

"InfoCamere"  
Società Consortile d'Informatica delle Camere di Commercio Italiane per azioni

**Ente Certificatore InfoCamere**  
**Certificati di Sottoscrizione**  
**Manuale Operativo**  
**Codice documento: ICCA-MO**

Funzione emittente U.O. Firma Digitale

Redatto da Carolina Simonato

Verificato da Alfredo Esposito

Approvato da Pio Barban

*Nome file: Manuale Operativo v2r4.doc*

Questa pagina è lasciata  
intenzionalmente bianca

## Indice

---

<b>1. Introduzione al documento.....</b>	<b>6</b>
1.1 Scopo e campo di applicazione del documento .....	7
1.2 Riferimenti .....	7
1.3 Definizioni .....	7
1.4 Acronimi e abbreviazioni.....	9
<b>2. Generalità .....</b>	<b>11</b>
2.1 Identificazione del documento .....	11
2.2 Attori e Domini applicativi .....	11
2.2.1 Certificatore .....	11
2.2.2 Uffici di Registrazione.....	12
2.2.3 Registro dei Certificati.....	12
2.2.4 Applicabilità .....	12
2.3 Contatto per utenti finali .....	13
2.4 Rapporti con l'AIPA .....	13
<b>3. Regole Generali .....</b>	<b>14</b>
3.1 Obblighi e Responsabilità .....	14
3.1.1 Obblighi del Certificatore .....	14
3.1.2 Obblighi dell'Ufficio di Registrazione .....	14
3.1.3 Obblighi dei Titolari .....	15
3.1.4 Obblighi degli Utenti .....	15
3.2 Limitazioni e indennizzi.....	15
3.2.1 Limitazioni della garanzia e limitazioni degli indennizzi.....	15
3.3 Riferimenti alle leggi vigenti .....	16
3.3.1 Leggi applicabili .....	16
3.3.2 Clausola risolutiva espressa.....	16
3.3.3 Comunicazioni.....	16
3.4 Pubblicazione .....	16
3.4.1 Pubblicazione di informazioni relative al Certificatore .....	16
3.4.2 Pubblicazione dei certificati .....	16
3.5 Verifica di conformità.....	17
3.6 Tutela dei dati personali.....	17
3.7 Tariffe .....	17
3.7.1 Rilascio, rinnovo, revoca e sospensione del certificato .....	17
3.7.2 Accesso al certificato e alle liste di revoca .....	17
<b>4. Identificazione .....</b>	<b>18</b>
4.1 Registrazione iniziale.....	18
4.2 Rinnovo delle chiavi e certificati .....	18
4.3 Richiesta di Revoca o di Sospensione.....	18
4.3.1 Richiesta da parte del Titolare .....	18
<b>5. Operatività.....</b>	<b>19</b>
5.1 Registrazione dei Richiedenti la certificazione.....	19

5.1.1	Procedura di Registrazione .....	19
5.1.2	Informazioni che il Richiedente deve fornire .....	20
5.2	Richiesta del certificato .....	20
5.2.1	Caso A: Chiavi generate in presenza del Richiedente .....	20
5.2.2	Caso B: Chiavi generate dal Certificatore .....	20
5.2.3	Generazione delle chiavi .....	21
5.2.4	Protezione delle chiavi private .....	21
5.3	Emissione del certificato .....	21
5.3.1	Formato e contenuto del certificato .....	21
5.3.2	Pubblicazione del certificato .....	21
5.3.3	Validità del certificato .....	21
5.4	Revoca e sospensione di un certificato .....	22
5.4.1	Motivi per la revoca di un certificato .....	22
5.4.2	Procedura per la richiesta di revoca .....	22
5.4.3	Procedura per la revoca immediata .....	23
5.4.4	Motivi per la Sospensione di un certificato .....	23
5.4.5	Procedura per la richiesta di Sospensione .....	23
5.4.6	Ripristino di validità di un Certificato sospeso .....	24
5.4.7	Pubblicazione e frequenza di emissione della CRL .....	24
5.4.8	Tempistica .....	24
5.5	Sostituzione delle chiavi e rinnovo del Certificato .....	25
5.6	Servizio di Marcatura Temporale .....	25
5.6.1	Richiesta di emissione o di verifica di marca temporale .....	25
5.6.2	Emissione o verifica di marca temporale .....	26
5.6.3	Gestione della coppia di chiavi asimmetriche della TSA .....	27
5.6.4	Marca Temporale .....	28
5.6.5	Registrazione delle marche generate .....	29
5.6.6	Sicurezza del sistema di validazione temporale .....	29
5.6.7	Protezione dei documenti informatici .....	29
5.7	Controllo del sistema di certificazione .....	30
5.7.1	Strumenti automatici per il controllo di sistema .....	30
5.7.2	Verifiche di sicurezza e qualità .....	30
5.8	Dati archiviati .....	30
5.8.1	Procedure di salvataggio dei dati .....	31
5.9	Sostituzione delle chiavi del Certificatore .....	31
5.10	Cessazione del servizio .....	31
5.11	Sistema di qualità .....	31
5.12	Disponibilità del servizio .....	32
<b>6.</b>	<b>Misure di Sicurezza .....</b>	<b>33</b>
6.1	Guasto al dispositivo di firma del Certificatore .....	33
6.2	Compromissione della chiave di certificazione .....	33
6.3	Procedure di Gestione dei Disastri .....	33
<b>7.</b>	<b>Amministrazione del Manuale Operativo .....</b>	<b>34</b>
7.1	Procedure per l'aggiornamento .....	34
7.2	Regole per la pubblicazione e la notifica .....	34
7.3	Responsabile dell'approvazione .....	34
7.4	Conformità .....	34
<b>Appendice A: Descrizione delle misure di sicurezza .....</b>		<b>35</b>
A.1	Sicurezza fisica .....	35

---

A.2	Sicurezza delle procedure .....	35
A.3	Sicurezza logica .....	35

## 1. Introduzione al documento

Novità introdotte rispetto alla precedente emissione

<b>Versione/Release n° :</b>	2.1a	<b>Data Versione/Release:</b>	10/07/2000
<b>Descrizione modifiche:</b>	Revisione del documento per la prima emissione in produzione – Modifica nome del sito web del Certificatore e riferimento circolare AIPA del 19 giugno 2000.		
<b>Motivazioni:</b>	Rilascio del servizio		

<b>Versione/Release n°:</b>	2.2	<b>Data Versione/Release:</b>	5/4/2001
<b>Descrizione modifiche:</b>	<p>E' prevista una nuova modalità di distribuzione dei dispositivi di firma, con generazione delle chiavi da parte del Certificatore (§ 5.1, 5.1.1, 5.2, 5.2.1, 5.2.2, 5.2.3, 5.3).</p> <p>Sono accettati come documenti di riconoscimento anche quelli equipollenti alla carta d'identità, secondo quanto stabilito dal Testo Unico (§ 4.1).</p> <p>Sono stati aggiornati i massimali dell'assicurazione (§ 3.2.1).</p> <p>I riferimenti al DPR 513/97 sono stati sostituiti con quelli al DPR 445/2000, Testo Unico delle Disposizioni Legislative e Regolamentari in materia di Documentazione Amministrativa.</p> <p>Sono stati modificati la durata del certificato e le relative tariffe (§ 3.7.1 e 5.3.3).</p>		
<b>Motivazioni:</b>	Revisione procedura di riconoscimento e di rilascio dei dispositivi di firma, modifica della durata di validità dei certificati.		

<b>Versione/Release n°:</b>	2.3	<b>Data Versione/Release:</b>	7/9/2001
<b>Descrizione modifiche:</b>	<p>E' stato aggiornato il nome del Rappresentante legale dell'organizzazione (§ 2.2.1).</p> <p>La sostituzione delle chiavi del certificatore è stata anticipata a due anni prima della scadenza della chiave di certificazione corrente; è stata modificata la durata dei certificati di cross-certification a due anni (§ 5.8).</p>		
<b>Motivazioni:</b>	Aggiornamento dati riguardanti l'organizzazione InfoCamere S.C.p.A, modifica tempi di sostituzione delle chiavi del certificatore e durata dei certificati di cross-certification generati in fase di sostituzione medesima.		

<b>Versione/Release n°:</b>	2.4	<b>Data Versione/Release:</b>	27/9/2002
<b>Descrizione modifiche:</b>	Vengono indicate le procedure per la validazione temporale di documenti elettronici e le modalità di conservazione delle marche temporali associate al relativo documento informatico.		
<b>Motivazioni:</b>	Fornitura del Servizio di validazione temporale		

## 1.1 Scopo e campo di applicazione del documento

Il documento ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCamere per l'emissione dei certificati per chiavi di sottoscrizione, nonché le procedure per la fornitura del servizio di validazione temporale su richiesta degli utenti, in conformità con la vigente normativa in materia di firma digitale.

Le indicazioni di questo documento hanno validità per le attività relative ad InfoCamere nel ruolo di Certificatore, per gli Uffici di Registrazione, i Titolari e per gli Utenti.

Il contenuto si basa sulle regole tecniche contenute nell'*Allegato Tecnico* del Decreto del Presidente del Consiglio dei Ministri dell'8 Febbraio 1999 e recepisce le raccomandazioni del documento "*Request for Comments: 2527 – Certificate Policy and certification practices framework*" © Internet Society 1999.

Il contenuto del presente Manuale Operativo è Copyright © 2000, 2001, 2002 di InfoCamere S.C.p.A.

