Poste Italiane S.p.A.

Servizio Postecert

Firma Digitale, Sigillo Elettronico e Marche Temporali

Manuale Operativo

INDICE

Sezione I –

Informazioni generali

0 Definizioni

Di seguito si riportano le definizioni specifiche del presente Manuale Operativo.

In aggiunta valgono le definizioni previste nella normativa vigente.

Certificatore: si vedano gli articoli 26 e 27 del Codice dell'Amministrazione Digitale (CAD) e s.m.i.
Certificazione: il risultato della procedura informatica, applicata alla chiave pubblica e rilevabile dai sistemi di validazione, mediante la quale si garantisce la corrispondenza biunivoca tra chiave pubblica e soggetto Titolare cui essa appartiene, si identifica quest'ultimo e si attesta il periodo di validità della predetta chiave ed il termine di scadenza del relativo certificato
Chiave privata: elemento della coppia di chiavi asimmetriche, destinato ad essere conosciuto soltanto dal soggetto Titolare, mediante il quale si appone la firma digitale sul documento informatico
Chiave pubblica: elemento della coppia di chiavi asimmetriche destinato ad essere reso pubblico, con il quale si verifica la firma digitale apposta sul documento informatico dal Titolare delle chiavi asimmetriche
Coppia di chiavi: coppia di chiavi asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi crittografici
CRL: Vedi Lista di revoca dei certificati
CSL: Vedi Lista di sospensione dei certificati
Dati per la creazione della firma: l'insieme dei codici personali e delle chiavi crittografiche private, utilizzate dal firmatario per creare una firma elettronica
Utente: destinatario di un documento e/o di una evidenza informatica firmati digitalmente
Agenzia per l'Italia Digitale (ex DigitPA): Organismo istituito con DL 83/2012 dove sono confluiti risorse e compiti del DigitPA e l'Agenzia per l'Innovazione. Svolge compiti di vigilanza sulle attività dei Certificatori Accreditati.
Firma Elettronica Qualificata: un particolare tipo di firma elettronica avanzata che sia basata su un certificato qualificato e realizzata mediante un dispositivo sicuro per la creazione della firma;

Firma Digitale: un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e 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
Giorni festivi: festività riconosciute a livello italiano quali 1 gennaio, 6 gennaio, Pasqua e giorno seguente, 25 aprile, 1 maggio, 2 giugno, 15 agosto, 1 novembre, 8 dicembre, 25 dicembre, 26 dicembre.
HSM: Hardware Security Module - insieme di hardware e software che realizza dispositivi sicuri per la generazione delle firme in grado di gestire in modo sicuro una o più coppie di chiavi crittografiche
Incaricato: soggetto autorizzato a ricevere le credenziali dal Cliente, tramite la compilazione della scheda cliente. Ha la responsabilità della gestione delle credenziali e del ciclo di vita del certificato di Sigillo
Lista di revoca dei certificati (CRL): lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da un riferimento temporale, contenente i certificati dalla stessa emessi e revocati
Lista di sospensione dei certificati (CSL): lista firmata digitalmente, tenuta ed aggiornata dal Certificatore, contrassegnata da un riferimento temporale, contenente i certificati dalla stessa emessi e sospesi
Manuale Operativo: documento pubblico depositato presso l'Agenzia per l'Italia Digitale che definisce le procedure applicate dal Certificatore nello svolgimento della propria attività
Marca temporale: il riferimento temporale che consente la validazione temporale, ossia l'attribuzione di ora e data certa opponibile a terzi
OID (Object Identifier Number): numero identificativo univoco di un documento in ambito internazionale
Rappresentante Legale: soggetto al quale è stato conferito il potere di compiere atti e negozi giuridici in nome e per conto di un altro soggetto rappresentato
Registro dei certificati: registro contenente i certificati emessi dal Certificatore, la lista dei certificati revocati e la lista dei certificati sospesi, accessibili telematicamente
Revoca del certificato: operazione con cui il Certificatore annulla la validità del certificato da un dato momento, non retroattivo, in poi
Richiedente: soggetto che richiede al Certificatore i servizi di Certificazione e richiede la revoca o sospensione del certificato

Riferimento temporale: informazione, contenente data e ora, che viene associata ad un documento informatico
Sigillo Elettronico: dati in forma elettronica acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica utilizzati per garantire l'origine e l'integrità di questi ultimi.
Sospensione del certificato: operazione con cui il Certificatore sospende la validità del certificato per un determinato periodo di tempo
QSSCD: dispositivo sicuro qualificato per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II del Regolamento eIDAS
Terzo Interessato: persona fisica o giuridica/organizzazione che dà il consenso, in conformità alle norme, all'inserimento nel certificato qualificato delle seguenti informazioni: qualifiche specifiche del Titolare, poteri di rappresentanza, limiti d'uso e limiti di valore. Può richiedere la revoca o sospensione del certificato
Titolare: Persona fisica a favore del quale è stato emesso - o ci si appresta ad emettere - un certificato qualificato ed a cui è attribuita la firma digitale.
TSA: la Time Stamping Authority del Certificatore per il rilascio di marche temporali
Validità del Certificato: efficacia ed opponibilità della chiave pubblica e dei dati contenuti nel certificato stesso
Ufficio Delegato: Ufficio che svolge, per conto del Certificatore e secondo modalità da questo definite, le attività individuate e descritte nel presente Manuale.

1 Introduzione

1.1 Premessa

Il Manuale Operativo definisce le procedure applicate dal Certificatore nello svolgimento della propria attività di certificazione ed è rivolto a tutti i soggetti che entrano in relazione con il Certificatore:

- Titolare;
- Richiedente;
- Terzo Interessato;
- Utente, ovvero quanti accedono per la verifica della firma.

All'interno del presente documento, per i soggetti sopra elencati sono definiti gli obblighi e le corrispondenti responsabilità.

Il presente documento riporta i dati identificativi del Certificatore, della versione del Manuale Operativo e l'indicazione del responsabile del Manuale Operativo medesimo.

I certificati qualificati emessi da Poste Italiane, nel rispetto di quanto previsto nel presente Manuale Operativo e della normativa richiamata nel seguito, sono validi ai fini dell'apposizione della Firma Digitale, Firma Elettronica Qualificata e Sigillo Elettronico su documenti informatici opponibili ai terzi.

I dispositivi sicuri per la generazione della Firma Digitale scelti dal certificatore sono i medesimi dispositivi previsti dalle regole tecniche per la Firma Elettronica Qualificata e Sigillo Elettronico.

All'interno del presente Manuale Operativo, quindi, Firma Elettronica Qualificata e Firma Digitale sono da considerarsi equivalenti.

1.2 Contesto normativo

Il Manuale Operativo è conforme a quanto previsto dalla legge italiana e in particolare:

DPCM 22/02/2013	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
D.Lgs 82/2005	Decreto Legislativo 7 marzo 2005, n° 82 e successive modificazioni *Codice dell'Amministrazione Digitale*
D.Lgs 159/2006	Decreto Legislativo 4 aprile 2006, n° 159 *Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n.82, recante codice dell'amministrazione digitale*
CNIPA/CR/48	Circolare CNIPA 6 settembre 2005, n° CNIPA/CR/48 Modalità per presentare la domanda di iscrizione nell'elenco pubblico

	dei certificatori di cui all'articolo 28, comma 1, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445
Regolamento europeo (UE) 679/2016	Regolamento europeo in materia di protezione dei dati
Regolamento eIDAS	Regolamento (UE) N. 910/2014 del Parlamento Europeo e del Consiglio del 23 luglio 2014 in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE.
Determinazione N. 147/2019	Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate.

2 Dati identificativi del Certificatore

Denominazione e Ragione sociale	**Poste Italiane S.p.A.**
Numero Partita IVA	**01114601006**
Codice Fiscale e Numero Registro Imprese di Roma	97103880585
REA	842633
Rappresentante legale	Matteo Del Fante
Sede legale	Viale Europa n.190, 00144 Roma
Telefono	+39 06 59581
Indirizzo PEC	poste@pec.posteitaliane.it
Indirizzo Internet	https://postecert.poste.it https://www.poste.it/prodotti/firma-digitale-remota.html
Call Center	https://www.poste.it/assistenza.html Il Servizio Clienti è attivo: • tramite Operatore - dal lunedì al sabato dalle ore 8.00 alle ore 20.00; • tramite Assistente Digitale su canale telefonico, attivo 24 ore su 24, 7 giorni su 7, festivi inclusi.

3 Manuale Operativo

3.1 Modifiche introdotte rispetto alle emissioni precedenti

Versione n.	Pagina n.	Motivo della revisione	Data
1.0		Prima emissione	17/02/2017
1.1	10	Aggiornamento del Rappresentante Legale del Certificatore	11/05/2017
1.2	12 48	Fusione per incorporazione di Postecom S.p.A. in Poste Italiane Firma digitale verificata	23/02/2018
2.0	14 48 51 56	Aggiornamento della politica per la protezione dei dati personali Sistema di verifica delle firme qualificate Gestione delle chiavi di certificazione e di marcatura temporale Modalità per l'apposizione e la definizione del riferimento temporale	19/11/2018
2.1	9 33	Riferimenti call center Modalità di identificazione, registrazione del Titolare che dispone della soluzione di Identità Digitale PosteID rilasciata dall'Identity provider Poste Italiane	18/02/2019
2.2	28 33	Conformità dei certificati con la Determinazione AgID N. 121-147/2019 Modalità di identificazione e registrazione Titolari intestatari di servizi finanziari/bancari	06/07/2019
2.3	34	Modalità di identificazione e registrazione Titolari possessori di un Account Poste Verificato	31/08/2020
2.4	17	Punto di pubblicazione delle tariffe del servizio applicate da Poste Italiane	16/02/2021

2.5	Intero documento 29 38	Riferimenti al Sigillo Elettronico Tipologia di certificato - Certificato qualificato rilasciato a Persona giuridica Modalità di identificazione e registrazione di persone giuridiche	06/07/2022
2.6	45	Rinnovo del certificato qualificato utilizzato su dispositivi smart card	10/03/2023
2.7	10 13	Revisione informazioni di contatto assistenza	21/04/2023
2.8	17 22 33 39 40	Segnalazioni di un potenziale data breach Revisione paragrafo ufficio delegato Revisione modalità di identificazione Revisione per cancellazione riferimenti processi ARX Cosign non più utilizzati	28/02/2024

3.2 Responsabilità del Manuale Operativo, contatto per utenti finali e comunicazioni

La responsabilità del presente Manuale Operativo è di Poste Italiane, nella persona di Fabio Sensidoni, responsabile del servizio di certificazione e validazione temporale.

Il corrispondente file in formato elettronico, conservato presso i locali del Certificatore e depositato presso l'Organismo di Vigilanza, è identificabile dal nome "MOP01_PI_v2.8.pdf" ed è consultabile per via telematica all'indirizzo Internet: https://postecert.poste.it nella sezione "Firma digitale – Risorse – Documentazione" e all'indirizzo internet https://www.poste.it/prodotti/firma-digitale-remota.html .

Questo manuale si riferisce ai servizi di:

- Certificazione chiavi pubbliche;
- Generazione di marche temporali a richiesta per documenti elettronici.

Questo Manuale Operativo è referenziato dai seguenti OID (Object Identifier Number):

- 1.3.76.48.1.4.1.1 e 2.5.29.32.0 – Policy per servizi di certificazione;
- 0.4.0.2023.1.1– Policy per certificati di marcatura temporali;
- 1.3.76.48.1.2.3.1 – Policy per certificati qualificati di firma remota;
- 1.3.76.48.1.2.3.2 – Policy per certificati qualificati di firma automatica;
- 1.3.76.48.1.2.3.3 – Policy per certificati qualificati di firma su dispositivo smartcard.

A tale proposito si evidenzia che a partire dal sito https://postecert.poste.it "Firma Digitale - Risorse - Documentazione" e dal sito https://www.poste.it/prodotti/firma-digitale-remota.html .

