Manuale Operativo del Certificatore Accreditato INTESA per le procedure di firma remota in ambito bancario e finanziario

Codice documento: MO-REMBAN

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione 13/06/2012

Revisione: 03

INTESA

An IBM company

REVISIONI

Revisione n°:	**01**	**Data Revisione:**	**01/11/2011**
Descrizione modifiche:	**Nessuna**		
Motivazioni:	**Prima emissione**		

Revisione n°:	**02**	**Data Revisione:**	**02/04/2012**
Descrizione modifiche:	**B.4.2. - Introdotta sistema di riconoscimento dell'identità del titolare (*Adeguata verifica*) senza la presenza fisica del medesimo.** **C.5. – Introdotte modalità del sistema di riconoscimento dell'identità del titolare (*Adeguata verifica*).** **F.1.3. - Inserito limite d'uso standard.** **G. - Inserita modalità di comunicazione email delle conferme operative.**		
Motivazioni:	**Aggiornamento**		

Revisione n°:	**03**	**Data Revisione:**	**13/06/2012**
Descrizione modifiche:	**Estensione del manuale all'ambito finanziario (Istituti di Pagamento) oltreché bancario.**		
Motivazioni:	**Aggiornamento**		

Sommario

A. Introduzione

A.1. Proprietà intellettuale

Il presente Manuale Operativo è di esclusiva proprietà di In.Te.S.A. S.p.A. (di seguito anche solo "INTESA"), che è Titolare di ogni relativo diritto intellettuale.

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

A.2. Il Manuale Operativo

Il presente documento costituisce il *Manuale Operativo del Certificatore Accreditato INTESA per i servizi di Firma Remota in ambito bancario e finanziario,* al quale d'ora in poi si farà riferimento anche solo come *Manuale Operativo*.

Il contenuto del Manuale Operativo è conforme con quanto definito nelle regole tecniche contenute nel Decreto del Presidente del Consiglio del 30 Marzo 2009 e decreto legislativo 7 marzo 2005, n. 82, e successive modificazioni, recante il codice dell'amministrazione digitale e, in particolare, il capo II, che disciplina le firme elettroniche e i certificatori, e l'Art.71.

Questo documento descrive pertanto le regole e le procedure operative del Certificatore Accreditato INTESA per l'emissione dei certificati qualificati, la generazione e la verifica della firma elettronica qualificata e le procedure del servizio di validazione temporale in conformità con la vigente normativa quando questa è gestita all'interno di progetti bancari o finanziari.

In questa tipologia di progetti le stesse banche o istituti di pagamento, erogatori dei servizi di home banking e delle applicazioni di sportello, fungeranno anche, come vedremo nel seguito, da Registration Authority per conto del Certificatore.

Nel seguito tali entità bancarie o finanziarie verranno richiamate con il termine di *Banca o Istituto di Pagamento*.

Si precisa pertanto che tutti i processi di sottoscrizione di documenti saranno implementati esclusivamente all'interno di applicazioni bancarie o finanziarie.

A.3. Validità

Quanto descritto in questo documento si applica al Certificatore Accreditato INTESA, 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.4 del DPCM, al comma 4 che indica le seguenti tipologie di chiavi e servizi:

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 e alle loro liste di revoca (CRL) o sospensione (CSL), ovvero alla sottoscrizione dei certificati relativi a chiavi di marcatura temporale;
c) chiavi di marcatura temporale, destinate alla generazione e verifica delle marche temporali.

A.4. Riferimenti di legge

Di seguito i riferimenti normativi.

DPR 445/00	Decreto del Presidente della Repubblica del 28 dicembre 2000, n.445 - "*Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa*. (G.U. n.42 del 20 febbraio 2001)
DLGS 196 30/06/03	Codice in materia di protezione dei dati personali. (G.U. n.174 del 29 luglio 2003, suppl. ord.) .
DPCM 30/03/2009	Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale, dei documenti informatici. (G.U. n. 129 del 6 Giugno 2009).
DLGS 82 07/03/2005	Decreto Legislativo 7 Marzo 2005, n. 82 - *Codice dell'amministrazione Digitale* (nel seguito indicato semplicemente come CAD), e successive modificazioni. (G.U. n.112 del 16 Maggio 2005)
Deliberazione CNIPA n.45 21/05/2009	Deliberazione CNIPA 21 Maggio 2009 - *Regole per il riconoscimento e la verifica del documento informatico*. (G.U. n.282 del 3/12/2009)
Determinazione commissariale DigitPA N.69/2010 28/07/2010	Modifiche alla Deliberazione 21 maggio 2009 n. 45 del Centro Nazionale per l'Informatica nella pubblica Amministrazione, recante *Regole per il riconoscimento e la verifica del documento informatico*, pubblicata il 3 dicembre 2009 sulla Gazzetta Ufficiale della Repubblica Italiana - Serie generale - n. 282. (G.U. n. 191 del 17/08/2010)
DPCM 10/02/2010	Fissazione del termine che autorizza l'autocertificazione circa la rispondenza dei dispositivi automatici di firma ai requisiti di sicurezza. (G.U. n.98 del 28 Aprile 2010).
DLGS 235 30/12/2010	Modifiche ed integrazioni al decreto legislativo 7 marzo 2005, n. 82, recante *Codice dell'amministrazione digitale*, a norma dell'articolo 33 della legge 18 giugno 2009, n.69. (G.U. n.6 del 10/01/2011)

A.5. Definizioni e acronimi

Non sono riportati i significati di alcuni acronimi e termini specifici di uso comune.