## 1.2 Riferimenti

- [1] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001)
- [2] Decreto del Presidente del Consiglio dei Ministri 8 Febbraio 1999 (G. U. n. 87 del 15/4/1999)
- [3] Circolare AIPA/CR/22 del 26 Luglio 1999
- [4] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8
- [5] RFC 2459 (1999): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"
- [6] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
- [7] RFC 3161 (2001): "Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
- [8] Deliverable ETSI TS 102 023 "*Policy requirements for time-stamping authorities*" - - Aprile 2002
- [9] Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 (c.d. "Misure Minime di Sicurezza")
- [10] Circolare AIPA/CR/24 del 19 giugno 2000 (Linee Guida per l'interoperabilità dei Certificatori)

## 1.3 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal TU [1] e dal DPCM 8 febbraio 1999 [2] si rimanda alle definizioni stabilite dai decreti relativi. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

### **Accordi di Certificazione [Cross-certification]**

La *cross-certification* si esercita tra Certification Authority che appartengono a domini diversi. In questo processo i Certificatori si certificano l'un l'altro. Condizione necessaria affinché possa

avvenire la *cross-certification* è che essi accettino e condividano regole equivalenti nel Manuale Operativo.

**Autorità per la marcatura temporale [Time-stamping authority]**

Il sistema software/hardware, gestito dal Certificatore, che eroga il servizio di marcatura temporale

**Certificato, Certificato Digitale, Certificato X.509 [Digital Certificate]**

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.

Nel certificato compaiono altre informazioni tra cui:

- il Certificatore che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- altri campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

**Certificatore [Certification Authority] – cfr. TU [1]****Chiave Privata e Chiave Pubblica – cfr. TU [1]****Dispositivo di firma – cfr. DPCM [2]**

Il dispositivo di firma utilizzato dall'utente è costituito da una carta plastica delle dimensioni di una carta di credito in cui è inserito un microprocessore. E' chiamato anche **carta a microprocessore** o **smart card**.

**Evidenza informatica**

Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

**Firma digitale [digital signature] – cfr. TU [1]****Giornale di controllo**

Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dal Regolamento tecnico.

**Lista dei Certificati Revocati o Sospesi [Certificate Revocation List]**

E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza. L'operazione è chiamata revoca se definitiva, sospensione se temporanea.

Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene quindi pubblicata nel registro dei certificati.

**Marca temporale [Time Stamp Token] – cfr. DPCM [2]****Manuale Operativo – cfr. art. 45 DPCM [2]**

Il Manuale Operativo definisce le procedure che il Certificatore applica nello svolgimento del servizio. Nella stesura del Manuale sono state seguite le indicazioni espresse da AIPA [3] [10] e quelle della letteratura internazionale [4] [5] [6].

**Registro dei Certificati [Directory] – cfr. art. 43 DPCM [2]**

Il Registro dei Certificati è un archivio pubblico che contiene:

- tutti i certificati validi emessi dal Certificatore;
- la lista dei certificati revocati e sospesi (CRL).

**Revoca o sospensione di un Certificato**

È l'operazione con cui il Certificatore annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.

**Richiedente**

Il Richiedente è la persona fisica che richiede al Certificatore, tramite l'Ufficio di Registrazione, la certificazione di una chiave pubblica.

**Tempo Universale Coordinato [Coordinated Universal Time]**

Scala dei tempi con precisione del secondo come definito in ITU-R Recommendation TF.460-5

**Titolare – cfr. DPCM [2]**

I Titolari sono persone fisiche che hanno ottenuto dal Certificatore la certificazione di una chiave pubblica.

**Uffici di Registrazione [Registration Authority]**

Il rilascio di un certificato ad un titolare segue una procedura iniziale di registrazione, durante la quale viene eseguita:

- l'identificazione fisica degli utenti (basata su carta d'identità o documenti equipollenti secondo l'articolo 35, comma 2 TU [1]).
- la verifica della completezza dei dati e della documentazione che l'utente deve fornire in fase di registrazione per il rilascio di un certificato;

L'Ufficio di Registrazione è l'entità che per conto del Certificatore esegue le operazioni preliminari di identificazione e raccolta dei dati relativi ai Richiedenti i certificati.

**Utente**

Gli utenti dei Certificati sono soggetti pubblici e privati che accettano il Manuale Operativo del Certificatore cui un certificato fa riferimento, e quindi verificano nelle modalità previste dal Certificatore la validità della firma generata. Accedono al Registro dei Certificati del Certificatore per richiedere e verificare l'esistenza del certificato, la validità e, controllando la CRL, l'eventuale revoca o sospensione.

## 1.4 Acronimi e abbreviazioni

**AIPA – Autorità per l'Informatica nella Pubblica Amministrazione**

**CRL – Certificate Revocation List**

**DN – Distinguished Name**

Identificativo del Titolare di un certificato di chiave pubblica; tale codice è unico nell'ambito dei Titolari che abbiano un certificato emesso dal Certificatore.

**DPCM - Decreto del Presidente del Consiglio dei Ministri**

Ci si riferisce al DPCM 8 febbraio 1999, Rif. [2], e in senso più generale alle Regole Tecniche che ne costituiscono l'Allegato Tecnico.

**DTS - Digital Time Stamping**

Sistema per la marcatura temporale di certificati e documenti.

**ETSI - European Telecommunications Standards Institute**

**IETF - Internet Engineering Task Force**

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

**ISO - International Organization for Standardization**

Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

**ITU - International Telecommunication Union**

Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

**IUT – Identificativo Univoco del Titolare**

E' un codice associato al Titolare che lo identifica univocamente presso il Certificatore; il Titolare ha codici diversi per ogni certificato in suo possesso.

**LDAP – Lightweight Directory Access Protocol**

Protocollo utilizzato per accedere al registro dei certificati.

**OID – Object Identifier**

E' costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

**PIN – Personal Identification Number**

Codice associato ad un dispositivo di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.

**RRC – Revocation Request Code**

Codice preimbustato consegnato dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di revoca o sospensione di un certificato.

**TSA – Time Stamping Authority****TST – Time-Stamp token****TU – Testo Unico**

Ci si riferisce al DPR n. 445/2000, Rif. [1], *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*, che contiene la disciplina della firma digitale e abroga il precedente DPR n. 513/97.

**UID – Identificativo Univoco del Dispositivo di firma**

E' il codice identificativo univoco associato al dispositivo di firma al momento della sua personalizzazione.

## 2. Generalità

Un certificato lega la chiave pubblica ad un insieme d'informazioni che identificano il soggetto che possiede la corrispondente chiave privata: tale soggetto è il "Titolare" del certificato. Il certificato è usato da altri soggetti per reperire la chiave pubblica, distribuita con il certificato, e verificare la firma digitale di un documento.

Il certificato garantisce la corrispondenza tra la chiave pubblica ed il Titolare del certificato. Il grado d'affidabilità di quest'associazione è legato a diversi fattori: la modalità con cui il certificatore ha emesso il certificato, le misure di sicurezza adottate, gli obblighi assunti dal Titolare per la protezione della propria chiave privata, le garanzie offerte dal Certificatore.

Questo documento evidenzia le regole generali e le procedure seguite dal Certificatore InfoCamere per l'emissione e l'utilizzo dei certificati.

La descrizione delle pratiche seguite dal Certificatore nell'emissione del certificato, delle misure di sicurezza adottate, degli obblighi, delle garanzie e delle responsabilità, ed in generale di tutto ciò che rende affidabile un certificato, viene riportato nel presente Manuale Operativo.

Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nei certificati, il Certificatore consente agli utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione e quindi del legame chiave-Titolare.

### 2.1 Identificazione del documento

Questo documento è denominato "Ente Certificatore InfoCamere – Manuale Operativo" ed è caratterizzato dal codice documento: **ICCA-MO**.

La versione e il livello di rilascio sono identificabili in calce ad ogni pagina.

L'*object identifier* (OID) di questo documento è il seguente: 1.3.76.14.1.1.1

Tale OID identifica:

InfoCamere	1.3.76.14
certification-service-provider	1.3.76.14.1
certificate-policy	1.3.76.14.1.1
manuale-operativo-firma-digitale	1.3.76.14.1.1.1

Questo documento è pubblicato in formato elettronico presso il sito Web del Certificatore all'indirizzo: <http://www.card.infocamere.it/doc/manuali.htm>

### 2.2 Attori e Domini applicativi

#### 2.2.1 Certificatore

InfoCamere S.C.p.A. è il **Certificatore** che emette, pubblica nel registro e revoca i certificati, operando in conformità alle Regole Tecniche [2] e secondo quanto prescritto per l'iscrizione all'elenco dei Certificatori AIPA. In questo documento si usa il termine Certificatore per indicare InfoCamere.

I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Tabella 2-1

Denominazione Sociale	<b>InfoCamere - Società Consortile d'Informatica delle Camere di Commercio Italiane per azioni</b>
Sede legale	<b>Piazza Sallustio, 21 – 00187 Roma</b>
Rappresentante legale	<b>Dott. Giuseppe Pichetto</b> In qualità di Presidente del Consiglio d'Amministrazione
Direzione Generale	<b>Via G.B. Morgagni, 30H – 00161 Roma</b>
N° telefono	<b>06-442851</b>
N° fax	<b>06-44285255</b>
N° Iscrizione Registro Imprese	<b>Codice Fiscale 02313821007 (già Trib. di Roma 1 / 95)</b>
N° partita IVA	<b>02313821007</b>
Sito web	<a href="http://www.card.infocamere.it/">Http://www.card.infocamere.it/</a>
Nome X.500:	<b>CN=InfoCamere Firma Digitale, OU=Certification Service Provider, OU= Ente Certificatore del Sistema Camerale, O=InfoCamere SCpA, C=IT</b>
Sede Operativa	<b>Corso Stati Uniti, 14 – 35127 Padova</b>

### 2.2.2 Uffici di Registrazione

Il Certificatore si avvale sul territorio di Uffici di Registrazione, per svolgere principalmente le funzioni di:

- identificazione e registrazione dei Richiedenti,
- validazione della richiesta del certificato,
- distribuzione ed inizializzazione del dispositivo di firma,
- attivazione della procedura di certificazione della chiave pubblica del Richiedente,
- supporto al Titolare e al Certificatore nel rinnovo/revoca/sospensione dei certificati.

