Manuale Operativo
del Certificatore Accreditato In.Te.S.A. S.p.A. per le procedure di firma remota nell'ambito dei servizi di FINECO (Banca del Gruppo UniCredit)

Codice documento: MO-FNC

Redazione: Antonio Raia

Approvazione: Franco Tafini

Data emissione: 17/03/2014

Versione: 02

VERSIONI

Versione n°:	**02**	**Data Revisione:**	**17 Marzo 2014**
Descrizione modifiche:	**Aggiornamento agli Obblighi delle Registration Authority esterne (C.5) Aggiornamento riferimenti al DPCM 22 Febbraio 2013 Introduzione dell'utilizzo di Applicazioni per dispositivi mobili Aggiornato il Codice documento (MO-FNC)**		
Motivazioni:	**Aggiornamento**		

Versione n°:	**01**	**Data Revisione:**	**7 Novembre 2012**
Descrizione modifiche:	**Nessuna**		
Motivazioni:	**Prima emissione**		

Sommario

A. Introduzione

A.1. › Proprietà intellettuale

Questo documento è il Manuale Operativo per la procedura di Firma Digitale Remota nell'ambito dei Servizi forniti da FinecoBank S.p.A. (di seguito "Fineco" o anche "Banca"), con Sede Sociale in Piazza Durante 11, 20131 Milano - Direzione Generale in via Rivoluzione d'Ottobre, 16, 42123 Reggio Emilia - Capitale Sociale 200.070.430,89 euro interamente versato - Iscrizione al Registro Imprese di Milano, Codice Fiscale e P.IVA n. 12962340159 - appartenente al Gruppo Bancario UniCredit, iscritto all'albo dei Gruppi Bancari n. 02008.1 – Aderente al Fondo Interbancario di Tutela dei Depositi. Il presente Manuale Operativo è di esclusiva proprietà di Fineco.

A.2. › Il Manuale Operativo

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

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" oppure "Codice") e in particolare:

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

Per quanto non espressamente previsto nel presente Manuale Operativo si fa riferimento alle norme tempo per tempo vigenti.
In questo contesto i Titolari di un Certificato Qualificato sono solo i soggetti riconosciuti dalla stessa Fineco che, in virtù di specifico accordo con il Certificatore, è autorizzata a svolgere la funzione di Registration Authority.
Il processo prevede che il Titolare possa avviare la procedura di Firma Remota di documenti e/o contratti relativi a prodotti e servizi offerti dalla Banca.

A.3. › 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 previsti dal presente manuale, 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;

A.4. › Riferimenti di legge

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*", pubblicato sulla Gazzetta Ufficiale n.42 del 20 febbraio 2001. Nel seguito anche semplicemente indicato come "TU".
DLGS 196 30/06/03	Codice in materia di protezione dei dati personali. (G.U. n.174 del 29 luglio 2003, suppl. ord.) .
DLGS 82 07/03/2005	Decreto Legislativo 7 Marzo 2005, n. 82 (G.U. n.112 del 16 Maggio 2005). *Codice dell'amministrazione Digitale* (nel seguito indicato semplicemente come CAD ovvero Codice), e successive modificazioni
DLGS 235 30/12/2010	Decreto Legislativo del 30 dicembre 2010, n. 235 *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.*
Deliberazione CNIPA n.45 21/05/2009	Deliberazione CNIPA 21 Maggio 2009, n.45. *Regole per il riconoscimento e la verifica del documento informatico*.
Determinazione Commissariale 69/2010 28/07/2010	Determinazione Commissariale DigiPA 28/07/2010 n. 69/2010 *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».*
DPCM 22/02/2013	Decreto del Presodente del Consiglio dei ministri, 22 febbraio 2013 *Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali, ai sensi degli articoli 20, comma 3, 24, comma 4,28, comma 3, 32, comma 3, lettera b) , 35, comma 2, 36, comma 2, e 71.* (G.U. n. 117 del 21 Maggio 2013).