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo di seguito indicato:

Poste Italiane S.p.A.

Responsabile Servizio Postecert Firma Digitale

Viale Europa 175 - 00144 – Roma –

Indirizzo PEC: poste@pec.posteitaliane.it

Contatto per utenti finali

Nell'ambito del servizio è disponibile un servizio di assistenza clienti, i cui riferimenti sono consultabili all'indirizzo https://www.poste.it/assistenza.html:

- tramite Operatore - dal lunedì al sabato dalle ore 8.00 alle ore 20.00;
- tramite Assistente Digitale su canale telefonico, attivo 24 ore su 24, 7 giorni su 7, festivi inclusi.

In data 1 Aprile 2017 è avvenuta la fusione per incorporazione di Postecom S.p.A. in Poste Italiane S.p.A. che è subentrata in tutti i rapporti (attivi e passivi), nei diritti e negli obblighi facenti capo a Postecom.
La comunicazione di intervenuta fusione per incorporazione è pubblicata sui siti www.poste.it e postecert.poste.it.
L'informativa ai clienti sulla presa in carico dei servizi di Postecom da parte del TSP Poste Italiane è disponibile alla pagina https://postecert.poste.it/TSPdoc/TakenOverBy.shtml.
I Titolari di certificati qualificati rilasciati da Postecom S.p.A. possono trovare tutte le informazioni sulle procedure adottate nell'erogazione del servizio di certificazione in questo manuale operativo.

3.3 Amministrazione del Manuale Operativo

Procedure per l'aggiornamento

Il Certificatore si riserva di apportare modifiche al Manuale Operativo per esigenze tecniche oppure per modifiche di processo intervenute sia a causa di variazione o introduzione di nuove normative o regolamenti, che di ottimizzazioni del Servizio.

Ogni nuova versione annulla e sostituisce la precedente versione.

Ogni variazione al Manuale Operativo è sottoposta preventivamente all' approvazione dell'Agenzia per l'Italia Digitale.

Pubblicazione

Il presente Manuale Operativo è disponibile all'indirizzo Internet: https://postecert.poste.it nella sezione "Firma digitale – Risorse – Documentazione", (https://postecert.poste.it/manualioperativi/index.shtml) e nel link a "Manuali Operativi" inserito a piè pagina e alla pagina https://www.poste.it/prodotti/firma-digitale-remota.html .

Approvazione

Il Manuale Operativo è verificato da tutti i responsabili indicati nella Relazione della Struttura Organizzativa di Poste Italiane ed è approvato dal primo livello della struttura di Sistemi Informativi di Poste Italiane S.p.A.

4 Protezione dei dati personali

4.1 ORGANIZZAZIONE PRIVACY

I dati personali rilasciati dei soggetti che accedono al servizio Postecert Firma Digitale, Marche Temporali e Sigillo Elettronico sono trattati conformemente a quanto previsto dal Regolamento (UE) 2016/679 in materia di protezione dei dati personali.

Le figure a cui sono attribuiti specifici ruoli e responsabilità nel trattamento dei dati personali sono:

- Titolare
- Responsabile
- Incaricato

Titolare è la persona fisica o giuridica, l'autorità pubblica, il servizio o altro organismo che, singolarmente, o insieme ad altri, determina le finalità e i mezzi del trattamento.

Responsabile esterno del Trattamento è la persona fisica o giuridica che tratta i dati personali per conto del Titolare del trattamento

Incaricato è il Personale autorizzato al trattamento dei dati personali.

Il Modello Privacy di Poste Italiane S.p.A. è costituito dalle seguenti figure:

- Titolare è Poste Italiane S.p.A., rappresentata dall'Amministratore Delegato.
- Data Protection Officer (DPO) è nominato dal Titolare, ai sensi dell'articolo 37 del Regolamento UE 2016/679 e si avvale del supporto della Funzione CA/TA/Privacy per lo svolgimento dei compiti assegnati.
- Il delegato al Trattamento è la persona fisica che, designata dal Titolare del trattamento per iscritto, lo rappresenta per quanto riguarda gli obblighi relativi alle norme del GDPR.
- I Responsabili pro-tempore delle funzioni organizzative di primo livello sono nominati Delegati al Trattamento.
- Incaricati sono i dipendenti di Poste Italiane autorizzati al trattamento dei dati personali, ovvero le persone fisiche autorizzate dal Titolare, direttamente o per il tramite dei Delegati, a compiere operazioni di trattamento dei dati.
- Il Centro Servizi privacy presso la Funzione Corporate Affairs/Tutela Aziendale/Privacy è l'ufficio preposto alla gestione delle istanze per l'esercizio dei diritti ex articolo 15 e seguenti del Regolamento UE 2016/679 ove è possibile inoltrare le richieste:

  - E-mail: centroserviziprivacy@posteitaliane.it
  - Posta cartacea: Via August Von Platen, n. 9 – 87100 Cosenza
  - Fax: 06/9868.5343

4.2 MODALITA' DI PROTEZIONE DEI DATI

4.2.1 Dati personali

Ai sensi dell'art. 4 del Regolamento UE 2016/679 il «dato personale» è qualsiasi informazione riguardante una persona fisica identificata o identificabile («interessato»); si considera identificabile la persona fisica che può essere identificata, direttamente o indirettamente, con particolare riferimento a un identificativo come il nome, un numero di identificazione, dati relativi all'ubicazione, un identificativo online o a uno o più elementi caratteristici della sua identità fisica, fisiologica, genetica, psichica, economica, culturale o sociale.

Nell'ambito del servizio sono ritenuti dati personali relativi al titolare della casella o di eventuali terzi, nonché i dati contenuti nei campi informativi relativi alla modulistica utilizzata nel corso della fruizione del servizio.

4.2.2 Diritti degli interessati

Poste Italiane garantisce la tutela dei diritti degli interessati attraverso processi organizzativi e procedure che consentono di:

- fornire agli interessati adeguata informativa sul trattamento dei dati, ambiti e finalità;
- gestire le richieste degli interessati ai sensi degli articoli 15 e seguenti del Regolamento UE 2016/679;
- gestire i consensi richiesti all'interessato relativamente al trattamento dei propri dati personali nell'ambito del servizio di Posta Elettronica Certificata.

4.2.3 Sicurezza dei dati

Come previsto dalle norme, Poste Italiane adotta adeguate e preventive misure di sicurezza al fine di ridurre al minimo:

- i rischi di distruzione o perdita, anche accidentale, dei dati, di danneggiamento delle risorse hardware su cui sono registrati e dei locali ove vengono custoditi;
- l'accesso non autorizzato ai dati stessi;
- modalità di trattamento non consentite dalla legge o dai regolamenti aziendali.

Le misure di sicurezza adottate assicurano:

- l'integrità dei dati, da intendersi come salvaguardia dell'esattezza dei dati, difesa da manomissioni o modifiche da parte di soggetti non autorizzati;
- la disponibilità dei dati, da intendersi come la certezza che l'accesso sia sempre possibile quando necessario; indica quindi la garanzia di fruibilità dei dati e dei servizi, evitando la perdita o la riduzione dei dati e dei servizi;

- la confidenzialità/riservatezza dei dati, da intendersi come garanzia che le informazioni siano accessibili solo da persone autorizzate e come protezione delle trasmissioni e controllo degli accessi stessi.
- Il Sistema di Gestione Qualità e Sicurezza attuato in Poste Italiane è certificato secondo le norme ISO 9001 e ISO 27001 ed è stato strutturato per garantire la compliance normativa e tenere sotto controllo i possibili rischi sulla sicurezza dei sistemi informativi. Le procedure e le metodologie adottate ed applicate sono riferite all'intero ciclo di vita del servizio Postecert Firma Digitale, Marche Temporali e Sigillo Elettronico.

4.2.4 Segnalazioni di un potenziale data breach

Chiunque che venga a conoscenza o sospetti che sia avvenuta una violazione di dati personali, deve darne immediata comunicazione tramite invio di una pec all'indirizzo firmadigitale@pec.posteitaliane.it. La comunicazione deve contenere un'indicazione chiara dell'evento verificatosi e delle caratteristiche dei dati personali coinvolti.

La comunicazione ricevuta sarà successivamente condivisa con la funzione Privacy di Poste Italiane per le opportune verifiche al fine di valutarne il livello e le potenzialità di rischio.

5 Tariffe

Le tariffe applicate da Poste Italiane sono pubblicate on line all'indirizzo https://www.poste.it/prodotti/firma-digitale-remota.html.

Sezione II –

Obblighi e Responsabilità

6 Obblighi

Chiunque intenda utilizzare un sistema di chiavi asimmetriche o di firma elettronica qualificata è tenuto ad adottare tutte le misure organizzative e tecniche adeguate ad evitare danno ad altri.

6.1 Obblighi del Certificatore

Nello svolgimento della sua attività il Certificatore:

- adotta tutte le misure organizzative e tecniche adeguate ad evitare danno ad altri;
- si attiene alla normativa vigente in materia di Firma Digitale, Firma Elettronica Qualificata e Sigillo Elettronico
- genera un certificato qualificato per ciascuna delle chiavi di firma elettronica o qualificata e Sigillo Elettronico utilizzate dall'Agenzia per l'Italia Digitale per la sottoscrizione dell'elenco pubblico dei certificatori, lo pubblica nel proprio registro dei certificati e lo rende accessibile per via telematica al fine di verificare la validità delle chiavi utilizzate dall'Agenzia per l'Italia Digitale;
- mantiene copia della lista, sottoscritta dall'Agenzia, dei certificati relativi alle chiavi di certificazione che rende accessibile per via telematica per la specifica finalità della verifica delle firme elettroniche qualificate, digitali e sigilli elettronici;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione, in particolare i termini e le condizioni relative all'uso dei certificati, compresa ogni limitazione dell'uso, la procedura di rilascio, le procedure di reclamo e di risoluzione delle controversie. Tali informazioni possono essere trasmesse telematicamente;
- informa i richiedenti sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi e sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si accerta dell'autenticità della richiesta di certificazione;
- acquisisce ed inserisce nel certificato qualificato, su richiesta del Titolare le qualifiche specifiche del Titolare, i limiti d'uso e limiti di valore e, con il consenso del terzo interessato, i poteri di rappresentanza;
- identifica con certezza la persona che fa richiesta della registrazione ai fini della certificazione;
- nel caso di chiavi generate dal certificatore, assicura la consegna al legittimo titolare; nel caso di chiavi non generate dal certificatore, verifica il possesso della chiave privata da parte del titolare ed il corretto funzionamento della coppia di chiavi;

- genera la coppia di chiavi mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata;
- registra, nel giornale di controllo, l'emissione dei certificati qualificati, specificando il riferimento temporale relativo alla registrazione;
- non copia, né conserva le chiavi private di sottoscrizione dei Titolari;
- non si rende depositario di dati per la creazione della firma del titolare nel caso il dispositivo di firma sia rilasciato fisicamente al Titolare, in ogni caso gestisce le modalità per le quali almeno uno dei dati necessari per la creazione della firma sia sotto il controllo del Titolare che attiva la procedura di firma;
- adotta le misure di sicurezza per il trattamento dei dati personali ai sensi del Regolamento UE 2016/679;
- procede alla pubblicazione della revoca e della sospensione del certificato qualificato, in caso di richiesta da parte del Titolare, del Richiedente e del Terzo Interessato di perdita del possesso o della compromissione del dispositivo di firma, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del Titolare, di sospetti abusi o falsificazioni;
- garantisce un servizio di revoca e sospensione dei certificati elettronici, sicuro e tempestivo nonché garantisce il funzionamento efficiente, puntuale e sicuro degli elenchi dei certificati di firma emessi, sospesi e revocati;
- garantisce la disponibilità del servizio eccetto nei casi di manutenzione programmata notificata preventivamente ai clienti;
- tiene registrazione per venti anni, anche in forma elettronica, delle informazioni relative al certificato qualificato;
- conserva per almeno venti anni dalla data di emissione del certificato le informazioni relative alla reale identità del titolare, in particolare conserva per almeno venti anni copia del documento di riconoscimento, la dichiarazione di accettazione delle condizioni di servizio sottoscritta dal Titolare ed ogni altra informazione necessaria a dimostrare l'ottemperanza alla normativa vigente in materia;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati;
- 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 consultazio-

ne 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;

- fornisce o indica almeno un sistema che consenta di effettuare la verifica delle firme digitali;
- fornisce almeno un sistema che consenta la generazione delle firme digitali;
- comunica l'avvenuta revoca o sospensione del certificato al Titolare, al Richiedente e all'eventuale Terzo Interessato;
- rende disponibile ai propri titolari un sistema di validazione temporale conforme con il regolamento eIDAS.

