Manuale Operativo del
Certificatore Accreditato In.Te.S.A. S.p.A.
per le procedure di firma remota nell'ambito dei servizi di CABEL HOLDING S.p.A. e di aziende da essa partecipata

Codice documento: MO_CB
Data emissione: 27/06/2016
Ver.02

VERSIONI

Versione n°:	**01**	**Data Revisione:**	**20/01/2015**
Descrizione modifiche:	**nessuna**		
Motivazioni:	**primo rilascio**		
Versione n°:	**02**	**Data Revisione:**	**27/06/2016**
Descrizione modifiche:	**Aggiornamento dati societari e logo** **Formattazione Documento**		
Motivazioni:	**Variazione dati societari e logo**		

Sommario

A. Il Manuale Operativo

A.1. Proprietà intellettuale

Questo documento è il Manuale Operativo per la procedura di Firma Digitale Remota nell'ambito dei servizi forniti da *CABEL HOLDING S.p.A. - Sede Legale Via Cherubini 99 - 50053 Empoli (FI); Tel. 0571/020.000 Web: www.cabel.it; - Codice fiscale e N. Iscrizione al Registro delle Imprese di Firenze 01085080495 R.E.A. FI 0454743 – Partita IVA 044929070480* e da banche in possesso di una quota di capitale di Cabel Holding S.p.A., aziende e banche controllate e/o partecipate da Cabel Holding S.p.A. che possono erogare il servizio descritto in questo manuale e di seguito definite insieme a Cabel Holding S.p.A. "Gruppo Cabel":

- Banche in possesso di quote di capitale di Cabel Holding S.p.A.:
  - Banca di credito cooperativo di Cambiano
  - Banca di Pisa e Fornacette credito cooperativo
  - Banca di credito cooperativo di Castagneto Carducci
  - Banca di Viterbo credito cooperativo
- Aziende e banche controllate e/o partecipate:
  - Cabel Industry S.p.A.
  - Cabel Istituto di Pagamento S.c.p.A.
  - Invest Banca S.p.A.
  - DotDigital S.r.l.

Il Manuale Operativo descrive le procedure e relative regole utilizzate dal Certificatore Accreditato In.Te.S.A. S.p.A. (di seguito "Certificatore" o "INTESA") per l'emissione dei Certificati Qualificati, la generazione e la verifica della firma elettronica qualificata ai clienti delle società del gruppo Cabel (di seguito queste società verranno identificate genericamente con il termine "Provider") nell'ambito dei servizi offerti dalle stesse società.

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

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

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

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

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

A.2. Validità

Quanto descritto in questo documento si applica al Certificatore, cioè alle sue infrastrutture logistiche e tecniche e al suo personale, ai Titolari dei certificati da esso emessi e a quanti utilizzino tali certificati per verificare l'autenticità e l'integrità dei documenti cui sia apposta una firma elettronica qualificata relativa ad essi, anche avvalendosi delle marche temporali emesse da INTESA.

L'uso delle chiavi e dei relativi certificati emessi è regolato da quanto disposto dall'Art.5 del Decreto, al comma 4:

Ai fini del presente decreto, le chiavi di creazione e verifica della firma e i correlati servizi, si distinguono secondo le seguenti tipologie:

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

B. Generalità

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

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

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

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.02 del Manuale Operativo del Certificatore Accreditato In.Te.S.A. S.p.A. per le procedure di firma remota nell'ambito dei servizi di Cabel Holding SpA, rilasciato il 27/06/2016, in conformità con l'Art.40 del Decreto.

L'object identifier (OID) di questo documento è 1.3.76.21.1.50.2.

Il presente Manuale Operativo è pubblicato e consultabile per via telematica anche presso l'indirizzo Internet:

http://e-trustcom.intesa.it/ca_pubblica/mo_CB.pdf

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

Lo stesso manuale operativo viene pubblicato e aggiornato in simultanea anche sul sito delle aziende del Gruppo Cabel.

B.2. Dati identificativi del Certificatore

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

Denominazione sociale	**In.Te.S.A. S.p.A.**
Indirizzo della sede legale	**Strada Pianezza, 289** **10151 Torino**
Legale Rappresentante	**Amministratore Delegato**
Registro delle Imprese di Torino	**N. Iscrizione 1692/87**
N. di Partita I.V.A.	**05262890014**
N. di telefono (centralino)	**+39.011.19216.111**
Sito Internet	**www.intesa.it**
N. di fax	**+39.011.19216.375**
Indirizzo di posta elettronica	**marketing@intesa.it**
Indirizzo (URL) registro dei certificati	**ldap://x500.e-trustcom.intesa.it**
ISO Object Identifier (OID)	**1.3.76.21.1**

B.3. Responsabilità del Manuale Operativo

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

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

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

B.4. Entità coinvolte nei processi

All'interno della struttura del certificatore vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati.

