegamento audio/video, l'Operatore che effettua l'identificazione avvia il processo che non potrà essere interrotto e che consta dei seguenti passi:

a) acquisisce il consenso alla videoregistrazione e alla sua conservazione e informa che la videoregistrazione sarà conservata in modalità protetta per 20 (venti) anni;
b) fornisce l'informativa relativa ai trattamenti effettuati mediante la piattaforma *Ineo Sign* e richiede tutti i consensi necessari ai trattamenti previsti e comunicati al richiedente;
c) dichiara le proprie generalità;
d) acquisisce i dati identificativi forniti dal Richiedente e ne richiede la conferma;
e) chiede al Richiedente di confermare la data e l'ora della registrazione;
f) chiede conferma della volontà del Richiedente di voler ricevere il certificato qualificato e conferma i dati identificativi e gli altri dati inseriti nella modulistica online in fase di preregistrazione;
g) chiede conferma del numero di telefonia mobile e l'indirizzo e-mail del Richiedente;
h) verifica e-mail e numero di telefono mobile forniti dal Richiedente mediante invio di un SMS e di una mail contenente un link ad una URL appositamente predisposta per la verifica;
i) richiede l'esibizione davanti alla webcam di un documento d'identità valido, munito di fotografia recente e riconoscibile e di firma autografa del richiedente, rilasciato da un'amministrazione pubblica; il sistema ne acquisisce una copia per immagine;
j) richiede l'esibizione tramite webcam della tessera sanitaria in corso di validità (o di altro documento equivalente in caso di cittadino straniero), verifica il codice fiscale e ne acquisisce copia per immagine;
k) richiede al cliente di compiere una o più azioni casuali per rafforzare l'autenticità della interlocuzione;

l) richiede conferma dei dati raccolti, dei consensi al trattamento dati richiesti e della volontà di richiedere, alle condizioni previste e conosciute dal Richiedente, il rilascio di un certificato di firma qualificata.

L'operatore che effettua l'identificazione può escludere l'ammissibilità della sessione audio/video per qualunque ragione, inclusa l'eventuale inadeguatezza del documento presentato dal cliente.

La sessione audio/video è composta da più riprese ciascuna delle quali di durata non inferiore ai 2 minuti secondi.

La sessione audio/video è interamente registrata e conservata per 20 (venti) anni a cura di Ineo mediante apposito sistema di conservazione a norma fornito da un conservatore accreditato presso AgID per la conservazione a norma di documenti informatici.

In alcuni contesti, come ad esempio quello bancario, l'attività d'identificazione viene svolta anche con finalità ulteriori (ad esempio quella richiesta dalla normativa Antiriciclaggio di cui al D.lgs. 231/2007 s.m.i.) e mediante specifiche e innovative misure tecniche che si aggiungono ai controlli standard (tipo Scipafi):

- Controllo antifrode sul documento e sui dati inseriti dall'Operatore.
- Controllo Scipafi (solo in casi d'uso bancario e se Ineo è delegata dal soggetto obbligato aderente a Scipafi).
- Face Matching (confronto tra la fotografia del volto del Richiedente presente sul documento di riconoscimento acquisito e una sua immagine live raccolta dall'operatore tramite il dispositivo in dotazione).
- Controlli antifrode utili ad intercettare possibili tecniche di Deep Fake nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.2 e Par 9.2.3.

Tutte le attività sono eseguite solo dopo aver raccolto il consenso espresso da parte del Richiedente.

A seguito delle ulteriori attività di verifica dell'identità del Richiedente viene prodotto un apposito Report che riporta i risultati delle analisi antifrode ed eventuale antiriciclaggio. Il Report prodotto verrà conservato unitamente alla videoregistrazione e alle altre informazioni previste.

F.1.3. Riconoscimento stand-alone

F.1.3.1. Stand-alone con piattaforma WEB e supervisione offline ambito chiuso di utenti

Questa modalità di identificazione utilizza una piattaforma tecnologica appositamente studiata per permettere al richiedente di operare in autonomia garantendo comunque elevati standard di sicurezza come meglio di seguito specificato.

L'operatore non effettuerà l'identificazione qualora la qualità audio/video non sia ritenuta adeguata a consentire l'identificazione del Richiedente (la risoluzione minima accettata non potrà essere inferiore a 1080 X 720 pixel).

La sessione audio/video è unica e composta da più video e l'intero processo non potrà essere interrotto una volta avviato.

Gli step iniziali della procedura sono i seguenti:

- il Richiedente accede alla piattaforma, tramite link inviatogli e può farlo da smartphone, tablet o da PC; in questo ultimo caso il sistema verifica le caratteristiche tecniche della videocamera disponibile e nel caso non siano sufficienti genera un QR code per continuare la navigazione nella stessa area riservata tramite Mobile o Tablet;

- il Richiedente viene informato sui trattamenti effettuati tramite la procedura, fornisce gli eventuali consensi al trattamento e inserisce i propri dati personali o modifica/conferma gli stessi catturati prima dal riconoscimento biometrico dei documenti in base alla procedura utilizzata:
  - cognome e nome;
  - data e luogo di nascita;
  - codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano);
  - nazione di residenza
  - numero di telefono (mobile);
  - indirizzo di posta elettronica;
  - eventuale indirizzo PEC;
- si avvia la cattura, tramite procedura guidata, del fronte e retro di un documento di identità e della tessera sanitaria, allegando il File o fotografando i documenti tramite l'uso del dispositivo mobile personale;
- Si procede quindi alle riprese Video con le interazioni del Richiedente finalizzate a scongiurare tentativi di frode. Una delle azioni consiste nella registrazione di un video in cui il Richiedente mostra il documento di identità precedentemente allegato.

Si precisa che Il processo , nel rispetto di quanto previsto da standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3.

La piattaforma di Ineo, elaborando le informazioni raccolte, rende quindi disponibili al Richiedente una serie di documenti per i quali è richiesta la sua sottoscrizione:

- il contratto di servizio;
- il documento Modulo Richiesta Certificato Digitale;
- il documento Presa visione del Manuale Operativo INTESA;
- il documento Dichiarazione di autorizzazione al trattamento dei dati personali, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del Regolamento UE 679/2016.
- I documenti per la cui firma è stata fatta richiesta di questo processo da parte del Cliente.