Termine o acronimo	***Significato***
Analisi dei rischi	Vedi Risk Assessment.
Certificatore	Autorità Accreditata che presta servizi di certificazione delle firme elettroniche qualificate e altri servizi connessi quali, ad cesempio, l'erogazione delle marche temporali.
Certificate Policy	Un insieme di norme, contraddistinto da un codice, che indica l'applicabilità di un certificato ad una particolare comunità e/o a una classe di applicazioni aventi comuni esigenze di sicurezza.
Certificate Revocation List	Un elenco firmato che riporta un insieme di certificati non più considerati validi dal Certificatore che li ha emessi.
Certificate Suspension List	Lista dei certificati sospesi che generalmente viene inclusa nella CRL
Certification Practice Statement	Una dichiarazione delle prassi seguite da un Certificatore nell'emettere e gestire certificati.
CNIPA (ora DigitPA)	Centro Nazionale per l'informatica nella Pubblica Amministrazione
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma elettronica Avanzata	E' un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garantisce integrità, autenticità del documento sottoscritto e controllo esclusivo dello strumento di firma.
Firma elettronica Qualificata	E' un particolare tipo di firma elettronica avanzata basata su di un certificato qualificato, che garantisce l'identificazione univoca del titolare, rilasciato da un certificatore accreditato e realizzato mediante un dispositivo sicuro per la generazione della firma.
Firma remota	Particolare procedura di firma elettronica qualificata o di firma digitale che consente di garantire il controllo esclusivo del dispositivo di firma.
HASH	Funzione che prende in input una stringa di lunghezza variabile e ritorna una stringa di lunghezza fissa.

Termine o acronimo	***Significato***
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
LDAP	Lightweight Directory Access Protocol.
NTP	Network Time Protocol. Protocollo per la sincronizzazione del tempo.
Object Identifier	Sequenza di numeri, registrata secondo la procedura definita dallo standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
OID	Object Identifier (vedi).
Public Key Certificate	Certificato di Chiave Pubblica: una struttura di dati contenente la chiave pubblica di una End Entity (vedi) e altre informazioni, che è firmato in modo digitale con la chiave privata della CA (vedi) che l'ha emesso.
Public Key Infrastructure	Insieme di hardware, software, persone, norme e procedure necessarie per creare, gestire, conservare, distribuire e revocare i PKC basati su crittografia a chiave pubblica.
RA	Registration Authority. Autorità di Registrazione che su incarico del Certificatore esegue le registrazioni e le verifiche delle identità dei titolari dei certificati qualificati necessarie al Certificatore. In ogni caso la responsabilità delle operazioni di registrazione, identificazione e validazione è del Certificatore (INTESA S.p.A.).
Riferimento temporale	Informazione contenente la data e l'ora che viene associata ad un documento informatico
Security Policy	Insieme di regole e norme che specificano o regolamentano le modalità con cui un sistema o un'organizzazione fornisce servizi di sicurezza per proteggere risorse di sistema critiche o riservate. *(A set of rules and practices that specify or regulate how a system or organisation provides security services to protect sensitive and critical system resources).*
SHA-256	Funzione di hash crittografico che produce un'impronta del documento di 256 bit .
Titolare	Soggetto intestatario del certificato.
Time Stamping Authority	Autorità che rilascia marche temporali.

A.6. Riferimenti tecnici

RFC 1305	Network Time Protocol (Version 3) Specification, Implementation
ETSI TS 102 023	Deliverable ETSI TS 102 023 “Policy requirements for time-stamping authorities” – Aprile 2002
RFC 3280	RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
RFC 3161	RFC 3161 (2001): “ 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 2527 (1999): “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”
RFC 3039	RFC 3039 (2001) Internet X.509 Public Key Infrastructure Qualified Certificates Profile
ETSI TS 101 733	ETSI TS 101 733 V1.4.0 “Electronic Signatures and Infrastructure (ESI): Electronic Signature Formats” (2002-09)

B. Generalità

Il presente documento ha come obiettivo la descrizione, in termini generali, delle procedure e 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 proseguo del documento.

B.1. Dati identificativi della versione del Manuale Operativo

Il presente documento costituisce la versione n.01 del *Manuale Operativo del Certificatore Accreditato INTESA per le procedure di firma remota in ambito bancario e finanziario* rilasciata il 01/11/2011 in conformità con l'Art.36 del DPCM.

L’object identifier di questo documento è 1.3.76.21.1.3.1.170.

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

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

La pubblicazione di versioni aggiornate del presente Manuale Operativo avverrà sul sito sopra indicato solo successivamente al loro inoltro al DigitPA (già CNIPA - Centro Nazionale per l'Informatica nella Pubblica Amministrazione).

Lo stesso manuale operativo verrà sempre pubblicato ed eventualmente aggiornato in simultanea anche sui siti delle Banche che offriranno tale servizio.