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

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

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

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

B.5. Certification Authority (Certificatore Accreditato)

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

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

B.6. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (Firma Remota nell'ambito delle applicazioni di firma descritte in questo Manuale Operativo) il Certificatore ha rilasciato mandato a svolgere le funzioni di Registration Authority al Gruppo Cabel. In particolare, ognuna delle società indicate nel paragrafo A.1 potrà svolgere le seguenti attività:

- Identificazione del Titolare.
- Registrazione del Titolare.

Il Provider, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinché l'attività di riconoscimento si svolga nel rispetto della normativa vigente.

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

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

- Decreto Legislativo del 7 marzo 2005, n.82 e successive modifiche.
- Decreto Presidente del Consiglio dei Ministri 22 Febbraio 2013.
- Decreto Legislativo 30 giugno 2003, n.196, e successive modificazioni, recante codice in materia di protezione dei dati personali.

In particolare il Certificatore Accreditato:

- adotta tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- si attiene alle regole tecniche specificate nel Decreto;
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche e i requisiti di sicurezza previsti dall'Art.35 del CAD e all'Art.11 del Decreto;
- rilascia e rende pubblico il certificato qualificato, se non diversamente specificato dal Titolare, secondo quanto stabilito all'Art.32 del CAD;
- informa i richiedenti, in modo compiuto e chiaro, sulla procedura di certificazione, sui necessari requisiti tecnici per accedervi, sulle caratteristiche e sulle limitazioni d'uso delle firme emesse sulla base del servizio di certificazione;
- si attiene alle misure di sicurezza per il trattamento dei dati personali (DLgs 196 30/06/2003);
- non si rende depositario di dati per la creazione della firma del Titolare;
- procede alla pubblicazione della revoca e della sospensione del certificato elettronico in caso di richiesta da parte del Titolare o del terzo interessato;
- assicura la precisa determinazione della data e dell'ora di rilascio, di revoca e di sospensione dei certificati elettronici;
- tiene registrazione, anche elettronica, di tutte le informazioni relative al certificato qualificato per 20 (venti) anni in particolare al fine di fornire prova della certificazione in eventuali procedimenti giudiziari;
- assicura che il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
- predispone su mezzi di comunicazione durevoli tutte le informazioni utili ai soggetti che richiedono il servizio di certificazione. Tra questi citiamo: gli esatti termini e condizioni relative all'uso del certificato, compresa ogni limitazione dell'uso, l'esistenza di un sistema di accreditamento facoltativo e le procedure di reclamo e di risoluzione delle controversie. Dette informazioni, che possono essere trasmesse elettronicamente, devono essere scritte in linguaggio chiaro ed essere fornite prima dell'accordo tra il richiedente il servizio e il Certificatore;
- utilizza sistemi affidabili per la gestione del registro dei certificati con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza;
- registra l'emissione dei certificati qualificati nel giornale di controllo con la specificazione della data e dell'ora della generazione.

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

Inoltre, il Certificatore:

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

- garantisce l'interoperabilità del prodotto di verifica, di cui all'Art.14 del Decreto, ai documenti informatici sottoscritti con firma digitale emessa dalla struttura di certificazione della Rete unitaria della pubblica amministrazione e successive modifiche tecniche e organizzative;
- mantiene copia della lista, sottoscritta dall'Agenzia per l'Italia Digitale, dei certificati relativi alle chiavi di certificazione (di cui all'Art.43 del Decreto), e la rende accessibile per via telematica (Art.42, comma 3 del Decreto).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo è un cliente del Provider che opera da Registration Authority (o ha un rapporto con un Terzo Interessato che ha firmato un contratto con il Provider).

In quanto tale potrà ricevere un certificato qualificato di firma per sottoscrivere atti e documenti nell'ambito dei servizi di firma remota esposti dal Provider

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

Il Titolare della chiave deve inoltre:

- fornire tutte le informazioni richieste dal Certificatore, garantendone l'attendibilità sotto la propria responsabilità;
- inoltrare la richiesta di certificazione secondo le modalità indicate in questo Manuale Operativo;
- comunicare al Certificatore, tramite il Provider eventuali variazioni alle informazioni fornite all'atto della registrazione: dati anagrafici, residenza, recapiti telefonici, indirizzo di posta elettronica, ecc.;
- conservare con la massima cura e diligenza le informazioni di abilitazione all'uso della chiave privata;
- non utilizzare la chiave di firma per funzioni diverse da quelle previste dalla sua tipologia (Art.5, comma 5, del Decreto);
- dare immediata comunicazione al Provider, in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma, il Provider stesso provvederà all'immediato blocco degli stessi e dei canali di accesso ai servizi di firma digitale;
- inoltrare eventuali richieste di revoca e di sospensione del certificato digitale secondo quanto indicato nel presente Manuale Operativo.