La documentazione così predisposta viene visionata dal Richiedente che procede alla sua convalida mediante inserimento di una OTP comunicata tramite SMS al numero di cellulare dichiarato dal Richiedente stesso unitamente alla documentazione del soggetto richiedente da firmare.
Il processo, quindi, prosegue con l'attività di validazione da parte di un operatore Ineo che dovrà validare il processo verificando i controlli antifrode, analizzando il relativo Report prodotto automaticamente e verificando le immagini del documento con i dati inseriti e con le immagini dei volti (live e documento) e controllando i Video Live registrati con le interazioni richieste al Richiedente.

Esclusivamente nel caso in cui l'esito di tali controlli si completi positivamente, e il titolare risulti identificato, si potrà procedere con il completamento del riconoscimento e con la controfirma dei documenti da parte del Cliente di Ineo come descritto nel seguito. Nello specifico, questo tipo di casi d'uso indirizza il rilascio del Certificato Qualificato in quelle circostanze riconducibili a limitati utilizzi della firma elettronica qualificata in contesti chiusi di utenti. Tipico è il caso in cui l'oggetto della sottoscrizione è un contratto, anche composto da più documenti informatici.

Questo tipo di certificati, in piena aderenza alle previsioni contenute nella comunicazione AgID 0016101.07-06-2016, in presenza di determinati vincoli di dominio e di ambiti di utilizzo, consente l'uso della firma digitale prima di aver ultimato il dovuto processo di verifica dell'identità del titolare, alle seguenti condizioni:

Restrizione	*Responsabilità*
1. Il processo è riconducibile esclusivamente a sistemi di firma remota;	Certificatore
2. L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;	Certificatore
3. Nel certificato qualificato del titolare devono essere presenti stringenti limiti d'uso afferenti il rapporto specifico fra Titolare e cointeressato e cofirmatario (par. F.2.1);	Certificatore

4. Il certificato deve essere chiaramente distinguibile da quelli emessi con procedure più tradizionali. Il certificato qualificato del titolare deve contenere uno specifico OID, riscontrabile nel documento *CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico*, pubblicato all'URL https://www.intesa.it/e-trustcom/, in cui è descritto questo particolare processo e il suo ristretto ambito);	Certificatore
5. Devono sussistere stringenti limiti applicativi. L'applicazione che richiede la firma remota deve limitare i possibili oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario;	Cointeressato e Cofirmatario
6. Nel caso in cui la verifica dell'identità del titolare avvenga per mezzo di un incontro fisico fra titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario, se diverso dal certificatore;	Certificatore
7. Il cointeressato e cofirmatario può espletare la verifica dell'identità in vece del certificatore, attraverso sessioni audio-video, attraverso le procedure indicate dal certificatore e approvate dall'AgID, ovvero in applicazione della normativa afferente la verifica dell'identità di cui al D.lgs. 231/2007 e s.m.i., ove applicabile. Qualora, nell'ambito della verifica ai sensi di tale D.lgs., sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;	Cointeressato e Cofirmatario
8. All'apposizione della firma del titolare, il Certificatore si impegna a non apporre la marca temporale.	Certificatore
9. All'apposizione della firma del titolare, il Cointeressato e Cofirmatario si impegna a non apporre la marca temporale.	Cointeressato e Cofirmatario
10. Nel caso in cui il contratto sia costituito da più documenti informatici, che non vengono firmati in modo congiunto dal titolare del certificato e dal Cointeressato e Cofirmatario, la marca temporale, apposta obbligatoriamente solo dopo la firma del Cointeressato e Cofirmatario, deve essere applicata a ciascuno dei documenti firmati che costituiscono, nel loro complesso, il fascicolo contrattuale oggetto di sottoscrizione;	Cointeressato e Cofirmatario
11. Fino all'apposizione delle firme del Cointeressato e Cofirmatario e delle marche di cui al precedente punto 10, l'oggetto sottoscritto dal solo titolare non deve essere fornito ad alcuno e, qualora la verifica dell'identità del titolare non avesse buon fine, deve essere distrutto conservando traccia degli eventi in appositi log. In quest'ultimo caso, quale misura a maggior tutela del Cliente Prospect, il certificato viene revocato.	Cointeressato e Cofirmatario

Come ulteriore accorgimento di sicurezza finalizzato a diminuire l'esposizione dell'utente finale al rischio dell'utilizzo della propria firma digitale, il certificato per firma in ambiti chiusi di utenti prevede un intervallo di tempo massimo per l'espletamento del riconoscimento di 30 giorni.

Nell'ambito di questo intervallo di 30 giorni, nel caso in cui il certificato non sia di tipo one-shot, onde garantire maggior tutela per il sottoscrittore, il certificato viene sospeso cautelativamente e verrà riattivato solo al completamento della verifica dell'identità del sottoscrittore di cui ai punti che seguono.

Si precisa che i certificati così emessi, non di tipo one-shot, una volta espletata positivamente la fase di identificazione del titolare, saranno riattivati ed utilizzati anche successivamente come certificati di firma remota.

Tutte le attività eseguite dall'operatore e i check effettuati vengono registrate nel Report finale che verrà prodotto in PDF in modo tale da essere messo a disposizione sia al Richiedente che al QTSP.

Tale report relativo alle attività di verifica sarà sottoscritto dall'operatore che le ha effettuate riportandone l'esito.

OID Specifico

Per ottemperare al punto 4), il certificato emesso sotto queste condizioni è distinguibile dagli altri certificati in quanto contiene, nel campo *CertificatePolicies*, uno dei seguenti OID (ognuno definito in riferimento alla CA di root che ha emesso il certificato):

- **1.3.76.21.1.3.1.1.1**
- **1.3.76.21.1.5.1.1.1**
- **1.3.76.21.10.2.1.2.1**

F.1.3.2. Stand-alone con APP KYC Ineo e supervisione offline ambito chiuso di utenti

Questa modalità di identificazione prevede il download da parte del Richiedente dell'APP Ineo e permette al Richiedente di operare in autonomia garantendo comunque elevati standard di sicurezza come meglio di seguito specificato.