INTESA ha adottato, come propria Certificate Policy, quanto indicato all'interno del documento ETSI 101 456 (OID 0.4.0.1456.1.1). Tale decisione è stata confortata dal fatto che la maggior parte dei certificatori europei hanno adottato tali indicazioni per le proprie certificate policy. Inoltre, tale certificate policy è stata riconosciuta comparabile alla US Federal Bridge CA Certificate Policy, Medium Level. L'adozione di tale policy permetterà quindi una più facile interoperabilità in sede europea e un'eventuale più agevole interazione con le amministrazioni del governo USA.

B.2. Dati identificativi del Certificatore

Dati identificativi del Certificatore

Il Certificatore di cui il presente documento costituisce il "Manuale Operativo" ai sensi dell'Art.29 del Codice dell'Amministrazione Digitale è la società INTESA, di cui di seguito sono forniti i dati identificativi.

Denominazione sociale	In.Te.S.A. S.p.A.
Indirizzo della sede legale	Corso Orbassano, 367 - 10137 Torino
Legale Rappresentante	Antonio Taurisano Amministratore Delegato e Direttore Generale
Registro delle Imprese di Torino	N. Iscrizione 1692/87
N. di Partita I.V.A.	05262890014
N. di telefono (centralino)	+39-011-0043.611
Sito Internet	www.intesa.it
N. di fax	+39-011-0043.503
Indirizzo di posta elettronica	marketing@intesa.it
Indirizzo (URL) registro dei certificati	ldap://x500.e-trustcom.intesa.it
ISO Object Identifier (OID)	1.3.76.21.1

Il personale responsabile delle attività di certificazione, in conformità con l'Art.34 del DPCM, è articolato nelle figure seguenti:

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

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

B.4. Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo è di INTESA, nella persona di Antonio Raia (DPCM Art.36 comma 3.c), il quale ne cura la stesura, la pubblicazione e l'aggiornamento.

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:	per le chiamate dall'Italia 800.80.50.93
	per le chiamate dall'estero +39 011.30.11.202
un recapito fax:	+39 011.00.43.503

B.5. 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 accreditato INTESA espletando, per la parte di loro competenza, le attività a loro attribuite.

Pertanto saranno di seguito descritti gli ambiti nei quali il certificatore accreditato opera e, di conseguenza, le entità coinvolte.

B.5.1. Certification Authority (Certificatore Accreditato)

INTESA, operando nell'ottemperanza di quanto previsto nelle Regole Tecniche (DPCM) e al Codice dell'Amministrazione Digitale, espleta le attività di certificatore accreditato. Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di certificati qualificati.

I dati identificativi del certificatore accreditato INTESA sono riportati al precedente paragrafo B.3.

B.5.2. Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio (Firma Remota nell'ambito delle applicazioni bancarie e finanziarie) descritta in questo Manuale Operativo, il Certificatore rilascerà il mandato a svolgere la funzione di Registration Authority alla Banca o all'Istituto di Pagamento che avranno acquisito il servizio.

In virtù di specifici accordi, la Registration Authority svolgerà le seguenti attività :

- Identificazione dei Titolari
- Registrazione dei Titolari

In particolare, è importante notare che, essendo queste funzioni svolte all'interno dei servizi offerti dalla Banca o dall'Istituto di Pagamento, l'identificazione del Titolare è svolta coerentemente a quanto previsto dalla vigente normativa in materia di antiriclaggio.

La Banca o l'Istituto di Pagamento, in qualità di Registration Authority del Certificatore e nel rispetto della normativa antiriclaggio, potranno identificare il Titolare (*adeguata verifica*) anche se questi non si presenterà fisicamente in un'agenzia.

In questo caso la Banca o l'Istituto di Pagamento dovranno comunque :

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

C. Obblighi

C.1. Obblighi del Certificatore Accreditato

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

- Decreto Legislativo del 7 marzo 2005, n.82 (CAD); e successive modifiche
- Decreto Presidente del Consiglio dei Ministri 30 Marzo 2009;
- 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 DPCM,
- garantisce che il proprio Sistema qualità sia conforme alle norme ISO 9001;
- assicura che il dispositivo sicuro per la generazione delle firme (HSM) abbia le caratteristiche e i requisiti di sicurezza previsti dall'Art.35 del CAD e all'Art.9 del DPCM,
- rilascia il certificato qualificato secondo quanto stabilito all'Art.32 del CAD;
- specifica, nel certificato qualificato su richiesta dell'istante e con il consenso del Terzo Interessato, la sussistenza dei poteri di rappresentanza o di altri titoli relativi all'attività professionale o a cariche rivestite, previa verifica della sussistenza degli stessi secondo quanto indicato nel cap. F.1;
- 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.10 del DPCM, il Certificatore fornisce ovvero indica almeno un sistema che consenta di effettuare la verifica delle firme digitali.

Inoltre, il Certificatore:

- genera un certificato qualificato, per ciascuna delle chiavi di firma elettronica avanzata utilizzate da DigitPA per la sottoscrizione dell'elenco pubblico dei certificatori, e lo pubblica nel proprio registro dei certificati (Art.38 DPCM);
- indica un sistema di verifica della firma come richiesto dall'Art.10 del DPCM ;
- mantiene copia della lista, sottoscritta da DigitPA, dei certificati relativi alle chiavi di certificazione (di cui all'Art.39 del DPCM), e la rende rende accessibile per via telematica (Art.38, comma 3 del DPCM).