L'Ufficio di Registrazione, anche tramite suoi incaricati, svolge in sostanza tutte le attività di interfaccia tra il Certificatore ed il Richiedente la certificazione.

Gli Uffici di Registrazione sono attivati dal Certificatore a seguito di un adeguato addestramento del personale impiegato, che potrà svolgere le funzioni previste anche presso il Richiedente.

Il Certificatore verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo Manuale.

### 2.2.3 Registro dei Certificati

Tutti i certificati emessi dal Certificatore sono pubblicati nel registro dei certificati come pure le liste di revoca e di sospensione dei certificati.

### 2.2.4 Applicabilità

L'utilizzo dei certificati di sottoscrizione emessi dal Certificatore è il seguente:

- il certificato emesso dal Certificatore sarà usato per verificare la firma del Titolare cui il certificato appartiene. Prerequisito è l'utilizzo di applicativi per la verifica della firma rilasciati dal Certificatore o che siano certificati ITSEC E2 e supportino gli stessi algoritmi di hashing e crittografia del Certificatore, nonché i medesimi formati standard di busta crittografica e sistemi di codifica.
- in presenza di accordi di certificazione, il Certificatore riconosce la validità delle regole del certificatore con cui stipula l'accordo e viceversa. Pertanto il certificato emesso per l'altro

certificatore sarà usato unicamente per verificare la firma di tale certificatore sui certificati da questi emessi.

### **2.3 Contatto per utenti finali**

InfoCamere è responsabile della definizione, pubblicazione ed aggiornamento di questo documento. La persona da contattare per questioni riguardanti questo documento ed il servizio descritto è:

InfoCamere S.C.p.A.  
Responsabile U.O. Firma Digitale  
Corso Stati Uniti 14  
35127 Padova

Telefono: 049 828 8111  
Fax : 049 828 8406

Call Center Firma Digitale: 06 4428 5555  
Web: <http://www.card.infocamere.it>  
e-mail: [firma.digitale@infocamere.it](mailto:firma.digitale@infocamere.it)

### **2.4 Rapporti con l'AIPA**

Il presente Manuale Operativo, compilato dal Certificatore nel rispetto delle indicazioni legislative, è stato consegnato, in copia, all'Autorità per l'Informatica nella Pubblica Amministrazione (AIPA) che lo approva e lo rende disponibile pubblicamente.

Allo scadere di un anno dalla precedente richiesta o comunicazione il Certificatore conferma all'AIPA per iscritto la permanenza dei requisiti per l'esercizio dell'attività di certificazione.

Al momento della richiesta d'iscrizione, il Certificatore fornisce all'AIPA i dati identificativi richiesti (vedi §. 3.4.1), che vengono sottoscritti, conservati e pubblicati dall'AIPA.

Il Certificatore si impegna a comunicare all'AIPA la data di cessazione della propria attività di certificazione con un anticipo di almeno sei mesi e ad informare i possessori dei certificati da questo emessi della revoca dei certificati al momento della cessazione dell'attività.

Allo scadere del periodo di validità delle proprie chiavi di certificazione, il Certificatore avvierà la procedura di sostituzione e fornirà all'AIPA i certificati con firme incrociate previsti dalla procedura di rinnovo, attraverso il canale sicuro da essa predisposto.

### **3. Regole Generali**

In questo capitolo si descrivono le condizioni generali con cui il Certificatore eroga il servizio di certificazione descritto in questo manuale.

#### **3.1 Obblighi e Responsabilità**

##### **3.1.1 Obblighi del Certificatore**

Il Certificatore è tenuto a garantire che (cfr. art. 28 del TU [1]):

1. siano soddisfatte le regole tecniche specificate nel DPCM [2];
2. il Sistema Qualità sia conforme alle norme ISO9001;
3. la richiesta di certificazione sia autentica;
4. la chiave pubblica di cui si richiede la certificazione non sia già stata certificata, per un altro soggetto Titolare, nell'ambito del proprio dominio. Per la verifica nel dominio degli altri certificatori, il Certificatore si impegna a stabilire accordi con gli altri certificatori presenti nell'Albo AIPA, in base alle attuali conoscenze tecnologiche, per l'attivazione di tali controlli;
5. il certificato sia rilasciabile e accessibile per via telematica;
6. i richiedenti siano informati in modo compiuto e chiaro sulla procedura di certificazione e sui necessari requisiti tecnici per accedervi;
7. il proprio sistema di sicurezza dei dati sia rispondente alle misure minime di sicurezza per il trattamento dei dati personali, secondo il DPR 318/99 [9];
8. il certificato sia revocato tempestivamente in caso di richiesta da parte del Titolare, di provvedimento dell'autorità, d'acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti, di abusi o falsificazioni;
9. sia certa l'associazione tra chiave pubblica e Titolare;
10. il codice identificativo assegnato a ciascun Titolare sia univoco nell'ambito dei propri utenti;
11. non si rende depositario di chiavi private;
12. le proprie chiavi private siano accuratamente protette mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
13. siano conservate per almeno 10 anni le informazioni ottenute in fase di registrazione, di richiesta di certificazione, di revoca e di rinnovo;
14. siano custodite per 10 anni in forma accessibile i certificati delle proprie chiavi pubbliche di certificazione.

##### **3.1.2 Obblighi dell'Ufficio di Registrazione**

L'Ufficio di Registrazione è tenuto a garantire:

1. che il Richiedente la certificazione sia espressamente informato riguardo agli obblighi da quest'ultimo assunti in merito alla protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi di firma;
2. che il Richiedente sia informato in merito agli accordi di certificazione stipulati con altri certificatori;
3. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, DPR 318/99 [9];
4. la verifica d'identità del Richiedente il certificato e la registrazione dei dati dello stesso, secondo le procedure di registrazione di cui ai paragrafi 4.1 e 5.1 del presente Manuale Operativo;
5. la custodia con la massima diligenza delle proprie chiavi private e dei dispositivi di firma che le contengono, ai fini di preservarne la riservatezza e l'integrità;
6. la comunicazione al Certificatore di tutti i dati e documenti acquisiti durante la registrazione del Richiedente allo scopo di attivare la procedura di emissione del certificato;
7. la verifica e inoltro al Certificatore delle richieste di revoca o di sospensione attivate dal Titolare presso l'Ufficio di Registrazione;

8. l'esecuzione, ove prevista a suo carico dal presente Manuale Operativo, della revoca o sospensione dei certificati.

L'Ufficio di Registrazione terrà direttamente i rapporti con il Richiedente/Titolare ed è tenuto ad informarlo circa le disposizioni contenute nel presente Manuale Operativo.

### **3.1.3 Obblighi dei Titolari**

Il Titolare deve garantire:

1. la correttezza e la completezza delle informazioni fornite all'Ufficio di Registrazione e al Certificatore per la richiesta di certificato;
2. la protezione e la conservazione delle proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
3. l'utilizzo del certificato per le sole modalità previste nel Manuale Operativo e dalle vigenti leggi nazionali e internazionali;
4. la richiesta di revoca o di sospensione dei certificati in suo possesso nei casi previsti dal presente Manuale Operativo ai paragrafi 5.4.1 e 5.4.4;
5. la protezione e conservazione del codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità del dispositivo di firma in luogo sicuro e diverso da quello in cui è custodito il dispositivo contenente la chiave;
6. la protezione e conservazione del codice di autenticazione (RRC) per richiedere la revoca o sospensione del proprio certificato;
7. l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

### **3.1.4 Obblighi degli Utenti**

L'utente che utilizza un certificato del quale non è il Titolare, ha i seguenti obblighi:

1. verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta. Deve verificare con particolare attenzione il periodo di validità e che il certificato non risulti sospeso o revocato controllando le relative liste nel registro dei certificati;
2. conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel Manuale Operativo del Certificatore stesso;
3. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

Se viene accertato che l'utilizzatore del certificato ha agito in maniera contraria a tali obblighi, non potrà avanzare pretese in caso di contenzioso.

## **3.2 Limitazioni e indennizzi**

### **3.2.1 Limitazioni della garanzia e limitazioni degli 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

Il Certificatore ha stipulato un contratto assicurativo per la copertura dei rischi dell'attività e dei danni causati a terzi, il cui testo è stato trattato ed accettato dall'AIPA, che ha come massimali:

- 1.549.369 euro per singolo sinistro
- 1.549.369 euro per annualità.

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

Il Certificatore si assume ogni responsabilità assegnata dal TU [1] ai soggetti che svolgono funzione di Certificatore ivi compresa l'identificazione della persona che fa richiesta di certificazione.

### **3.3 Riferimenti alle leggi vigenti**

#### **3.3.1 Leggi applicabili**

Il presente Manuale Operativo fa riferimento alla vigente legislazione. In particolare vengono recepite ed attuate le norme sancite in:

- Legge del 15 marzo 1997, n.59 (c. d. legge Bassanini)
- Legge del 23 dicembre 1993, n. 547
- Decreto del Presidente della Repubblica del 28 dicembre 2000, n. 445
- Decreto del Presidente del Consiglio dei Ministri del 8 febbraio 1999
- Legge del 24 dicembre 1993, n. 537
- Legge del 31 dicembre 1996, n. 675
- Decreto del Presidente della repubblica 28 luglio 1999, n. 318

#### **3.3.2 Clausola risolutiva espressa**

Il Certificatore avrà la facoltà di risolvere in ogni momento il rapporto contrattuale, ai sensi dell'articolo 1456 del codice civile, al verificarsi del mancato rispetto della controparte degli obblighi previsti a suo carico.

#### **3.3.3 Comunicazioni**

Domande, osservazioni e richieste di chiarimento sulle disposizioni di carattere legale e contrattuale di questo Manuale Operativo dovranno essere indirizzate al contatto per gli utenti finali presentato nel precedente paragrafo 2.3

### **3.4 Pubblicazione**

#### **3.4.1 Pubblicazione di informazioni relative al Certificatore**

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web del Certificatore (cfr. § 2.1)
- in formato cartaceo, richiedibile sia al Certificatore sia al proprio Ufficio di Registrazione.