L'identificazione non potrà essere effettuata qualora la qualità audio/video non sia ritenuta adeguata a consentire l'identificazione del Richiedente (la risoluzione minima accettata non potrà essere inferiore a 1080 X 720 pixel).

La sessione audio/video è unica e composta da più video e l'intero processo non potrà essere interrotto una volta avviato.

Gli step iniziali della procedura sono i seguenti:

- il Richiedente accede all'Applicazione, dotata di elevati livelli di sicurezza che ne impediscono la contraffazione, tramite link inviatogli all'email o altro dato di contatto specificato dal Richiedente nelle fasi iniziali di ingaggio, e può farlo da smartphone, tablet;
- verifica che il telefono non sia in modalità root o jailbreak;
- il Richiedente viene informato sui trattamenti effettuati tramite la procedura, fornisce gli eventuali consensi al trattamento;
- si avvia la cattura, tramite procedura guidata, del fronte e retro di un documento di identità e della tessera sanitaria;
- seguendo le istruzioni fornite dall'Applicazione, il Richiedente riprende il documento di identità (CIE, Carta di identità, Patente, Passaporto); per le carte d'identità cartacee si procederà con una lettura tramite tecniche di OCR. Se presente un lettore RFID sul dispositivo del Richiedente potrà essere letto l'NFC sia per la CIE che per il passaporto (per quest'ultimo documento verrà letto anche l'ICAO). Nel caso di lettura NFC della componente ICAO viene verificata la firma presente sui dati letti dalla componente ICAO, nonché la firma e catena di trust sul certificato che ha firmato i dati letti;
- in caso di Passaporto elettronico e CIE 3 (e qualora non si voglia/possa procedere all'identificazione sfruttandone il relativo certificato di autenticazione) l'App KYC di Ineo riconosce la tipologia di documento e, se previsto dallo specifico accordo con il cliente o requisito relativo al processo di riconoscimento, ne forza la lettura via NFC per il confronto dei dati contenuti nel documento con quelli acquisiti e rappresentati biometricamente dalla ripresa del documento di identità e del volto del prospect di cui al prosieguo del presente paragrafo;

Prima della sessione di face matching viene verificato quanto segue:

- sia utilizzata la telecamera del telefono e non una telecamera virtuale;
- che l'app non giri su un emulatore

Si procede quindi alle riprese Video con le interazioni del Richiedente; una delle azioni consiste nella registrazione di un video in cui il Richiedente mostra il documento di identità precedentemente allegato, nel rispetto di quanto previsto dallo standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3.

Il processo prosegue con l'attività di face matching, nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3, alla quale sono necessariamente associate ulteriori attività di analisi antifrode, come meglio descritto in seguito (vd. più sotto, Controlli antifrode e di liveness).

Nello specifico, viene richiesto un riconoscimento facciale tramite ripresa video live del volto del richiedente, i cui frame vengono salvati limitatamente a quelli utilizzati per la verifica liveness, nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3 (vd. più sotto, Controlli antifrode e di liveness), e viene da subito effettuato un confronto in real time automatico con il volto del documento sulla base della tecnologia di Face Matching brevettata da Ineo.

Tale tecnologia è la stessa adottata nel processo di identificazione valutato conforme all'Art 24, comma 1, lett. d) del Reg. eIDAS da un Conformity Assessment Body.

Al completamento della procedura, è conservato solo l'esito del Face matching e non i dati ricavati dall'analisi del volto. Una immagine frontale viene riprodotta nel report antifrode in PDF insieme alla immagine della foto riportata nel documento di identità.

Si precisa comunque che le evidenze audio e video utilizzate per i controlli descritti nella presente sezione sono conservati per il periodo imposto dalla normativa vigente.

Il richiedente visiona i propri dati personali e modifica/conferma gli stessi catturati prima dal riconoscimento biometrico dei documenti in base alla procedura utilizzata:

- cognome e nome;
- data e luogo di nascita;
- codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano);
- nazione di residenza;
- numero di telefono (mobile);
- indirizzo di posta elettronica; eventuale indirizzo PEC.

L'Applicazione di Ineo, elaborando le informazioni raccolte, rende quindi disponibili al Richiedente una serie di documenti per i quali è richiesta la sua sottoscrizione:

- il contratto di servizio;
- il documento Modulo Richiesta Certificato Digitale;
- il documento Presa visione del Manuale Operativo INTESA;
- il documento Dichiarazione di autorizzazione al trattamento dei dati personali, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del Regolamento UE 679/2016;
- i documenti per la cui firma è stata fatta richiesta di questo processo da parte del Cliente.

La documentazione così predisposta viene visionata dal Richiedente che procede alla sua convalida mediante inserimento di una OTP comunicata tramite SMS al numero di cellulare dichiarato dal Richiedente stesso unitamente alla documentazione del soggetto richiedente da firmare.

Il processo, quindi, prosegue con l'attività di validazione da parte di un operatore Ineo che dovrà validare il processo verificando i controlli antifrode, analizzando il relativo Report prodotto automaticamente e verificando le immagini del documento con i dati inseriti e con le immagini dei volti (live e documento) e controllando i Video Live registrati con le interazioni richieste al Richiedente.

Esclusivamente nel caso in cui l'esito di tali controlli si completi positivamente, ed il titolare risulti identificato, si potrà procedere con il completamento del riconoscimento e con la controfirma dei documenti da parte del Cliente di Ineo come descritto nel seguito.

Nello specifico, questo tipo di casi d'uso indirizza il rilascio del Certificato Qualificato in quelle circostanze riconducibili a limitati utilizzi della firma elettronica qualificata in contesti chiusi di utenti. Tipico è il caso in cui l'oggetto della sottoscrizione è un contratto, anche composto da più documenti informatici.