C.3. Obblighi degli utilizzatori dei certificati

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

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

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato, avendo preso visione del presente Manuale Operativo e dei servizi descritti, può richiedere l'inserimento nel certificato di un Ruolo o l'indicazione dell'Organizzazione cui il Titolare è collegato.

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

C.5. Obblighi della Registration Authority esterna

Il Certificatore, per esigenze connesse alla fornitura del servizio, si avvale su tutto il territorio nazionale di ulteriori soggetti (nel seguito anche denominati Provider) per svolgere una parte delle attività proprie dell'Ufficio di registrazione. In particolare, un Provider deve espletare le seguenti funzioni:

- identificazione certa del Titolare del certificato;
- registrazione del Titolare;
- consegna al Titolare dei codici che gli permettano di accedere alla propria chiave di firma nel rispetto degli Artt. 8 e 10, comma 2, del Decreto.

Il Certificatore ha rilasciato mandato a svolgere la funzione di Registration Authority al Gruppo Cabel mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere il Provider cui INTESA assegna l'incarico di RA; in particolare si richiede di:

- vigilare affinché l'attività di riconoscimento posta in essere si svolga nel rispetto della normativa vigente (CAD e successive modificazioni);
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il DLgs. 196/03;
- rendere disponibile per il Certificatore il materiale raccolto nella fase di identificazione e l'autorizzazione all'uso dei dati personali.

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

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore – Limitazione agli indennizzi

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

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

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

Il Certificatore non sarà responsabile per i danni derivanti da un utilizzo non conforme del Certificato Qualificato per la Firma digitale Remota in relazione alla limitazione d'uso come specificata al paragrafo F.1.3.

D.2. Assicurazione

In base a quanto previsto dall'Art.15, comma 1, lettera i) del Decreto, il Certificatore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e degli eventuali danni causati a terzi, derivanti dall'erogazione del servizio di certificazione. il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi. Di tale contratto è stata inviata all'Agenzia per l'Italia Digitale apposita copia.

La copertura Assicurativa prevede i seguenti massimali:

- 250.000,00 (duecentocinquantamila) euro per singolo sinistro
- 1.500.000,00 (unmilionecinquecentomila) euro per annualità.

E. Tariffe

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

Queste verranno indicate nei contratti che verranno stipulati fra le aziende del Gruppo Cabel e Titolare.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

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

Questa operazione viene demandata alla Registration Authority che in ottemperanza con quanto previsto dalla vigente normativa e secondo le modalità descritte nel seguito.

Per i successivi rinnovi, se effettuati prima che il certificato qualificato già rilasciato non sia scaduto, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al Certificatore attraverso il Provider solo gli eventuali cambiamenti relativi ai propri dati di registrazione.

Fra i dati di registrazione necessari all'avviamento del servizio ricordiamo:

- Nome e Cognome;
- Data di nascita;
- Comune o stato estero di nascita;
- Codice fiscale;
- Indirizzo di residenza;
- Domicilio presso il quale saranno inviate le comunicazioni cartacee;
- Numero di telefono cellulare;
- Indirizzo di posta elettronica;
- Tipo e numero del documento d'identità esibito;
- Autorità che ha rilasciato il documento, data e luogo del rilascio, data di scadenza.

Pertanto, il personale del Provider, in ottemperanza con quanto previsto dalla vigente normativa e dalle normative interne al Provider stesso, svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

Il servizio di identificazione potrà essere gestito come segue:

- Il Richiedente, purché in possesso di un device (PC, tablet, smartphone) abilitato ad una connessione Internet e dotato sia di una webcam che di un sistema audio funzionante, si connette al sito della Registration Authority dove sono riportate tutte le istruzioni necessarie per eseguire i passi successivi e dove sono indicati i documenti necessari per l'identificazione.
- Precisiamo, a tal proposito, che la buona qualità del collegamento audio-video è fondamentale affinché la procedura di identificazione possa essere effettuata con successo; infatti, in caso di

disturbi sulla linea e/o problemi che non rendessero possibile la verifica certa dell'identità del Richiedente, l'operatore di Registration Authority interromperà la sessione, invitando il Richiedente a prendere un nuovo appuntamento quando saranno stati risolti i problemi riscontrati.