Il presente Manuale Operativo, la lista dei certificati delle chiavi di certificazione e le altre informazioni relative al Certificatore previste dal DPCM [2] sono pubblicate presso l'elenco AIPA dei certificatori.

#### **3.4.2 Pubblicazione dei certificati**

I certificati e le liste di revoca e di sospensione sono pubblicati nel registro dei certificati accessibile con protocollo LDAP all'indirizzo: <ldap://ldap.infocamere.it>

Il Certificatore potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

### **3.5 Verifica di conformità**

Con frequenza non superiore all'anno, il Certificatore esegue un controllo di conformità di questo Manuale Operativo al proprio processo di erogazione del servizio di certificazione.

### **3.6 Tutela dei dati personali**

Le informazioni relative al titolare di cui il Certificatore viene in possesso nell'esercizio delle sue tipiche attività, sono da considerarsi riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (chiave pubblica, certificato) e le date di revoca e di sospensione del certificato.

In particolare i dati personali vengono trattati dal Certificatore in conformità con la legge 675/96 e del regolamento contenente le misure minime di sicurezza per la loro protezione, DPR 318/99 [9].

### **3.7 Tariffe**

#### **3.7.1 Rilascio, rinnovo, revoca e sospensione del certificato**

Le tariffe per la prima emissione, per il rinnovo, revoca e sospensione dei certificati sono le seguenti:

- Prima emissione: euro 7,75
- Rinnovo: euro 5,16
- Revoca e/o Sospensione: gratuita

Tali tariffe sono comunque funzione delle quantità trattate e soggette all'andamento del mercato.

Le tariffe indicate non comprendono il servizio di registrazione e il costo del dispositivo di firma (smart card).

#### **3.7.2 Accesso al certificato e alle liste di revoca**

L'accesso al registro dei certificati pubblicati e alla lista dei certificati revocati o sospesi è libero e gratuito.

## **4. Identificazione**

Questo capitolo descrive le procedure usate dal Certificatore per l'identificazione dei Richiedenti/Titolari in relazione al rilascio, rinnovo, revoca e sospensione del certificato.

### **4.1 Registrazione iniziale**

Il Certificatore deve verificare con certezza l'identità del Richiedente la certificazione al momento della sua registrazione.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente da un incaricato del Certificatore, che ne verificherà l'identità attraverso il controllo della carta d'identità o di un documento ad essa equipollente (cfr. art. 35 comma 2 del TU [1]) in corso di validità.

Al momento della registrazione viene fornito al Richiedente un codice segreto di revoca (RRC), che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e Titolare (cfr. art. 25 DPCM [2]).

Sulla base delle dichiarazioni del Richiedente, verrà generato il certificato digitale in formato conforme a quanto previsto nelle Linee Guida per l'interoperabilità [10].

### **4.2 Rinnovo delle chiavi e certificati**

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "validità" (*validity*) con gli attributi "valido dal" (*not before*) e "valido fino al" (*not after*).

Al di fuori di questo intervallo di date il certificato è da considerarsi non valido.

Il Titolare che intende rinnovare il suo certificato digitale deve richiedere l'emissione di un nuovo certificato prima della scadenza di quello in suo possesso.

Oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere ad una nuova registrazione. La nuova generazione delle chiavi è a carico del Titolare, che può far riferimento alla documentazione fornita dall'Ufficio di Registrazione.

Il certificato scaduto resterà archiviato per la durata di 10 anni.

Le chiavi private di firma di cui sia scaduto il certificato della relativa chiave pubblica, non possono essere più utilizzate.

L'identificazione del Titolare da parte del Certificatore avviene attraverso la verifica della firma digitale che l'utente ha apposto sulla richiesta di rinnovo.

### **4.3 Richiesta di Revoca o di Sospensione**

La revoca o sospensione del certificato può avvenire su richiesta del Titolare, ovvero su iniziativa del Certificatore.

Il Certificatore, anche tramite l'Ufficio di Registrazione, si accerta dell'identità del richiedente e delle motivazioni della richiesta di revoca o di sospensione.

#### **4.3.1 Richiesta da parte del Titolare**

Se la richiesta viene effettuata per telefono o via Internet, il Titolare deve fornire il codice di revoca segreto (RRC), consegnato assieme al certificato che intende revocare.

Se la richiesta viene fatta presso l'Ufficio di Registrazione, le modalità di riconoscimento del Titolare sono analoghe a quelle usate in fase di registrazione.

## 5. Operatività

I passi principali che i Richiedenti devono fare per ottenere un certificato di sottoscrizione sono:

- a) rispettare le procedure di identificazione in accordo con quanto specificato nel capitolo 4;
- b) fornire all'Ufficio di Registrazione tutte le informazioni personali necessarie alla identificazione e registrazione corredate, ove richiesto, da idonea documentazione, che verranno inserite nel certificato;
- c) sottoscrivere, dopo presa visione, il contratto di adesione al servizio del Certificatore.

Conclusasi la fase di identificazione/registrazione del Richiedente il certificato, sono previste due diverse modalità per la consegna delle smart card e il rilascio dei certificati digitali.

La prima modalità (nel seguito **Caso A**) consente al Richiedente di concludere la procedura di certificazione entrando in possesso della smart card e del certificato di sottoscrizione immediatamente dopo la registrazione: in questo caso l'incaricato del certificatore avvierà la procedura di generazione della coppia di chiavi e, effettuate le opportune verifiche, di emissione del certificato, in presenza del Richiedente/Titolare che provvederà a personalizzare il dispositivo di firma tramite l'impostazione di un PIN segreto.

La seconda modalità (nel seguito **Caso B**) prevede una separazione tra la fase di registrazione, effettuata con il Richiedente, e quella di richiesta ed emissione del certificato, che viene effettuata da incaricati del Certificatore. In questo secondo caso la smart card viene personalizzata a cura del Certificatore e consegnata al Richiedente (ora Titolare) in un secondo momento.

Il dettaglio delle operazioni previste per le due modalità è illustrato qui di seguito.

### 5.1 Registrazione del Richiedenti la certificazione

#### 5.1.1 Procedura di Registrazione

Per assegnare un certificato ad un Richiedente è necessario eseguire una procedura di registrazione durante la quale ne viene accertata l'identità (autenticazione) e verificata la completezza delle informazioni che egli fornisce.

1. La registrazione è effettuata da un Incaricato alla Registrazione ed è richiesta la presenza fisica del soggetto richiedente il certificato.
2. L'incaricato verifica l'identità del Richiedente tramite la sua carta d'identità o altri documenti di riconoscimento equipollenti (cfr. § 4.1.).
3. L'incaricato registra i dati del Richiedente e li associa ad un codice personale;
4. Il Richiedente prende visione del contratto e firma la richiesta di registrazione e certificazione completa dei dati ivi riportati;
5. Si distinguono i due casi:
  - (**Caso A**): al Richiedente viene consegnato il dispositivo di firma, il codice di attivazione di default ad esso associato (PIN), l'identificativo univoco del titolare (IUT) e la busta contenente il codice segreto per la revoca del certificato (RRC). Sarà cura del Richiedente (ora Titolare) cambiare il PIN iniziale con uno a sua scelta.
  - (**Caso B**): al Richiedente viene consegnato solo la busta contenente il codice segreto per la revoca del certificato (RRC) e il PIN iniziale personalizzato.

Conclusa la fase di Registrazione avviene la richiesta di certificazione della chiave personale di firma.

### **5.1.2 Informazioni che il Richiedente deve fornire**

Nella richiesta di registrazione del Richiedente sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra il Certificatore e l'utente stesso. Il modulo della richiesta deve essere sottoscritto e firmato dal Richiedente.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso.
- Modalità di invio delle comunicazioni dal Certificatore al Richiedente/Titolare

## **5.2 Richiesta del certificato**

La richiesta del certificato può avvenire secondo le modalità anticipate al punto 5.1.

### **5.2.1 Caso A: Chiavi generate in presenza del Richiedente**

Questa procedura prevede la presenza del Richiedente in possesso della carta a microprocessore presso un Ufficio di Registrazione.

1. L'incaricato attiva la procedura di richiesta di certificato
2. L'utente sblocca il dispositivo di firma, usando il PIN di default, consentendo così la generazione della coppia di chiavi crittografiche
3. L'incaricato, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica del Richiedente e la invia al Certificatore.
4. Completata la procedura di certificazione, il Richiedente (ora Titolare) modifica il PIN del dispositivo di firma con uno a sua scelta.

### **5.2.2 Caso B: Chiavi generate dal Certificatore**

Questa procedura viene effettuata da incaricati del Certificatore, presso i locali del Certificatore o presso gli Uffici di Registrazione.

1. L'incaricato seleziona i dati di registrazione di un Richiedente e attiva la procedura di richiesta di certificato
2. La procedura automatica sblocca il dispositivo di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia
3. L'incaricato, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica del Richiedente e la invia al Certificatore.
4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo di firma inserendo il PIN già assegnato all'utente in fase di registrazione.

La segretezza del PIN personale durante le fasi di personalizzazione della smart card (dispositivo di firma) è garantita da adeguati sistemi di cifratura. Tale codice PIN, generato in modo casuale, è conservato in modo protetto all'interno dei sistemi del Certificatore, e viene comunicato secondo procedure sicure (procedure automatiche con imbustamento in busta chiusa) al solo Titolare (cfr. § 5.1.1, punto 6 caso B). La smart card così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.

### **5.2.3 Generazione delle chiavi**

Le chiavi asimmetriche sono generate all'interno della carta a microprocessore utilizzando le funzionalità offerte dalla smart card stessa. La lunghezza delle chiavi è di 1024 bit.

### **5.2.4 Protezione delle chiavi private**

La chiave privata del Titolare è generata e memorizzata in un'area protetta della carta a microprocessore che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.