Definizioni e acronimi

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

Termine o acronimo	***Significato***
AgID	Agenzia per l'Italia Digitale (già Cnipa e DigitPA)
Analisi dei rischi	Vedi Risk Assessment.
Certificatore	Autorità Accreditata che presta servizi di certificazione delle firme elettroniche qualificate e altri servizi connessi quali, ad esempio, 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	Centro Nazionale per l'informatica nella Pubblica Amministrazione. Successivamente DigitPA e oggi Agenzia per l'Italia Digitale.
Documento Informatico	La rappresentazione informatica di atti, fatti o dati giuridicamente rilevanti.
Firma elettronica Avanzata	È un particolare tipo di firma elettronica che, allegando oppure connettendo un insieme di dati in forma elettronica ad un documento informatico, garntisce integrità, autenticità del documento sottoscritto e controllo esclusivo dello strumento di firma.
Firma elettronica Qualificata	È un particolare tipo di firma elettronica avanzata basata su un certificate 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.
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. Questa attività è completamente demandata alla Banca (FinecoBank S.p.A.). 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.5. › 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) l 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.02 del *Manuale Operativo del Certificatore Accreditato INTESA per le procedure di firma remota nell'ambito dei servizi di FINECO* rilasciata il 17/03/2014, in conformità con l'Art.40 del Decreto.
L'object identifier di questo documento è 1.3.76.21.1.3.1.160.

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 _FINECO.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 della Banca.

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	Corso Orbassano, 367 - 10137 Torino
Legale Rappresentante	Enrico Cereda Amministratore Delegato
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.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.3. › Responsabilità del Manuale Operativo

La responsabilità del presente Manuale Operativo, ai sensi dell'Art. 40 comma 3 lett. c) del Decreto è di INTESA, nella persona di Antonio Raia, il quale ne cura la stesura, la pubblicazione, l'aggiornamento e ogni eventuale revisione, in accordo e in collaborazione con la Banca.
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.4. › Entità coinvolte nei processi

All'interno della struttura del certificatore vengono identificate delle entità che prendono parte ai processi relativi all'emissione dei certificati. Tali attori operano in ottemperanza alle regole e ai processi posti in opera dal Certificatore espletando, per la parte di loro competenza, le attività a loro attribuite.

B.4.1. › Certification Authority (Certificatore Accreditato)

INTESA, operando in ottemperanza con quanto previsto dal Decreto e dal CAD, espleta le attività di Certificatore Accreditato. Tali attività prevedono l'emissione, la pubblicazione, la revoca e la sospensione di Certificati Qualificati per la firma digitale remota
I dati identificativi del certificatore accreditato INTESA sono riportati al precedente paragrafo B.2.

B.4.2. › Registration Authority (Ufficio RA)

Per la particolare tipologia di servizio offerto (Firma Remota nell'ambito delle applicazioni della Banca descritte in questo Manuale Operativo) il Certificatore ha rilasciato mandato a svolgere le funzioni di Registration Authority a Fineco. In particolare, la Banca svolge le seguenti attività:

- Identificazione del Richiedente e/o Titolare.
- Registrazione del Richiedente.

La Banca, nello svolgimento della sua funzione di Registration Authority, deve vigilare affinchè 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 della Banca che opera da Registration Authority.

In quanto tale potrà ricevere un certificato qualificato per la Firma Digitale Remota per sottoscrivere contratti e documenti relativi a prodotti e /o servizi offerti dalla Banca.

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).

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 la Banca, 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 alla Banca, in caso di perdita o furto dei codici utilizzati per accedere alle proprie chiavi di firma, la Banca 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, 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 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 nei servizi descritti dal presente Manuale Operativo è Fineco.

Pertanto la Banca deve verificare che il cliente sia in possesso di tutti i requisiti necessari ed autorizza il cliente stesso a richiedere il rilascio del Certificato Qualificato per la Firma Digitale Remota.

La Banca nella sua veste di Terzo Interessato svolge un'attività di supporto al Titolare; in particolare sarà la Banca ad indicare al Certificatore:

- eventuali ulteriori limitazioni d'uso del Certificato Qualificato per la Firma Digitale oltre a quelle previste al paragrafo F.1.1;
- informazioni specifiche relative al Titolare, quali a titolo esemplificativo, ma non esaustivo, eventuali poteri di rappresentanza del Titolare.

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 Registration Authority 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 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 a Fineco mediante la stipula di un Contratto di Mandato sottoscritto da entrambe le parti.

In tale contratto sono esplicitati gli obblighi cui si deve attenere la Banca 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, Decreto e normativa in materia di Antiriciclaggio);
- 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.

Il personale della Banca, in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa, ovvero in conformità ad analoghe procedure adottate secondo la normativa antiriciclaggio vigente al tempo in cui è stata effettuata l'identificazione (anche se in epoca anteriore al presente Manuale), svolge tutte le operazioni necessarie all'identificazione e registrazione del Richiedente.