- Il Richiedente compila sul sito della Registration Authority una richiesta di certificato digitale compilando un form in cui è previsto vengano inseriti tutti i dati utili ad una sua registrazione.
- Compilato questo form, viene richiesto al Richiedente di prendere visione del presente Manuale Operativo, che dovrà essere aperto in lettura - lo stesso Manuale Operativo sarà anche agevolmente scaricabile dal sito stesso.
- Fra le operazioni che necessariamente il Richiedente dovrà svolgere vi è anche la scelta del consenso privacy.
- Il Richiedente, sempre grazie alle funzionalità esposte sul sito, una volta presa visione del Manuale Operativo e dato il consenso, dovrà inviare alla RA una copia scannerizzata dei documenti di identità (ad esempio carta d'identità, passaporto, tesserino fiscale e/o codice sanitario nazionale per i paesi anglosassoni. L'invio preventivo di tali documenti conferma la volontà del Richiedente nel completare la procedura di identificazione finalizzata all'emissione di un certificato qualificato utilizzabile esclusivamente nell'ambito dei servizi di firma remota esposti da Gruppo Cabel o dall'azienda per la quale ha ricevuto il mandato di eseguire il riconoscimento.
- Completata la fase di inserimento dati ed invio dei documenti necessari per l'identificazione, il Richiedente potrà richiedere di continuare la sessione attivando appena possibile il collegamento via web cam o fissare un successivo appuntamento con gli operatori di Registration Authority per completare in un momento successivo a lui più comodo la procedura di identificazione.
- Gli operatori di Registration Authority, sulla base dei documenti ricevuti, eseguono dei controlli utilizzando specifiche banche dati, come SCIPAFI (il Sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento - attualmente quelle dell'Agenzia delle Entrate, Ministero dell'Interno, Ministero delle Infrastrutture e dei Trasporti, INPS e INAIL), oppure altre banche dati private (ad es. CRIF, Cerved, ecc.) in grado di erogare servizi di verifica dati e documenti d'identità. Questo riscontro si configura quindi come efficace strumento di prevenzione per i "furti d'identità", sia totali che parziali, garantendo un'identificazione certa del Titolare.
- Durante la sessione on-line (via web cam), l'operatore di RA domanda al soggetto richiedente di presentarsi con i documenti di riconoscimento precedentemente inviati; controlla che i documenti siano gli stessi e che nella foto del documento sia riconoscibile il Richiedente.
- L'intera sessione viene registrata in modalità audio e video (sia lato Richiedente che lato operatore) e la sequenza viene poi cifrata con una chiave pubblica messa a disposizione dalla Certification Authority. La stessa CA conserva la chiave privata e la rende disponibile solo in caso di contenzioso ad un perito di parte e/o agli enti di vigilanza che richiedessero un controllo sulle attività svolte.
- La registrazione audio/video della sessione deve essere di buona qualità (immagine a colori, definizione delle riprese chiare e a fuoco, adeguata luminosità e contrasto, ripresa del testo eventualmente inquadrato distinguibile. L'intera sessione audio/video deve essere fluente e continua, senza alcuna interruzione.
- L'operatore:
  - deve essere libero di rifiiutare la registrazione dell'utente, qualora abbia o emerga dubbio, anche soggettivo, circa l'effettiva identità del soggetto richiedente.
  - chiede all'utente, durante la registrazione, di effettuare azioni estemporanee al fine di accertare la reale presenza nella postazione remota del soggetto richiedente
- Completati i controlli relativi ai documenti di riconoscimento presentati, al Richiedente vengono date le informazioni necessarie per permettergli successivamente di utilizzare il certificato qualificato che sta per essergli emesso e di firmare digitalmente.
- In particolare, vengono date tutte le informazioni necessarie per utilizzare successivamente, nel momento della firma, uno strumento di autenticazione implementato per funzionare su mobile e/o smartphone in alternativa a token OTP fisici che risultano inadeguati per le modalità di erogazione della firma digitale previste dal presente manuale operativo.

- Si precisa che il certificatore, in ottemperanza con quanto previsto dall'Art.35, comma5 del CAD, prevede esclusivamente l'impiego di dispositivi di autenticazione che abbiano ottenuto una valutazione positiva di conformità da parte di AGID.
- L'impiego di dispositivi che prevedono l'impiego di mobile e/o smartphone richiede che gli stessi vengano censiti in un'anagrafica gestita e mantenuta dal Provider. Pertanto, anche questa operazione di censimento viene eseguita durante la sessione gestita con web cam. Al termine dell'operazione di censimento, l'operatore di Registration Authority chiama il Richiedente al numero telefonico appena censito. E solo se il Richiedente risponde in diretta e visto dall'operatore la procedura di identificazione potrà dirsi effettivamente conclusa.
- A questo punto, dopo che è stato eseguito il controllo dei documenti sulle banche dati disponibili e ricevuto dalle stesse un documento attestante l'esito del controllo, il certificato digitale viene emesso dalla Certification Authority e al Titolare viene anche associato un identificativo univoco presso il Certificatore.

