Ente Certificatore InfoCert
Certificati di Autenticazione
Manuale Operativo

Codice documento: ICERT-INDI-MOCA

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n°:	1.2	**Data Versione/Release**:	20/06/11
Descrizione modifiche:	Indirizzi e dati aziendali		
Motivazioni:			

Versione/Release n°:	1.1	**Data Versione/Release**:	15/10/2007
Descrizione modifiche:	Indirizzo operativo e numero call center		
Motivazioni:			

Versione/Release n°:	1.0	**Data Versione/Release**:	05/07/2007
Descrizione modifiche:	nessuna		
Motivazioni:	Prima emissione		

1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole che governano l'emissione e l'uso dei **Certificati di Autenticazione** sottoscritti dal Certificatore InfoCert e descrive le procedure operative adottate dal Certificatore stesso per i servizi di certificazione digitale.
Le indicazioni di questo documento hanno validità per le attività relative ad InfoCert nel ruolo di Certificatore, per gli Uffici di Registrazione, per i soggetti incaricati ad effettuare l'identificazione/registrazione dei Titolari e/o a consegnare i dispositivi sicuri di firma ai medesimi, per gli stessi Titolari e per gli Utenti.

Per la compilazione di questo documento si è fatto riferimento ai seguenti documenti:
- **InfoCert** Ente Certificatore – Certificati di Sottoscrizione - Manuale Operativo
- **IETF** RFC 2527 (1999): "Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework".

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come CAD)

[2] Decreto Legislativo 4 aprile 2006, n.159 (G.U. n.99 del 29 aprile 2006) - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.

[3] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (G.U. n. 42 del 20/2/2001) e sue modificazioni secondo DPR 137/2003 (nel seguito referenziato come TU)

[4] Deliberazione CNIPA 17 febbraio 2005, n.4/2005 (G.U. n.51 del 03 marzo 2005) – Regole per il riconoscimento e la verifica del documento informatico

[5] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003)

Riferimenti tecnici

[6] Deliverable ETSI TS 102 042 "*Policy requirements for certification authorities issuing public key certificates*" – Aprile 2002

[7] RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile"

[8] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"

[9] RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"

[10] Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

[11] Ente Certificatore InfoCert - Certificati di Sottoscrizione, Manuale Operativo, ICERT-INDI-MO

1.4 Definizioni

1.5 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal TU, dal CAD e dal DPCM 13 gennaio 2004 si rimanda alle definizioni in essi stabilite. 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.

Accreditamento facoltativo
Il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Autocertificazione:
E' la dichiarazione, rivolta al Certificatore, effettuata personalmente dal soggetto che risulterà Titolare del certificato digitale, tramite sottoscrizione della sussistenza di stati, fatti, qualità, ai sensi dell'art. 46 del DPR 445/00 ed assunzione delle responsabilità stabilite per legge.

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

Certificato Qualificato – cfr. CAD

Certificatore *[Certification Authority]* – cfr. CAD

Certificatore Accreditato – cfr. CAD

Certificatore Qualificato – cfr. CAD

Chiave Privata e Chiave Pubblica – cfr. CAD

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

Dati per la creazione di una firma – cfr. CAD

Dati per la verifica della firma – cfr. CAD

Dispositivo sicuro per la creazione della firma – cfr.CAD
Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da un supporto plastico (in genere una carta plastica delle dimensioni di una carta di credito) in cui è inserito un microprocessore rispondente a requisiti di sicurezza determinati dalla legge. 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 elettronica – cfr. CAD

Firma elettronica qualificata – cfr. CAD

Firma digitale *[digital signature]* – cfr. CAD

Giornale di controllo
Il giornale di controllo consiste nell'insieme delle registrazioni, effettuate automaticamente o manualmente, degli eventi previsti dalle Regole Tecniche.

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 CRL, che viene quindi pubblicata nel **registro pubblico**.

Marca temporale *[Time Stamp Token]* – cfr. DPCM

Manuale Operativo – cfr. art. 38 DPCM
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 CNIPA e quelle della letteratura internazionale

Pubblico ufficiale
Soggetto che, nell'ambito delle attività esercitate, è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

RAO – Registration Authority Officer

Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.