Questo tipo di certificati, in piena aderenza alle previsioni contenute nella comunicazione AgID 0016101.07-06-2016, in presenza di determinati vincoli di dominio e di ambiti di utilizzo, consente l'uso della firma digitale prima di aver ultimato il dovuto processo di verifica dell'identità del titolare, alle seguenti condizioni:

Restrizione	*Responsabilità*
1. Il processo è riconducibile esclusivamente a sistemi di firma remota;	Certificatore

2.	L'uso della firma digitale deve avvenire in ambiti chiusi di utenti;	Certificatore
3.	Nel certificato qualificato del titolare devono essere presenti stringenti limiti d'uso afferenti il rapporto specifico fra Titolare e cointeressato e cofirmatario (par. F.2.1);	Certificatore
4.	Il certificato deve essere chiaramente distinguibile da quelli emessi con procedure più tradizionali. Il certificato qualificato del titolare deve contenere uno specifico OID, riscontrabile nel documento *CPS - Certification Practice Statement e CP - Certificate Policy per i Certificati Qualificati di Firma Elettronica e di Sigillo Elettronico*, pubblicato all'URL https://www.intesa.it/e-trustcom/, in cui è descritto questo particolare processo e il suo ristretto ambito);	Certificatore
5.	Devono sussistere stringenti limiti applicativi. L'applicazione che richiede la firma remota deve limitare i possibili oggetti di sottoscrizione ai soli documenti proposti dal cointeressato e cofirmatario;	Cointeressato e Cofirmatario
6.	Nel caso in cui la verifica dell'identità del titolare avvenga per mezzo di un incontro fisico fra titolare e addetto alla verifica dell'identità, quest'ultimo deve essere personale del certificatore o soggetto da esso delegato, ma non del cointeressato e cofirmatario, se diverso dal certificatore;	Certificatore
7.	Il cointeressato e cofirmatario può espletare la verifica dell'identità in vece del certificatore, attraverso sessioni audio-video, attraverso le procedure indicate dal certificatore e approvate dall'AgID, ovvero in applicazione della normativa afferente la verifica dell'identità di cui al D.lgs. 231/2007 e s.m.i., ove applicabile. Qualora, nell'ambito della verifica ai sensi di tale D.lgs., sia utilizzato il bonifico bancario, deve essere verificato che tale bonifico provenga da un conto bancario intestato esclusivamente al titolare del certificato;	Cointeressato e Cofirmatario
8.	All'apposizione della firma del titolare, il Certificatore si impegna a non apporre la marca temporale.	Certificatore
9.	All'apposizione della firma del titolare, il Cointeressato e Cofirmatario si impegna a non apporre la marca temporale.	Cointeressato e Cofirmatario
10.	Nel caso in cui il contratto sia costituito da più documenti informatici, che non vengono firmati in modo congiunto dal titolare del certificato e dal Cointeressato e Cofirmatario, la marca temporale, apposta obbligatoriamente solo dopo la firma del Cointeressato e Cofirmatario, deve essere applicata a ciascuno dei documenti firmati che costituiscono, nel loro complesso, il fascicolo contrattuale oggetto di sottoscrizione;	Cointeressato e Cofirmatario
11.	Fino all'apposizione delle firme del Cointeressato e Cofirmatario e delle marche di cui al precedente punto 10, l'oggetto sottoscritto dal solo titolare non deve essere fornito ad alcuno e, qualora la verifica dell'identità del titolare non avesse buon fine, deve essere distrutto conservando traccia degli eventi in appositi log. In quest'ultimo caso, quale misura a maggior tutela del Cliente Prospect, il certificato viene revocato.	Cointeressato e Cofirmatario

Come ulteriore accorgimento di sicurezza finalizzato a diminuire l'esposizione dell'utente finale al rischio dell'utilizzo della propria firma digitale, il certificato per firma in ambiti chiusi di utenti prevede un intervallo di tempo massimo per l'espletamento del riconoscimento di 30 giorni.

Nell'ambito di questo intervallo di 30 giorni, nel caso in cui il certificato non sia di tipo one-shot, onde garantire maggior tutela per il sottoscrittore, il certificato viene sospeso cautelativamente e verrà riattivato solo al completamento della verifica dell'identità del sottoscrittore di cui ai punti che seguono.

Si precisa che i certificati così emessi, non di tipo one-shot, una volta espletata positivamente la fase di identificazione del titolare, saranno riattivati e utilizzati anche successivamente come certificati di firma remota.

Tutte le attività eseguite dall'operatore e i check effettuati vengono registrate nel Report finale che verrà prodotto in PDF in modo tale da essere messo a disposizione sia al Richiedente che al QTSP.
Tale report relativo alle attività di verifica sarà sottoscritto dall'operatore che le ha effettuate riportandone l'esito.

OID Specifico

Per ottemperare al punto 4), il certificato emesso sotto queste condizioni è distinguibile dagli altri certificati in quanto contiene, nel campo *CertificatePolicies*, uno dei seguenti OID (ognuno definito in riferimento alla CA di root che ha emesso il certificato):

- **1.3.76.21.1.3.1.1.1**
- **1.3.76.21.1.5.1.1.1**
- **1.3.76.21.10.2.1.2.1**

F.1.3.3. Stand-alone con piattaforma WEB e supervisione offline

Questa modalità di identificazione utilizza una piattaforma tecnologica appositamente studiata per permettere al richiedente di operare in autonomia garantendo comunque elevati standard di sicurezza come meglio di seguito specificato.

L'operatore non effettuerà l'identificazione qualora la qualità audio/video non sia ritenuta adeguata a consentire l'identificazione del Richiedente (la risoluzione minima accettata non potrà essere inferiore a 1080 X 720 pixel).

La sessione audio/video è unica e composta da più video e l'intero processo non potrà essere interrotto una volta avviato.

Gli step iniziali della procedura sono i seguenti:

- il Richiedente accede alla piattaforma, tramite link inviatogli e può farlo da smartphone, tablet o da PC; in questo ultimo caso il sistema verifica le caratteristiche tecniche della videocamera disponibile e nel caso non siano sufficienti genera un QR code per continuare la navigazione nella stessa area riservata tramite Mobile o Tablet;
- il Richiedente viene informato sui trattamenti effettuati tramite la procedura, fornisce gli eventuali consensi al trattamento e inserisce i propri dati personali o modifica/conferma gli stessi catturati prima dal riconoscimento biometrico dei documenti in base alla procedura utilizzata:
  - cognome e nome;
  - data e luogo di nascita;
  - codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano);
  - nazione di residenza
  - numero di telefono (mobile);
  - indirizzo di posta elettronica;
  - eventuale indirizzo PEC;
- si avvia la cattura, tramite procedura guidata, del fronte e retro di un documento di identità e della tessera sanitaria, allegando il File o fotografando i documenti tramite l'uso del dispositivo mobile personale.