## **5.3 Emissione del certificato**

L'emissione del certificato viene effettuata in modo automatico dalle procedure del Certificatore secondo i seguenti passi:

- 1) viene verificata la correttezza della richiesta di certificato controllando che:
  - il Richiedente sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
  - al Richiedente sia assegnato un codice identificativo unico nell'ambito degli utenti del Certificatore (IUT);
  - la chiave pubblica che si intende certificare sia una chiave valida, della lunghezza prevista e non sia già stata certificata per un altro soggetto titolare;
  - la richiesta sia autentica e il richiedente possieda la corrispondente chiave privata;
- 2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta
- 3) si procede alla generazione del certificato
- 4) il certificato viene pubblicato nel registro dei certificati, assieme alla marca temporale che attesta il momento della pubblicazione
- 5) il certificato emesso e la relativa marca temporale vengono inviati al Titolare; il certificato viene memorizzato all'interno del dispositivo di firma del Titolare
- 6) si distinguono i due casi:
  - (*Caso A*): il Titolare è già in possesso del dispositivo di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di sottoscrizione.
  - (*Caso B*): il dispositivo di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di Registrazione personalmente al Titolare.

### **5.3.1 Formato e contenuto del certificato**

Il certificato viene generato con le informazioni fornite dal titolare ed indicate nella richiesta di registrazione.

Il formato del certificato prodotto è conforme a quanto specificato nelle Linee Guida per l'Interoperabilità dei Certificatori [10]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.

### **5.3.2 Pubblicazione del certificato**

Al buon esito della procedura di registrazione il certificato viene rilasciato e pubblicato secondo quanto specificato al punto 3.4.2..

### **5.3.3 Validità del certificato**

Il periodo di validità del certificato si estende per due anni a partire dalla data d'emissione.

## **5.4 Revoca e sospensione di un certificato**

La revoca o la sospensione di un certificato ne tolgono la validità prima della scadenza stabilita e rendono **non valide** le firme apposte successivamente al momento della pubblicazione della revoca o sospensione.

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore, emessa e pubblicata nel registro dei certificati con periodicità prestabilita.

Il Certificatore può forzare un'emissione non programmata della CRL in circostanze particolari.

L'efficacia della revoca e della sospensione si ha dal momento di pubblicazione della lista, attestato con marca temporale.

### **5.4.1 Motivi per la revoca di un certificato**

Il Certificatore esegue la revoca del certificato su propria iniziativa o su richiesta del Titolare. Le condizioni per cui deve essere effettuata la richiesta di revoca sono le seguenti:

1. la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
  - sia stato smarrito il dispositivo di firma che contiene la chiave;
  - sia venuta meno la segretezza della chiave o del suo codice d'attivazione (PIN);
  - si sia verificato un qualunque evento che abbia compromesso il livello d'affidabilità della chiave;
2. il Titolare non riesce più ad utilizzare il dispositivo di firma in suo possesso (perdita del PIN, guasto del dispositivo, ecc.);
3. si verifica un cambiamento dei dati del Titolare presenti nel certificato tale da rendere detti dati non più corretti e/o veritieri;
4. termina il rapporto tra il Titolare e il Certificatore;
5. viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo.

### **5.4.2 Procedura per la richiesta di revoca**

La richiesta di revoca viene effettuata con modalità diverse a seconda del richiedente. Sono previsti i seguenti casi:

#### **Revoca su iniziativa del Titolare**

Il Titolare deve richiedere la revoca con una delle seguenti modalità:

1. utilizzando la funzione di revoca disponibile nel sito Web del Certificatore. Per effettuare la richiesta l'utente deve comunicare i propri dati identificativi, l'identificativo univoco a lui assegnato (IUT), la motivazione della revoca, il codice di revoca del certificato (RRC);
2. telefonando al Call Center del Certificatore e fornendo le informazioni di cui al punto precedente. In assenza del codice RRC, e solo nel caso in cui la motivazione della revoca sia la compromissione della chiave privata, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una sospensione del certificato in attesa della richiesta scritta del titolare;
3. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la revoca al Certificatore.

In tutti i casi sopra elencati il richiedente è tenuto a sottoscrivere la richiesta di revoca e consegnarla all'Ufficio di Registrazione o inviarla direttamente al Certificatore.

Il Titolare potrà verificare la revoca del proprio certificato, al più tardi dopo 24 ore dalla richiesta della medesima tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito all'indirizzo:

[http://www.card.infocamere.it/servizi/servizi\\_home.htm](http://www.card.infocamere.it/servizi/servizi_home.htm).

### Revoca su iniziativa del Certificatore

Il Certificatore attiva una richiesta di revoca con la seguente modalità:

1. il Certificatore comunica al Titolare l'intenzione di revocare il certificato, fornendo il motivo della revoca, nonché la data e l'ora di decorrenza;
2. la procedura di revoca del certificato viene completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL) gestita dal Certificatore medesimo.

Il Titolare potrà verificare la revoca del proprio certificato, al più tardi dopo 24 ore dalla notifica da parte del Certificatore medesimo tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito all'indirizzo: [http://www.card.infocamere.it/servizi/servizi\\_home.htm](http://www.card.infocamere.it/servizi/servizi_home.htm).

#### 5.4.3 Procedura per la revoca immediata

Nel caso di compromissione della segretezza della chiave privata è necessario attivare la procedura di **revoca immediata**. Il Titolare è tenuto ad effettuare la richiesta di revoca specificando l'avvenuta o sospetta compromissione della chiave, dando luogo così alla revoca immediata.

Il processo di revoca segue i passi descritti nei casi precedenti con la particolarità che la pubblicazione della lista dei certificati revocati (CRL) avviene immediatamente (cfr. i paragrafi 5.4.7 e 5.4.8).

#### 5.4.4 Motivi per la Sospensione di un certificato

Il Certificatore esegue la sospensione del certificato su propria iniziativa o su richiesta del Titolare. La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità e/o validità della richiesta;
2. il Titolare o il Certificatore acquisiscano elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato specificandone la durata; alla scadenza di tale periodo, alla sospensione seguirà o una revoca definitiva oppure la ripresa di validità del certificato.

#### 5.4.5 Procedura per la richiesta di Sospensione

La richiesta di sospensione viene effettuata con modalità diverse a seconda del richiedente. Sono previsti i seguenti casi:

##### Sospensione su iniziativa del Titolare

Il titolare deve richiedere la sospensione con una delle seguenti modalità:

1. utilizzando la funzione di sospensione disponibile nel sito Web del Certificatore. Per effettuare la richiesta l'utente deve comunicare i propri dati identificativi, l'identificativo univoco a lui assegnato (IUT), la motivazione e il periodo di durata della sospensione, il codice di revoca del certificato (RRC);
2. telefonando al Call Center del Certificatore e fornendo le informazioni di cui al punto precedente. In assenza del codice RRC e solo nel caso in cui si tratti di una richiesta di revoca per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una **sospensione immediata** del certificato in attesa della richiesta scritta del Titolare;
3. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione al Certificatore.

In tutti i casi sopra elencati il richiedente è tenuto a sottoscrivere la richiesta di sospensione e consegnarla all'Ufficio di Registrazione o inviarla direttamente al Certificatore.

Il Titolare potrà verificare l'avvenuta sospensione del proprio certificato, al più tardi dopo 24 ore dalla richiesta della medesima tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito all'indirizzo [http://www.card.infocamere.it/servizi/servizi\\_home.htm](http://www.card.infocamere.it/servizi/servizi_home.htm).

#### **Sospensione su iniziativa del Certificatore**

Il Certificatore attiva una richiesta di sospensione con la seguente modalità:

1. il Certificatore comunica al titolare l'intenzione di sospendere il certificato, fornendo il motivo della sospensione, la data di decorrenza e la durata della sospensione.
2. La procedura di sospensione del certificato viene completata con l'inserimento nella lista di revoca e sospensione (CRL) gestita dal Certificatore medesimo.

Il Titolare potrà verificare l'avvenuta sospensione del proprio certificato, al più tardi dopo 24 ore dalla notifica da parte del Certificatore medesimo tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito all'indirizzo:  
[http://www.card.infocamere.it/servizi/servizi\\_home.htm](http://www.card.infocamere.it/servizi/servizi_home.htm).

#### **5.4.6 Ripristino di validità di un Certificato sospeso**

Alla scadenza del periodo di sospensione richiesto, la validità del certificato viene ripristinata tramite la rimozione del certificato dalla lista di revoca e sospensione (CRL).

Il Titolare potrà controllare il ripristino della validità del certificato tramite la funzionalità presente sul sito del Certificatore all'indirizzo: [http://www.card.infocamere.it/servizi/servizi\\_home.htm](http://www.card.infocamere.it/servizi/servizi_home.htm).

#### **5.4.7 Pubblicazione e frequenza di emissione della CRL**

I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL), firmata dal Certificatore, immessa e pubblicata nel registro dei certificati.

La CRL viene pubblicata in modo programmato ogni settimana (emissione ordinaria) e nel caso vi siano revoche o sospensioni pendenti si effettua giornalmente una pubblicazione aggiuntiva (emissione straordinaria).

Il Certificatore può in circostanze particolari forzare un'emissione non programmata della CRL (emissione straordinaria immediata), ad esempio nel caso in cui la revoca o la sospensione di un certificato avvenga per la sospetta compromissione della segretezza della chiave privata (revoca o sospensione immediata).

L'acquisizione e consultazione della CRL è a cura degli utenti utilizzatori. La CRL è emessa sempre integralmente e il momento della pubblicazione è asseverato mediante l'apposizione di una marca temporale. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di richiesta della revoca o sospensione.

#### **5.4.8 Tempistica**

Il tempo di attesa tra la richiesta di revoca o di sospensione e la sua realizzazione tramite pubblicazione della CRL è al massimo di 24 ore.

In caso di revoca o sospensione immediata il tempo di attesa è al massimo di 2 ore.