Registro dei Certificati

Il Registro dei Certificati è un archivio che contiene tutti i certificati validi emessi dal Certificatore.

Registro pubblico *[Directory]*

Il Registro pubblico è un archivio che contiene:

- tutti i certificati validi emessi dal Certificatore per i quali sia stata richiesta dal titolare la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Regole tecniche

Regole tecniche per la formazione, la trasmissione, la conservazione, la duplicazione, la riproduzione e la validazione, anche temporale, dei documenti informatici (DECRETO DEL PRESIDENTE DEL CONSIGLIO DEI MINISTRI 13 gennaio 2004).

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 *[Subscriber]*

E' il soggetto che richiede all'Ente Certificatore il rilascio di certificati digitali. Se diverso dal Titolare, l'identità del Richiedente è inserita nel campo Organization del certificato X.509.

Ruolo

Il termine Ruolo indica genericamente il Titolo e/o Abilitazione professionale in possesso del Titolare del certificato, ovvero l'eventuale Potere di rappresentare persone fisiche o enti di diritto privato o pubblico, ovvero l'Appartenenza a detti enti nonché l'Esercizio di funzioni pubbliche.

Tempo Universale Coordinato *[Coordinated Universal Time]*

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

Terzo Interessato – cfr. CAD

La persona fisica o giuridica che, ove previsto, presta il proprio consenso all'inserimento nel certificato di sottoscrizione di un Ruolo del Titolare o che autorizza o richiede l'inserimento nel certificato dell'indicazione dell'Organizzazione a cui il Titolare è collegato

Titolare *[Subject]*– cfr. CAD

La persona fisica identificata nel certificato come il possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso; al Titolare è attribuita la firma digitale generata con la chiave privata della coppia.

Uffici di Registrazione *[Registration Authority]*

Ente incaricato dal Certificatore a svolgere le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale nonché alla consegna del dispositivo sicuro di firma.

Utente *[Relying Party]*

Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma digitale basata su quel certificato.

1.6 Acronimi e abbreviazioni

ACBI – Associazione per il Corporate Banking Interbancario

CNIPA – Centro Nazionale per l'informatica nella Pubblica Amministrazione

CAD – Codice dell'amministrazione digitale

Ci si riferisce al D. Lgs n. 82/2005 e sue successive modificazioni, *"Codice dell'amministrazione digitale"*.

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 13 gennaio 2004.

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

ETSI - European Telecommunications Standards Institute

HSM – Hardware Secure Module
E' un dispositivo sicuro per la creazione della firma, con funzionalità analoghe a quelle delle smart card, ma con superiori caratteristiche di memoria e di performance.

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 sicuro di firma, utilizzato dal Titolare per accedere alle funzioni del dispositivo stesso.

PUK
Codice personalizzato per ciascuna Smartcard, utilizzato dal Titolare per riattivare il proprio dispositivo in seguito al blocco dello stesso per errata digitazione del PIN.

RRC
Acronimo di Revocation Request Code, nome assegnato in precedenza al codice di emergenza e saltuariamente ancora utilizzato.

TSA – Time Stamping Authority
L'autorità di certificazione registrata presso il CNIPA che certifica le chiavi dei sistemi (cfr. TSU) che firmano le marche temporali (Time Stamp Token).

TST – Time-Stamp Token
Termine usato nella pubblicistica internazionale per la marca temporale.

TSU – Time Stamp Unit
Il componente fidato, le cui chiavi, certificate dalla TSA, firmano le marche temporali.

TU – Testo Unico
Ci si riferisce al DPR n. 445/2000 e sue successive modificazioni, *"Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa"*.

2. Generalità

Un certificato digitale è l'associazione tra una chiave pubblica di crittografia ed un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata, chiamato anche Titolare della coppia di chiavi asimmetriche (pubblica e privata). Il certificato è utilizzato da altri soggetti (gli Utenti) per ricavare la chiave pubblica, contenuta e distribuita con il certificato, e verificare, tramite questa, il possesso della corrispondente chiave privata, identificando in tal modo il Titolare della stessa.