Dopo che il Titolare è stato identificato, l'operatore del Provider provvede anche alla consegna di un Codice Utente e di un Personal Identification Number (PIN), tramite i quali sarà possibile accedere all'area riservata del portale, al fine di garantire un accesso sicuro ai servizi di firma remota fornito dall'azienda del Gruppo Cabel.

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

Lo stesso PIN potrà essere utilizzato dal Titolare come codice di emergenza (in caso, ad esempio, di smarrimento e/o perdita del mobile) per sospendere o revocare definitivamente il certificato digitale a lui emesso.

In questa fase vengono anche fornite al Titolare le necessarie informazioni per permettergli di cambiare in un qualsiasi momento il numero di cellulare precedentemente fornito.

La documentazione precedente, relativa alla registrazione dei Titolari, viene conservata da INTESA per 20 (venti) anni dalla scadenza del certificato, a cura del Responsabile dei servizi tecnici e logistici.

Sul cellulare predefinito dal Titolare o su indirizzo email indicato dal cliente, il Provider invierà degli specifici SMS/email che possano avvisarlo relativamente alle operazioni eseguite attraverso l'impiego del certificato digitale (firma di un documento, ma anche sospensione, revoca o rinnovo del certificato digitale stesso).

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

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

F.1.1. Titoli e abilitazioni professionali

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

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

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

INTESA, in caso di autocertificazione, non si assume alcuna responsabilità, salvo i casi di dolo o colpa grave, per l'eventuale inserimento nel certificato d'informazioni autocertificate dal titolare.

F.1.2. Poteri di rappresentanza

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

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

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

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

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

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

F.1.3. Limiti d'uso

Nel caso in cui sia richiesta l'indicazione nel certificato qualificato di limiti d'uso ovvero un valore limite per i negozi per i quali può essere usato il certificato stesso, il richiedente deve sottoscrivere idonea documentazione attestante la richiesta. Una copia di tale documentazione viene conservata dal Certificatore.

Specifici limiti d'uso potranno essere concordati con il Provider purché non eccedano i 200 caratteri.

F.1.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno pseudonimo in alternativa ai propri dati reali. Anche in questo caso, poiché comunque ci si riferisce a certificati qualificati, il Certificatore conserverà le informazioni relative alla reale identità dell'utente per 20 (venti) anni dopo la scadenza del certificato stesso.

G. Modalità operative per la sottoscrizione di documenti

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

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

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

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

A conferma dell'effettuazione delle operazioni di firma, verranno inviati degli SMS, qualora un Titolare possegga uno smartphone abilitato alla lettura della corrispondenza; su richiesta del Titolare stesso, in alternativa potranno essere inviate alla sua attenzione delle e-mail.

G.1. Autenticazione di tipo "Call Drop"

Questa modalità di autenticazione richiede all'utente, già precedentemente identificato, di effettuare una chiamata ad un numero telefonico specifico fornito nell'ambito del servizio con il proprio telefono cellulare (ossia dallo stesso numero fornito in fase di identificazione) per confermare la propria volontà di firmare un documento.

Al ricevimento di una tale telefonata, ne viene verificata la provenienza dal numero di telefono (Call Identifier) preventivamente associato all'utente in fase di registrazione e viene, in caso di verifica positiva, autorizzata l'operazione di firma elettronica qualificata.

Pertanto, quando il Titolare vorrà firmare un documento accedendo al portale del Provider, utilizzerà un'autenticazione a due fattori attraverso l'inserimento di un PIN (informazione che solo l'utente conosce) ed un numero di telefono (dato dalla SIM che solo l'utente possiede).

Questo tipo di autenticazione viene anche detta "Call Drop" in quanto quando il Titolare chiama per essere autenticato non viene attivata una conversazione e la telefonata, in meno di un secondo, viene chiusa. L'utente Titolare non riceve mai una risposta alla propria chiamata e pertanto non incorre in alcun costo telefonico.

Tra i vantaggi di questa tecnica vi sono l'estrema economicità e praticità, in quanto non è richiesto l'uso di alcun dispositivo fisico di autenticazione, ed è molto facile da usare.

Vedremo di seguito che per gestire queste situazioni si sia studiata una soluzione basata su una gestione dinamica dei numeri telefonici da chiamare per finalizzare il processo di autenticazione proprio in quelle che chiameremo stazioni presidiate.

G.1.1. Processo di Firma Remota

Entrato in possesso dei necessari codici durante la fase di identificazione il Titolare potrà in un momento successivo procedere poi alla firma di un documento secondo le modalità di seguito descritte.

