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

Ente Certificatore InfoCamere

Manuale Operativo

Codice documento: ICCA-MO

Funzione emittente	U.O. Firma Digitale
Redatto da	Ferdinando Soldan
Verificato da	Enzo Berno
Approvato da	Pio Barban

Nome file: ICCA-MOv2r1a

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

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

1.2 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 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, gli Utenti Titolari e gli Utenti Utilizzatori.
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.

1.3 Riferimenti

[1] Decreto del Presidente della Repubblica 10 Novembre 1997, n. 513 (G.U. n. 60 del 13/3/1998)

[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] Decreto del Presidente della Repubblica 28 luglio 1999, n. 318 (c.d. "Misure Minime di Sicurezza")

[8] Circolare AIPA/CR/24 del 19 giugno 2000 (Linee Guida per l'interoperabilità dei Certificatori)

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal DPR 513/97 [1] e dal DPCM 8 febbraio 1999 [2] si rimanda alla 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 le regole equivalenti nel Manuale Operativo.

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 – CA] – cfr. DPR513 [1]

Chiave Privata e Chiave Pubblica – cfr. DPR513 [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**.

Firma digitale *[digital signature]* – cfr. DPR513 [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 – CRL]*

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 – 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] [8] 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

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

Titolare – cfr. DPCM [2]

I titolari sono persone fisiche che richiedono al Certificatore, tramite l'Ufficio di Registrazione, la certificazione di una chiave pubblica.

Uffici di Registrazione *[Registration Authority – RA]*

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

- la convalida di tutti i dati che fornisce l'utente;
- l'identificazione fisica degli utenti (basata su carta d'identità o passaporto).

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 Utilizzatore

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

1.5 Acronimi e abbreviazioni

AIPA – Autorità per l'Informatica nella Pubblica Amministrazione

CRL – Certificate Revocation List
Lista dei certificati revocati o sospesi.

DN – Distinguished Name
Identificativo del titolare di un certificato di chiave pubblica; tale codice è unico nell'ambito degli utenti del 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.

DPR – Decreto del Presidente della Repubblica
Ci si riferisce al DPR 513/97, Rif. [1], che costituisce il Regolamento per la firma digitale.

DTS - Digital Time Stamping
Sistema per la marcatura temporale di certificati e documenti.

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 ruolo per il quale può firmare.

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 dall'utente per accedervi alle funzioni.

RRC – Revocation Request Code
Codice preimbustato consegnato dall'Ufficio di Registrazione all'utente titolare per l'autenticazione della richiesta di revoca di un certificato.

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 di 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 di affidabilità di questa 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 nella 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 descritto 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/firma/cps/cps.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	**InfoCamere - Società Consortile di Informatica delle Camere di Commercio Italiane per azioni**
Sede legale	**Piazza Sallustio, 21 – 00187 Roma**

Rappresentante legale	**Avv. Angelo Mancusi** in qualità di Presidente del Consiglio di Amministrazione
Direzione Generale	**Via G.B. Morgagni, 30H – 00161 Roma**
N° telefono	**06-442851**
N° fax	**06-44285255**
N° Iscrizione Registro Imprese	**Trib. di Roma 1 / 95**
N° partita IVA	**02313821007**
Sito web	http://www.card.infocamere.it/
Nome X.500:	**CN=InfoCamere Firma Digitale,** **OU=Certification Service Provider,** **OU= Ente Certificatore del Sistema Camerale,** **O=InfoCamere SCpA,** **C=IT**
Sede Operativa	**Corso Stati Uniti, 14 – 35127 Padova**

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 degli utenti titolari,
- validazione della richiesta del certificato,
- distribuzione ed inizializzazione del dispositivo di firma,
- attivazione della procedura di certificazione della chiave pubblica del titolare,
- supporto al titolare e al Certificatore nel rinnovo/revoca dei certificati.

L'Ufficio di Registrazione svolge in sostanza tutte le attività di interfaccia tra il Certificatore e l'utente titolare della firma.
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 cliente/titolare.
Il Certificatore verifica la rispondenza delle procedure utilizzate dall'Ufficio di Registrazione a quanto stabilito da questo manuale.

2.2.3 Titolari

I Titolari (o utenti titolari) sono persone fisiche. Ad essi è attribuita una coppia di chiavi asimmetriche (di cui sono "titolari") la cui chiave pubblica è certificata dal Certificatore.

2.2.4 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.