Il certificato garantisce la corrispondenza tra la chiave pubblica e il Titolare. Il grado di affidabilità di questa associazione è legato a diversi fattori, quali, ad esempio, la modalità con cui il Certificatore ha emesso il certificato, le misure di sicurezza adottate e le garanzie offerte dallo stesso, gli obblighi assunti dal Titolare per la protezione della propria chiave privata.
A tale proposito i certificati di Autenticazione emessi dall'Ente Certificatore InfoCert sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso, e rilasciati su dispositivo sicuro di firma (Smart card).

Il presente documento contiene le regole che governano l'emissione e l'uso dei Certificati di Autenticazione (in seguito anche chiamati più brevemente **Certificati**) sottoscritti dal Certificatore InfoCert, e descrive le procedure operative adottate dallo stesso per i servizi di certificazione digitale.

I **Certificati di Autenticazione** sono rilasciati e gestiti dal Certificatore InfoCert secondo le procedure indicate nel presente manuale Operativo, analoghe a quelle già definite per i Certificati di Sottoscrizione (cfr. il relativo Manuale Operativo, ICERT-INDI-MO): i Certificati di Autenticazione devono essere utilizzati nell'ambito dei protocolli S/MIME e SSL, con strumenti quali i Web browser e i prodotti di posta elettronica per verificare firme elettroniche avanzate create tramite dispositivo sicuro. Possono, se richiesto, inoltre essere adoperati per l'autenticazione dell'utente nell'accesso a domini gestiti da server Microsoft (SmartLogon).

Pubblicando tale Manuale Operativo e inserendo i riferimenti a tale documento nei Certificati, il Certificatore consente ai Richiedenti e agli Utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione.

2.1 Identificazione del documento

Questo documento è denominato "**Certificati di Autenticazione - Manuale Operativo**" ed è caratterizzato dal codice documento: **ICERT-INDI-MOCA**.

La versione e la data di emissione sono identificabili in calce ad ogni pagina.

L'*object identifier* (OID) di questo documento, referenziato nei certificati, è il seguente: 1.3.76.36.1.1.3
Tale OID identifica:

InfoCert	1.3.76.36
Certification-service-provider	1.3.76.36.1
certificate-policy	1.3.76.36.1.1
cp-certificati-di-autenticazione	1.3.76.36.1.1.3

Questo documento è distribuito in formato elettronico presso il sito Web del Certificatore all'indirizzo http://www.firma.infocert.it/doc/manuali.htm.

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCert è il **Certificatore** che emette, pubblica nel registro e revoca i **Certificati di Autenticazione**, operando in conformità a quanto descritto nel presente manuale operativo.
I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Tabella 2

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Piazza Sallustio 9 00187 Roma**
Sede operativa	**Via G.B. Morgagni 30H 00161 Roma**
Rappresentante legale	**Fernando Zilio** In qualità di Presidente del Consiglio d'Amministrazione
Amministratore Delegato	
N° telefono	**06-442851**
N° fax	**06-44285255**
N° Iscrizione Registro Imprese	**Codice Fiscale 07945211006**
N° partita IVA	**07945211006**
Sito web	http://www.firma.infocert.it/

2.2.2 Uffici di Registrazione

Il Certificatore si avvale, sul territorio, di Uffici di Registrazione, che, anche tramite loro incaricati, svolgono le seguenti attività di interfaccia tra il Certificatore stesso e il Richiedente:

- Identificazione e registrazione del Richiedente;
- validazione della richiesta del certificato;
- distribuzione ed inizializzazione del dispositivo sicuro di firma (Smart card);
- attivazione della procedura di certificazione della chiave pubblica del Richiedente/Titolare;
- supporto al Titolare e al Certificatore nel rinnovo, revoca e sospensione dei certificati.

Gli Uffici di Registrazione sono attivati dal Certificatore a seguito di un adeguato addestramento del personale impiegato, che potrà svolgere le funzioni di identificazione, ed eventualmente registrazione, 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

Le liste di revoca e di sospensione dei certificati sono pubblicate in un **registro pubblico** che contiene anche i certificati dei titolari che ne hanno fatto espressa richiesta.