6.2 Obblighi dell'Ufficio Delegato

Le attività di identificazione e registrazione, oltre che svolte in maniera diretta dal personale del Certificatore, possono essere delegate a terzi che agiscono sotto il controllo e la responsabilità del Certificatore stesso. I soggetti che svolgono le attività di identificazione e registrazione vengono definiti Operatori dell'Ufficio Delegato. Il Certificatore è responsabile dell'identificazione del Titolare anche se tale attività è delegata soggetti terzi. Gli Operatori, laddove non appartenenti a Società del Gruppo Poste Italiane, saranno preventivamente identificati dal Certificatore.

Nelle attività delegate dal Certificatore l'Ufficio Delegato è tenuto a:

- verificare con certezza l'identità del Titolare mediante il confronto dei dati personali riportati sui documenti di riconoscimento con quelli inseriti in fase di registrazione;
- fornire al Titolare tutta la documentazione prevista ed indicata dal Certificatore ed assicurarsi che il Titolare ne abbia preso corretta visione;
- inoltrare al Certificatore tutti i dati ed i documenti acquisiti nel corso delle attività di identificazione del Titolare nelle modalità comunicate dal Certificatore stesso;
- verificare ed inoltrare al Certificatore le richieste di Revoca e Sospensione presentate dal Titolare;
- Informare il certificatore in caso di un incidente di sicurezza informatico o di una accertata, possibile o sospetta violazione dei dati personali dei titolari (c.d. Data breach).

6.3 Obblighi del Titolare

Il Titolare è tenuto ad assicurare la custodia dei dati per la creazione della firma e ad adottare tutte le misure organizzative e tecniche adeguate ad evitare danno ad altri. È altresì tenuto ad utilizzare personalmente il dispositivo di firma.

Il Titolare della chiave deve inoltre:

- prendere visione del presente Manuale Operativo prima di inoltrare la richiesta di certificazione;
- garantire la veridicità di tutti i dati personali comunicati in occasione della registrazione ed identificazione, assumendo la responsabilità di cui all'art. 495-bis del codice penale, e impegnarsi a fornire tutte le informazioni richieste dal Certificatore;
- fornire tutte le informazioni necessarie alla fornitura del servizio richieste dal Certificatore garantendone, sotto la propria responsabilità, l'attendibilità ai sensi del DPR 445/2000;
- comunicare al Certificatore ogni variazione dei dati forniti in fase di registrazione;
- generare, ove sia lui a farlo, la coppia di chiavi, all'interno del dispositivo sicuro per la creazione della firma rilasciato o indicato dal Certificatore;
- assicurare la custodia del dispositivo di firma e ad adottare tutte le misure organizzative e tecniche adeguate ad evitare danno ad altri; è altresì tenuto ad utilizzare personalmente il dispositivo di firma;
- conservare con la massima diligenza i codici riservati ricevuti dal Certificatore, al fine di garantirne l'integrità e la massima riservatezza;
- conservare le informazioni di abilitazione all'uso della chiave privata in luogo diverso dal dispositivo contenente la chiave;
- utilizzare esclusivamente il dispositivo sicuro per la creazione della firma fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso;
- non apporre firme digitali su documenti contenenti macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che ne renderebbero, quindi, nulla l'efficacia;
- mantenere in modo esclusivo la conoscenza o la disponibilità di almeno uno dei dati per la creazione della firma, nel rispetto dell'art. 8 comma 5 lettera d) del DPCM 22 febbraio 2013 e fatto salvo quanto previsto dai commi 3 e 4 dello stesso articolo;
- garantire la protezione della segretezza e la conservazione del dispositivo e/o dei codici utilizzati per l'attivazione della procedura di firma ed impegnarsi a richiedere l'immediata revoca dei certificati qualificati relativi alle chiavi contenute in dispositivi di firma di cui abbia perduto il possesso o difettosi, o qualora abbia il ragionevole dubbio che i dati e/o i codici possano essere utilizzati abusivamente da persone non autorizzate;
- garantire la protezione della segretezza e la conservazione del "codice di emergenza", che il titolare dovrà utilizzare per richiedere la sospensione del certificato nei casi di emergenza previsti nel presente Manuale Operativo nella sezione "Revoca e Sospensione dei certificati qualificati - Richiesta per la sospensione immediata"
- adottare le principali regole di comportamento per la sicurezza della propria postazione;

- inoltrare, la richiesta di revoca munita della sottoscrizione, specificandone la motivazione, nei casi e con le modalità previste nel Manuale Operativo al paragrafo "Revoca e Sospensione dei certificati qualificati";
- inoltrare, la richiesta di sospensione munita della sottoscrizione, specificando la motivazione, nei casi e con le modalità previste nel Manuale Operativo al paragrafo "Revoca e Sospensione dei certificati qualificati";
- presentarsi presso l'Ufficio Delegato o uffici del Certificatore, a seguito della richiesta di sospensione immediata del certificato, e richiedere per iscritto la revoca o la riattivazione dello stesso.
- E' vietata la duplicazione della chiave privata e dei dispositivi che la contengono.
- Non è consentito l'uso di una coppia di chiavi per funzioni diverse da quelle previste dalla sua tipologia.

6.4 Obblighi dell'Utente

L'Utente è il soggetto che intende utilizzare i documenti a cui è stata apposta la firma digitale utilizzando il certificato generato dal Certificatore. L'Utente è tenuto ad adottare tutte le misure organizzative e tecniche adeguate ad evitare danno ad altri, in particolare ha l'obbligo di verificare:

- la validità del certificato contenente la chiave pubblica del firmatario del documento;
- l'assenza del certificato dalle Liste di Revoca e Sospensione (CRL) dei certificati;
- che il certificato del Titolare sia verificabile con un certificato di certificazione di Poste Italiane, presente nell' Elenco Pubblico mantenuto dall' Agenzia per l'Italia Digitale;
- l'esistenza di eventuali limitazioni all'uso del certificato utilizzato dal Titolare, o di un eventuale valore limite di valore per il quale può essere usato il certificato stesso;
- la presenza, nel documento verificato, di eventuali macro istruzioni o codici eseguibili che ne modifichino gli atti o i fatti negli stessi rappresentati e che renderebbero, quindi, nulla la sottoscrizione del documento;
- che siano adottate le principali regole di comportamento per la sicurezza della propria postazione;
- che nel certificato sia presente l'identificativo (OID), relativo al certificato qualificato come indicato nel presente Manuale Operativo;
- che la tipologia di uso della chiave del certificato sia esclusivamente "Non Ripudio".

6.5 Obblighi del Terzo Interessato

Il Terzo Interessato si obbliga a seguire quanto previsto dal presente Manuale Operativo. Inoltre

adotta tutte le misure tecnico-organizzative adeguate ad evitare danno a terzi.

Il Terzo Interessato, sia esso persona fisica o giuridica provvede, anche su indicazione del Richiedente, a raccogliere i dati necessari alla registrazione, avendo cura di organizzarli secondo il tracciato dati ricevuto dal Certificatore.

Il Terzo Interessato ha, inoltre, l'obbligo di richiedere la sospensione e/o la revoca dei certificati ogni qualvolta vengano meno i requisiti in base ai quali tali certificati sono stati rilasciati. In caso di cessazione o modifica delle qualifiche o dei titoli inseriti nel certificato su richiesta del Terzo Interessato, la richiesta di revoca deve essere inoltrata non appena lo stesso venga a conoscenza della variazione di tali qualifiche o titoli.

A titolo esemplificativo si riportano le seguenti circostanze:

- variazione o cessazione dei poteri di rappresentanza;
- variazione di ruoli e qualifiche interne;
- cessazione del rapporto di dipendenza;
- variazione dei dati identificativi (es. denominazione sociale, sede legale, etc.) o cessazione della persona giuridica;
- ed ogni altro dato rilevante ed incidente ai fini dell'uso del certificato.

La richiesta di revoca o sospensione, da parte del Terzo Interessato, dovrà essere inoltrata al Certificatore munita di sottoscrizione e corredata dalla documentazione giustificativa connessa.

6.6 Obblighi del Richiedente

Il Richiedente si obbliga a seguire quanto previsto dal presente Manuale Operativo.

7 Responsabilità

Il Certificatore è responsabile per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività di Certificatore Accreditato secondo quanto stabilito dalla normativa vigente in materia.

Il Certificatore non assume responsabilità per:

- l'uso improprio dei certificati;
- danni, diretti ed indiretti, derivanti da caso fortuito, forza maggiore o per altra causa non imputabile al Certificatore stesso;
- danni, diretti ed indiretti, derivanti dalla violazione di obblighi in carico al Richiedente, al Titolare, al terzo Interessato ed all'Utente;
- l'uso dei certificati che ecceda i limiti posti dallo stesso o derivanti dal superamento del valore limite.

7.1 Limitazioni ed indennizzi

Il Certificatore ha stipulato un contratto assicurativo, per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato inviato all' Agenzia Italia Digitale. Si riportano i valori economici:

- 1.000.000 Euro per singolo sinistro;
- 2.000.000 Euro per anno assicurativo.

Sezione III –

Caratteristiche e ciclo di vita dei certificati qualificati

8 Caratteristiche generali

8.1 Tipologie di certificati qualificati

I Certificati qualificati sono suddivisi nelle seguenti tipologie:

- Certificato qualificato rilasciato a Persona fisica senza indicazione di qualifiche specifiche.
- Certificato qualificato rilasciato a Persona fisica con indicazione di qualifiche specifiche senza indicazione del Terzo Interessato/organizzazione
- Certificato qualificato rilasciato a Persona fisica con eventuale indicazione di qualifiche specifiche/poteri di rappresentanza con indicazione del Terzo Interessato/organizzazione.
- Certificato qualificato rilasciato a Persona giuridica (Sigillo Elettronico).

8.2 Informazioni contenute nel certificato qualificato

I certificati elettronici rilasciati da Poste Italiane sono conformi alla specifica RFC-5280 e applicano le raccomandazioni descritte nelle linee guida di AgID, contenenti le "Regole Tecniche e Raccomandazioni afferenti la generazione di certificati elettronici qualificati, firme e sigilli elettronici qualificati e validazioni temporali elettroniche qualificate" (Determinazione N. 121 e 147/2019)

Questa conformità dei certificati è dichiarata attraverso la codifica, nel campo CertificatePolicies (OID 2.5.29.32), di un elemento PolicyIdentifier con valore agIDcert (OID 1.3.76.16.6).

Oltre ai dati anagrafici identificativi necessari ed a quanto previsto dalla normativa vigente, il certificato qualificato, ove richiesto dal Titolare o dal Terzo Interessato, può contenere le seguenti informazioni, di cui all'art. 28 comma 3 del CAD, se pertinenti allo scopo per il quale il certificato è richiesto:

- eventuali limiti d'uso del certificato;
- eventuali limiti di valore del certificato;
- eventuali qualifiche specifiche del Titolare, quali l'appartenenza ad ordini o collegi professionali, l'iscrizione ad albi o il possesso di altre abilitazioni professionali, nonché poteri di rappresentanza.