Il servizio di identificazione potrà essere gestito in due modalità:

1) Modalità tramite Personal Financial Adviser - il Titolare potrà chiedere di essere contattato da un Personal Financial Adviser che, fissatogli un appuntamento, lo supporterà in tutte le procedure inerenti l'apertura di un Conto Corrente, tra le quali l'identificazione ai sensi della vigente normativa antiriciclaggio. Dopo essere stato identificato e registrato, il Cliente potrà richiedere l'emissione di un certificato di firma qualificata.

2) Modalità diretta on line – il Titolare richiede l'apertura di un Conto Corrente in modalità diretta on-line. In questo caso l'identificazione ai sensi della vigente normativa antiriciclaggio sarà effettuata dalla Banca mediante l'acquisizione dei dati identificativi ed il riscontro su una copia di un documento di identità non scaduto; un'ulteriore verifica dei dati acquisiti sarà svolta dalla Banca secondo le modalità ritenute più opportune.

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

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.1.1.

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 stato 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

Il Servizio viene fornito da FinecoBank S.p.A. ai propri Clienti, senza oneri e non è pertanto soggetto a tariffazione.

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 Banca che in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriclaggio identificherà e registrerà il Titolare.

Per i successivi rinnovi, se effettuati prima che il certificato qualificato già rilasciato non sia scaduto, tale attività non dovrà essere ripetuta: sarà cura del Titolare comunicare al Certificatore attraverso la Banca 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 e data e luogo del rilascio.

Per l'accesso ai servizi offerti da Fineco, la stessa consegna ai propri clienti un Codice Utente e un Codice di attivazione, tramite i quali sarà possibile impostare la Password necessaria per accedere all'area riservata del sito www.fineco.it e un Personal Identification Number (PIN) che garantiscano un accesso sicuro ai servizi dispositivi e al servizio di firma remota fornito dalla Banca stessa.

Queste credenziali potranno essere successivamente modificate/aggiornate dal Titolare usufruendo dei servizi resi disponibili dalla Banca.

Per le successive operazioni (rilascio del certificato qualificato e successiva procedura di firma) invece di far uso dei più tradizionali strumenti OTP (One time Password) basati su token fisici il Titolare di un certificato qualificato potrà disporre di un servizio alternativo denominato SMS P.I.N.

Tale servizio fornisce ai Clienti che vi abbiano aderito tramite la procedura di attivazione un alto livello di sicurezza e consiste nella generazione e nell'invio di un messaggio SMS sul telefono cellulare del Cliente. Questo messaggio è praticamente un codice "usa e getta", OTP, (c.d. SMS P.I.N.), da utilizzarsi in aggiunta al PIN dispositivo standard per la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dalla Banca.

Il messaggio SMS, oltre al codice OTP, contiene elementi distintivi della specifica operazione richiesta dal cliente, in particolare ricordiamo che:

- Ogni codice SMS P.I.N. generato è associato ad una singola operazione richiesta dal cliente e non è in alcun modo riutilizzabile.
- L'attivazione del Servizio è consentita esclusivamente ai clienti il cui numero di cellulare presente in Anagrafe Generale risulti "certificato".
- L'attivazione del Servizio è indispensabile per poter accedere alla fase di provisioning dei certificati digitali di firma.

Sempre in questa fase potranno essere fornite al Titolare ulteriori informazioni e un codice di emergenza, grazie al quale l'utente in un qualsiasi momento potrà sospendere il certificato digitale a lui emesso (nelle applicazioni descritte dal presente Manuale Operativo verrà considerato come codice di emergenza il codice SMS PIN definito in precedenza).

Per certificare il numero di cellulare, il Cliente deve accedere all'area riservata del sito www.fineco.it mediante inserimento del codice utente e della password e quindi:

- Accedere alla sezione "Gestione Contatti".
- Inserire in apposita maschera il numero di cellulare che si vuole certificare convalidando l'operazione tramite PIN dispositivo.
- Attendere la ricezione al numero di cellulare inserito, di un SMS contenente il codice di controllo (viene inviata anche una e-mail informativa).
- Conferma dell'operazione inserendo sul sito il codice di controllo ricevuto.
- A conferma dell'avvenuta certificazione viene inviata un e-mail al cliente. Ed un SMS al numero di cellulare appena attivato.

In caso di modifica del numero di cellulare, il servizio sarà trasferito automaticamente sul nuovo recapito telefonico in seguito all'avvenuta certificazione dello stesso. Fino a tale momento, il servizio continuerà ad essere attivo sul precedente numero. Per garantire la massima sicurezza, in caso di un eventuale cambio del numero di cellulare, verranno inviati due SMS di cui uno al vecchio numero ed uno al nuovo.