Il registro dei certificati, che contiene **tutti** i certificati emessi dal Certificatore, **non** è pubblico.
Il Certificatore utilizza sistemi affidabili per la gestione del **registro pubblico** e del **registro dei certificati** con modalità tali da garantire che soltanto le persone autorizzate possano effettuare inserimenti e modifiche, che l'autenticità delle informazioni sia verificabile, che i certificati siano accessibili alla consultazione del pubblico soltanto nei casi consentiti dal Titolare del certificato e che l'operatore possa rendersi conto di qualsiasi evento che comprometta i requisiti di sicurezza.
L'indirizzo e le modalità di accesso al registro sono descritte al § 6.3.3.

2.2.4 Applicabilità

L'ambito d'utilizzo del Certificato di Autenticazione è costituito dai prodotti di posta elettronica e dai Web browser, oltre a specifiche applicazioni rilasciate o approvate dal Certificatore.

Con i prodotti di posta elettronica, tramite lo standard **S/MIME**, è possibile utilizzare il Certificato di Autenticazione per verificare l'identità del mittente di un messaggio oltre che per garantirne la riservatezza e l'integrità del contenuto.
Con i Web browser, attraverso lo standard **SSL**, è possibile verificare l'identità di un soggetto in possesso del Certificato di Autenticazione che si connetta ad un dominio a sua volta certificato.
Più generalmente, un soggetto, attraverso l'utilizzo della chiave privata, per la cui corrispondente chiave pubblica esista un Certificato di Autenticazione, genera una firma elettronica avanzata che assicura l'origine delle informazioni da lui trasmesse in rete e la loro integrità (non alterazione da parte di terzi).
Nei domini di rete Microsoft è possibile utilizzare funzioni di autenticazione forte basate su smart card (smart logon). Per tale utilizzo, oltre alle informazioni base identificative del Titolare, nel certificato possono essere inserite informazioni di controllo tipiche dell'ambiente Microsoft necessarie ad abilitare tali servizi.

Affinché un Utente possa fare affidamento sull'utilizzo di una chiave privata, il Certificato corrispondente deve essere valido, cioè non scaduto, sospeso o revocato.
Nel caso in cui un certificato di un Titolare venga utilizzato allo scopo di inviare allo stesso un messaggio cifrato (riservatezza del contenuto), la perdita della chiave privata da parte del Titolare comporterà l'impossibilità di decifrare il messaggio: il Certificatore, infatti, non effettua, in nessun caso, il backup della chiave privata del Titolare.

In presenza di accordi di certificazione, il Certificatore riconosce la validità delle regole del certificatore con cui stipula l'accordo e viceversa. 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 e comunicazioni

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.
Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

InfoCert S.p.A.
Responsabile Certificazione Digitale e Sistemi
Corso Stati Uniti 14
35127 Padova

Telefono: 049 828 8111
Fax : 049 828 8406

Call Center Firma Digitale: 199.500.130.

Web: http://www.firma.infocert.it
e-mail: firma.digitale@infocert.it

Le comunicazioni del Certificatore verso il Richiedente saranno effettuate via posta elettronica all'indirizzo dichiarato dal Richiedente medesimo al momento della Identificazione.

3. Regole Generali

In questo capitolo sono descritte 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:

1. l'associazione tra il Titolare e la chiave pubblica certificata;
2. di non rendersi depositario di chiavi private relative ai corrispondenti Certificati di Autenticazione;
3. il rilascio e il rinnovo di un certificato richiesto secondo le presenti procedure e la sua accessibilità per via telematica;
4. la revoca o la sospensione del certificato dandone tempestiva pubblicità secondo le previsioni del presente Manuale Operativo;
5. la protezione accurata delle proprie chiavi private mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
6. la gestione delle operazioni e dell'infrastruttura relativa al servizio di certificazione digitale secondo le regole e procedure descritte nel presente Manuale Operativo;
7. l'adeguamento del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, Decreto Legislativo 30 giugno 2003, n.196.