C.2. Obblighi del Titolare

Il Titolare richiedente un certificato digitale per i servizi descritti nel presente Manuale Operativo dovrà essere un cliente della Banca o dell'Istituto di Pagamento che operano da Registration Authority.

In quanto tale potrà ricevere un certificato qualificato con cui poter effettuare firme elettroniche qualificate nelle modalità descritte nel capitolo G.

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

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;
- indicare esplicitamente nella richiesta di certificazione le informazioni che egli desidera non siano inserite nel certificato;
- 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.4, comma 5, DPCM);
- fare immediata denuncia alle Autorità competenti e alla Banca o all'Istituto di Pagamento, in caso di perdita o furto dei codici e/o dei dispositivi indicati per accedere alle proprie chiavi di firma, sarnno la Banca o l'Istituto di Pagamento poi a provvedere, anche in mancanza di tali codici, a provvedere all'immedita revoca del certificato;
- 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 utilizzino evidenze informatiche firmate digitalmente, sono tenuti a:

- verificare la validità del certificato contenente la chiave pubblica del Titolare firmatario del messaggio, secondo quanto indicato allo standard ISO 9594-8, e il momento della sua emissione;
- verificare l'assenza del certificato dalle Liste di Revoca (CRL) e Sospensione (CSL) dei certificati e il momento della sua emissione;
- verificare la validità del percorso di certificazione, basato sull'elenco pubblico dei certificatori;
- verificare i dati identificativi del titolare del certificato e l'esistenza di eventuali limitazioni all'uso del certificato (informazioni reperibili verificando gli attributi associati al certificato con le funzionalità esposte dal software di verifica).

C.4. Obblighi del Terzo Interessato

Il Terzo Interessato nei servizi descritti dal presente Manuale Operativo sono la Banca o l'Istituto di Pagamento stessi.

Pertanto la Banca o l'Istituto di Pagamento devono verificare che, prima di richiedere il rilascio di un certificato digitale al proprio Cliente, lo stesso sia in possesso di tutti i requisiti necessari.

La Banca o l'Istituto di Pagamento, nella veste di Terzo Interessato, non svolgeranno soltanto un'attività di supporto al Titolare, ma saranno loro stessi ad indicare al Certificatore eventuali limitazioni d'uso del certificato, eventuali poteri di rappresentanza e qualsiasi variazione delle stesse.

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.

La richiesta di revoca o sospensione da parte del Terzo Interessato dovrà essere immediatamente inoltrata quando vengano meno i requisiti in base ai quali al titolare era stato rilasciato un certificato dìgitale.

C.5. Obblighi delle RA esterne

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

- identificazione certa del Titolare del certificato;

- registrazione del Titolare;
- consegna al Titolare dei dispositivi e/o codici che gli permettano di accedere alla propria chiave di firma nel rispetto degli Artt. 7 e 9 comma 2 del DPCM.

La documentazione raccolta verrà successivamente trasmessa all'Uffico RA del Certificatore, salvo differenti accordi rirportati sul contratto di mandato.

Le RA esterne sono attivate a seguito di un adeguato addestramento del personale della Banca o dell'Istituto di Pagamento con le quali è stipulato un regolare Contratto di Mandato sottoscritto da entrambe le parti. In tale contratto sono esplicitati gli obblighi cui si devono attenere la Banca o l'Istituto di Pagamento 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;
- utilizzare e trattare i dati personali acquisiti in fase di riconoscimento in accordo con il Dlgs. 196/03.

Il servizio di identificazione (*adeguata verifica*) potrà svolgersi in modalità diverse purchè rispettose delle norme antiriclaggio; in particolare sono previste tre modalità, qui di seguito descritte:

1) Canonica: il titolare viene identificato presso una filiale bancaria o dell'Istituto di Pagamento.
2) On demand: all'apertura di un nuovo conto corrente, il Titolare potrà chiedere di essere contattato da un Personal Financial Adviser che, fissatogli un appuntamento, supporterà il Cliente in tutte le procedure inerenti all'apertura di un Conto Corrente. In questa fase il Cliente verrà guidato (dopo essere stato identificato e registrato) anche nella richiesta di un certificato di firma qualificata.
3) On line: se invece il titolare dovesse scegliere la modalità di adesione diretta ed è già titolare di un conto corrente presso una Banca sul territorio nazionale, per essere riconosciuto ai fini di legge potrà ricorrere o a una procedura RID (Rimessa Interbancaria Diretta) oppure disporre un bonifico dal conto corrente già aperto presso la Banca di cui prima.

Attraverso le procedure di cui sopra, la LRA della Banca o dell'Istituto di Pagamento entrerà in possesso di tutte le informazioni previste dalla legge, in totale sicurezza e nel pieno rispetto della privacy.

D. Responsabilità e limitazioni agli indennizzi

D.1. Responsabilità del Certificatore

INTESA è responsabile, verso i Titolari, per l'adempimento di tutti gli obblighi discendenti dall'espletamento delle attività previste dal DPCM, dal DLgs 196/03 e dal

DLGS n.82 07/03/2005 (CAD) e successive modificazioni e integrazioni (vedi Capitolo C, paragrafo C.1 "Obblighi del Certificatore Accreditato").