2.2.5 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 a 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 condividano gli stessi algoritmi di hashing e crittografia del Certificatore,
- 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

2.4 Rapporti con l'AIPA

Il presente Manuale Operativo, compilato dal Certificatore nel rispetto delle indicazioni legislative, è stato consegnato, in copia, alla 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 di 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 della attività.
Alla scadenza del proprio certificato, 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. 9 del DPR513 [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 [7];

8. il certificato sia revocato tempestivamente in caso di richiesta da parte del titolare o del terzo da cui ne derivino i poteri, di provvedimento dell'autorità, di acquisizione della conoscenza di cause limitative della capacità del titolare, di sospetti di abusi o falsificazioni;
9. sia certa l'associazione tra chiave pubblica ed utente 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 [7];
4. la verifica d'identità del richiedente il certificato e la registrazione dei dati dello stesso;
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 titolare 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 dall'utente titolare presso l'Ufficio di Registrazione.

L'Ufficio di Registrazione terrà direttamente i rapporti con l'utente 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 dei certificati relativi a chiavi di cui stata compromessa la sicurezza oppure contenute in dispositivi di firma di cui abbia perduto il possesso o che siano diventati difettosi;
5. la richiesta di sospensioni dei certificati in caso sospetti di abusi o falsificazioni;
6. 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;
7. l'adozione di tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.1.4 Obblighi degli Utenti Utilizzatori

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:

- 500.000.000 (500 milioni) di lire (258.228 euro) per singolo sinistro
- 3.000.000.000 (3 miliardi) di lire (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 DPR-513/97 [1] ai soggetti che svolgono funzione di Certificatore ivi compresa la 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 10 novembre 1997, n. 513
- 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 che 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 [7].

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: Lit. 10.000 (euro 5,16)
- Rinnovo: Lit. 5.000 (euro 2,58)
- Revoca e/o Sospensione: gratuita

Tali tariffe sono comunque funzione delle quantità trattate e soggetti 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 per l'identificazione degli utenti 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, titolare di una coppia di chiavi asimmetriche, 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 del passaporto validi.
Al momento della registrazione viene fornito al titolare/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 [8]. Dettagli sul contenuto del certificato e sul significato dei suoi campi sono riportati nel sito Web del Certificatore.

4.2 Rinnovo delle chiavi e certificati

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo *"validity period"* (periodo di validità) con gli attributi *" not after"* (non dopo il) e *"not before"* (non prima del).
Al di fuori di questo intervallo di date il certificato è da considerarsi non valido.

L'utente 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 dell'utente 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

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

5.1 Registrazione degli utenti titolari

I passi principali che gli utenti titolari devono fare per essere certificati 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, e che verranno inserite nel certificato;
c) firmare il contratto di adesione al servizio del Certificatore;

d) generare la coppia di chiavi (pubblica/privata) e presentare quella pubblica al Certificatore in formato tale che sia possibile per quest'ultimo riconoscere l'autenticità della richiesta.

Il dettaglio delle operazioni è illustrato di seguito.

5.1.1 Procedura di Registrazione

Per assegnare un certificato ad un utente titolare che ne faccia richiesta è necessario eseguire una procedura di registrazione durante la quale ne vengono accertata l'identità (autenticazione) e verificate le informazioni che egli fornisce.

1. La registrazione è effettuata dall'Ufficio di Registrazione ed è richiesta la presenza fisica del soggetto richiedente il certificato.
2. L'incaricato del Certificatore verifica l'identità dell'utente titolare tramite la sua carta d'identità o il suo passaporto validi.
3. L'incaricato registra l'associazione tra i dati dell'utente e il numero del dispositivo di firma (UID) e genera l'identificativo univoco del titolare (IUT).
4. L'utente prende visione del contratto e firma la richiesta di registrazione e certificazione completa dei dati ivi riportati.
5. All'utente viene consegnato il dispositivo di firma, il codice di attivazione di default ad esso associato (PIN), il codice segreto per la revoca del certificato (RRC) e l'identificativo univoco del titolare (IUT). Sarà cura dell'utente cambiare il PIN iniziale con uno a sua scelta.

Informazioni che il titolare deve fornire

Nella richiesta di registrazione dell'utente titolare 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 titolare richiedente.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- Tipo e numero, ente che lo ha emesso e data di rilascio del documento di identità presentato per il riconoscimento

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

5.2 Richiesta del certificato

1. L'incaricato del Certificatore attiva la procedura di richiesta di certificato
2. L'utente sblocca il dispositivo di firma, usando il PIN, per generare la coppia di chiavi di crittografia
3. L'incaricato, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica dell'utente e la invia al Certificatore.

5.2.1 Generazione delle chiavi

L'utente titolare utilizzando le funzionalità offerte dalla carta a microprocessore (il dispositivo di firma), genera all'interno della carta la coppia di chiavi per la firma. La lunghezza delle chiavi è di 1024 bit.

5.2.2 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 titolare sia stato correttamente registrato
   - al titolare sia assegnato un codice identificativo unico nell'ambito degli utenti del Certificatore
   - la chiave pubblica fornita dal titolare sia una chiave valida, della lunghezza prevista e non sia già stata certificata per un altro soggetto titolare
   - la richiesta sia autentica e il titolare 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.