1. Il Titolare si connette all'applicazione di firma attraverso i suoi codici personali per l'accesso all'applicazione;
2. Selezione e verifica il documento da firmare;
3. Inserisce quindi il suo PIN;
4. Appena validato il PIN il Titolare in un tempo configurato (ma non superiore ai 30') utilizzando il cellulare precedentemente censito deve, per confermare la propria intenzione di firmare il documento, immediatamente chiamare un numero telefonico che gli sarà nel frattempo comparso a video;
5. Il sistema rilevando che il numero chiamante è proprio quello censito in precedenza ed associato al Titolare procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa;
6. Se invece, trascorso il tempo prefissato, senza che il sistema abbia ricevuto una telefonata al numero indicato al punto 4 l'operazione viene considerata nulla e conclusa senza la sottoscrizione del documento;
7. Qualora i documenti da firmare fossero più di uno il Titolare per ogni documento deve reiterare i passi dal 2 al 5.

G.2. Autenticazione di tipo OTP Mobile

In alternativa allo strumento di autenticazione denominato "call drop" viene reso disponibile una seconda modalità di autenticazione denominata "OTP mobile".

Per attivare questa modalità il Titolare dovrà disporre di uno smartphone fra quelli specificati dal Provider stesso adeguati per tale servizio.

Eseguita questa verifica, in fase di identificazione al Titolare verrà comunicato un indirizzo internet specifico sul sito del Provider da cui scaricare sul suo smartphone un'applicazione definita di "OTP Mobile" ed un PIN (ricevuto durante la procedura di identificazione propedeutica all'emissione del certificato qualificato).

G.2.1. Processo di Firma Remota

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

1. Il Titolare si connette all'applicazione di firma attraverso i suoi codici personali per l'accesso all'applicazione;
2. Selezione e verifica il documento da firmare;
3. Inserisce quindi il suo PIN;
4. Lancerà poi l'applicazione precedentemente scaricata sul suo smartphone ricevendone un "OTP mobile" da inserire successivamente al PIN;
5. Il sistema rilevando la correttezza del PIN e dell'OTP mobile appena inseriti procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa;
6. Qualora i documenti da firmare fossero più di uno, il Titolare per ogni documento deve reiterare i passi dal 2 al 5.

G.3. Autenticazione di tipo invio codice di sicurezza a mezzo SMS

Altra modalità potrà essere quella dell'invio a mezzo SMS di un codice randomico generato dal sistema verso il cellulare indicato e verificato in fase di censimento.

G.3.1. Processo di Firma Remota

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

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

G.4. Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF; tale formato di sottoscrizione (previsto dall'Art.21, comma 8 e 15 della Deliberazione CNIPA n. 45) è considerato infatti di facile utilizzo nell'ambito delle applicazioni di firma remota.

Infatti la verifica dei documenti sottoscritti potrà essere agevolmente effettuata utilizzando il software Acrobat Reader scaricabile gratuitamente dal sito www.adobe.com/it insieme all'add on specifico per la firma digitale reperibile anche questo, gratuitamente, all'indirizzo www.adobe.it/firmadigitale .

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

H.1. Generazione delle chiavi di certificazione

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

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

Le operazioni successive alla generazione delle coppie di chiavi del Certificatore sono possibili solamente attraverso particolari dispositivi di autorizzazione (smartcard/token usb): l'accesso privilegiato agli HSM è possibile solamente attraverso la chiave contenuta in tali dispositivi di autorizzazione di cui sopra.

Per maggior sicurezza, tali chiavi sono divise su più dispositivi, secondo una logica del tipo "n di m", in modo che solo la concomitante presenza di almeno n due m parti della chiave permettano di operare con gli opportuni privilegi. Pertanto esse vengono custodite in apposite casseforti distinte.

La lunghezza delle chiavi di certificazione è di 2048 bit.

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

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

La lunghezza delle chiavi del sistema di validazione temporale è di 2048 bit.

H.3. Generazione delle chiavi di sottoscrizione

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

Il Titolare potrà avviare la procedura di generazione delle chiavi e richiesta del Certificato di firma ad esse associato autenticandosi al sistema fornitogli dal Provider in una delle modalità precedentemente descritte.

Il PIN e l'OTP (generata secondo le modalità precedentemente descritte) costituiscono l'insieme di dati di cui il Titolare deve avere in modo esclusivo la conoscenza e il possesso ai sensi dell'Art.8 comma 5 lett.d) del Decreto; questi stessi dati gli saranno richiesti tutte le volte che voglia sottoscrivere un documento secondo quanto richiesto dall'Art.35, comma 2 del CAD.

Lo stesso sistema di autenticazione permetterà al Titolare di conservare in modo esclusivo il controllo delle proprie chiavi di firma ai sensi dell'Art.8 comma 5 lett. d) del Decreto.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è di almeno 2048 bit) vengono create su dispositivi sicuri, Hardware Security Module, conformi a quanto previsto dalla normativa vigente.