3.1.2 Obblighi dell'Ufficio di Registrazione

L'Ufficio di Registrazione è tenuto a garantire:

1. la verifica d'identità del Richiedente e la registrazione dei dati dello stesso;
2. che lo stesso Richiedente sia espressamente informato riguardo alla necessità di protezione della segretezza della chiave privata ed alla conservazione ed all'uso dei dispositivi sicuri di firma;
3. la comunicazione al Certificatore di tutti i dati e documenti acquisiti in fase di identificazione allo scopo di attivare la procedura di emissione del certificato;
4. la verifica e l'inoltro al Certificatore delle richieste di revoca o di sospensione attivate dal Titolare presso l'Ufficio di Registrazione;
5. che le operazioni relative al servizio di certificazione digitale, affidate all'Ufficio di Registrazione dal Certificatore, siano effettuate secondo le regole e procedure descritte nel presente Manuale Operativo;
6. la rispondenza del proprio sistema di sicurezza dei dati alle misure minime di sicurezza per il trattamento dei dati personali, Decreto Legislativo 30 giugno 2003, n.196.

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

3.1.3 Obblighi dei Titolari

Il Titolare è tenuto a:

1. garantire la correttezza, la completezza e l'attualità delle informazioni fornite al Certificatore per la richiesta di certificato;

2. proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
3. proteggere e conservare il codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità del dispositivo sicuro di firma, in luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;
4. proteggere e conservare il codice di sblocco (PUK) utilizzato per la riattivazione del dispositivo sicuro di firma in luogo protetto e diverso da quello in cui è custodito il dispositivo stesso;
5. adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e del dispositivo sicuro di firma;
6. utilizzare personalmente il dispositivo sicuro di firma non cedendolo o dandolo in uso a terzi;
7. utilizzare le chiavi e il certificato per le sole modalità previste nel presente Manuale Operativo;
8. inoltrare al Certificatore senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo (§ 6.4);
9. adottare 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. conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel presente Manuale Operativo;
2. verificare la validità del certificato prima di usare la chiave pubblica in esso contenuta. La validità del certificato viene accertata verificando che questo non sia scaduto, o non sia stato revocato o sospeso;
3. utilizzare i dati contenuti nel registro dei certificati (es. liste di revoca) solo ai fini di verifica di validità del certificato;
4. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

L'Utente è l'unico responsabile per gli utilizzi del certificato posti in essere in maniera non conforme a quanto sopra indicato.

3.2 Responsabilità

3.2.1 Limitazioni di responsabilità

Il Certificatore in nessun caso risponderà di eventi ad esso non imputabili ed in particolare di danni subiti dall'Ufficio di Registrazione, dal Titolare, dal Richiedente, dagli Utenti o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.
Il Certificatore non sarà responsabile di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

3.2.2 Clausola risolutiva espressa

Il Certificatore ha facoltà di risolvere il rapporto contrattuale, ai sensi dell'articolo 1456 del codice civile, secondo quanto previsto nel contratto intercorso con la controparte.

3.3 Pubblicazione

3.3.1 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, disponibile sia presso il Certificatore che presso gli Uffici di Registrazione.

3.3.2 Pubblicazione dei certificati

I certificati emessi usualmente non sono pubblicati.
L'utente che voglia rendere pubblico il proprio certificato può farne richiesta inviando l'apposito modulo (disponibile sul sito www.firma.infocert.it), firmato digitalmente con la chiave corrispondente al certificato di cui è richiesta la pubblicazione. L'invio deve avvenire via e-mail indirizzata a richiesta.pubblicazione@cert.legalmail.it seguendo la procedura descritta sul sito stesso.

3.3.3 Pubblicazione delle liste di revoca e sospensione

Le liste di revoca e di sospensione sono pubblicate nel registro pubblico dei certificati accessibile con protocollo LDAP all'indirizzo: **ldap://ldap.infocert.it**
Tale accesso può essere effettuato tramite i software messi a disposizione dal Certificatore e/o le funzionalità presenti nei prodotti disponibili sul mercato che interpretano il protocollo LDAP.
Il Certificatore potrà rendere disponibili altre modalità oltre a quella indicata per consultare la lista dei certificati pubblicati e la loro validità.

3.4 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, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (es. chiave pubblica, certificato, date di revoca e di sospensione del certificato).
In particolare i dati personali vengono trattati dal Certificatore in conformità con il Decreto Legislativo 30 giugno 2003, n.196.