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 [8]; 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

Il certificato viene rilasciato e pubblicato entro 48 ore dal momento in cui il Certificatore riceve la richiesta dall'Ufficio di Registrazione.

5.3.3 Validità del certificato

Il periodo di validità del certificato si estende per un anno a partire dalla data di emissione.

5.4 Revoca e sospensione di un certificato

La revoca o la sospensione di un certificato ne tolgono la validità e rendono **non valide** le firme emesse successivamente al momento di revoca o sospensione.
I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore, emessa e pubblicata con periodicità prestabilita nel registro dei certificati.
Il Certificatore può forzare una 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 può eseguire la revoca del certificato su propria iniziativa o su richiesta del titolare o del terzo interessato da cui derivino poteri o titoli del titolare (cfr. art. 9 comma 2 lettera c del DPR 513 [1]). La revoca va richiesta nel caso si verifichino le seguenti condizioni:

- 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 di attivazione (PIN);
  - si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave;
- il titolare non riesce più ad utilizzare il dispositivo di firma in suo possesso (perdita del PIN, guasto del dispositivo, ecc.);
- si verifica un cambiamento dei dati del titolare presenti nel certificato;

- termina il rapporto tra il titolare e il Certificatore;
- 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
L'utente titolare può richiedere la revoca:
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.

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 e la data di decorrenza;
2. la procedura di revoca del certificato viene completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL) e ne viene data comunicazione al titolare.

Revoca su iniziativa di soggetti terzi
La richiesta di revoca su iniziativa di soggetti terzi viene effettuata con la seguente modalità:
1. il soggetto terzo richiede per iscritto al Certificatore la revoca del certificato specificando i dati del titolare del certificato e allegando la documentazione a suffragio della richiesta;
2. al titolare viene notificata la richiesta di revoca;
3. il Certificatore, verificata l'autenticità e la validità della richiesta, procede alla revoca del certificato e ne dà comunicazione al titolare.

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 può eseguire la sospensione del certificato su propria iniziativa o su richiesta del titolare o del terzo interessato da cui derivino poteri o titoli del titolare (cfr. art. 9 comma 2 lettera c del DPR 513 [1]). La sospensione va richiesta nel caso si verifichino le seguenti condizioni:
- è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il titolare, il terzo interessato o il Certificatore acquisiscono elementi di dubbio sulla validità del certificato;
- è necessaria una interruzione della validità del certificato.

Nei casi citati si richiederà la sospensione del certificato per un periodo da indicare; alla sospensione seguirà o una revoca definitiva oppure, alla scadenza del periodo, 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 può richiedere la sospensione:
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.

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; la procedura di sospensione del certificato viene completata con l'inserimento nella lista di revoca e sospensione CRL;
2. viene notificata al titolare l'avvenuta sospensione del certificato.

Sospensione su iniziativa di soggetti terzi
La richiesta di sospensione su iniziativa di soggetti terzi viene effettuata con la seguente modalità:
1. il soggetto terzo richiede al Certificatore per iscritto la sospensione del certificato specificando i dati del titolare del certificato, la motivazione, la durata della sospensione e allegando la documentazione a suffragio della richiesta;
2. il Certificatore, verificata la validità della richiesta, notifica al titolare la richiesta di sospensione e procede alla sospensione inserendo la nuova entrata nella lista di revoca e sospensione CRL.

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.

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 una 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 un anno 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 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.

5.6.1 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 degli stati del sistema, delle azioni fra le seguenti tipologie:

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

5.6.2 Verifiche di sicurezza e qualità

Le procedure operative e le procedure di sicurezza del Certificatore sono soggette a controlli periodici legati sia alla verifiche ispettive per il mantenimento della certificazione di qualità (ISO 9001) che a verifiche predisposte dalla funzione di auditing interno. Tali verifiche 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.

5.7 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.

5.7.1 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.

5.8 Sostituzione delle chiavi del Certificatore

Il Certificatore avvia le procedure di sostituzione periodica della chiave privata di certificazione almeno 12 mesi prima della scadenza della chiave in esercizio.
Quindi 12 mesi prima della scadenza del certificato corrente 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.

Le chiavi di certificazione hanno durata di 6 anni.
I certificati ai punti 3. e 4. servono per la reciproca certificazione delle diverse chiavi del Certificatore e la loro durata è di 1 anno, 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.

5.9 Cessazione del servizio

Nell'eventualità di cessazione della 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 essa emessi. Nella comunicazione sarà chiaramente specificato che tutti i certificati non ancora scaduti al momento della cessazione della attività del Certificatore saranno revocati.

5.10 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.

5.11 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 Giorni lavorativi

(*) 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.

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 antiintrusione 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 una 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.