## **5.5 Sostituzione delle chiavi e rinnovo del Certificato**

Il certificato ha validità di due anni dalla data di emissione. La procedura di richiesta di un nuovo certificato, che prevede la generazione di una nuova coppia di chiavi, deve essere avviata da parte del Titolare prima della scadenza del certificato (Cfr. § 4.2)

## **5.6 Servizio di Marcatura Temporale**

Su richiesta degli utenti l'Ente Certificatore InfoCamere fornisce un servizio di validazione temporale di documenti informatici, siano essi firmati digitalmente ovvero non firmati.

La validazione temporale è, invece, sempre applicata a certificati e liste di revoca e sospensione come richiesto dalla vigente normativa, in modo tale da attestarne il momento della pubblicazione.

In generale, il servizio di marcatura temporale consente di stabilire l'esistenza di un documento informatico **prima** di un certo istante temporale associando all'evidenza informatica una data e ora certe, ovvero validandola temporalmente

Un'evidenza informatica è sottoposta a validazione temporale con la generazione di una marca temporale ad essa associata: la marca temporale è una struttura di dati firmata digitalmente che lega in modo sicuro e verificabile un qualsiasi documento informatico ad un riferimento affidabile di tempo (data e ora).

La marca temporale viene firmata ed emessa da un sistema centrale ed affidabile, detto *Time Stamping Authority* (TSA), al quale gli utenti indirizzano le loro richieste secondo necessità; chiunque abbia richiesto e conservato una marca temporale per un certo documento potrà, in seguito, dimostrare che tale documento effettivamente esisteva alla data/ora riportate nella marca firmata da quella TSA.

In particolare, la validazione temporale di un **documento firmato digitalmente** consente di verificare e considerare valida la firma digitale apposta anche quando il certificato del sottoscrittore risulti scaduto o revocato, purché l'assegnazione della marca temporale al documento sia stata effettuata durante il periodo di validità del certificato medesimo.

### **5.6.1 Richiesta di emissione o di verifica di marca temporale**

Il servizio di marcatura temporale prevede di indirizzare le richieste di emissione o verifica delle marche temporali di documenti informatici al server della TSA tramite moduli software opportunamente predisposti.

La richiesta di emissione/verifica di marca temporale può essere effettuata utilizzando il software di firma/verifica fornito da InfoCamere, che consente di apporre la marca temporale a documenti **firmati digitalmente** e di eseguirne un'immediata verifica. L'utente può, inoltre, effettuare la richiesta via Web: in questo caso, potranno essere validati temporalmente documenti informatici generici. Le modalità di erogazione del servizio sono stabilite dall'Ente Certificatore InfoCamere.

Successivamente ad accettazione e registrazione della richiesta ed effettuati gli opportuni controlli di correttezza, il server della *Time Stamping Authority* elabora la richiesta, genera la marca temporale e la rinvia al client, che restituisce all'utente l'esito della verifica opportunamente predisposto per la visualizzazione.

Le tipologie di richiesta previste dal servizio di marcatura temporale consistono in:

- **emissione** di marca temporale
- **verifica** di marca temporale.

Per la richiesta di *emissione* di marca temporale, l'utente seleziona il documento informatico da marcare dal proprio personal computer e, calcolato l'hash e inviato alla TSA per la marcatura, riceve come risultato un unico file in formato MIME contenente il documento originale e la marca temporale ad esso associata.

Non è prevista l'emissione di più marche temporali per la stessa evidenza informatica, sottoscritte con chiavi diverse da parte della medesima TSA.

Per la richiesta di *verifica* di marca temporale, l'utente deve fornire, come dati in ingresso il file in formato MIME, contenente la marca temporale e il documento informatico a cui la marca è associata.

L'utente che riceve la marca temporale svolge, mediante le procedure opportunamente predisposte, i seguenti controlli:

- a) verifica la firma della TSA, validando la catena di certificazione, usando la chiave pubblica corrispondente alla chiave privata utilizzata per la generazione della marca temporale
- b) verifica che il valore dell'impronta contenuto nella marca temporale corrisponda allo stesso valore dell'impronta che è stata inviata alla TSA in fase di richiesta.

Il sistema, effettuate tutte le necessarie verifiche, visualizza le seguenti informazioni:

- data e ora di creazione della marca temporale
- numero seriale, identificativo della marca temporale
- identificativo dell'ente emittente la marca temporale.

Il verificarsi di situazioni di errore durante la richiesta di emissione o verifica di marcatura temporale viene esplicitamente segnalato all'utente.

### **5.6.2 Emissione o verifica di marca temporale**

L'emissione della marca temporale viene effettuata in modo automatico da un sistema elettronico sicuro (server della TSA), gestito dal Certificatore, in grado di calcolare con precisione la data e ora di generazione della marca temporale con riferimento al Tempo Universale Coordinato, generare la struttura di dati contenente le informazioni specificate nel successivo paragrafo 5.6.4, sottoscrivere digitalmente detta struttura di dati.

L'operazione avviene secondo le fasi seguenti:

- l'utente richiedente, mediante le procedure predisposte dal Certificatore, invia la richiesta di marcatura temporale del documento informatico, eventualmente prendendone precedente visione, al server della TSA
- La TSA, ricevuta la richiesta di marcatura temporale contenente l'impronta dell'evidenza informatica da sottoporre a validazione temporale calcolata secondo l'algoritmo di hash SHA-1, provvede a generare la struttura di dati di cui al successivo paragrafo 5.6.4: detta struttura contiene, tra le varie informazioni, l'impronta medesima e la data/ora correnti ottenute da una fonte esatta. Il server della TSA appone la firma alla struttura dati generata, ottenendo la marca temporale. Terminata correttamente la procedura di generazione della marca temporale, quest'ultima viene inviata all'utente.

### **5.6.3 Gestione della coppia di chiavi asimmetriche della TSA**

#### **5.6.3.1 Generazione della chiave di marcatura temporale della TSA**

La coppia di chiavi asimmetriche è generata all'interno di un dispositivo crittografico hardware conforme ai requisiti di sicurezza previsti dal DPCM 8 febbraio 1999. Viene usato l'algoritmo asimmetrico **RSA** con chiavi di lunghezza non inferiore a **1024 bit**.

#### **5.6.3.2 Protezione della chiave privata della TSA**

Il dispositivo per la generazione della coppia di chiavi asimmetriche della TSA può essere attivato solo da operatori appositamente autorizzati che provvedono allo sblocco del dispositivo crittografico inserendo una coppia di smartcard ciascuna accompagnata dall'apposito PIN.

La chiave privata della TSA è generata e memorizzata all'interno del dispositivo crittografico in modo tale da impedirne l'esportazione.

#### **5.6.3.3 Ciclo di vita della chiave di marcatura della TSA**

Ogni coppia di chiavi utilizzata per la validazione temporale è univocamente associata al sistema che fornisce il servizio. Al fine di limitare il numero di marche temporali generate con la medesima coppia, le chiavi di marcatura temporale vengono sostituite dopo un mese di utilizzazione, indipendentemente dalla validità del certificato di chiave pubblica corrispondente.

La sostituzione mensile della chiave di marcatura temporale avviene senza revocare il corrispondente certificato di chiave pubblica.

#### **5.6.3.4 Distribuzione della chiave pubblica per la verifica della marca temporale**

È garantita l'integrità e l'autenticità della chiave pubblica del server della TSA in quanto distribuita tramite emissione di un certificato di chiave pubblica **sottoscritto** dal Certificatore Infocamere S.C.p.A.

L'emissione del certificato per la verifica delle marche temporali emesse viene effettuato in modo automatico dalle procedure del Certificatore secondo i seguenti passi:

- viene generata la richiesta di certificato da parte del personale autorizzato e inoltrata alla CA InfoCamere dedicata alla certificazione di chiavi di marcatura temporale
- si procede alla generazione del certificato
- il certificato viene pubblicato nel registro dei certificati e reso disponibile a tutti.

Il formato del certificato di marcatura temporale, contenente la chiave pubblica della TSA, è conforme a quanto specificato nelle Linee Guida per l'Interoperabilità dei Certificatori [10]; in questo modo ne è garantita la piena leggibilità e verificabilità nel contesto della normativa e dei certificatori italiani.

Per la certificazione di chiavi di marcatura temporale il Certificatore utilizza, secondo la vigente normativa, una coppia di chiavi diversa da quella utilizzata per firmare certificati relativi alle usuali chiavi di sottoscrizione, anch'esse con validità pari a 6 anni.

36 mesi prima della scadenza della chiave in esercizio il Certificatore avvia le procedure di sostituzione periodica della chiave privata di certificazione di chiavi di marcatura temporale secondo le modalità indicate al paragrafo 5.9.

### **5.6.3.5 Validità della marca temporale**

Il periodo di validità del certificato di marcatura temporale si estende per tre anni a partire dalla data di emissione. Una marca temporale ha validità fino alla scadenza del suddetto certificato: il periodo di validità della marca temporale può essere ulteriormente esteso associando, prima della scadenza del corrispondente certificato, una nuova marca all'intera evidenza informatica costituita dal documento originale marcato e dalla precedente/precedenti marca/che temporale/i.

### **5.6.4 Marca Temporale**

#### **5.6.4.1 Formato e contenuto della marca temporale**

Il formato delle marche temporali ed il protocollo di colloquio con la TSA rispettano le specifiche tecniche esposte in RFC 3161 "*Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)*" - PKIX Working Group IETF – Agosto 2001 [7]. Queste specifiche soddisfano i requisiti della legge italiana (DPCM 8/2/99) per quanto riguarda le funzionalità ritenute essenziali dal legislatore relativamente al servizio di marcatura temporale.