INTESA non assume alcuna responsabilità per le conseguenze derivanti da un uso dei certificati diverso da quanto disposto dall'Art.4 del DPCM, e in particolare dal mancato rispetto da parte del Titolare, degli utilizzatori dei certificati e dal Terzo Interessato di quanto indicato nel presente Manuale Operativo e dalla mancata osservanza da parte degli stessi della normativa vigente.

Si ricorda, in particolare, di conservare con speciale diligenza i dispositivi OTP e i codici segreti indispensabili per accedere alle chiavi di firma.

Per quanto non esplicitamente riportato si fa specifico riferimento a quanto espresso nel Codice dell'Amministrazione Digitale C*apo II, Sezione II Firme elettroniche e Certificatori*, Art.32 *Obblighi del Titolare e del Certificatore*.

INTESA non potrà essere ritenuta responsabile delle conseguenze dovute a cause ad essa non imputabili, quali, a solo titolo di esempio: calamità naturali, 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.

D.2. Assicurazione

Il Certificatore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui contenuto è in linea con quanto necessario per svolgere l'attività professionale di cui trattasi.

Di tale contratto è stato inviata al DigitPA apposita dichiarazione di stipula.

La copertura Assicurativa prevede i seguenti massimali:

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

D.3. Limitazioni agli indennizzi

Il Certificatore, fatto salvo i casi di dolo e colpa grave, esclude ogni responsabilità per danni subiti dagli utenti o da terzi in conseguenza di:

- mancato rispetto delle procedure e delle regole stabilite dal Certificatore stesso;
- danno causato da disservizio;
- uso improprio dei certificati di sottoscrizione da parte di applicazioni di terze parti.

Il Certificatore non si ritiene, peraltro, responsabile dei danni causati agli utenti Titolari e utilizzatori o a terzi conseguenti al non rispetto, da parte del Titolare, delle regole definite nel presente Manuale Operativo.

Il Titolare, a seguito della presa visione del presente Manuale Operativo, deve porre in opera tutte quelle misure di speciale diligenza atte ad evitare danni a terzi legati all'uso improprio di quanto fornito dal certificatore accreditato.

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 la Banca o l'Istituto di Pagamento e il Titolare.

F. Modalità di identificazione e registrazione degli utenti

F.1. Identificazione degli utenti

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

Questa operazione viene demandata al personale della Banca o dell'Istituto di Pagamento che in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriclaggio verificherà l'identità e registrerà il Titolare.

Per i successivi rinnovi tale attività non sarà più ripetuta: sarà cura del Titolare comunicare al Certificatore, attraverso la Banca o l'Istituto di Pagamento, 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;
- Recapito per la corrispondenza;
- 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.

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

In alternativa ad un token OTP fisico, la Banca o l'Istituto di Pagamento potranno indicare ai Titolari come attivare un sistema di autenticazione software per dispositivi

mobili (qualora il Titolare ne disponesse di uno e scegliesse questa modalità come preferibile per comodità d'uso rispetto all'impiego di un Token fisico). Tale sistema software permetterà la generazione di una One Time Password sul dispositivo mobile del Titolare e potrà essere pertanto utilizzato come strumento di autenticazione ai sistemi di firma remota.

Oltre all'OTP, verranno forniti al Titolare le informazioni e un Personal Identification Number (PIN) che possano garantirgli un accesso sicuro al servizio di firma remota resogli disponibile dalla Banca o dal l'Istituto di Pagamento stessi; lo stesso PIN potrà essere utilizzato come codice di emergenza (in caso ad esempio di smarrimento e/o perdita del Token OTP o del mobile) per sospendere con urgenza il certificato digitale a lui emesso.

Il PIN potrà essere successivamente modificato/aggiornato dal titolare usufruendo dei servizi che la Banca o l'Istituto di Pagamento gli avranno messo a disposizione.

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.

Inoltre, direttamente allo sportello della Banca o dell'Istituto di Pagamento, oppure successivamente, collegandosi al servizio di internet banking esposto dalla stessa Banca o dall'Istituto di Pagamento, ma in ogni caso preventivamente alla richiesta di rilascio di un certificato digitale, il titolare dovrà:

1. prendere visione del Manuale Operativo Intesa;
2. autorizzare la Banca o l'Istituto di Pagamento al trattamento dei propri dati personali per le finalità legate all'emissione di un certificato digitale qualificato.

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

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. Copia di tale documentazione viene conservata per 20 (venti) anni dalla scadenza del certificato.

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 od 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 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

Tutti i certificati emessi conterranno sempre una limitazione d'uso.

La formula standard utilizzata sarà:

L'utilizzo del certificato è limitato ai rapporti con *Nome Banca*/*Istituto di Pagamento*.
The certificate may only be used for relations with Nome Banca/*Istituto di Pagamento*.**

Specifici limiti d'uso potranno essere concordati con la Banca o con l'Istituto di Pagamento, purché non eccedano i 200 caratteri.

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

F.1.4. Uso di pseudonimi

Il Titolare può richiedere, in particolari casi, che il certificato riporti uno pseudonimo in alternativa ai propri dati reali. Le informazioni relative alla reale identità dell'utente saranno conservate per 20 (venti) anni.