In seguito all'attivazione del servizio SMS PIN, il Cliente potrà richiedere l'emissione del Certificato Qualificato.

Il cliente, identificato dalla Banca in ottemperanza con quanto previsto dalla vigente normativa in materia di Antiriciclaggio e dalle normative interne alla Banca stessa, potrà attivare la procedura di generazione del Certificato Qualificato per la Firma Digitale all'interno di un'apposita sezione del sito o delle Applicazioni per dispositivi mobili (utilizzate su Smatphone e Tablet con sistema operativo Apple IOS, Android e Windows Phone 8), mediante inserimento del proprio codice utente e della password di accesso. Una volta entrato in questa sezione dovrà:

- prendere visione del Manuale Operativo;
- verificare i propri dati anagrafici che saranno inseriti nel Certificato Qualificato per la Firma Digitale;

Ultimati i passi precedenti, il cliente inserisce il PIN Dispositivo e attende la ricezione sul cellulare del messaggio contenente l'SMS P.I.N.

Conferma on line l'operazione inserendo il codice ricevuto per dare avvio alla procedura di generazione delle chiavi e richiesta del Certificato.

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

Il Cliente può procedere alla conferma dell'operazione immediatamente o in un momento successivo ma comunque entro il termine di validità dell'SMS P.I.N.

In caso di mancata ricezione del codice SMS P.I.N. il Cliente può: chiedere un nuovo invio dell'SMS P.I.N. cliccando sul link "Non hai ricevuto l'SMS?", presente nell'area in cui è richiesto l'inserimento del codice. Sono consentite 3 richieste di nuovo invio.

A fronte del corretto inserimento dell'sms pin viene inviato un sms a conferma dell'avvenuta operazione.

Diversamente, trascorso il tempo prefissato senza che il sistema abbia ricevuto una conferma, l'operazione viene considerata nulla e conclusa senza l'emissione del certificato.

F.1.1. › Limiti d'uso

Nel Certificato Qualificato per la Firma Digitale, emesso nell'ambito dei servizi descritti nel presente Manuale e offerti dalla Banca, è inserita la seguente limitazione d'uso: "**Il presente certificato è utilizzabile esclusivamente per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da FinecoBank S.p.A**.".

G. Modalità operative per la sottoscrizione di documenti

Il Certificatore attraverso i servizi della Banca rende disponibile ai Titolari un'applicazione di firma conformemente a quanto previsto dalla normativa vigente.

La particolare tipologia del servizio non richiede che tale applicazione di firma sia installata sul proprio personal computer ma piuttosto la funzionalità di firma sarà resa disponibile accedendo ai servizi offerti dalla Banca attraverso l'area protetta del sito www.fineco.it o delle Applicazioni per dispositivi mobili (utilizzate su Smatphone e Tablet con sistema operativo Apple IOS, Android e Windows Phone 8). Le firme elettroniche qualificate ottenibili attraverso queste procedure saranno conformi a quanto previsto dal Decreto all'Art.4 comma 2 relativamente agli algoritmi utilizzati.

I documenti sottoscritti con tale applicazione di firma, come richiesto dall'Art.4 comma 3 dello stesso Decreto, 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.

Inoltre tali documenti saranno sempre disponibili, per il sottoscrittore, all'interno di specifica sezione dell'area protetta del sito www.fineco.it.

G.1. › Processo di Firma

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 del Certificato Qualificato per la Firma Digitale, accedendo all'area riservata del sito www.fineco.it o delle Applicazioni per dispositivi mobili (utilizzate su Smatphone e Tablet con sistema operativo Apple IOS, Android e Windows Phone 8), mediante inserimento del codice utente e della password in un'apposita sezione, richiede la sottoscrizione digitale di documenti e contratti relativi a prodotti o servizi offerti dalla Banca stessa.
2. Prende visione del\i documento\i da firmare digitalmente e di eventuale ulteriore documentazione informativa.
3. Avvia il processo di firma accettando la sottoscrizione del\i contratto\i mediante l'inserimento del PIN dispositivo.
4. Attende la ricezione sul cellulare del messaggio contenente l'SMS P.I.N.
5. Conferma online l'operazione digitando il codice ricevuto. Il Cliente può procedere alla conferma dell'operazione immediatamente o in un momento successivo - ma comunque entro il termine di validità dell'SMS P.I.N. - accedendo ad apposita sezione che conterrà i documenti ancora "Da confermare" e inserendo l'SMS P.I.N. ricevuto sul cellulare. E' anche possibile confermare l'operazione inoltrando l'SMS ricevuto ad apposito numero, senza cancellare il testo del messaggio originale.
6. A fronte del corretto inserimento dell'sms pin viene inviato un sms a conferma dell'avvenuta operazione.
7. In caso di mancata ricezione del codice SMS P.I.N. il Cliente può: chiedere un nuovo invio dell'SMS P.I.N. cliccando sul link "Non hai ricevuto l'SMS?", presente nell'area in cui è richiesto l'inserimento del codice. Sono consentite 3 richieste di nuovo invio.
8. Se invece, trascorso il tempo prefissato, senza che il sistema abbia ricevuto una conferma come indicato al punto 5 l'operazione viene considerata nulla e conclusa senza la sottoscrizione del\i documento\i.