3.5 Tariffe

3.5.1 Rilascio e rinnovo del certificato

Sono previste tariffe riguardanti l'emissione e il rinnovo del Certificato di Autenticazione. Tali tariffe sono funzione delle quantità trattate e soggette all'andamento del mercato.
Le tariffe sono disponibili presso gli Uffici di Registrazione.

Il costo del dispositivo sicuro di firma (che può essere già a disposizione del Titolare per il Certificato di Sottoscrizione) e del lettore di smart card non sono compresi in queste tariffe.

3.5.2 Revoca e sospensione del certificato

La revoca e sospensione del Certificato è gratuita.

3.5.3 Accesso al certificato e alle liste di revoca

L'accesso al **registro pubblico** (certificati pubblicati e lista dei certificati revocati o sospesi) è libero e gratuito.

4. Amministrazione del Manuale Operativo

4.1 Procedure per l'aggiornamento

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

Errori, aggiornamenti o suggerimenti di modifiche possono essere comunicati al contatto per gli utenti indicato al § 2.3.
Correzioni editoriali e tipografiche e altre modifiche minori 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 modifica tecnica o procedurale a questo manuale operativo verrà prontamente comunicata agli Uffici di Registrazione.

4.2 Regole per la pubblicazione e la notifica

Il Manuale Operativo è pubblicato:
- in formato elettronico sul sito Web del Certificatore all'indirizzo http://www.firma.infocert.it/doc/manuali.htm
- in formato cartaceo può essere richiesto agli Uffici di Registrazione o al contatto per gli utenti finali (vedi §. 2.3).

4.3 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Responsabile di "Certificazione Digitale e Sistemi" e dal Responsabile di "Amministrazione, Controllo di gestione e Legale" di InfoCert.

5. Identificazione e Autenticazione

Questo capitolo descrive le procedure usate per:
- l'identificazione del Richiedente al momento della richiesta di rilascio del certificato di Autenticazione;
- l'autenticazione del Titolare, nel caso di rinnovo, revoca e sospensione di certificati di Autenticazione.

5.1 Identificazione ai fini del primo rilascio

Il Certificatore verifica con certezza l'identità del Richiedente prima di procedere al rilascio del certificato di Autenticazione richiesto.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente da uno dei soggetti di cui al § 5.1.1, 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) in corso di validità.

5.1.1 Soggetti abilitati ad effettuare l'identificazione

L'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati:

1. Il Certificatore, anche tramite suoi Incaricati;
2. L'Ufficio di Registrazione, anche tramite suoi Incaricati;
3. Un Pubblico Ufficiale.

5.1.2 Procedure per l'identificazione

L'identificazione è effettuata da uno dei soggetti indicati al § 5.1.1 ed è richiesta la presenza fisica del Richiedente.

Il soggetto che effettua l'identificazione verifica l'identità del Richiedente tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'art. 35, Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445:

- Carta d'identità
- Passaporto
- Patente di guida
- Patente nautica
- Libretto di pensione
- Patentino di abilitazione alla conduzione di impianti termici
- Porto d'armi

Sono ammesse ulteriori tessere di riconoscimento oltre a quelle indicate, purché munite di fotografia e di timbro, rilasciate da un'Amministrazione dello Stato.

Al momento dell'identificazione viene fornito al Richiedente un codice di emergenza, che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e lo stesso Titolare.

L'identificazione da parte dei Pubblici Ufficiali può essere altresì effettuata in base a quanto disposto dalle normative che disciplinano la loro attività, ivi comprese le disposizioni di cui al D.L. 3 maggio 1991, n. 143 e successive modifiche ed integrazioni.

5.1.2.1 Richiesta di rilascio del certificato

I passi principali a cui il Richiedente deve attenersi per ottenere un certificato di Autenticazione sono:

a) prendere visione del presente Manuale Operativo e dell'eventuale ulteriore documentazione informativa;
b) seguire le procedure di identificazione adottate dal Certificatore come descritte nei paragrafi che seguono;
c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
d) sottoscrivere la richiesta di registrazione accettando le condizioni contrattuali che disciplinano l'erogazione del servizio.

5.1.2.2 Informazioni che il Richiedente deve fornire

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra il Certificatore ed il Richiedente/Titolare. Il modulo di richiesta deve essere sottoscritto dal Richiedente/Titolare.