Tali informazioni dovranno essere richieste in base a quanto stabilito dall'art.19 del DPCM 22 febbraio 2013

8.3 Inserimento Qualifiche specifiche/poteri di rappresentanza

Tali informazioni dovranno essere richieste dal Titolare in base a quanto stabilito dall'art.19 del DPCM 22 febbraio 2013 nelle seguenti modalità:

1) Nel caso di Certificato qualificato rilasciato a Persona fisica con indicazione di qualifiche specifiche senza indicazione del Terzo Interessato/organizzazione: fornendo al Certificatore una dichiarazione sostitutiva ai sensi del DPR 28 dicembre 2000 n.445 munita di consenso espresso del Terzo Interessato;
2) Nel caso di Certificato qualificato rilasciato a Persona fisica con eventuale indicazione di qualifiche specifiche/poteri di rappresentanza e con indicazione del Terzo Interessato/organizzazione: presentando al Certificatore apposita autorizzazione all'emissione del certificato richiesta al Terzo Interessato. Il Titolare, in questo caso dovrà comunicare al Terzo Interessato, il Certificatore cui intende rivolgersi.

   La documentazione, attestante la qualifica di cui si richiede l'inserimento nel certificato qualificato, va presentata in fase di riconoscimento e non dovrà essere anteriore di oltre 30 giorni rispetto alla data della richiesta del Servizio.
3) Nel caso di registrazione on-line la richiesta di inserimento di qualifiche specifiche sul certificato di firma digitale è realizzata a seguito di identificazione certa e tramite autocertificazione, ovvero dichiarazione sostitutiva di certificazione (art. 46 e 47 D.P.R.28 dicembre 2000 n. 445).

8.4 Modalità con cui si indica un certificato qualificato

L'indicazione che il certificato elettronico è un certificato qualificato è presente nel campo Certificate Policy, con l'inserimento dell'identificativo (OID) relativo al certificato qualificato.

Ai certificati qualificati richiesti dai Titolari per l'apposizione di firme automatiche, Poste Italiane attribuisce uno specifico OID, al fine di permettere l'identificazione di tali tipologie di firme.

In coerenza alla normativa vigente, il certificato qualificato, contiene inoltre l'attributo **qcStatements**, identificate nel documento ETSI TS 101 862 come segue:

1) id-etsi-qcs-QcCompliance (OID: 0.4.0.1862.1.1);
2) id-etsi-qcs-QcLimitValue (OID: 0.4.0.1862.1.2) – presente se sono applicabili limiti nelle negoziazioni;
3) id-etsi-qcs-QcRetentionPeriod (OID: 0.4.0.1862.1.3) – il valore indicato all'interno dei certificati è pari "20";
4) id-etsi-qcs-QcSSCD (OID: 0.4.0.1862.1.4)

Poste Italiane, sul sito postecert.poste.it e https://www.poste.it/prodotti/firma-digitale-remota.html, mette a disposizione il documento "Guida alla comprensione degli OID presenti nei certificati rilasciati da POSTE ITALIANE S.P.A", che descrive le varie tipologie di certificato elettronico.

8.5 Validità del certificato

L'inizio e la fine del periodo di validità delle chiavi sono contenuti all'interno dei relativi certificati.

Il periodo di validità dei certificati qualificati è determinato in funzione della robustezza delle chiavi di creazione e verifica impiegate e dei servizi cui essi sono destinati. Detto periodo non eccede comunque i 3 anni.

9 Ciclo di vita dei certificati qualificati

9.1 Modalità di identificazione e registrazione dei Titolari

Le procedure per il rilascio di un certificato qualificato prevedono:

- che il Titolare sia registrato presso il Certificatore anche attraverso soggetti terzi;
- che il Titolare venga identificato con certezza dal Certificatore o dai suoi delegati.

Le attività di registrazione e identificazione, oltre che svolte in maniera diretta dal personale del Certificatore, possono essere delegate a terzi che agiscono sotto il controllo e la responsabilità del Certificatore stesso.

La funzione di Ufficio Delegato può essere svolta:

- dal personale del Certificatore;
- dal personale delle società del Gruppo Poste Italiane;
- da soggetti a cui Poste Italiane delega l'attività di identificazione.

I soggetti che espletano la funzione di Ufficio Delegato devono possedere requisiti e adeguata formazione in relazione ai processi legati all'attività di Registration Authority.

Il Titolare, a seguito della registrazione, dovrà recarsi presso un Ufficio Delegato portando con sé i documenti necessari all'identificazione, la documentazione contrattuale e di registrazione, l'eventuale ulteriore documentazione necessaria in relazione alla tipologia di certificato richiesto.

L'Operatore addetto all'identificazione ritira la documentazione presentata dal Titolare e:

- controlla la validità del documento di identità prodotto sia in originale che in copia e verifica l'identità del Titolare;
- verifica la corrispondenza dei dati contenuti nelle copie con il documento in originale;
- verifica la completezza e la correttezza dei dati di registrazione.

L'Operatore, dopo aver compiuto le verifiche descritte:

- fa sottoscrivere, in duplice copia i documenti di registrazione al Titolare il quale, dopo averlo letto, lo firma per accettazione. Il Titolare è tenuto a verificare puntualmente la correttezza delle informazioni di registrazione;
- firma e timbra le due copie dei documenti di registrazione;
- consegna una copia della documentazione di registrazione al Titolare e trattiene l'altra.

Nel caso in cui il rilascio dei certificati avvenga su richiesta del Richiedente, lo stesso dovrà essere oggetto di specifico accordo tra il Certificatore e il Richiedente stesso.

Nell'ambito di tale accordo saranno preventivamente individuate, sulla base delle specifiche esigenze del Richiedente, nonché dei requisiti tecnici del Certificatore, le tipologie di certificati da emettere, le condizioni e le modalità di richiesta e di rilascio dei certificati.

Documenti richiesti ai fini dell'identificazione e registrazione

L'identificazione del Titolare avviene attraverso l'esibizione di uno dei documenti di riconoscimento di cui all'art.35 del D.P.R. 445/2000.tra cui:

- Carta di identità;
- Patente di guida;
- Passaporto;
- Patente Nautica;
- Libretto di Pensione;
- Porto d'armi;
- Il patentino di abilitazione alla conduzione di impianti termici;
- Tessere di riconoscimento purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato. (es. tessere AT e BT)

I suddetti documenti devono essere validi, non scaduti e presentati in originale, corredati della relativa fotocopia.

Il Titolare deve inoltre produrre gli estremi del codice fiscale rilasciato dallo Stato Italiano.

In caso di impossibilità di individuare un codice identificativo personale non sarà possibile proseguire l'iter di rilascio del dispositivo di firma.

Nel caso in cui il Titolare desideri citare nel certificato la sussistenza di eventuali abilitazioni professionali o ruoli rivestiti, deve essere presentata prova del possesso della qualifica dichiarata, in conformità alle norme, disposizioni ed ordinamenti vigenti secondo quanto specificato ai punti precedenti.

Il Titolare assume la responsabilità della veridicità dei dati e dei documenti forniti per l'identificazione e registrazione.

9.2 Ulteriori modalità di identificazione e registrazione degli utenti

Poste Italiane ai fini della identificazione e registrazione dei Titolari al servizio, mette a disposizione dei clienti modalità basate su processi di identificazione digitali. In particolare, in una logica "once only", sono previste le seguenti modalità/strumenti di identificazione:

- Certificato qualificato rilasciato da Certificatore Accreditato
- Identificazione del Titolare già intestatario di servizi finanziari/bancari
- Account Poste Verificato rilasciato a clienti di Poste Italiane
- Registrazione del Titolare da parte di Pubbliche Amministrazioni e Società del Gruppo Poste Italiane

- PosteID, abilitato a SPID

Modalità di identificazione e registrazione Titolari in possesso di un certificato qualificato rilasciato da un Certificatore Accreditato

La richiesta di registrazione potrà – nei casi specifici previsti dal Certificatore – essere effettuata anche da Titolari in possesso di un certificato di firma digitale o firma elettronica qualificata in corso di validità al momento dell'accettazione della richiesta da parte del Certificatore Poste Italiane S.p.A.

In questo caso l'identificazione si intende assolta in modalità telematica, essendo il titolare del certificato qualificato già stato identificato, anche da diverso Certificatore, ai fini del rilascio del certificato stesso.

Il Titolare, successivamente alla sua autenticazione al sistema, confermerà i dati di registrazione e accetterà on line le Condizioni Generali del Servizio.

Il certificatore in fase di verifica e accettazione della richiesta firmata digitalmente, apporrà una marca temporale e conserverà in modalità elettronica i dati elettronici ricevuti e generati.

Modalità di identificazione e registrazione Titolari intestatari di servizi finanziari/bancari

Nel caso in cui il Titolare sia stato già identificato per il rilascio dei servizi finanziari e bancari da un Intermediario Finanziario o da altro soggetto Esercente attività Finanziaria, in aderenza alla normativa anti riciclaggio (D.Lgs.231/2007 e s.m.i.) ed al Regolamento Delegato (UE) 2018/389 (che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri) la fase di identificazione si intende assolta, e verrà utilizzata dal Certificatore ai fini del rilascio del certificato qualificato di firma digitale.

I certificati rilasciati secondo tale modalità potranno eventualmente contenere una limitazione d'uso, a seconda dello specifico contesto e/o accordo con il Cliente.

All'interno dello specifico contesto di utilizzo messo a disposizione dall'Intermediario Finanziario o da altro soggetto Esercente attività Finanziaria o dal Certificatore, il Titolare accetterà online le Condizioni Generali del Servizio del Servizio di Firma Digitale.

Il Certificatore conserverà in modalità elettronica i dati elettronici ricevuti e generati.

Modalità di identificazione e registrazione Titolari possessori di un Account Poste Verificato

La richiesta di registrazione al servizio di Firma Digitale potrà essere effettuata anche da Titolari in possesso di un Account Poste Verificato.

L'Account Poste Verificato viene attribuito da Poste Italiane ai propri clienti per la richiesta e la fruizione di servizi on-line erogati tramite il sito poste.it, quali ad esempio servizi finanziari, servizi di Ritiro Digitale delle Raccomandate e Servizi Fiduciari, che prevedono certezza dell'identità dell'utente.

L'Account di Poste Verificato, ovvero il possesso di credenziali di livello 'forte' richieste per la Custo-

mer Strong Authentication, realizza l'evoluzione del profilo 'base' che il cliente ha acquisito in fase di registrazione on line sul sito Poste.it.

L'Account Poste Verificato è rilasciato sulla base dei dati identificativi acquisiti e verificati a seguito del processo di verifica dell'identità svolto in aderenza alla normativa anti riciclaggio (D.Lgs.231/2007 e s.m.i.) ed al Regolamento Delegato (UE) 2018/389 (che integra la direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio per quanto riguarda le norme tecniche di regolamentazione per l'autenticazione forte del cliente e gli standard aperti di comunicazione comuni e sicuri).

Al termine del processo di verifica della identificazione, all'Utente sono associate credenziali di sicurezza di livello LoA3 che garantiscono la verifica dell'identità in fase di accesso ai servizi online di Poste.