F.2. Registrazione degli utenti

Successivamente alla fase di identificazione, viene eseguita la registrazione dei dati dei Titolari sugli archivi del Certificatore. Questa operazione potrà essere eseguita mediante un'applicazione software direttamente richiamabile dagli applicativi della Banca o dell'Istituto di Pagamento.

Durante la registrazione dei dati del Titolare viene generato l'identificativo univoco del Titolare presso il Certificatore.

G. Modalità operative per la sottoscrizione di documenti

Il Certificatore, attraverso i servizi della Banca o dell'Istituto di Pagamento, rende disponibile ai Titolari quanto necessario a generare 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 o accedendo al servizio di home banking della Banca o dell'Istituto di Pagamento oppure direttamente allo sportello di una filiale della Banca o dell'Istituto di Pagamento.

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.

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

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

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) al fine di confermare la propria volontà di firmare un documento.

Al ricevimento della suddetta 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 della Banca o dell'Istituto di Pagamento utilizzerà un'autenticazione a due fattori attraverso l'inserimento di un PIN (informazione che solo l'utente conosce) e 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, dopo qualche 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 nel seguito come questa autenticazione appena descritta sia altamente gradita quando il Titolare si trovi da operare in stazioni non presidiate (tipicamente collegandosi ai servizi della Banca o dell'Istituto di Pagamento con il proprio PC attraverso i servizi di home banking esposti dalla Banca o dell'Istituto di Pagamento stessi), ma, invece, sia poco praticabile quando il Titolare si trovi ad operare di fronte ad un operatore esterno, ad esempio in una stazione presidiata da un cassiere della Banca o dell'Istituto di Pagamento.

Per gestire queste ultime situazioni, si è 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 in stazioni non presidiate (Home banking)

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

1. Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione;
2. Seleziona e verifica il documento da firmare;
3. Inserisce il proprio codice PIN;
4. Appena validato il PIN, il Titolare, in un tempo configurato (non superiore al minuto primo) e 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 e associato al Titolare, procede nell'operazione di firma e provvede ad inviare una conferma del successo dell'operazione stessa;
6. Se, invece, è 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.1.2. Processo di Firma in stazioni presidiate (Sportello bancario o finanziario)

Una volta ottenuto il certificato qualificato, il Titolare potrà procedere alla sottoscrizione di un documento.

Come detto in precedenza, presso uno sportello bancario o finanziario e di fronte ad un operatore il Titolare potrebbe trovarsi in difficoltà ad inserire codici personali e riservati quali ad esempio un PIN.

Si è perciò pensato anche ad un soluzione alternativa, che garantisca comunque il massimo della sicurezza:

1. L'utente si presenta allo sportello di una filiale bancaria o dell'Istituto di Pagamento (stazione presidiata) e viene riconosciuto dal personale addetto (il cassiere ad esempio) in modalità canonica;
2. Visionato il documento da firmare, il Titolare può avviare il processo di firma;
3. Viene a questo punto reso disponibile su di un video, visibile al titolare, un numero telefonico (scelto randomicamente all'interno di un numeroso set di numeri disponibili) e contemporaneamente viene fatto partire un timer;
4. Il Titolare, in un tempo configurato (non superiore al minuto primo), deve, per confermare la propria intenzione di sottoscrivere il documento, chiamare il numero che gli è apparso a video (utilizzando il proprio cellulare, censito in precedenza);
5. Il sistema, a questo punto, se rileva la correttezza del chiamante, provvede ad eseguire la sottoscrizione del documento e ad inviare via SMS una conferma dell'operazione stessa;
6. Se, invece, è trascorso il tempo prefissato senza che il sistema abbia ricevuto una telefonata al numero indicato al punto 3, l'operazione viene annullata;
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 *Call Drop*, è resa disponibile una seconda modalità di autenticazione denominata "*OTP Mobile*".

Per attivare questa modalità, il Titolare dovrà disporre di uno smartphone fra quelli specificati dalla Banca o dall'Istituto di Pagamento stessi come adeguati per tale servizio.

Eseguita questa verifica, in fase di identificazione al Titolare sarà comunicato un indirizzo internet specifico sul sito della Banca o dell'Istituto di Pagamento da cui scaricare sul suo smartphone un'applicazione definita di "*OTP Mobile*" e un PIN (sempre consegnatogli presso lo sportello bancario o fianaziario dove è avvenuta la registrazione del Titolare).

Anche per questa seconda modalità di autenticazione descriviamo il processo di sottoscrizione a seconda che si svolga o meno in stazioni presidiate.

G.2.1. Processo di Firma in stazioni non presidiate (Home banking)

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

1. Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione;
2. Seleziona 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.2.2. Processo di Firma in stazioni presidiate (Sportello bancario o dell'Istituto di Pagamento)

Anche in questo caso si è studiata una soluzione che non richieda al Titolare di inserire davanti al personale della Banca o dell'Istituto di Pagamento codici riservati che possano essere poi riutilizzati in maniera fraudolenta ai suoi danni.

Entrato in possesso del proprio certificato qualificato, il Titolare potrà sottoscrivere un documento come segue.