I. Modalità di emissione dei certificati

I.1. Procedura di emissione dei Certificati di certificazione

In seguito alla generazione delle chiavi di certificazione, descritta nel paragrafo H.3, vengono generati i certificati delle chiavi pubbliche, nel formato ISO 9594-8 (2001), conformemente a quanto disposto dal Decreto, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

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

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

I.2. Procedura di emissione dei Certificati di sottoscrizione

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

Dopo la generazione della coppia di chiavi di sottoscrizione, descritta nel paragrafo H.3, è possibile generare una richiesta di nuovo certificato nel formato PKCS#10, che fornisce automaticamente la prova di possesso della chiave privata e la verifica del corretto funzionamento della coppia di chiavi.

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

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

I.3. Informazioni contenute nei certificati

I certificati emessi da INTESA soddisfano lo standard ISO 9594-8-2001.

I certificati INTESA sono conformi a quanto indicato nella deliberazione CNIPA n.45 del 21/05/09 e successive modificazioni e integrazioni. In seguito a ciò è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani.

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

Ogni Certificato Qualificato per la Firma Digitale contiene, a titolo esemplificativo ma non esaustivo, le seguenti informazioni:

- numero di serie;
- ragione o denominazione sociale del Certificatore;
- codice identificativo unico del Titolare presso il Certificatore;
- nome, cognome, codice fiscale del Titolare;
- valore della chiave pubblica;
- algoritmi di generazione e verifica utilizzabili;
- inizio e fine del periodo di validità del certificato;
- algoritmo di sottoscrizione del certificato;
- tipologia delle chiavi;
- limitazioni nell'uso della coppia di chiavi.

Tutti i Certificati Qualificati emessi nell'ambito dei servizi descritti nel presente Manuale, conterranno sempre una limitazione d'uso

I.4. Codice di Emergenza

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

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

J. Modalità di revoca e sospensione dei certificati

J.1. Revoca dei certificati

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

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

La CRL, firmata dal Certificatore, viene aggiornata con periodicità prestabilita e ad ogni revoca o sospensione. La lista è disponibile anche sul registro dei certificati.

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

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

J.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca del certificato, che potrà essere inoltrata utilizzando i canali di comunicazione definiti con il Provider.

Il Certificatore, avvertito dal Provider, provvederà all'immediata revoca del certificato.

J.1.2. Revoca su richiesta del Terzo Interessato

Anche un Terzo Interessato può richiedere la revoca del certificato.

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

Il Certificatore, accertata la correttezza della richiesta, darà notizia della revoca ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso e inserirà il certificato nella lista di revoca, che sarà emessa il prima possibile.

J.1.3. Revoca su iniziativa del Certificatore

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

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

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

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

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

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

J.2. Sospensione dei certificati

Sulle modalità di sospensione e di notifica della medesima vale quanto detto per le modalità di revoca al capitolo J.1.

La sospensione di un certificato è prevista nel caso in cui si debba fare un supplemento di indagine per verificare se debba effettivamente essere revocato.

La richiesta di sospensione può essere avanzata da tutte le entità previste dal Decreto agli Artt. 27, 28 e 29 (Certificatore, Titolare, Terzo Interessato).

In assenza di comunicazioni ulteriori, il certificato sarà automaticamente revocato dopo il periodo di sospensione indicato (non superiore ai novanta giorni) o comunque entro la data di scadenza del certificato stesso.

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

J.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione del certificato, che potrà essere inoltrata utilizzando i canali di comunicazione definiti con il Provider. Il Certificatore, avvertito dal Provider provvederà alla immediata sospensione del certificato.

Successivamente il Titolare potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre dal Provider.

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

J.2.2. Sospensione su richiesta del Terzo Interessato

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

Il Certificatore, accertata la correttezza della richiesta, sospenderà immediatamente il certificato e ne darà notizia della sospensione ai Titolari interessati utilizzando i canali di comunicazione definiti con il Titolare all'atto della registrazione dello stesso.

J.2.3. Sospensione su iniziativa del Certificatore

Il Certificatore salvo i casi di motivata urgenza potrà sospendere il certificato dandone preventiva comunicazione al Titolare all'indirizzo di posta certificata comunicato in fase di registrazione specificando i motivi della sospensione e data e ora a partire dalle quali tale sospensione sarà efficace.