Ogni marca temporale emessa contiene tutte le informazioni richieste dalla normativa, ovvero:

- l'identificativo dell'emittente la marca temporale.
- il numero di serie della marca temporale.
- l'algoritmo di sottoscrizione della marca temporale. Nella fattispecie l'algoritmo utilizzato l'RSA.
- l'identificativo del certificato relativo alla chiave pubblica della TSA.
- la data e l'ora di generazione della marca.
- l'identificativo dell'algoritmo di hash utilizzato per generare l'impronta dell'evidenza informatica sottoposta a validazione temporale
- il valore dell'impronta dell'evidenza informatica.

#### **5.6.4.2 Precisione del riferimento temporale**

In fase di generazione di una marca temporale, il server della TSA ricava la data/ora dal clock del sistema, mantenuto allineato con l'ora esatta UTC (Tempo Universale Coordinato) grazie al segnale di sincronismo ottenuto da un ricevitore esterno di qualità: il server di marcatura temporale ricava il tempo da un ricevitore radio sintonizzato con il segnale emesso dall'Istituto Elettronico Nazionale (IEN) "Galileo Ferraris". Il ricevitore utilizzato è stato preventivamente tarato e certificato dallo IEN stesso; il segnale orario così ottenuto rispetta i margini di precisione richiesti dalla normativa vigente (DPCM 8/2/99).

#### **5.6.4.3 Tempistica**

La generazione delle marche temporali garantisce che il tempo di risposta, misurato come differenza tra il momento della ricezione della richiesta e l'ora riportata nella marca temporale, a meno di impedimenti nell'emissione della marca stessa, non sarà superiore al minuto primo.

### **5.6.5 Registrazione delle marche generate**

Tutte le marche temporali emesse, assieme alle relative richieste sono conservate in un database relazionale.

Periodicamente, le marche temporali più "vecchie" vengono archiviate su supporto non riscrivibile da un apposito processo, mediante un masterizzatore di CD-R: un operatore autorizzato provvede alla sostituzione periodica dei supporti di archiviazione (CD-R).

L'accesso ai dati, contenuti nei diversi archivi, è consentito solo agli operatori abilitati.

### **5.6.6 Sicurezza del sistema di validazione temporale**

Il sistema per il servizio di marcatura temporale può essere attivato solo da operatori autorizzati tramite l'utilizzo di una serie di password e disponendo di un certo numero di smartcard.

Una volta attivato, il sistema non necessita di ulteriori procedure interattive di login, tranne che per arrestarlo e riattivarlo a scopo di manutenzione.

Un eventuale arresto del sistema può essere risolto solamente dagli operatori abilitati.

Il sistema di TSA dispone, inoltre, di uno specifico componente dedicato al monitoraggio delle seguenti condizioni:

1. tentativi di manomissione della sicurezza del sistema
2. perdita del segnale di sincronismo con la fonte esterna di tempo
3. degrado delle prestazioni in termini di tempo di risposta
4. disponibilità del supporto di archiviazione non riscrivibile

Al verificarsi di una o più delle suddette condizioni, viene valutata la gravità dell'evento, provvedendo all'arresto del servizio di marcatura temporale qualora non sussistano le necessarie misure di sicurezza.

### **5.6.7 Protezione dei documenti informatici**

Ai sensi dell'articolo 59 del DPCM 8/2/99, è stato realizzato da parte del Certificatore InfoCamere un servizio per l'archiviazione sicura di documenti informatici, siano essi firmati digitalmente oppure non firmati: di ogni documento archiviato viene garantita nel tempo l'immodificabilità, la reperibilità, la visualizzazione previa abilitazione.

*Nel caso in cui i file siano firmati digitalmente*, la procedura si fa carico, al momento dell'acquisizione del file, di marcarlo temporalmente qualora non sia già stata assegnata ad esso una marca temporale; provvede, poi, su richiesta dell'utente, ad estenderne la validità legale nel tempo, apponendovi le opportune successive marche temporali, secondo quanto previsto dall'articolo 60 del DPCM 8/2/99.

#### **5.6.7.1 Procedure per la richiesta di conservazione di documenti informatici**

L'utente che desidera conservare i propri documenti informatici potrà avvalersi del servizio descritto, seguendo le procedure riportate nel relativo manuale utente.

La richiesta del servizio è gestita secondo le modalità previste da apposito contratto.

Per tutto ciò che concerne l'utilizzo dell'applicazione e le funzionalità da esso offerte relativamente la scelta delle modalità di conservazione del documento, le operazioni per la sua gestione una volta archiviato, nonché le modalità per richiederne copia, si rimanda al relativo manuale utente.

## **5.7 Controllo del sistema di certificazione**

Sono predisposte procedure e sistemi automatici per il controllo dello stato del sistema di certificazione e dell'intera infrastruttura tecnica del Certificatore.

### **5.7.1 Strumenti automatici per il controllo di sistema**

Sono installati strumenti di controllo automatico che consentono al Certificatore di controllare il sistema valutando gli eventi e gli stati in cui il sistema stesso viene a trovarsi.

Il sistema è configurato in modo da intraprendere, in funzione dell'evoluzione dei suoi stati, delle azioni fra le seguenti tipologie:

- memorizzazione degli eventi;
- riconoscimento di eventi;
- risoluzione dei problemi;
- notificazione agli operatori.

### **5.7.2 Verifiche di sicurezza e qualità**

Le procedure operative e le procedure di sicurezza del Certificatore sono soggette a controlli periodici legati sia alle verifiche ispettive per il mantenimento della certificazione di qualità (ISO 9001) che alle verifiche predisposte dalla funzione di auditing interno. Tali controlli mirano a verificare la corretta applicazione delle procedure previste e la loro effettiva funzionalità in relazione agli obiettivi prefissati.

Oltre alle attività di auditing di processi sono pianificate le analisi e i controlli da effettuare sulle registrazioni prodotte dalle applicazioni e dai sistemi durante il normale funzionamento. Tale attività ha lo scopo di controllare che tutti gli eventi verificatisi rientrino nella normale operatività e che non si verifichino eventi pregiudicanti la sicurezza. La registrazione e la conseguente imputabilità degli eventi verificatisi costituiscono inoltre una valida misura di sicurezza.

Gli eventi registrati e controllati (in modo automatico o manuale) sono:

- richiesta, emissione e revoca dei certificati;
- registrazione del titolare;
- inizio e fine sessione di lavoro;
- modifiche al registro dei certificati;
- personalizzazione dei dispositivi di firma;
- accesso ed uscita dai locali protetti;
- blocchi e malfunzionamenti del sistema;
- periodi di indisponibilità del registro dei certificati;
- periodi di indisponibilità del sistema;
- identificazione di chiave pubblica duplicata.

Le registrazioni di questi eventi costituiscono il giornale di controllo.

## **5.8 Dati archiviati**

Negli archivi gestiti dal Certificatore sono conservati e mantenuti i seguenti dati:

- certificati emessi, sospesi e revocati e relative marche temporali;
- dati di registrazione dei titolari delle chiavi;
- associazione tra codice identificativo del titolare e dispositivo di firma;
- dati di sessione al sistema e ai servizi;
- dati inerenti al giornale di controllo;
- certificati delle chiavi di marcatura temporale.

L'accesso ai dati contenuti nei diversi archivi è consentito agli operatori opportunamente abilitati.  
I dati archiviati sono conservati per 10 anni.

### **5.8.1 Procedure di salvataggio dei dati**

Il salvataggio periodico dei dati relativi ai sistemi collegati in rete è effettuato giornalmente tramite un sistema di archiviazione automatizzato. Periodicamente copia dei supporti contenenti i dati del salvataggio viene archiviata in un armadio di sicurezza, il cui accesso è consentito unicamente all'operatore addetto che appartiene alla struttura del Certificatore.

Periodicamente copia di tali supporti è inoltre trasportata in un luogo sicuro esterno alla sede del Certificatore, in modo da averne la disponibilità anche in caso di eventi disastrosi.

A garanzia della possibilità di poter ripristinare il sistema completo a seguito di guasti, sono effettuati salvataggi di tutti gli altri dati e programmi necessari per l'erogazione del servizio. Le modalità e i tempi di archiviazione dei salvataggi sono gli stessi delle procedure di salvataggio dei dati.

## **5.9 Sostituzione delle chiavi del Certificatore**

Il Certificatore avvia le procedure di sostituzione periodica della chiave privata di certificazione utilizzata alla firma di certificati di sottoscrizione almeno 24 mesi prima della scadenza, ovvero 36 mesi prima nel caso di chiavi di certificazione di chiavi di marcatura temporale.

Quindi 24 mesi prima della scadenza del certificato corrente, ovvero 36 mesi prima, sono previste le seguenti operazioni:

1. Generazione della nuova coppia di chiavi per il Certificatore;
2. Emissione del certificato contenente la nuova chiave pubblica firmato utilizzando la nuova chiave privata;
3. Emissione del certificato della vecchia chiave pubblica firmato utilizzando la nuova chiave privata;
4. Emissione del certificato della nuova chiave pubblica firmato utilizzando la vecchia chiave privata;
5. Pubblicazione di questi certificati nel registro dei certificati.

I certificati ai punti 3. e 4. servono per la reciproca certificazione delle diverse chiavi del Certificatore e la loro durata è di 2 anni nel caso di certificazione di chiavi di sottoscrizione, ovvero 3 anni nel caso di certificazione di chiavi di marcatura temporale, ossia fino alla scadenza del precedente certificato corrente.

La ciclicità del rinnovo delle chiavi e la durata dei certificati sono tali da consentire all'utente di poter utilizzare il certificato in suo possesso fino al momento del rinnovo.

## **5.10 Cessazione del servizio**

Nell'eventualità di cessazione dell'attività di certificazione, il Certificatore comunicherà questa intenzione all'AIPA con un anticipo di almeno sei mesi, indicando il certificatore sostitutivo, il depositario del registro dei certificati e della relativa documentazione.

Con pari anticipo il Certificatore informa della cessazione della attività tutti i possessori di certificati da esso emessi. Nella comunicazione sarà chiaramente specificato che tutti i certificati non ancora scaduti al momento della cessazione della attività del Certificatore saranno revocati.