1. L'utente si presenta allo sportello di una filiale bancaria o dell'Istituto di Pagamento (stazione presidiata) e viene riconosciuto dal personale addetto (il cassiere ad esempio) in modalità canonica;
2. Al momento della firma viene attivato di fronte all'utente uno specifico monitor dotato di webcam;
3. Il Titolare, una volta verificato su tale monitor il documento da firmare e deciso di procedere con l'operazione di sottoscrizione, lancia dal proprio smartphone la generazione di un OTP che viene visualizzata anche in formato di codice a barre;
4. Il Titolare può a questo punto, posizionando il proprio smartphone verso la webcam, permettere la lettura dell'OTP generata al passo 3 e avviare la procedura di sottoscrizione vera e propria;
5. Il sistema una volta firmato il documento provvede a darne immediata notifica attraverso l'invio di un SMS al Titolare stesso;
6. Per firmare più documenti verranno reiterati i passi dal 2 al 5.

G.3. Autenticazione con Token OTP

Infine, può essere utilizzata un'autenticazione legata all'utilizzo di Token OTP fisici (molto diffusi nel mondo bancario e finanziario).

L'utilizzo di questo Token OTP fisico è oggi previsto solo per accessi in stazioni non presidiate (tipicamente una postazione remota di home banking).

Il Titolare si connette all'applicazione bancaria o finanziaria attraverso i suoi codici personali per l'accesso all'applicazione e per avviare la procedura di firma inserirà il PIN e il codice OTP che avrà nel frattempo generato e visualizzato sul display del Token.

G.4. Modalità operative per la verifica della firma

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

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 DPCM all'Art.6 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 inoltre alla presenza di un numero di responsabili aziendali ritenuto adeguato e sufficiente ad evitare operazioni illecite.

Una volta generate le coppie di chiavi, quelle private vengono suddivise in più parti, ciascuna delle quali viene trascritta su due set di smartcard / token usb e assegnati ciascuno ad una delle persone aziendali presenti, le quali vi associeranno una propria password che manterranno segreta, e conservati in modo sicuro (così come le password).

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.45 del DPCM.

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 dalla Banca o dall'Istituto di Pagamento in una delle modalità precedentemente descritte.

Il PIN e l'OTP (generata secondo le modalità descritte) costituiscono l'insieme di dati di cui il Titolare deve avere in modo esclusivo la conoscenza e il possesso ai sensi dell'Art.7 comma 3 lett.d) del DPCM. Questi stessi dati gli saranno richiesti tutte le volte che voglia sottoscrivere un documento secondo quanto richiesto dall'Art.35, comma 2 del CAD.

Le coppie di chiavi di sottoscrizione (la cui lunghezza è di 1024 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 H1, vengono generati i certificati delle chiavi pubbliche, nel formato ISO 9594-8 (2001), conforme con quanto disposto dal DPCM, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati al DigitPA attraverso il sistema di comunicazione di cui all'Art.12, comma 1, del DPCM .

Il Certificatore genera un certificato qualificato per ciascuna delle chiavi di firma elettronica qualificata utilizzate 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 da DigitPA, dei certificati relativi alle chiave di certificazione e lo rende disponibile per via telematica (DPCM, Art.38, commi 1 e 3).

I.2. Procedura di emissione dei Certificati di sottoscrizione

INTESA emette certificati con un sistema conforme con l'Art.29 del DPCM .

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 della Banca o dell'Istituto di Pagamento al Certificatore.

Il Certificatore elabora nel più breve tempo possibile la richiesta ricevuta.

La generazione dei certificati è registrata nel giornale di controllo (DPCM, Art.14, 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.

In seguito a ciò è garantita la loro interoperabilità nel contesto delle attività dei certificatori accreditati italiani.

I.4. Codice di Emergenza

Il Certificatore garantisce, in conformità con quanto previsto dall'Art.17 del DPCM, 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 PIN consegnato al Titolare all'atto della sua registrazione.

J. Modalità di revoca e sospensione dei certificati

J.1. Revoca dei certificati

La revoca dei certificati viene asseverata dal loro inserimento nella lista CRL (Art.18 DPCM).

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

La CRL, firmata dal Certificatore, viene aggiornata con periodicità giornaliera 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. 19, 21, 23 e 25 del DPCM), il Certificatore notifica al Titolare la richiesta e il momento in cui entrerà in vigore l'evento richiesto.

In fase di richiesta, saranno specificate la data e l'ora a partire dalla quale il certificato risulterà revocato (Art.20, comma 1, DPCM).

J.1.1. Revoca su richiesta del Titolare

Il Titolare può richiedere la revoca accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca o dell'Istituto di Pagamento oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto di Pagamento.

Il Certificatore, avvertito dalla Banca o dall'Istituto di Pagamento, che nel frattempo avrà anche bloccato i codici di accesso del Titolare, provvederà alla immediata revoca del certificato.

J.1.2. Revoca su richiesta del Terzo Interessato

La Banca o l'Istituto di Pagamento, in qualità di Terzo Interessato, possono richiedere la revoca del certificato .

Accertata la correttezza della richiesta, sarà data notizia della revoca ai Titolari interessati e il certificato sarà inserito nella lista di revoca, che sarà emessa immediatamente.

J.1.3. Revoca su iniziativa del Certificatore

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

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

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

Nei casi di:

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

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

Entro 24 ore, il Certificatore notificherà la revoca al DigitPA 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 (ad esempio nei casi in cui si tema lo smarrimento/furto del Token OTP, o si debbano fare riscontri per avere

certezza dell'effettiva cessazione del Titolare dalla mansione per la quale gli era stato emesso il certificato, ecc.).