Il processo di rilascio dell'Account Poste Verificato prevede inoltre la certificazione:

- del numero di cellulare dichiarato dal Cliente mediante l'invio via SMS al numero di telefono cellulare medesimo di un codice di sicurezza alfanumerico, OTP, monouso che il Cliente dovrà utilizzare per completare l'operazione
- dell'e-mail di contatto del Cliente attraverso l'invio di una e-mail contenente un link e le istruzioni che il Cliente deve seguire per completare il processo.
- Le condizioni generali per l'attivazione dell'account Poste verificato, per la fruizione di tutte le funzionalità/Servizi accessibili dal Sito e nel rispetto di quanto previsto da ciascun servizio, comportano l'assunzione di responsabilità esplicita del Titolare a conservare le credenziali con la massima diligenza e a non consentirne l'utilizzo a terzi, manlevando e tenendo indenne Poste da ogni e qualsiasi responsabilità al riguardo.
- In fase di sottoscrizione del contratto di acquisto del servizio di firma digitale, assolta l'identificazione attraverso l'Account Poste Verificato, il rilascio del certificato di firma digitale qualificata al Titolare avviene soltanto a seguito dell'accettazione da parte del Titolare delle Condizioni Generali del Servizio del Servizio di Firma Digitale.

Modalità di identificazione, registrazione del Titolare con archiviazione della documentazione da parte di Pubbliche Amministrazioni e Società del Gruppo Poste Italiane

Nel caso di Pubbliche Amministrazioni e Società del Gruppo Poste Italiane le attività in carico agli Operatori dell'Ufficio Delegato potranno essere svolte dai dipendenti delle stesse.

In tale fattispecie le Pubbliche Amministrazioni e le Società del Gruppo Poste Italiane provvederanno, inoltre, all'archiviazione della documentazione necessaria al rilascio dei certificati.

Modalità di identificazione, registrazione del Titolare che dispone della soluzione di Identità Digitale PosteID, abilitato a SPID, rilasciata dall'Identity provider Poste Italiane

Nel caso in cui il Titolare sia residente in Italia e sia stato già identificato per il rilascio dell'Identità Digitale PosteID (abilitata ad essere utilizzata come identità SPID con un livello di sicurezza delle credenziali pari a 2, corrispondente al Level of Assurance LoA3 dello standard ISO/IEC DIS 29115), ai fini del rilascio da parte di Poste Italiane del certificato qualificato di Firma Digitale, la fase di identificazione si intende assolta con l'esito positivo dell'autenticazione da parte del Titolare tramite identità PosteID.

Sarà onere dell'Identity Provider Poste Italiane conservare tutta la documentazione afferente il processo di identificazione del Titolare dell'Identità Digitale PosteID per 20 anni decorrenti dalla data di cessazione dell'Identità Digitale stessa.

In coerenza con gli avvisi n. 12 e n. 17 del 24 gennaio 2019 dell'AgID, a partire dal 1 marzo 2019, i certificati qualificati di firma rilasciati da Poste a seguito dell'identificazione del Titolare tramite identità PosteID contengono la seguente limitazione d'uso:

- OID 1.3.76.16.5 - Certificate issued through Sistema Pubblico di Identità Digitale (SPID) digital identity, not usable to require others SPID digital identity.

Il Titolare accetterà on line le Condizioni Generali di Servizio di Firma Digitale attraverso le credenziali SPID.

Il Certificatore conserverà in modalità elettronica i dati anagrafici ricevuti e generati.

9.3 Modalità di identificazione e registrazione di persone giuridiche

La richiesta di certificato per persona giuridica deve essere effettuata da una persona fisica identificata secondo le modalità di seguito descritte.

Il Titolare coincide con la persona giuridica a cui sarà intestato il Certificato Qualificato di Sigillo, il Richiedente (Responsabile Legale) coincide con la persona fisica che sottopone la richiesta al Certificatore che espleta la fase di identificazione.

Le procedure per il rilascio di un certificato per Sigillo Elettronico prevedono:

- che il Richiedente sia registrato presso il Certificatore;
- che il Richiedente venga identificato con certezza dal Certificatore;
- che il Richiedente possegga una firma digitale qualificata valida che utilizzerà per sottoscrivere tutta la documentazione prevista, in alternativa al riconoscimento de visu.

I soggetti che espletano la funzione di identificazione devono possedere requisiti e adeguata formazione in relazione ai processi legati all'attività di Registration Authority.

Il Richiedente, dovrà recarsi presso la Registration Authority portando con sé i documenti necessari

all'identificazione, la documentazione relativa alla persona giuridica, la documentazione utile ad attestare il possesso delle deleghe aziendali necessarie a presentare la richiesta a nome della persona giuridica, la documentazione contrattuale e di registrazione, l'eventuale ulteriore documentazione necessaria in relazione alla tipologia di certificato richiesto.

Nel caso il riconoscimento avvenga con firma digitale qualificata la documentazione verrà inviata dal richiedente via e-mail alla Registration Authority all'indirizzo registrazione@posteitaliane.it.

L' addetto all'identificazione ritira la documentazione presentata dal Richiedente e:

- controlla la validità del documento di identità prodotto sia in originale che in copia e verifica l'identità del Titolare;
- verifica la corrispondenza dei dati contenuti nelle copie con il documento in originale;
- verifica la completezza e la correttezza dei dati di registrazione.

L'addetto all'identificazione, dopo aver compiuto le verifiche descritte:

- fa sottoscrivere, in duplice copia i documenti di registrazione al Richiedente il quale, dopo averlo letto, lo firma per accettazione. Il Richiedente è tenuto a verificare puntualmente la correttezza delle informazioni di registrazione;
- firma e timbra le due copie dei documenti di registrazione;
- consegna una copia della documentazione di registrazione al Richiedente e trattiene l'altra.

Potrà essere inoltre designata – nei casi specifici previsti – una persona fisica incaricata (Incaricato) alla gestione del ciclo di vita dei certificati digitali.

Documenti richiesti ai fini dell'identificazione e registrazione

L'identificazione del Titolare avviene attraverso l'esibizione di uno dei documenti di riconoscimento di cui all'art.35 del D.P.R. 445/2000.tra cui:

- Carta di identità;
- Patente di guida;
- Passaporto;
- Patente Nautica;
- Libretto di Pensione;
- Porto d'armi;
- Il patentino di abilitazione alla conduzione di impianti termici;
- Tessere di riconoscimento purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato. (es. tessere AT e BT).

Inoltre, sono richiesti i seguenti documenti:

- Visura camerale;
- Eventuali deleghe formali.

I suddetti documenti devono essere validi, non scaduti e presentati in originale, corredati della relativa fotocopia.

Il Richiedente deve inoltre produrre gli estremi del codice fiscale rilasciato dallo Stato Italiano.

In caso di impossibilità di individuare un codice identificativo personale non sarà possibile proseguire l'iter di rilascio.

Il Richiedente assume la responsabilità della veridicità dei dati e dei documenti forniti per l'identificazione e registrazione.

9.4 Modalità di generazione delle chiavi per la creazione e la verifica della firma e del sigillo elettronico

L'emissione dei certificati qualificati da parte del Certificatore avviene nel rispetto delle modalità di generazione previste dagli Art.18 e Art. 33 del DPCM 22/02/2013.

La generazione delle chiavi di sottoscrizione avviene all'interno del dispositivo sicuro di firma che può essere personalizzato:

- dal Certificatore,
- dal Titolare seguendo le istruzioni e utilizzando i sistemi messi a disposizione dal Certificatore.

Il Titolare deve avvalersi solo del dispositivo di firma indicato e/o consegnato dal Certificatore.

La generazione della coppia di chiavi è effettuata mediante apparati e procedure che assicurano, in rapporto allo stato delle conoscenze scientifiche e tecnologiche, l'unicità e la robustezza della coppia generata, nonché la segretezza della chiave privata.

Il sistema di generazione delle chiavi, a norma dell'art.6, comma II, del DPCM 22 febbraio 2013 assicura:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- L'utilizzo di algoritmi che consenta l'equiprobabilità di generazione di tutte le coppie possibili;
- L'autenticazione informatica del soggetto che attiva la procedura di generazione;

Le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico sono generate utilizzando le stesse procedure adottate per la generazione delle chiavi corrispondenti a Certificati Qualificati per Firma Elettronica.

Dispositivi sicuri di firma

I dispositivi sicuri utilizzati per la generazione delle firme rispondono ai requisiti di conformità indicati nell'Allegato III della Direttiva 1999/CE/93 nonché all'articolo 35 del Codice dell'amministrazione digitale, comprovati dall'OCSI o da altro organismo designato e notificato da un altro Stato membro dell'Unione Europea.

Il dispositivo sicuro di firma può essere attivato esclusivamente dal titolare mediante credenziali di autenticazione personali prima di poter procedere alla generazione della firma.

Se il soggetto appone la sua firma per mezzo di una procedura automatica, deve utilizzare una coppia di chiavi diversa da tutte le altre in suo possesso. Se la procedura automatica fa uso di un insieme di dispositivi, deve essere utilizzata una coppia di chiavi diversa per ciascun dispositivo utilizzato dalla procedura automatica.

La duplicazione della chiave privata o dei dispositivi che la contengono è vietata.

Per la firma remota Poste Italiane prevede la replicazione in sicurezza delle chiavi private del firmatario su HSM per realizzare un servizio ad alta disponibilità nell'ambito delle configurazioni sottoposte a certificazione fra quelle previste dagli Art. 12 e Art. 13 del DPCM 22/02/2013.

9.5 Modalità di emissione dei certificati

Emissione su dispositivo smart card a cura del certificatore

- A seguito del corretto svolgimento delle attività di registrazione e identificazione del Titolare, la relativa documentazione viene inoltrata a Poste Italiane secondo le specifiche modalità operative previste.
- Il Certificatore, verificata la completezza e congruità dei dati, effettua nei casi previsti la personalizzazione del dispositivo di firma e l'emissione del certificato qualificato.
- Nel caso in cui il dispositivo sicuro di firma sia una smart card, quest'ultima e la busta cieca, contenente le credenziali segrete di accesso e sblocco della carta (PIN/PUK) e il codice di emergenza (codice di sospensione immediata), vengono inviate separatamente al Titolare.

Emissione su dispositivo smart card a cura del Titolare e del Richiedente

- Il Richiedente ed il Titolare, seguendo le istruzioni fornite ed utilizzando i sistemi messi a disposizione dal Certificatore per la specifica modalità operativa, siti eventualmente presso l'Ufficio Delegato, generano la richiesta di certificazione e la inoltrano a Poste Italiane.
- Il Titolare deve utilizzare esclusivamente il dispositivo sicuro per la generazione delle firme fornito dal certificatore, ovvero un dispositivo scelto tra quelli indicati dal certificatore stesso. Il Certificatore, ricevuta la richiesta di generazione del certificato, la verifica, attiva il processo di generazione e di invio del certificato qualificato al Titolare che ne ha fatto richiesta.
- Al Titolare viene consegnato il codice di emergenza per la sospensione immediata.

Emissione su dispositivo HSM per la creazione di una firma remota, automatica e sigillo elettronico

- A seguito del corretto svolgimento delle attività di identificazione e registrazione del Titolare, la relativa documentazione viene raccolta e conservata secondo le specifiche modalità operative previste.
- Il Certificatore, con servizi che espone su canale sicuro e su protocollo SSL/TLS per indirizzi di rete abilitati, riceve la richiesta da parte del Titolare di generazione del certificato, ne verifica l'autenticità, e attiva il processo di emissione e di restituzione del certificato per la copia sul dispositivo HSM.
- Il processo di attribuzione e di verifica delle credenziali di autenticazione del Titolare del certificato di firma/sigillo elettronico avviene in conformità con i metodi di strong authentication dichiarati dall'accertamento di conformità del QSSCD.
- Per la creazione di una firma remota, automatica e sigillo elettronico, il Certificatore garantisce che la chiave privata:
- sia riservata;
- non possa essere derivata e che la relativa firma sia protetta da contraffazioni;
- possa essere sufficientemente protetta dal Titolare dall'uso da parte di terzi.
- In funzione della soluzione di firma e del particolare QSSCD adottato - AliasLab CryptoAccelerator – e della modalità di firma, il Certificatore assicura che l'accesso da parte del Titolare alla chiave privata del certificato avvenga con l'adozione dei seguenti metodi di autenticazione:

QSSCD CryptoAccelerator – Firma Remota

- User-Id univoca, associata dal sistema al Titolare del certificato
- PIN personale
- SMS OTP, inviato su un recapito di telefonia mobile fornito dal titolare in fase di registrazione e verificato dal Certificatore

QSSCD CryptoAccelerator – Firma Automatica e Sigillo Elettronico

- User-Id univoca, associata dal sistema al Titolare del certificato;
- PIN personale provvisorio (da cambiare in fase di attivazione del certificato).