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

K. Modalità di sostituzione delle chiavi

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

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

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

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

K.2. Sostituzione delle chiavi del Certificatore

K.2.1. Sostituzione in emergenza delle chiavi del sistema di generazione dei certificati

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

K.2.2. Sostituzione pianificata delle chiavi di certificazione

Almeno 90 (novanta) giorni prima della scadenza del certificato relativo alla coppia di chiavi utilizzate dal sistema di emissione dei certificati il Certificatore procederà all'emissione di nuove chiavi in base a quanto stabilito dall'Art.30 del Decreto.

K.2.3. Sostituzione in emergenza delle chiavi del sistema di validazione temporale

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

K.2.4. Sostituzione pianificata delle chiavi del sistema di validazione temporale

Non oltre due giorni prima della scadenza della chiave privata del sistema di validazione temporale, le stesse persone previste per l'inizializzazione del dispositivo di firma (HSM) ripeteranno quanto descritto al paragrafo H.2.

K.2.5. Chiavi di marcatura temporale

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

L. Registro dei certificati

L.1. Modalità di gestione del Registro dei certificati

Nel registro dei certificati, INTESA pubblica:

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

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

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

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

L.2. Accesso logico al Registro dei certificati

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

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

Il Certificatore consente l'accesso a CRL/CSL via Internet attraverso il protocollo http.

L.3. Accesso fisico ai locali dei sistemi preposti al registo dei certificati

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

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

M. Modalità di protezione della riservatezza

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

N. Procedura di gestione della copie di sicurezza

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

- REGISTRO DEI CERTIFICATI, archivio digitale contenente quanto specificato alla sezione L.
- INFORMAZIONI OPERATIVE, archivio digitale in cui sono memorizzate tutte le informazioni ricevute dal Titolare al momento della registrazione e della richiesta di un certificato e le richieste di revoca e sospensione, corredate delle relative documentazioni.

- GIORNALE DI CONTROLLO, archivio costituito dall'insieme delle registrazioni effettuate automaticamente dai sistemi installati presso il servizio di certificazione del Certificatore (Art.36 del Decreto).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.53, comma 1, del Decreto).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.52 del Decreto).

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

O. Procedura di gestione degli eventi catastrofici

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

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

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

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

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

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

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

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

L'I.N.RI.M fornisce un servizio di sincronizzazione per sistemi informatici collegati alla rete Internet, basato su due server NTP primari installati nel Laboratorio di Tempo e Frequenza Campione. Essi sono sincronizzati, attraverso un generatore di codice di data, dai campioni atomici a fascio di cesio utilizzati per generare la scala di tempo nazionale italiana UTC(IT). Lo scarto di tempo tra i server NTP dell'I.N.RI.M

e la scala di tempo nazionale italiana viene tenuto sotto controllo ed è normalmente inferiore ad alcuni millisecondi. La precisione di sincronizzazione ottenibile dipende dalla tipologia della rete e dalla distanza interposta tra il server NTP e il calcolatore che si vuole sincronizzare; i valori di scarto tipici sono inferiori al millisecondo per sistemi appartenenti alla stessa rete e possono arrivare a qualche centinaio di millisecondi per reti remote.

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

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

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

P.1. Modalità di richiesta e verifica marche temporali

Il Certificatore appone una marca temporale su tutti i documenti sottoscritti dal Titolare nell'ambito dei servizi descritti da questo Manuale Operativo.

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

Q. Riferimenti tecnici

RFC 5905	Network Time Protocol (Version 4) Specification, Implementation
ETSI TS 102 023	Deliverable ETSI TS 102 023 "Policy requirements for time-stamping authorities" – Aprile 2002
RFC 5280	RFC 3280 (2008): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 5816	RFC 5816 (2010): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
ISO/IEC 9594-8 2001:(E)	Information Technology – Open Systems Interconnection – The Directory: Authentication 01/08/2001 Framework; ITU-T Recommendation X.509 (2001) | ISO/IEC 9594-8
RFC 2527	RFC 3647 (2003): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
RFC 3039	RFC 3739 (2004) Internet X.509 Public Key Infrastructure Qualified Certificates Profile
ETSI TS 102 778-1..5	ETSI TS 102 778-1..5) V1.1.1 "Electronic Signatures and Infrastructure (ESI); PDF Advanced Electronic Signature Profiles;" Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles; Part 1: PAdES Overview - a framework document for PAdES Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles; Part 2: PAdES Basic - Profile based on ISO 32000- 1 Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles Electronic Signatures and Infrastructures (ESI); PDF Advanced Electroni c Signature Profiles ; Part 4: PAdES Long Term - PAdES- LTV Profile Electronic Signatures and Infrastructures (ESI); PDF Advanced Electronic Signature Profiles; Part 5: PAdES for XML Content - Profiles for XAdES signatures
ETSI TS 101 733	ETSI TS 101 733 V1.5.1"Electronic Signatures and Infrastructure (ESI): Electronic Signature Formats" (2002-12)