## **5.11 Sistema di qualità**

Tutti i processi operativi del Certificatore descritti in questo Manuale Operativo, come ogni altra attività del Certificatore, sono conformi allo standard ISO9001.

Il Certificatore è in possesso della certificazione ISO9001 del sistema qualità aziendale.

## 5.12 Disponibilità del servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (comprende i certificati e le CRL)	Dalle 0:00 alle 24:00 7 giorni su 7
Revoca e sospensione dei certificati	Dalle 0:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione, pubblicazione, rinnovo (*)	Dalle 9:00 alle 17:00 dal lunedì al venerdì esclusi i festivi Dalle 9.00 alla 13.00 il sabato
Richiesta e/o verifica di marca temporale	Dalle 00:00 alle 24:00 dal lunedì al venerdì

(\*) L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono scegliere diversi orari di sportello. In ogni caso il Certificatore garantisce l'erogazione del proprio servizio negli orari sopra riportati.

## **6. Misure di Sicurezza**

Il Certificatore ha realizzato un sistema di sicurezza del sistema informativo relativo al servizio di certificazione digitale.

Il sistema di sicurezza implementato è articolato su tre livelli:

- un livello fisico che mira a garantire la sicurezza degli ambienti in cui il Certificatore gestisce il servizio,
- un livello procedurale, con aspetti prettamente organizzativi,
- un livello logico, tramite la predisposizione di misure tecnologiche hardware e software che affrontano i problemi e i rischi connessi con la tipologia del servizio e con l'infrastruttura utilizzata.

Tale sistema di sicurezza è realizzato per evitare rischi derivanti dal malfunzionamento dei sistemi, della rete e delle applicazioni, oltre che dall'intercettazione non autorizzata o dalla modifica dei dati.

Informazioni più dettagliate sul sistema di sicurezza adottato sono descritte in Appendice A.

### **6.1 Guasto al dispositivo di firma del Certificatore**

In caso di guasto del dispositivo di firma del Certificatore si fa ricorso alla copia di riserva della chiave di certificazione, opportunamente salvata e custodita, e non vi è necessità di revocare il corrispondente certificato del Certificatore (cfr. § A.3).

### **6.2 Compromissione della chiave di certificazione**

In caso di compromissione della segretezza della chiave privata di certificazione il Certificatore deve:

- a) revocare il certificato della chiave di certificazione compromessa;
- b) notificare la revoca all'Autorità per l'Informatica nella Pubblica Amministrazione entro 24 ore;
- c) informare tutte i possessori di certificati sottoscritti con la chiave privata appartenente alla coppia revocata;
- d) saranno revocati i certificati per i quali risultano contemporaneamente compromessa sia la chiave di certificazione sia quella utilizzata per la generazione della marcatura temporale;
- e) nel caso di revoca del punto precedente saranno riemessi i certificati delle chiavi pubbliche dei titolari utilizzando una nuova chiave di certificazione.

### **6.3 Procedure di Gestione dei Disastri**

Il Certificatore ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità o di disastro.

## **7. Amministrazione del Manuale Operativo**

### **7.1 Procedure per l'aggiornamento**

Il Certificatore si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute sia a causa di norme di legge o regolamenti, sia per ottimizzazioni del ciclo lavorativo.

Ogni nuova versione del Manuale Operativo annulla e sostituisce le precedenti versioni, che rimangono tuttavia applicabili ai certificati emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

Variazioni che non hanno un impatto significativo sugli utenti comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.

Ogni anno il Certificatore comunica all'AIPA la permanenza dei requisiti per l'esercizio dell'attività di certificazione e fornisce la versione aggiornata del manuale operativo.

Ogni modifica tecnica o procedurale a questo manuale operativo verrà prontamente comunicata agli Uffici di Registrazione.

### **7.2 Regole per la pubblicazione e la notifica**

Il Manuale Operativo è pubblicato:

- in formato elettronico sul sito web del Certificatore  
(indirizzo: <http://www.card.infocamere.it/firma/cps/cps.htm>);
- in formato elettronico nell'elenco pubblico dei certificatori tenuto dall'AIPA;
- in formato cartaceo può essere richiesto agli Uffici di Registrazione o al contatto per gli utenti finali (vedi §. 2.3).

### **7.3 Responsabile dell'approvazione**

Questo Manuale Operativo viene approvato dal Responsabile dell'Unità Organizzativa Firma Digitale di InfoCamere S.C.p.A..

### **7.4 Conformità**

I contenuti del presente Manuale Operativo sono pienamente rispondenti alle regole tecniche descritte nel DCPM dell' 8 febbraio 1999 [2].

## **Appendice A: Descrizione delle misure di sicurezza**

### **A.1 Sicurezza fisica**

Le misure adottate forniscono adeguate garanzie di sicurezza in merito a :

- Caratteristiche dell'edificio e della costruzione;
- Sistemi anti-intrusione attivi e passivi;
- Controllo degli accessi fisici;
- Alimentazione elettrica e condizionamento dell'aria;
- Protezione contro gli incendi;
- Protezione contro gli allagamenti;
- Modalità di archiviazione dei supporti magnetici;
- Siti di archiviazione dei supporti magnetici.

### **A.2 Sicurezza delle procedure**

A garanzia che nessun individuo possa singolarmente compromettere o alterare la sicurezza globale del sistema oppure svolgere attività non autorizzate nella gestione dei certificati, è previsto di affidare la gestione operativa del sistema a persone diverse con compiti separati e ben definiti.

Il personale addetto alla progettazione ed erogazione del servizio di certificazione è dipendente dal Certificatore ed è stato selezionato in base alla esperienza nella progettazione, realizzazione e conduzione di servizi informatici e a caratteristiche di affidabilità e riservatezza.

Interventi di formazione sono pianificati periodicamente per sviluppare la consapevolezza dei compiti assegnati. In particolare, prima dell'inserimento del personale nell'attività operativa di certificazione, sono realizzati interventi formativi allo scopo di fornire ogni competenza (tecnica, organizzativa e procedurale) necessaria a svolgere i compiti assegnati

### **A.3 Sicurezza logica**

#### **Generazione della coppia di chiavi**

Il Certificatore per svolgere la sua attività ha bisogno di generare le seguenti chiavi:

- Chiave di certificazione per la firma dei certificati dei titolari e del sistema di validazione temporale;
- Chiavi del sistema di validazione temporale per la marcatura temporale.

Le chiavi sono generate solamente da personale esplicitamente incaricato di tale funzione.

La generazione delle chiavi e della firma avviene all'interno di moduli crittografici dedicati.

La generazione delle chiavi di firma del titolare avviene all'interno del dispositivo di firma (carta a microprocessore) rilasciato al titolare stesso. L'attivazione del dispositivo, e quindi l'utilizzo delle chiavi in esso contenute, è subordinato alla digitazione del PIN.

#### **Lunghezza delle chiavi**

Le chiavi RSA usate dal Certificatore per firmare i certificati DTS sono di lunghezza: 2048 bit

Le chiavi RSA usate dal Certificatore per firmare i certificati degli utenti sono di lunghezza: 2048 bit

Le chiavi per la firma delle marche temporali sono di lunghezza: 1024 bit .

Le chiavi di firma usate dall'utente finale per apporre la firma digitale devono essere chiavi RSA ed avere una lunghezza di 1024 bit.

**Protezione della chiave privata del Certificatore**

La protezione delle chiavi private del Certificatore viene svolta dal modulo crittografico di generazione ed utilizzo della chiave stessa.

La chiave privata può essere generata solo con la presenza contemporanea di due operatori incaricati della generazione.

Le chiavi private del Certificatore vengono duplicate, al solo fine del loro ripristino in seguito alla rottura del dispositivo di firma, secondo una procedura controllata che prevede la suddivisione della chiave su più dispositivi.

**Sicurezza dei sistemi del Certificatore**

Per garantire la sicurezza dei dati e delle operazioni, tutto il software di sistema ed applicativo utilizzati per le funzioni del Certificatore realizza le seguenti funzioni di sicurezza:

- Identificazione e autenticazione degli utenti e dei processi che richiedono di operare nel sistema;
- Controllo accessi
- Imputabilità ed audit di ogni evento riguardante la sicurezza;
- Gestione delle risorse di memorizzazione volta ad impedire la possibilità di risalire alle informazioni in precedenza contenute o registrate da altri utenti;
- Autodiagnostica ed integrità dei dati e del software (controllo allineamento tra le copie operative e quelle di riferimento, controllo della configurazione del software, protezione dai virus).
- Configurazione hardware e software per garantire la continuità del servizio.

**Livello di sicurezza dei sistemi operativi degli elaboratori**

Il sistema operativo degli elaboratori utilizzati nelle attività di certificazione per la generazione delle chiavi, la generazione dei certificati e la gestione del registro dei certificati, sono conformi alle specifiche previste dalla classe ITSEC F-C2/E2, equivalenti a quella C2 delle norme TCSEC.

**Sicurezza della rete**

Il Certificatore ha ideato per il servizio di certificazione un'infrastruttura di sicurezza della rete basata sull'uso di meccanismi di firewalling e di reti VPN in modo da realizzare un canale sicuro tra gli Uffici di Registrazione ed il sistema di certificazione, nonché tra questo e gli amministratori/operatori. Il sistema è altresì supportato da specifici prodotti di sicurezza (anti intrusione di rete, monitoraggio, protezione da virus) e da tutte le relative procedure di gestione.

**Controlli sul modulo di crittografia**

Il modulo di crittografia utilizzato per la generazione delle chiavi e per la firma ha requisiti tali da assicurare:

- la rispondenza della coppia ai requisiti imposti dagli algoritmi di generazione e di verifica utilizzati;
- l'equiprobabilità di generazione di tutte le coppie possibili;
- l'identificazione del soggetto che attiva la procedura di generazione;
- che la generazione della firma avvenga all'interno del dispositivo in modo tale che non sia possibile l'intercettazione del valore della chiave privata utilizzata.