Per l'utilizzo dei certificati, oltre alle credenziali precedentemente indicate, è richiesta una coppia di credenziali aggiuntive per l'autenticazione al layer applicativo del sistema di firma digitale.

Per le soluzioni di firma remota, automatica e sigillo elettronico che prevedono l'emissione di certificati di firma qualificata su dispositivo HSM, il Certificatore Poste Italiane richiede all'AgID, conformemente all'Art. 11 del DPCM del 22/02/2013 e ai sensi dell'art. 35 del CAD, comma 5, la valutazione dell'adeguatezza tecnologica dei sistemi di autenticazione per quanto riguarda l'interazione fra il Titolare e il QSSCD, tenendo conto del traguardo di sicurezza del dispositivo e del contesto di utilizzo della soluzione.

9.6 Revoca, sospensione e riattivazione dei certificati qualificati di firma digitale e sigillo elettronico

La revoca di un certificato qualificato è l'operazione con cui il Certificatore annulla la validità, con efficacia non retroattiva, di un certificato.

La sospensione di un certificato qualificato è l'operazione con cui il Certificatore sospende la validità del certificato.

Le informazioni sulla revoca e sospensione dei certificati sono pubblicate dal Certificatore e rese disponibili tramite le liste di revoca e sospensione (CRL/CSL).

La revoca o la sospensione di un certificato qualificato viene effettuata, dal Certificatore, mediante l'inserimento del suo codice identificativo in una delle liste di certificati revocati e sospesi (CRL/CSL).

Le liste di revoca e sospensione sono pubblicate ed accessibili all'indirizzo riportato all'interno del certificato.

Se la revoca avviene a causa della possibile compromissione della segretezza della chiave privata, il Certificatore procede tempestivamente alla pubblicazione dell'aggiornamento della lista.

All'interno di una stessa lista sono contenuti sia i certificati revocati, sia quelli sospesi.

Il Certificatore provvede a rimuovere, dalla lista, i certificati che non sono più sospesi a seguito della riattivazione, nel qual caso, conformemente alle disposizioni vigenti, il certificato, ai fini del valore giuridico delle firme ad esso associate, è da considerarsi come mai sospeso.

Il certificato, revocato o sospeso, rimane nella lista di revoca e sospensione (CRL/CSL) anche successivamente alla sua naturale scadenza.

In caso di revoca di un certificato qualificato sospeso, la data della revoca decorre dalla data di inizio del periodo di sospensione.

La revoca, la sospensione e la riattivazione di un certificato sono registrate nel Giornale di controllo ed hanno effetto a partire dal momento della pubblicazione della lista che le contiene. Il momento di pubblicazione della lista è asseverato mediante l'apposizione di un riferimento temporale.

Contestualmente alla pubblicazione della lista di revoca e sospensione, il Certificatore provvede ad inviare comunicazione dell'avvenuta revoca/sospensione/riattivazione del certificato al Titolare, al Terzo Interessato e al Richiedente.

Inoltre, potranno essere disponibili ulteriori modalità di accesso alle informazioni di revoca o sospensione, in particolare attraverso l'OCSP.

Il certificato qualificato può essere revocato o sospeso su iniziativa del:

- Certificatore
- Titolare
- Terzo Interessato

- Il Richiedente
- Responsabile legale/Incaricato per certificato digitale per persona giuridica

Il certificato qualificato è revocato o sospeso dal certificatore, ove quest'ultimo abbia notizia della compromissione della chiave privata o del dispositivo sicuro per la generazione delle firme.

Il Certificatore, qualora venga a conoscenza di sospetti abusi, falsificazioni, negligenze, si riserva la facoltà di revocare o sospendere i certificati, previa comunicazione motivata, salvo i casi d'urgenza, ai Titolari degli stessi.

Richiesta di Revoca

Il Titolare deve procedere alla richiesta di revoca nei seguenti casi:

- perdita del possesso del dispositivo di firma (smarrimento, furto);
- guasto o malfunzionamento del dispositivo di firma;
- compromissione della segretezza della chiave privata;
- variazione di uno qualunque dei dati presenti nel certificato (ad esempio fine del potere di rappresentanza dichiarato dal Terzo Interessato o perdita del ruolo dichiarato nel certificato).

Il Terzo Interessato ha l'onere di richiedere la revoca dei certificati qualificati ogni qualvolta vengano meno i requisiti in base ai quali questi ultimi sono stati rilasciati ai Titolari. In caso di cessazione o modifica delle qualifiche o del titolo inserite nel certificato su richiesta del terzo interessato, la richiesta di revoca è inoltrata non appena il terzo venga a conoscenza della variazione di stato.

Il Terzo Interessato ha la facoltà di richiedere la revoca dei certificati nel caso di abusi, falsificazioni o di uso non conforme degli stessi agli scopi per i quali sono stati emessi, e per ogni altra motivazione dallo stesso ritenuta valida.

Il Titolare, il Richiedente, il Terzo Interessato e Il Responsabile legale/Incaricato hanno la facoltà di richiedere la revoca di un certificato per un qualunque motivo dagli stessi ritenuto valido ed in qualsiasi momento.

La richiesta di revoca deve essere inoltrata, al Certificatore, munita di sottoscrizione da parte del soggetto che ha presentato la richiesta medesima (Titolare, Terzo Interessato, Richiedente, Responsabile legale/Incaricato).

Il Titolare, il Richiedente, il Terzo Interessato e il Responsabile legale/Incaricato possono inoltrare la richiesta di revoca del certificato qualificato attraverso le seguenti modalità:

- <u>Richiesta on-line</u>

Per ciascun certificato qualificato emesso il Certificatore fornisce al Titolare un codice riservato (codice di revoca/sospensione/riattivazione), da utilizzare per richiedere la revoca del certificato tramite l'apposito servizio on-line. Il codice riservato viene comunicato al Titolare tramite modalità che ne

assicurino la segretezza.

Il servizio on-line di revoca/sospensione/riattivazione del certificato prevede che il Titolare inserisca il codice di revoca/sospensione/riattivazione e il codice identificativo attribuito dal Certificatore.

Sono garantiti i seguenti livelli di servizio: la richiesta viene presa in carico entro 24 ore dalla sottomissione on-line della richiesta, la revoca viene effettuata entro 1 ora dalla presa in carico della richiesta.

- Richiesta cartacea con firma autografa

Il Titolare/Terzo Interessato/Richiedente/Responsabile legale/Incaricato compila e sottoscrive un apposito modulo cartaceo.

Il Titolare consegna il modulo compilato e sottoscritto presso un Ufficio Delegato, solo se non è più in possesso dei codici per utilizzare il servizio on-line e per apporre la sua firma digitale.

Per quanto riguarda un certificato per persona giuridica, il Responsabile legale/Incaricato consegna il modulo compilato e sottoscritto presso la Registration Authority.

Il Terzo Interessato/Richiedente invia al Certificatore, all'indirizzo registrazione@postecert.it, copia del modulo compilato e sottoscritto unitamente a copia di un documento di riconoscimento in corso di validità.

Il modulo deve essere presentato/inviato almeno 1 (un) giorno feriale prima del termine di decorrenza indicato nella richiesta stessa. L'attivazione della procedura di revoca/sospensione/riattivazione avviene entro 24h lavorative (calcolate nei giorni/orari lun-ven 9-18) dalla data e ora di ricezione della richiesta.

- Richiesta sottoscritta digitalmente

Il Titolare/Terzo Interessato/Richiedente/Responsabile legale/Incaricato inoltra la richiesta al Certificatore almeno 1 (un) giorno feriale prima del termine di decorrenza indicato nella stessa, compilando e firmando digitalmente l'apposito modulo elettronico reso disponibile dal certificatore e inviandolo all'indirizzo registrazione@postecert.it

L'attivazione della procedura di revoca/sospensione avviene entro 24h lavorative (calcolate nei giorni/orari lun-ven 9-18) dalla ricezione della e-mail.

Il certificatore conserva le richieste di revoca per 20 (venti) anni.

Richiesta di Sospensione

Il Titolare, il Richiedente, il Terzo Interessato e il Responsabile legale/Incaricato hanno la facoltà di richiedere la sospensione di un certificato per un qualunque motivo dagli stessi ritenuto valido ed in qualsiasi momento.

Il Certificatore sospende il certificato ogni qualvolta, ricevuta una richiesta di revoca da parte del Titolare, del Richiedente o del Terzo Interessato, non ha la possibilità di accertare in tempo utile l'autenticità della richiesta stessa o vi siano dubbi sulla validità del certificato o sulla sicurezza del di-

spositivo.

Il Certificatore, qualora venga a conoscenza di sospetti usi non conformi, si riserva la facoltà di sospendere i certificati, previa comunicazione ai Titolari, salvo i casi d'urgenza.

Il Titolare, il Richiedente, il Terzo Interessato e il Responsabile legale/Incaricato possono inoltrare la richiesta di sospensione del certificato qualificato attraverso le medesime modalità sopra descritte per la revoca del certificato.

La richiesta di sospensione inoltrata nelle modalità descritte potrà essere seguita da una richiesta di revoca o di riattivazione del certificato.

Richiesta per la riattivazione di un certificato precedentemente sospeso

La riattivazione di un certificato sospeso ne determina nuovamente la validità (pertanto la cancellazione dalle Liste di revoca e sospensione).

Il Titolare, il Richiedente, il Terzo Interessato e Responsabile legale/Incaricato possono inoltrare la richiesta di riattivazione del certificato qualificato attraverso le medesime modalità sopra descritte per la revoca e la sospensione del certificato. Ad eccezione della modalità di richiesta sottoscritta digitalmente che non si applica per il Titolare: se il certificato è sospeso il titolare non può apporre la propria firma digitale.

La richiesta di riattivazione non sarà accettata se il certificato di firma digitale/sigillo elettronico risulta revocato.

Disponibilità dei servizi di revoca o sospensione

Il Certificatore predispone, per ogni modalità di inoltro delle richieste di revoca o sospensione, una diversa disponibilità del servizio ad essa connessa:

- in caso di richiesta di revoca o sospensione presentata presso l'Ufficio Delegato, gli orari di disponibilità del servizio sono resi noti al pubblico dall'Ufficio stesso;
- per le richieste di revoca o sospensione immediata inoltrate via Internet, il servizio di accettazione delle richieste stesse è disponibile 24 ore su 24
- in caso di richiesta di revoca o sospensione inoltrata via e-mail, il servizio di accettazione è disponibile dal lunedì al venerdì dalle 9 alle 17

Aggiornamento delle CRL e delle CSL

Le liste di revoca o sospensione dei certificati sono aggiornate in seguito ad ogni richiesta di revoca o sospensione.

La pubblicazione delle Liste di revoca e sospensione avviene, comunque, al massimo ogni 24 (ventiquattro) ore.

9.7 Rinnovo del certificato qualificato utilizzato su dispositivi smart card

Il servizio di rinnovo non è previsto per certificati emessi su dispositivi smart card e HSM.

Il Titolare che intende continuare ad avvalersi del servizio di certificazione, dovrà richiedere una nuova smart card e certificato.

Periodicità e modalità alternative potranno essere definite negli accordi stipulati tra le Parti.

10 Registro dei certificati

Il Certificatore pubblica nel Registro dei certificati:

1. lista dei certificati revocati (CRL);
2. lista dei certificati sospesi (CSL).

Inoltre, il Certificatore, dietro consenso da parte del Titolare, pubblica i certificati emessi nel Registro dei Certificati.