G.2. › Modalità operative per la verifica della firma

I documenti che verranno sottoscritti con le modalità descritte in precedenza saranno esclusivamente in formato PDF (come previsto dall'Art. 21 comma 8 e 15 della Deliberazione CNIPA n. 45) e pertanto potranno essere verificati utilizzando il software Acrobat Reader scaricabile gratuitamente dal sito www.adobe.com/it.

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

H.1. › Generazione delle chiavi di certificazione

La generazione delle chiavi 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 dalla Banca in una delle modalità precedentemente descritte.

Il PIN associato alla OTP (generata secondo le modalità descritte) costituiscono l'insieme di dati di cui il Titolare deve avere in modo esclusivo la conoscenza ed 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. 7 comma 3 lett. d) del Decreto.
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 al paragrafo H.1 sono generati i certificati delle chiavi pubbliche, nel formato ISO 9594-8 (2001), conforme con quanto disposto dal Decreto, firmati con le rispettive chiavi private e registrati nel registro dei certificati secondo le modalità previste.

I certificati delle chiavi di certificazione sono inviati all'Agenzia per l'Italia Digitale attraverso il sistema di comunicazione di cui all'Art.16, 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 della Banca al Certificatore.

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

I.3. › Informazioni contenute nei certificati

I certificati 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. 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, contengono almeno la seguente limitazione d'uso: *"Il presente certificato è utilizzabile esclusivamente per la sottoscrizione di documenti e/o contratti relativi a prodotti e/o servizi offerti da FinecoBank S.p.A."*.

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 del Certificato.

Nelle applicazioni descritte dal presente Manuale Operativo sarà considerato come codice di emergenza il codice SMS PIN 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 accedendo ad una specifica sezione resa disponibile nell'ambito dei servizi della Banca oppure mettendosi in contatto diretto con il Servizio Clienti della Banca.

Il Certificatore avvertito dalla Banca, provvederà alla immediata revoca del certificato.

J.1.2. › Revoca su richiesta del Terzo Interessato

La Banca in qualità di Terzo Interessato può richiedere la revoca del certificato.

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, salvo i casi di motivata urgenza, potrà revocare il certificato dandone preventiva comunicazione al Titolare all'indirizzo di posta certificata 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 (HSM),
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 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. 23, 24 e 25 (Certificatore, Titolare, Terzo Interessato).

In assenza di comunicazioni da parte del Titolare, il certificato verrà automaticamente revocato dopo un periodo di sospensione di 90 (novanta) giorni o comunque entro la data di scadenza del certificato stesso.

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

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 oppure mettendosi in contatto diretto con il Servizio Clienti della Banca.

Il Certificatore avvertito dalla Banca provvederà alla immediata sospensione del certificato.

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

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

J.2.2. › Sospensione su richiesta del Terzo Interessato

La Banca in qualità di Terzo Interessato potrà richiedere la sospensione del certificato.

Il Certificatore, accertata la correttezza della richiesta, sospenderà immediatamente il certificato e 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 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 12 (dodici) mesi dalla data di emissione.

Tali certificati verranno tacitamente rinnovati per altri due anni.

Al termine dei tre anni si renderà invece necessaria l'emissione di un nuovo certificato e la sostituzione delle chiavi precedentemente utilizzate dal Titolare con una procedura del tutto simile a quella seguita per l'emissione di un nuovo certificato (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 nuovi 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.3. › 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 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. I 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.*** Il Certificatore consente l'accesso alle CRL anche 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 minime previste dal DLgs 196/03 e succesive 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 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 (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 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 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.