Si procede quindi alle riprese Video con le interazioni del Richiedente finalizzate a scongiurare tentativi di frode; una delle azioni consiste nella registrazione di un video in cui il Richiedente mostra il documento di identità precedentemente allegato, nel rispetto di quanto previsto da standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.2 e Par 9.2.3.

Il processo prosegue con l'attività di validazione da parte di un operatore Ineo che dovrà validare il processo verificando i controlli antifrode, analizzando il relativo Report prodotto automaticamente e verificando le immagini del documento con i dati inseriti e con le immagini dei volti (live e documento) e controllando i Video Live registrati con le interazioni richieste al Richiedente.

Esclusivamente nel caso in cui l'esito di tali controlli si completi positivamente, ed il titolare risulti identificato, si potrà procedere con l'emissione del certificato e l'apposizione della firma secondo quanto riportato nei paragrafi seguenti.

Tutte le attività eseguite dall'operatore e i check effettuati vengono registrate nel Report finale che verrà prodotto in PDF in modo tale da essere messo a disposizione sia al Richiedente che al QTSP.
Tale report relativo alle attività di verifica sarà sottoscritto dall'operatore che le ha effettuate riportandone l'esito

A seguito di esito positivo, La piattaforma di Ineo, elaborando le informazioni raccolte, rende quindi disponibili al Richiedente una serie di documenti per i quali è richiesta la sua sottoscrizione:

- il contratto di servizio;
- il documento Modulo Richiesta Certificato Digitale;
- il documento Presa visione del Manuale Operativo INTESA;
- il documento Dichiarazione di autorizzazione al trattamento dei dati personali, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del Regolamento UE 679/2016;
- I documenti per la cui firma è stata fatta richiesta di questo processo da parte del Cliente.

La documentazione così predisposta viene visionata dal Richiedente che procede alla sua convalida mediante inserimento di una OTP comunicata tramite SMS al numero di cellulare dichiarato dal Richiedente stesso unitamente alla documentazione del soggetto richiedente da firmare.

F.1.3.4. Stand-alone con APP KYC Ineo e supervisione offline

Questa modalità di identificazione prevede il download da parte del Richiedente dell'APP Ineo e permette al Richiedente di operare in autonomia garantendo comunque elevati standard di sicurezza come meglio di seguito specificato.

L'identificazione non potrà essere effettuata qualora la qualità audio/video non sia ritenuta adeguata a consentire l'identificazione del Richiedente (la risoluzione minima accettata non potrà essere inferiore a 1080 X 720 pixel).

La sessione audio/video è unica e composta da più video e l'intero processo non potrà essere interrotto una volta avviato.

Gli step iniziali della procedura sono i seguenti:

- il Richiedente accede all'Applicazione, dotata di elevati livelli di sicurezza che ne impediscono la contraffazione, tramite link inviatogli all'email o altro dato di contatto specificato dal Richiedente nelle fasi iniziali di ingaggio, e può farlo da smartphone, tablet;
- verifica che il telefono non sia in modalità root o jailbreak;
- il Richiedente viene informato sui trattamenti effettuati tramite la procedura, fornisce gli eventuali consensi al trattamento;
- si avvia la cattura, tramite procedura guidata, del fronte e retro di un documento di identità e della tessera sanitaria;
- seguendo le istruzioni fornite dall'Applicazione, il Richiedente riprende il documento di identità (CIE, Carta di identità, Patente, Passaporto); per le carte d'identità cartacee si procederà con una lettura tramite tecniche di OCR. Se presente un lettore RFID sul dispositivo del Richiedente potrà essere letto l'NFC sia per la CIE che per il passaporto (per quest'ultimo documento verrà letto anche l'ICAO).
  Nel caso di lettura NFC della componente ICAO viene verificata la firma presente sui dati letti dalla componente ICAO, nonché la firma e catena di trust sul certificato che ha firmato i dati letti;
- in caso di Passaporto elettronico e CIE 3 (e qualora non si voglia/possa procedere all'identificazione sfruttandone il relativo certificato di autenticazione) l'App KYC di Ineo riconosce la tipologia di documento e, se previsto dallo specifico accordo con il cliente o requisito relativo al processo di riconoscimento, ne forza la lettura viene solo letto l'via NFC del documento elettronico per il confronto dei dati contenuti nel documento con quelli acquisiti e rappresentati biometricamente dalla ripresa del documento di identità di cui al punto successivo e del volto del prospect di cui al prosieguo del presente paragrafo.

Prima della sessione di face matching viene verificato quanto segue:

- sia utilizzata la telecamera del telefono e non una telecamera virtuale
- che l'app non giri su un emulatore

Si procede quindi alle riprese Video con le interazioni del Richiedente; una delle azioni consiste nella registrazione di un video in cui il Richiedente mostra il documento di identità precedentemente allegato, nel rispetto di quanto previsto dallo standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3.

Il processo prosegue con l'attività di face matching, nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3, alla quale sono necessariamente associate ulteriori attività di analisi antifrode, come meglio descritto in seguito (vd. più sotto, Controlli antifrode e di liveness).

Nello specifico, viene richiesto un riconoscimento facciale tramite ripresa video live del volto del richiedente, i cui frame vengono salvati limitatamente a quelli utilizzati per la verifica liveness, nel rispetto dello standard ETSI 119 461 V1.1.1 (2021-07), Par 9.2.3 (vd. più sotto, *Controlli antifrode e di liveness*), e viene da subito effettuato un confronto in real time automatico con il volto del documento sulla base della tecnologia di Face Matching brevettata da Ineo. Tale tecnologia è la stessa adottata nel processo di identificazione valutato da un Conformity Assessment Body conforme all'Art. 24, comma 1, del Reg. eIDAS (lett. d).

Al completamento della procedura, è conservato solo l'esito del Face matching e non i dati ricavati dall'analisi del volto. Una immagine frontale viene riprodotta nel report antifrode in PDF insieme alla immagine della foto riportata nel documento di identità.
Si precisa comunque che le evidenze audio e video utilizzate per i controlli descritti nella presente sezione sono conservati per il periodo imposto dalla normativa vigente.