10.1 Modalità di gestione del Registro dei certificati

Il Certificatore mantiene una copia di riferimento del Registro dei certificati inaccessibile dall'esterno (Directory Server Master), allocata su un sistema sicuro istallato in locali protetti.

Sistematicamente, verifica la conformità tra la copia operativa (Directory Server Shadow) e la copia di riferimento del Registro, annotando ogni discordanza nel Registro operativo.

Modifiche al contenuto del Registro dei certificati sono effettuate esclusivamente da personale autorizzato. Tali operazioni sono inoltre registrate sul Giornale di controllo.

La data e l'ora di inizio e fine di ogni intervallo di tempo nel quale il Registro dei certificati non risulta accessibile dall'esterno, nonché quelle relative a ogni intervallo di tempo nel quale una sua funzionalità interna non risulta disponibile, sono annotate sul Giornale di controllo e comunicate all' Agenzia per l'Italia Digitale e agli utenti, come previsto dall'art. 32, comma 3, lettera m-bis) del D.lgs 7 marzo 2005, n. 82.

Il Certificatore cura l'allineamento tra copia di riferimento e copia operativa e mantiene una copia di sicurezza (backup) del Registro dei certificati.

Il Certificatore provvede all'aggiornamento del Registro dei certificati quando:

- emette nuovi certificati;
- pubblica le Liste di revoca/sospensione con la periodicità definita nel paragrafo "Aggiornamento delle CRL e delle CSL" del presente Manuale Operativo.

10.2 Modalità di accesso al Registro dei certificati

Il registro dei certificati di Poste Italiane, contiene i certificati emessi e pubblicati dietro consenso da parte del Titolare, è un Internet Directory Server compatibile con le specifiche X.500 1993 e supporta LDAP v.3.

Il Registro dei certificati è pubblicamente consultabile 24 ore al giorno, 7 giorni la settimana, salvo manutenzione programmata, all'indirizzo ldap://certificati.postecert.it.

Le liste pubblicate dei certificati revocati e sospesi, nonché i certificati qualificati resi accessibili alla

consultazione del pubblico, sono utilizzabili da chi le consulta per le sole finalità di applicazione delle norme che disciplinano la verifica e la validità della firma qualificata di firma digitale.

Sezione IV –

Procedure operative per la firma e la verifica

11 Modalità operative per la generazione e la verifica delle firme

11.1 Generazione della firma

Si distinguono due modalità operative per l'utilizzo della firma digitale:

- in "locale": la firma digitale viene generata in uno strumento nel possesso fisico del titolare, smartcard o token
- da "remoto": la firma digitale viene generata usando strumenti di autenticazione (user id+ PIN +OTP) in possesso del Titolare che consentono la generazione della propria firma su un dispositivo HSM custodito dal prestatore del servizio fiduciario qualificato.

Poste Italiane, agli utenti che acquistano il servizio/prodotto di firma, offre l'apposito client firmaOK! con diverse funzionalità.

L'operazione di generazione della firma attraverso firmaOK! permette di:

- ➲ selezionare il certificato (e la relativa coppia di chiavi di firma), in corso da validità, da utilizzare;
- ➲ visualizzare il documento informatico che si intende firmare;
- ➲ inserire il PIN della smart card oppure le credenziali per la Firma Digitale Remota;
- ➲ salvare sul proprio computer il file firmato.

11.2 Sistema di verifica delle firme qualificate

Il documento informatico firmato digitalmente, può essere verificato dal destinatario:

- ➲ tramite l'applicativo client fornito da Poste Italiane ai propri titolari dei certificati qualificati;
- ➲ accedendo alla funzionalità che Poste Italiane rende disponibile on–line sul sito postecert.poste.it e sul sito https://www.poste.it/prodotti/firma-digitale-remota.html.

I suddetti sistemi verificano la conformità al regolamento europeo UE 910/2014 e soddisfano i requisiti normativi previsti dalla Determinazione n. 147/2019 dell'AgID. Nell'ambito della verifica vengono effettuate le seguenti operazioni:

- la convalida dell'integrità - che accerta che il documento non sia stato modificato dopo la firma;
- la verifica della credibilità – che verifica se il documento è stato firmato da un soggetto "credibile" nell'ambito dell'elenco pubblico dei certificatori in conformità al Regolamento eIDAS la verifica di validità - controlla che il certificato non sia scaduto;
- la verifica di CRL/CSL - che verifica che il certificato non risulti revocato o sospeso;
- la verifica alla data – che verifica la validità del certificato a partire dalla data presente nel file firmato (se marca temporale) o a partire dalla data impostata dal Titolare;
- la lettura delle informazioni presenti nel certificato
- il salvataggio dei risultati delle operazioni di verifica su apposito supporto informatico

Il sistema di verifica consente, per via telematica, l'aggiornamento delle informazioni pubblicate nell'Elenco Pubblico dei Certificatori.

Nel corso della verifica il destinatario deve controllare la presenza di eventuali limitazioni d'uso nel certificato del sottoscrittore; deve verificare inoltre la presenza nel documento verificato di eventuali macro istruzioni o codici eseguibili che renderebbe nullo il documento firmato digitalmente.

11.3 Firma digitale verificata

In coerenza con la Determinazione n. 63 – 2014, il certificatore accreditato Poste Italiane, nel caso in cui il dispositivo di generazione della firma sia sotto il suo pieno controllo, prevede la disponibilità di una modalità di firma digitale atta a garantire, in ogni circostanza, la verifica della validità del certificato qualificato al momento della generazione della firma, dichiarando tale caratteristica all'interno del certificato qualificato.

Tale dichiarazione è effettuata attraverso la codifica nel campo CertificatePolicies del certificato qualificato dei seguenti elementi:

a. PolicyIdentifier object identifier (OID) 1.3.76.16.3;

b. i seguenti userNotice di tipo explicitText:

- The qualified certification service provider that issued this certificate ensures that the signatures based on this certificate have been generated during the period of validity of the certificate

- Il certificatore garantisce che le firme basate su questo certificato qualificato sono valide in quanto il certificato ad esse associato era valido al momento della generazione delle firme.

Nella firma verificata l'attributo signingTime, contenente l'indicazione temporale del momento di generazione della firma, è valorizzato dal certificatore Poste Italiane.

L'ora assegnata al riferimento temporale corrisponde alla scala di tempo UTC(IEN), di cui al decreto del Ministro dell'industria, del commercio e dell'artigianato 30 novembre 1993, n. 591, con una diffe-

renza non superiore ad un minuto primo.

La verifica delle firme digitali basate su certificati conformi alla Deliberazione n. 63 – 2014, non richiede l'accesso alle informazioni di revoca pubblicate dal certificatore ai sensi dell'articolo 34, comma 1, del DPCM 22 febbraio 2013.

11.4 Formato dei documenti informatici

Gli applicativi di *Office Automation*, utilizzati per la generazione di documenti informatici, mettono a disposizione nativamente alcune funzionalità, che possono rendere dinamico il contenuto del documento, in funzione del contesto e del momento della sua visualizzazione (ad esempio l'aggiornamento automatico di una data presente nel documento o altre macroistruzioni similari).

Il DPCM 22/2/2013 Art.4, comma 3, sancisce che l'apposizione della firma digitale su documenti elettronici contenenti "macroistruzioni o codici eseguibili, tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati", non produce gli effetti previsti dalla normativa vigente per la firma elettronica qualificata.

Il Certificatore, attraverso le applicazioni distribuite, visualizza al Titolare, in fase di sottoscrizione, un messaggio informativo sulla possibile presenza di "macro o codici eseguibili tali da attivare funzionalità che possano modificare gli atti, i fatti o i dati nello stesso rappresentati". Il titolare deve accertarsi che il documento presenti un formato di tipo statico e non incorpori, quindi, campi dinamici come sopra descritti.

Sezione V –

Gestione delle chiavi di certificazione e di marcatura temporale

12 Chiavi di certificazione

Il Certificatore si avvale delle seguenti chiavi di certificazione:

- chiavi di certificazione per firmare digitalmente i certificati relativi alle chiavi di sottoscrizione, le liste di revoca e sospensione (CRL/CSL);
- chiavi di certificazione per firmare digitalmente i certificati relativi alle chiavi di marcatura temporale.

Le chiavi di certificazione possono inoltre essere utilizzate per le seguenti finalità:

- rilascio di certificati di autenticazione;
- fino alla revoca dell'Agenzia con il provvedimento di cui al successivo capoverso, emissione di certificati elettronici per usi diversi dalla Firma Digitale basata su certificato qualificato, referenziati in apposite policy identificate con specifici OID riportati nel certificato, oltre che caratterizzati da keyUsage diversi da nonRepudiation.

L'AgID - con provvedimento del 24 Marzo 2016 - ha revocato l'autorizzazione per l'utilizzo delle chiavi di certificazione ai fini della sottoscrizione di certificati con keyUsage diversi da nonRepudiation. Tale revoca ha avuto effetto a partire dal 30 Giugno 2016. Pertanto a partire da tale data non è più possibile utilizzare le chiavi di certificazione per le finalità oggetto della revoca. Non è invece oggetto di revoca l'utilizzo delle chiavi di certificazione per la sottoscrizione di certificati di autenticazione destinati alle Carte Nazionali dei Servizi.

12.1 Generazione delle chiavi di certificazione

La generazione delle chiavi di certificazione è effettuata esclusivamente in presenza del Responsabile del Servizio della Certificazione e Validazione Temporale, che le utilizzerà. La generazione della coppia di chiavi di certificazione avviene all'interno del dispositivo di firma, personalizzato, dalla postazione predisposta a tale funzione, dal Certificatore.

Per ciascuna chiave di certificazione il certificatore genera un certificato sottoscritto con la chiave privata della coppia cui il certificato si riferisce.

Le chiavi corrispondenti a Certificati Qualificati per Sigillo Elettronico sono generate utilizzando le stesse procedure adottate per la generazione delle chiavi corrispondenti a Certificati Qualificati per Firma Elettronica.

12.2 Revoca dei certificati relativi a chiavi di certificazione

Il Certificatore procede alla revoca del certificato relativo ad una coppia di chiavi di certificazione esclusivamente nei seguenti casi:

- compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
- guasto del dispositivo di firma;
- cessazione dell'attività, salvo il caso in cui sia individuato un certificatore sostitutivo.

La revoca del certificato relativo ad una coppia di chiavi di certificazione è notificata all' Agenzia per l'Italia Digitale ed a tutti i possessori di certificati qualificati, sottoscritti con la chiave privata appartenente alla coppia revocata, entro le 24 ore successive.

I certificati qualificati, per i quali venga revocato il certificato relativo alla chiave con cui sono stati sottoscritti, vengono anch'essi revocati.

Il Certificatore procede alla revoca dei certificati relativi alle chiavi di certificazione, inserendoli nella Lista di revoca (CRL), che rende pubblica dopo avervi apposto un riferimento temporale.

La revoca è annotata nel Giornale di controllo.

12.3 Sostituzione delle chiavi di certificazione

La procedura di sostituzione delle chiavi di certificazione assicura che non siano stati emessi certificati qualificati con data di scadenza posteriore al periodo di validità del certificato relativo alla coppia sostituita.

I certificati generati a seguito della sostituzione delle chiavi di certificazione sono inviati all' Agenzia per l'Italia Digitale, che provvede all'aggiornamento della lista dei certificati delle chiavi di certificazione contenuta nell'Elenco Pubblico dei Certificatori ed al suo inoltro ai Certificatori per la pubblicazione.

13 Chiavi di marcatura temporale

Le chiavi di marcatura temporale sono destinate alla generazione e verifica delle marche temporali.

La marca temporale è un servizio che il certificatore Poste Italiane, in qualità di prestatore di servizi fiduciari qualificato, eroga in accordo con gli articoli 41 e 42 del Regolamento eIDAS, in accordo con quanto previsto dai requisiti descritti in ETSI EN 319 422, e con la specifica RFC-5280, consentendo di associare data e ora, certe e legalmente valide, a un documento informatico e permettendo una validazione temporale del documento opponibile a terzi.