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
- Indirizzo di posta elettronica personale del Titolare.

5.2 Autenticazione per 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).*

NOTA
le date indicate negli attributi suddetti sono espresse nel formato

anno-mese-giorno-ore-minuti-secondi-timezone
{AAAAMMGGHHMMSSZ}

nella rappresentazione UTCTime prevista dallo standard di riferimento [7].

Al di fuori di questo intervallo di date, comprensive di ore, minuti e secondi, il certificato è da considerarsi non valido.

Il Titolare del certificato può rinnovarlo, prima della sua scadenza, inviando al Certificatore la richiesta di rinnovo autenticata con la firma elettronica avanzata: quest'ultima è generata con la chiave privata della coppia di chiavi da rinnovare.

5.3 Autenticazione per richiesta di Revoca o di Sospensione

La revoca o sospensione del certificato può avvenire:

- su richiesta del Titolare;
- su iniziativa del Certificatore.

Il Certificatore verifica la provenienza della richiesta di revoca o di sospensione.

5.3.1 Revoca o Sospensione su richiesta del Titolare

Il Certificatore, anche tramite l'Ufficio di Registrazione, autentica il Titolare richiedente la revoca o sospensione e si accerta delle motivazioni della stessa.

Se la richiesta viene effettuata per telefono o via Internet, per la sola sospensione il Titolare si autentica fornendo il codice di emergenza, consegnato assieme al certificato che intende revocare.
Se la richiesta viene fatta presso l'Ufficio di Registrazione, l'autenticazione del Titolare avviene con le modalità previste per l'identificazione.

6. Operatività

Questo capitolo descrive le operazioni necessarie per compiere le attività di emissione, revoca, sospensione e rinnovo di un Certificato di Autenticazione.

6.1 Registrazione iniziale

Per procedere all'emissione del certificato è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore.
La registrazione iniziale è effettuata presso il Certificatore oppure presso un Ufficio di Registrazione.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e la consegna del dispositivo sicuro di firma sono previste due diverse modalità.

La prima modalità (nel seguito **Caso A**) consente al Titolare/Richiedente di concludere la procedura di certificazione entrando in possesso della smart card e del certificato di autenticazione immediatamente dopo la registrazione: in questo caso il RAO avvierà la procedura di generazione della coppia di chiavi e, effettuate le opportune verifiche, di emissione del certificato in presenza del Richiedente/Titolare.

La seconda modalità (nel seguito **Caso B**) prevede una separazione tra la fase di identificazione, effettuata in presenza del Richiedente, Titolare del certificato, e quella di registrazione ed emissione dello stesso, che viene effettuata successivamente dai RAO.
In entrambi i casi la smart card viene personalizzata a cura del Certificatore con il PIN consegnato al Richiedente al momento dell'identificazione.
Nel **Caso B** la smart card personalizzata è consegnata al Richiedente (ora Titolare) in un secondo momento.

Le modalità operative per la registrazione iniziale, il rilascio del certificato e la consegna della smart card, nei casi di identificazione da parte di un Pubblico Ufficiale, anche se svolte all'estero, sono descritte separatamente nell'appendice A del presente Manuale Operativo.

6.2 Rilascio del certificato

6.2.1 Caso A: Chiavi generate in presenza del Richiedente

Questa procedura prevede la presenza del Richiedente/Titolare in possesso della carta a microprocessore presso un Ufficio di Registrazione o presso il Certificatore.

1. Il RAO, contestualmente all'identificazione, registra il Titolare e attiva la procedura di rilascio di certificato.
1. La procedura automatica sblocca il dispositivo sicuro di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia. Nel caso in cui il dispositivo sicuro di firma abbia un PIN differente da quello di default, la procedura richiede l'inserimento del PIN da parte del Titolare.
2. Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica del Richiedente e la invia al Certificatore.
3. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo sicuro di firma inserendo il PIN già consegnato al Richiedente in fase di identificazione

6.2.2 Caso B: Chiavi generate dal Certificatore

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

1. Il RAO seleziona i dati di registrazione di un Richiedente/Titolare e attiva la procedura di richiesta di certificato.
2. La procedura automatica sblocca il dispositivo sicuro di firma con il PIN di default consentendo la generazione della coppia di chiavi di crittografia.
3. Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della smartcard e la invia al Certificatore.
4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza il dispositivo sicuro di firma inserendo il PIN già consegnato al Richiedente in fase di identificazione

La segretezza del PIN personale durante le fasi di personalizzazione della smart card (dispositivo sicuro 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. La smart card così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.