Il richiedente visiona i propri dati personali e modifica/conferma gli stessi catturati prima dal riconoscimento biometrico dei documenti in base alla procedura utilizzata:

- cognome e nome;
- data e luogo di nascita;
- codice fiscale (o analogo nel caso di cittadini stranieri non in possesso di codice fiscale italiano);
- nazione di residenza;
- numero di telefono (mobile);
- indirizzo di posta elettronica; eventuale indirizzo PEC.

Il processo, quindi, prosegue con l'attività di validazione da parte di un operatore Ineo che dovrà validare il processo verificando i controlli antifrode, analizzando il relativo Report prodotto automaticamente e verificando le immagini del documento con i dati inseriti e con le immagini dei volti (live e documento) e controllando i Video Live registrati con le interazioni richieste al Richiedente.

Esclusivamente nel caso in cui l'esito di tali controlli si completi positivamente, ed il titolare risulti identificato, si potrà procedere con l'emissione del certificato e l'apposizione della firma secondo quanto riportato nei paragrafi seguenti.

Tutte le attività eseguite dall'operatore e i check effettuati vengono registrate nel Report finale che verrà prodotto in PDF in modo tale da essere messo a disposizione sia al Richiedente che al QTSP.
Tale report relativo alle attività di verifica sarà sottoscritto dall'operatore che le ha effettuate riportandone l'esito.

A seguito di esito positivo, l'Applicazione di Ineo, elaborando le informazioni raccolte, rende quindi disponibili al Richiedente una serie di documenti per i quali è richiesta la sua sottoscrizione:

- il contratto di servizio;
- il documento Modulo Richiesta Certificato Digitale;
- il documento Presa visione del Manuale Operativo INTESA;
- il documento Dichiarazione di autorizzazione al trattamento dei dati personali, in duplice copia, in cui dichiara di acconsentire all'utilizzo dei propri dati personali ai sensi del Regolamento UE 679/2016;
- i documenti per la cui firma è stata fatta richiesta di questo processo da parte del Cliente.

La documentazione così predisposta viene visionata dal Richiedente che procede alla sua convalida mediante inserimento di una OTP comunicata tramite SMS al numero di cellulare dichiarato dal Richiedente stesso unitamente alla documentazione del soggetto richiedente da firmare.

F.1.4. Riconoscimento basato sull'utilizzo di altro mezzo d'identificazione elettronica notificato ai sensi del Regolamento europeo 910/2014- eIDAS

Questa modalità prevede che il richiedente sia in possesso di uno dei mezzi di identificazione elettronica di seguito elencati:

- SPID

Nel caso di utilizzo di SPID, il Titolare, utilizzando le credenziali di livello 2 o superiore, è chiamato ad effettuare un'autenticazione su di un portale di una RA o di una sua LRA attraverso meccanismi del circuito SPID.

La richiesta e il rilascio del certificato avvengono in conformità all'Avviso n. 17 di AgID del 24 gennaio 2019 recante "Utilizzo identità digitali SPID al fine di rilasciare certificati qualificati". In particolare, il certificato conterrà l'OID 1.3.76.16.5, registrato dall'Agenzia, con la seguente descrizione: *"Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require other SPID digital identity".*

I dati di identificazione e registrazione, rappresentati dalle asserzioni scambiate tra il SP (Ineo) e l'IdP, sono conservati, in questi casi, esclusivamente in formato elettronico da parte della LRA e per il periodo imposto dalla normativa vigente in materia di firma elettronica qualificata.

F.1.5. Identificazione tramite credenziali utilizzate per l'emissione di un precedente certificato one-shot

In questa modalità, il Certificatore si basa sull'identificazione già effettuata durante l'emissione di un precedente certificato one-shot.

Possono essere individuati due tipi di casistiche:

a) Il certificato one-shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso nell'ambito della stessa sessione o processo di firma in cui è stato rilasciato il precedente certificato one-shot.

b) Il certificato one shot, rilasciato mediante le credenziali di un precedente certificato one-shot, viene emesso in una differente sessione o processo di firma.

Nel caso a): il Richiedente, in possesso dell'e-mail e del numero di cellulare certificati dal Certificatore nel corso del rilascio del precedente certificato one shot, può richiedere il rilascio del nuovo certificato one-shot solo dopo aver ricevuto, sull'e-mail e sul cellulare certificati, i nuovi codici One-Time, che dovranno essere verificati dal Richiedente per l'emissione e per l'utilizzo del nuovo certificato, purché ciò avvenga all'interno della stessa sessione o processo di firma.

Nel caso b): il Richiedente, già in possesso di credenziali fornite dal Certificatore o dalla LRA, si autentica al portale del Certificatore o della LRA e chiede l'emissione di un nuovo certificato one-shot, previa la conferma o l'aggiornamento dei dati di registrazione. E-mail e cellulare precedentemente certificati non potranno essere variati. In questo caso, per il rilascio e l'utilizzo del certificato è necessario che il Titolare inserisca la One-Time Password inviata al suo dispositivo OTP, ovvero OTP/SMS su cellulare, e che sia data l'autorizzazione a procedere dalla LRA o dal Terzo Interessato.

Qualora il Certificatore, durante il processo di emissione del precedente certificato one-shot, abbia certificato il possesso di strumenti di Strong Customer Authentication (SCA) riconducibili allo specifico Richiedente, tali credenziali SCA potranno essere utilizzate in luogo dei codici One-Time inviati su e-mail e cellulare nel caso a), ovvero dell'accesso all'area riservata e invio di OTP/SMS nel caso b).

F.2. Registrazione degli utenti richiedenti la certificazione

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi della Certification Authority.

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

F.2.1. Limiti d'uso

Nel Certificato Qualificato per la firma elettronica, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti dalla Società (l'impresa che si avvale dei servizi di Ineo), è inserito sempre un limite d'uso, che deve essere riportato sia in lingua italiana, sia in lingua inglese.

La formula standard è la seguente:

"L'utilizzo del certificato è limitato ai rapporti con Nome Società."