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata ad un sistema di validazione temporale e dal relativo certificato deve essere possibile individuare tale sistema di validazione.

13.1 Generazione delle chiavi di marcatura temporale

Per limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale sono sostituite ed un nuovo certificato è emesso, dopo non più di un anno di utilizzo, indipendentemente dalla durata del loro periodo di validità e senza revocare il corrispondente certificato. La generazione delle chiavi di marcatura temporale è attivata all'interno di un dispositivo sicuro di firma.

La marca temporale viene firmata ed emessa da una specifica autorità di certificazione denominata Time Stamping Authority (TSA) che emette e firma le marche temporali mediante uno o più sistemi dedicati (Time Stamping Server, TSS o TSU) al quale gli utenti indirizzano le loro richieste.

Per la sottoscrizione dei certificati relativi a chiavi di marcatura temporale vengono utilizzate chiavi di certificazione diverse da quelle utilizzate per i certificati relativi alle chiavi di sottoscrizione.

La lunghezza delle chiavi di marcatura temporale è di almeno 2048 bit.

13.2 Revoca dei certificati relativi a chiavi di marcatura temporale

Il Certificatore procede alla revoca del certificato, relativo ad una coppia di chiavi di marcatura temporale, esclusivamente nei seguenti casi:

- compromissione della chiave privata, intesa come diminuita affidabilità nelle caratteristiche di sicurezza della chiave privata;
- guasto del dispositivo sicuro di firma.

Il Certificatore procede alla revoca dei certificati relativi a chiavi di marcatura temporale, inserendoli nella Lista di revoca (CRL), che rende pubblica dopo avervi apposto un riferimento temporale.

La revoca viene annotata nel Giornale di controllo.

13.3 Sostituzione delle chiavi di marcatura temporale

La sostituzione delle chiavi di marcatura temporale è effettuata con frequenza annuale.

Sezione VI –

Modalità per l'apposizione e la definizione del riferimento temporale

14 Riferimento temporale

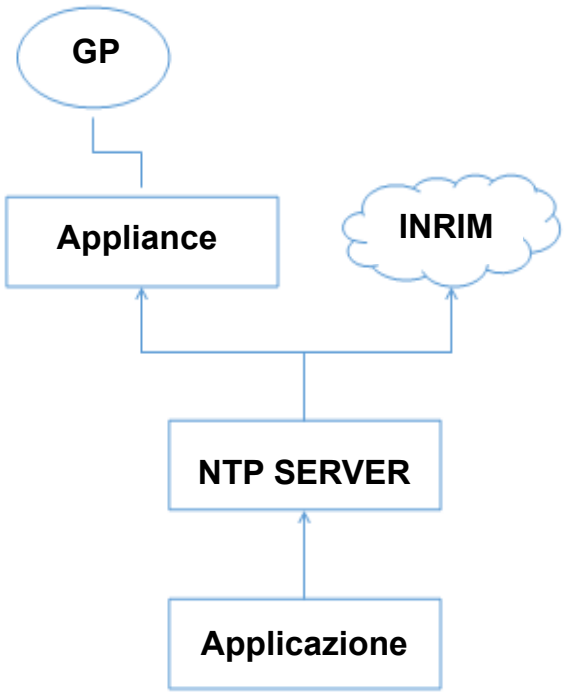
Poste Italiane appone sul Giornale di Controllo riferimenti temporali , in accordo con i requisiti definiti nelle *"Audit logging procedures"* dello standard ETSI EN 319411-1.

La data e l'ora contenute nel riferimento temporale apposto al Giornale di Controllo, sono specificate con riferimento al Tempo Universale Coordinato (UTC).

L'ora assegnata ad un riferimento temporale corrisponde al momento della sua generazione, con una differenza inferiore al minuto secondo rispetto alla scala di tempo UTC.

Si considera come sorgente del riferimento temporale l'orologio di sistema, la cui precisione è garantita dalla sua sincronizzazione con una sorgente esterna, che mantiene un'informazione temporale corrispondente alla scala temporale UTC.

La sincronizzazione oraria dei server all'interno della rete della Certification Authority si basa sul servizio NTP che è sincronizzato attraverso una modalità primaria basata su un segnale GPS che utilizza un appliance della Symmetricom oltre che da una modalità secondaria basata su un servizio esposto attraverso internet dall'INRIM (Istituto Elettrotecnico Nazionale "Galileo Ferraris" di Torino).



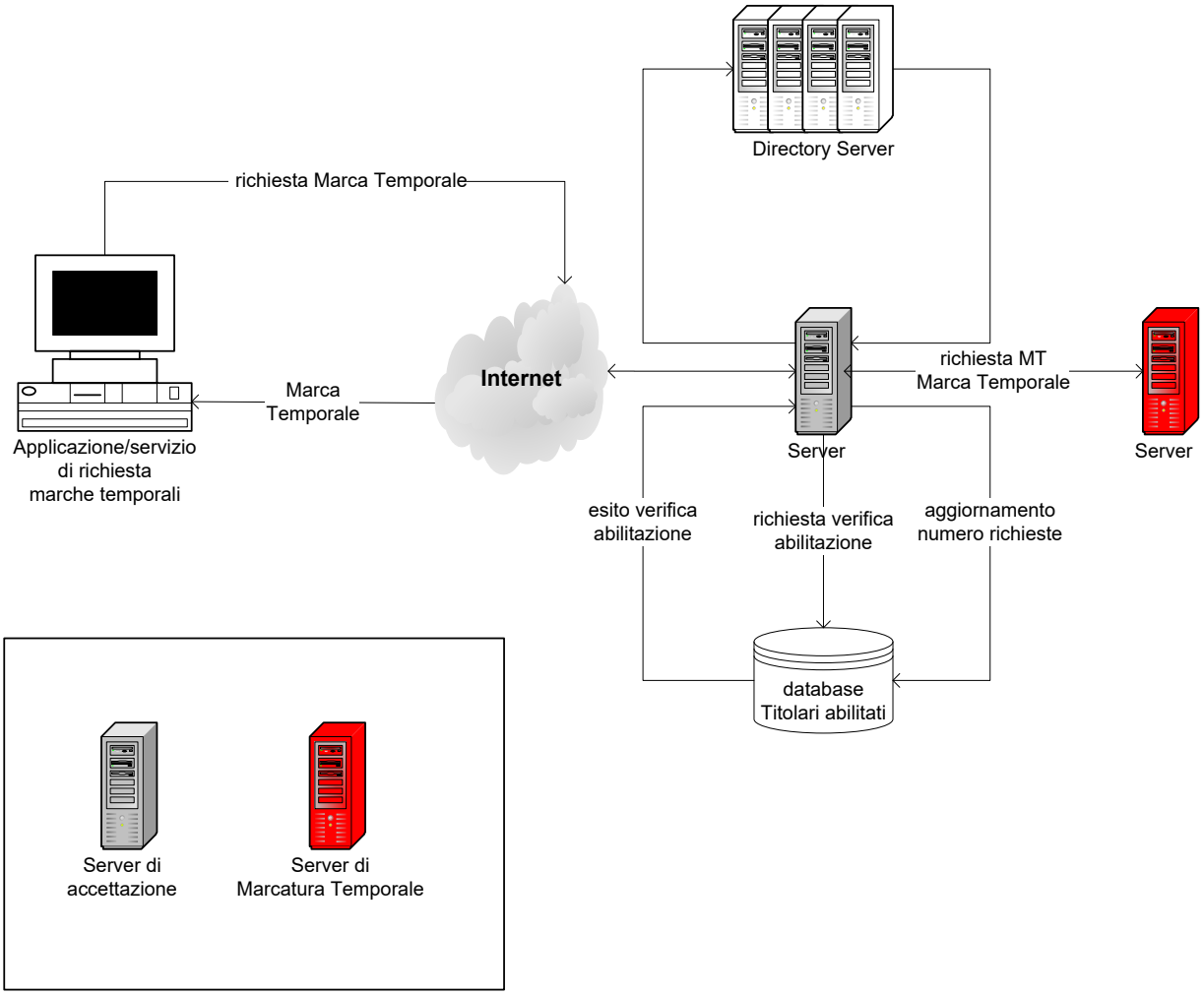
15 Marcatura temporale

La marcatura temporale è un particolare riferimento temporale, realizzato in conformità con le specifiche RFC 3161 e RFC 3628 e in grado di soddisfare i requisiti generali descritti in ETSI EN 319 421

La marca temporale qualificata emessa da Poste Italiane in particolare contiene le seguenti informazioni:

- Distinguished Name della Time Stamp Authority di Poste Italiane;
- numero di serie della marca temporale;
- algoritmo di sottoscrizione della marca temporale;
- identificativo del certificato del TSS relativo alla chiave di verifica della marca temporale;
- data ed ora di generazione, con riferimento al Tempo Universale Coordinato (UTC);
- algoritmo di hash utilizzato per generare l'impronta;
- valore dell'impronta del documento sottoposto a validazione temporale;
- precisione del riferimento temporale;
- OID della policy di time-stamp richiesto dallo standard ETSI (0.4.0.2023.1.1);
- estensione esi4-qtstStatement-1.
- url di pubblicazione della Dichiarazione di Trasparenza (PKI Disclosure Statement).

L'architettura del sistema di validazione temporale (TSA – *Time Stamping Authority*) prevede un server di accettazione delle richieste, che richiede l'emissione delle marche ad un server di marcatura temporale sui protocolli TCP (Transfer Control Protocol) e HTTP (Hypertext Transfer Protocol).



Il server di accettazione è un'applicazione server stand alone, in esecuzione su di una piattaforma Linux, in ascolto su una porta TCP/IP. Tramite tale porta, riceve le richieste dalle applicazioni/servizi e invia di ritorno le relative risposte, in conformità allo standard IETF corrispondente. Il formato della struttura dati, emessa dal server di marcatura temporale, è conforme alla normativa vigente. Il *time stamp token* emesso e la firma ad esso apposta sono incapsulati nella struttura dati firmata "*SignedData*".

15.1 Modalità di richiesta del servizio di marcatura temporale

Il servizio di marcatura temporale nasce come servizio centralizzato, il cui destinatario è, a sua volta, un servizio o un'applicazione. L'applicazione chiamante genera l'impronta del documento elettronico utilizzando l'algoritmo di hash SHA-256, firma le richieste di marche temporali e le trasmette, via http o https, al server di accettazione del servizio centralizzato di Poste Italiane, che restituisce la marca temporale emessa. Le modalità di inoltro della richiesta e di utilizzo di tale servizio vengono regolate da appositi accordi tra le Parti.

Il servizio di marcatura temporale è disponibile ai soli utenti abilitati: il sistema di TSA di Poste Ita-

liane, verificata l'autenticità della richiesta e l'abilitazione del Titolare, emette la marca temporale e la restituisce al servizio/applicazione chiamante.

15.2 Validità della marca temporale

Tutte le marche temporali emesse vengono conservate da Poste Italiane per un periodo non inferiore a venti (20) anni. La marca temporale è valida per l'intero periodo di conservazione.

SEZIONE VII –

Uffici Delegati – verifiche ispettive periodiche

16 Verifiche periodiche

Poste Italiane concorda con gli Uffici Delegati un piano di attività di verifiche periodiche tese ad assicurare il rispetto delle procedure concordate in merito alla delega delle funzioni di identificazione dei titolari e di raccolta e trasmissione dei dati di registrazione.

In particolare, qualora l'accordo di delega coinvolga anche la fornitura di apposite soluzioni di personalizzazione locale delle smart card, le verifiche saranno tese a rilevare la permanenza dei requisiti richiesti per il loro utilizzo sicuro e limitato al personale autorizzato.