La richiesta di sospensione può essere avanzata da tutte le entità previste dal DPCM agli Artt. 23, 24 e 25 (Certificatore, Titolare, Terzo Interessato).

In assenza di comunicazioni da parte del Titolare, il certificato verrà automaticamente revocato dopo il periodo di sospensione indicato dal Titolare nella richiesta.

In assenza di una qualche indicazione sul periodo di sospensione da parte del Titolare tale periodo è da considerasi di 90 (novanta) giorni, scaduti i quali il certificato verrà considerato revocato a partire dalla data di decorrenza della sospensione.

Si precisa inoltre che un certificato che dovesse giungere a naturale scadenza in uno stato di sospeso verrebbe considerato revocato dalla data di decorrenza della sospensione.

J.2.1. Sospensione su richiesta del Titolare

Il Titolare può richiedere la sospensione del certificato accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca o dell'Istituto di Pagamento oppure mettendosi in contatto diretto con il Servizio Clienti della Banca o dell'Istituto di Pagamento.

Il Certificatore procede alla sospensione che verrà comunicata al Titolare utilizzando specifiche funzioni rese disponibili all'interno dei servizi della Banca o dell'Istituto di Pagamento.

Il Titolare successivamente potrà richiedere il ripristino del certificato secondo le modalità rese disponibili sempre dalla Banca o dall'Istituto di Pagamento.

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

J.2.2. Sospensione su richiesta del Terzo Interessato

La Banca o l'Istituto di Pagamento, in qualità di Terzo Interessato, potranno richiedere la sospensione del certificato.

Il Certificatore, accertata la correttezza della richiesta, sospenderà tempestivamente il certificato e ne darà notizia della sospensione ai Titolari interessati tramite posta elettronica o con comunicazione attraverso i servizi esposti dalla Banca o dall'Istituto di Pagamento.

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 elettronica 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 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.

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

Se il Titolare provvederà ad inoltrare la richiesta di un nuovo certificato prima della scadenza del certificato in suo possesso le procedure per l'ottenimento di un nuovo certificato non vengono più ripetute le attività di identificazione e di registrazione dei dati del Titolare.

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 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, in presenza del Responsabile del servizio di certificazione e di responsabili aziendali in numero adeguato e sufficiente a garantire la sicurezza dell'operazione, si procederà all'esecuzione degli eventi sotto descritti, conformi con il DPCM, Artt. 13 e 26.

Sarà eseguita la seguente procedura:

1. Al dispositivo di firma viene fatta generare una nuova coppia di chiavi asimmetriche con il procedimento descritto al paragrafo H.1.
2. I certificati così generati, a seguito della sostituzione delle chiavi di certificazione, sono inviati a DigiPA.
3. Alla data di entrata in vigore delle nuove chiavi, le persone depositarie delle porzioni di chiavi si riuniranno per restituire i dispositivi contenenti le porzioni della vecchia chiave privata del Certificatore, accertarsi che le vecchie chiavi di cui erano responsabili siano rese inutilizzabili e per presenziare alla distruzione della chiave di firma scaduta del Certificatore.

Quanto fatto ai punti precedenti sarà verbalizzato e il verbale sarà conservato dal Certificatore per 20 (venti) anni dalla scadenza dei certificati.

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

Il procedimento utilizzato in caso di guasto del dispositivo di firma 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 ripeteranno quanto descritto al paragrafo.

K.3. Chiavi di marcatura temporale

In conformità con quanto indicato all'Art.45, comma 2, del DPCM, ai fini di limitare il numero di marche temporali generate con la medesima coppia di chiavi di 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. Certificati per le chiavi di firma del DigitPA (DPCM Art.38, comma 1).
4. 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* secondo il protocollo LDAP v2, come definito nello RFC 1777, o lo LDAP v3 come definito nello RFC 2251.

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

Gli addetti abilitati alla gestione diretta del registro dei certificati possono accedere al locale ove il sistema è installato e operarvi solo in modalità dual control onde 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 minime previste dal DLgs 196/03.

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.32 del DPCM).
- ARCHIVIO DIGITALE DELLE MARCHE TEMPORALI, contiene le marche temporali generate dal sistema di validazione temporale (Art.49, comma 1, del DPCM).
- REGISTRO OPERATIVO DEGLI EVENTI DI VALIDAZIONE TEMPORALE, registro sul quale sono automaticamente memorizzati gli eventi attinenti le attività

di validazione temporale per i quali è prevista la registrazione di qualunque anomalia o tentativo di manomissione che possa pregiudicare il funzionamento del sistema di validazione temporale (Art.48 del DPCM).

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 dello HW, anche della situazione di emergenza. È previsto inoltre l'intervento entro il medesimo lasso di tempo dei depositari delle componenti la chiave privata della CA ai fini di ricostruirla nel dispositivo di firma 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 sofware 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 (GG/MM/YYYY HH:MM:SS), con la precisione del secondo, che rappresentano l'ora locale, in base alla configurazione della macchina. Tali riferimenti sono conformi al DPCM Art.47.

Ogni registrazione effettuata sul giornale di controllo contiene un riferimento temporale che, essendo generato con la modalità qui descritta, è opponibile a terzi (Art.37 del DPCM).

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.