"This certificate may only be used in dealings with Nome Società."

Oppure*:*

"L'utilizzo del certificato è limitato ai rapporti con Ineo o con le società da cui ha ricevuto delega per offrire servizi per la stipula dei contratti."

"The use of the certificate is limited to relations with Ineo or with the companies from which it has been delegated to offer the service to conclude contracts."

Specifici limiti d'uso potranno essere concordati con la Società.

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.

F.2.2. 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.

Copia di tale documentazione viene conservata per 20 (venti) anni.

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.

Il QTSP INTESA non assume alcuna responsabilità, fatti salvi i *casi di dolo o colpa* (Reg. eIDAS, Art.13), per l'eventuale inserimento nel certificato di informazioni autocertificate dal Titolare.

F.2.3. Poteri di rappresentanza

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di poteri di rappresentanza (e.g. 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 e una dichiarazione dell'organizzazione o dell'ente di appartenenza, mediante la quale l'ente o l'organizzazione autorizza il QTSP 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 od organizzazioni di diritto pubblico sarà subordinato a specifici accordi con gli enti stessi. Sulla base di tali accordi sarà possibile specificare il ruolo ricoperto dal Titolare all'interno dell'ente o organizzazione pubblica.

La documentazione prodotta sarà conservata 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.2.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno Pseudonimo in alternativa ai propri dati reali.

Le informazioni relative alla reale identità dell'utente saranno conservate per 20 (venti) anni decorrenti dall'emissione del certificato.

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

G.1. Generazione delle chiavi di certificazione

La generazione delle chiavi all'interno dei dispositivi di firma avviene in presenza del Responsabile 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 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 dispositivi permettano di operare con gli opportuni privilegi. Pertanto, essi vengono custodite in apposite casseforti distinte.

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

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

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

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

G.3. Generazione delle chiavi di sottoscrizione

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

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato in una delle modalità descritte al par. *I. Modalità operative per la sottoscrizione di documenti*.

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 certificazione è conforme alla normativa tempo per tempo vigente.

H. Modalità di emissione dei certificati

H.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel par. *G.1*, sono generati i certificati delle chiavi pubbliche, conformemente con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

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

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate dall'Agenzia per la sottoscrizione dell'elenco pubblico dei 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).

H.2. Procedura di emissione dei Certificati di sottoscrizione

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

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel par. *G.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 alla Certification Authority del QTSP.

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

H.3. Informazioni contenute nei certificati di sottoscrizione

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

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

Ogni Certificato Qualificato per la firma elettronica è conforme al Regolamento eIDAS e alla DETERMINAZIONE AgID N. 147/2019 (*Linee guida contenenti le Regole Tecniche e Raccomandazioni afferenti la generazione di certificati*).

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale contengono una limitazione d'uso (par. *F.2.1*).

H.3.1. Codice di Emergenza

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

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

I. Modalità operative per la sottoscrizione di documenti

Il QTSP INTESA, attraverso i propri servizi di firma remota , rende disponibile ai Titolari quanto necessario a generare firme elettroniche qualificate conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia di servizio non richiede la fornitura di un'applicazione di firma da installare sul proprio personal computer, ma piuttosto delle funzionalità di firma richiamabili da un'applicazione Web di Ineo o dall'applicazione di firma resa disponibile dal soggetto obbligato AML che fanno già uso di certificati qualificati del QTSP Intesa.

Tale applicazione gestirà esclusivamente gli aspetti di visualizzazione del documento e ingaggio del processo di firma.

Le funzionalità di autenticazione e gestione della busta crittografica verranno assolte da componenti applicative fornite dal QTSP o fornite da terze parti opportunamente autorizzate dall'AgID.

Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno assolutamente conformi a quanto previsto dal DPCM all'Art.4 comma 2 relativamente agli algoritmi utilizzati.

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

Vengono di seguito descritte alcune modalità di autenticazione che, nel rispetto della normativa vigente, permettono ad un Titolare, una volta registrato, di procedere prima con la generazione delle chiavi di firma e richiesta di un certificato qualificato e poi di utilizzare le stesse per effettuare firme elettroniche qualificate.

A conferma dell'effettuazione delle operazioni di firma saranno inviati SMS. Qualora il Titolare disponga di uno smartphone abilitato alla lettura della corrispondenza, su richiesta del Titolare stesso, in alternativa, potranno essere inviati e-mail. Qualora il Titolare utilizzi l'applicazione Mobile, in alternativa, potranno essere mandate notifiche push sullo smartphone abilitato.

I.1. Autenticazione di tipo OTP Mobile

Uno degli strumenti di autenticazione maggiormente diffusi e applicabile in vari contesti applicativi è la soluzione denominata "*OTP Mobile*".

Durante la fase di identificazione il Titolare comunicherà il proprio numero di cellulare che verrà immediatamente verificato essere effettivamente in suo possesso.

Al momento della richiesta del certificato il Titolare sceglierà poi anche un PIN da associare al certificato.

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

1. Il Titolare si connette all'applicazione attraverso il link mandato su uno dei suoi riferimenti verificati (mail o cellulare) o semplicemente attraverso i suoi codici personali.
2. Seleziona e verifica il documento da firmare.
3. Inserisce quindi il suo PIN.
4. Riceve un OTP mobile/sms e lo inserisce successivamente al PIN.
5. Il sistema, rilevando la correttezza del PIN e dell'OTP mobile appena inseriti, procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa.

Qualora i documenti da firmare fossero più di uno, il Titolare deve reiterare i passi dal 2 al 5 per ogni documento.

Rimanendo nel caso di un processo di firma che avvenga in una stazione presidiata da un operatore, il Titolare potrà ricevere il codice OTP anche via SMS sul proprio dispositivo mobile (precedentemente censito secondo le procedure previste da Ineo). Inoltre, se la postazione presidiata è dotata di un tablet in grado di recepire attraverso una tastiera virtuale l'inserimento dell'OTP, il Titolare, una volta ricevuto lo stesso, potrà digitarlo alla presenza dell'operatore sul tablet stesso, confermando così la volontà di procedere con la firma del documento.

I.2. Firma con certificato di validità temporale limitata ("one shot")

Il TSP INTESA offre un servizio Firma Digitale, generata su HSM e conforme alla normativa vigente, mediante l'utilizzo di un certificato a validità temporale limitata (tipicamente 30 minuti dall'emissione o come altrimenti concordato con il cliente / terzo interessato). Essa è generata su di un HSM custodito e gestito sotto la responsabilità del TSP INTESA.

Il Titolare attiva la procedura di firma mediante sistemi di autenticazione consentiti dalla normativa vigente in materia.

Per questa tipologia di certificato, non è prevista la revoca o la sospensione. E' previsto uno specifico limite d'uso, da concordare con il cliente.

Conformemente alla normativa, viene inserita anche la marca temporale generata dal servizio di validazione temporale, descritto al par. *Q Modalità per l'apposizione e la definizione del riferimento temporale*.

J. Modalità operative per la verifica della firma

I documenti sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF: tale formato di sottoscrizione è considerato infatti di facile utilizzo nell'ambito, ad esempio, delle applicazioni bancarie o finanziarie.

La verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software *Acrobat Reader DC*, applicazione in grado di verificare tutte le tipologie di firma elettronica qualificata in formato PDF prodotte nell'Unione Europea in conformità con il Regolamento eIDAS.

Acrobat Reader DC è scaricabile gratuitamente dal sito di Adobe, *www.adobe.com/it/*

K. Modalità di revoca e sospensione dei certificati

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

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

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).

K.1. Revoca dei certificati

Un certificato può essere revocato su richiesta del Titolare, del Terzo Interessato o della Certification Authority (cioè il QTSP).

Il certificato revocato non può essere in alcun modo riattivato.

K.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi di Ineo oppure mettendosi in contatto diretto con il Servizio Clienti della stessa Ineo o della Società terza.

Il QTSP, avvertito da Ineo, che nel frattempo avrà anche bloccato i codici di accesso del Titolare, provvederà alla immediata revoca del certificato.

K.1.2. Revoca su richiesta del Terzo Interessato

La Società, in qualità di Terzo Interessato, potrà richiedere la revoca del certificato comunicando tale intenzione a Ineo, che a sua volta contatterà il QTSP.

Il QTSP, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione o successivamente aggiornati e comunicati dal Titolare al QTSP, anche per mezzo delle LRA.

K.1.3. Revoca su iniziativa del Certificatore

Il Certificatore che intende revocare il Certificato Qualificato, salvo casi di motivata urgenza, ne dà preventiva comunicazione via e-mail o PEC alla LRA Ineo, la quale provvederà ad avvertire la Società (Terzo interessato) e contemporaneamente sarà data comunicazione al Titolare utilizzando l'indirizzo e-mail fornito in fase di richiesta del certificato ovvero all'indirizzo di residenza, specificando i motivi della revoca nonché la data e l'ora a partire dalla quale la revoca è efficace.

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

Nei casi di:

- compromissione della chiave di certificazione,
- cessazione dell'attività,

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

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

K.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al precedente 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 (ad esempio nei casi in cui si tema lo smarrimento / furto del Token OTP, o si debbano fare riscontri per avere certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

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 accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi di Ineo oppure mettendosi in contatto diretto con il suo Servizio Clienti.

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

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

In assenza di comunicazioni ulteriori, il certificato sospeso sarà automaticamente revocato al termine del periodo di sospensione e la data di revoca coinciderà con la data di decorrenza della sospensione.

K.2.2. Sospensione su richiesta del Terzo Interessato

Le Società, in qualità di Terzo Interessato, potranno richiedere la sospensione del certificato.

Il Certificatore, accertata la correttezza della richiesta, sospenderà tempestivamente il certificato e ne darà notizia della sospensione ai Titolari interessati tramite posta elettronica o con comunicazione attraverso i servizi esposti da Ineo.

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 una validità che può durare fino a 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 se la procedura è effettuata prima della scadenza del certificato.

L.2. Sostituzione delle chiavi del Certificatore

L.2.1. Sostituzione in emergenza delle chiavi di certificazione

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

L.2.2. Sostituzione pianificata delle chiavi di certificazione

Con un periodo di tempo congruo alla normativa vigente, prima della scadenza del certificato relativo alle coppie di Chiavi di certificazione (CA e TSCA) utilizzate dai sistemi di emissione dei certificati di sottoscrizione e dei certificati di TSA, il 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).

Per la gestione delle chiavi del sistema di validazione temporale viene applicato quando descritto nel Manuale Operativo Intesa: Certificati qualificati di sottoscrizione & validazione temporale.

M. Registro dei certificati

M.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

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

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

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

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 (GDPR) e successive modificazioni e integrazioni.

O. Procedura di gestione delle copie di sicurezza

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

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato al par. *M*.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato nonché le richieste di revoca e sospensione, corredate delle relative documentazioni.
- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del QTSP (Art.36 del DPCM).

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

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

P. Procedura di gestione degli eventi catastrofici

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

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

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

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

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

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

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

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

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

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

Q.1. Modalità di richiesta e verifica marche temporali

Il 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.

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

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

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

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

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

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

S. Riferimenti Tecnici

ETSI-319.401	ETSI EN 319 401 v2.3.1 - Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers
ETSI-319.411-1	ETSI EN 319 411-1 V1.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements
ETSI-319.411-2	ETSI EN 319 411-2 V2.3.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates
ETSI-319.412-1	ETSI EN 319 412-1 V1.4.4 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures

ETSI-319.412-2	ETSI EN 319 412-2 V2.2.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 2: Certificate profile for certificates issued to natural persons
ETSI-319.412-5	ETSI EN 319 412-5 V2.3.1 - Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements
Rec ITU-R	Recommendation ITU-R TF.460-6, Annex 1 – Time Scales.
RFC5905	Network Time Protocol (Protocollo NTP)
ETSI-319.421	ETSI EN 319 421 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps
ETSI-319.422	ETSI EN 319 422 v1.1.1 - Electronic Signatures and Infrastructures (ESI); Time-stamping protocol and time-stamp token profiles
ETSI 119 461	ETSI TS 119 461 V1.1.1 - Electronic Signatures and Infrastructures (ESI); Policy and security requirements for trust service components providing identity proofing of trust service subjects

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