6.2.3 Generazione delle chiavi e protezione delle chiavi private

La coppia di chiavi per la firma è generata dal Titolare utilizzando le funzionalità offerte dalla carta a microprocessore (il dispositivo sicuro di firma o smart card).
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. L'algoritmo di crittografia asimmetrica utilizzato è l'RSA e la lunghezza delle chiavi è di 1024 bit.
Per utilizzare la chiave privata a bordo della smart card il possessore deve autenticarsi correttamente fornendo il proprio PIN segreto.

6.3 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/Titolare sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
   - al Richiedente/Titolare sia stato assegnato un codice identificativo unico nell'ambito degli utenti del Certificatore (IUT);
   - la chiave pubblica che si intende certificare sia una chiave valida e della lunghezza prevista;
   - la richiesta sia autentica e il Titolare possieda la corrispondente chiave privata;
   - la coppia di chiavi funzioni correttamente
2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta
3) si procede alla generazione del certificato e a pubblicarlo nel registro dei certificati;
4) il certificato viene memorizzato all'interno del dispositivo sicuro di firma del Titolare;
5) si distinguono i due casi:
   - (*Caso A*): il Titolare è già in possesso del dispositivo sicuro di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di autenticazione.
   - (*Caso B*): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di Registrazione personalmente al Titolare.

6.3.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni fornite dal Richiedente in fase di identificazione ed indicate nel modulo di richiesta da questo sottoscritto.
Il formato dei certificati è conforme allo standard X.509 V.3.

6.3.2 Validità del certificato

Il certificato ha validità fino a tre anni a partire dalla data di emissione ovvero fino alla data di pubblicazione della sua revoca o sospensione se precedentemente effettuate.

6.3.3 Pubblicazione del certificato

Al buon esito della procedura di certificazione il certificato sarà inserito nel registro di riferimento dei certificati e non sarà reso pubblico. Il Titolare che volesse rendere pubblico il proprio certificato potrà richiederlo tramite la procedura descritta al §3.3.2.

6.3.4 Uso del Certificato

L'ambito d'utilizzo del certificato di Autenticazione è costituito dai prodotti di posta elettronica e di Web browser, oltre a specifiche applicazioni rilasciate dal Certificatore, come descritto al § 2.2.4.

6.4 Revoca e sospensione di un certificato

La revoca o la sospensione di un certificato ne tolgono la validità e rendono **non validi** gli utilizzi della corrispondente chiave privata effettuati 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 e pubblicata con periodicità prestabilita nel registro dei certificati.
La revoca e la sospensione di un certificato hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso e degli utilizzi della corrispondente chiave privata effettuati successivamente a tale momento.

6.4.1 Motivi per la revoca di un certificato

Il Certificatore può eseguire la revoca del certificato su propria iniziativa o su richiesta del Titolare.

E' fatto obbligo di richiedere la revoca nel caso in cui si verifichino le seguenti condizioni:
- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
  - sia stato smarrito o rubato il dispositivo che contiene la chiave privata di firma;

  - sia venuta meno la segretezza della chiave privata o del codice di attivazione per accedervi;
  - si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata;
- il Titolare non riesce più ad utilizzare il dispositivo sicuro di firma contenente la chiave privata in suo possesso (es: guasto del dispositivo sicuro);
- 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 conformità del presente Manuale Operativo.

Il Titolare ha facoltà di richiedere la revoca di un certificato per un qualunque motivo dallo stesso ritenuto valido ed in qualsiasi momento.

6.4.2 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. telefonando al Call Center del Certificatore
2. tramite l'Ufficio di Registrazione presso cui è stato registrato.

Per effettuare la richiesta, il Titolare deve comunicare i propri dati identificativi, l'identificativo univoco a lui assegnato (IUT), la motivazione della revoca, il codice di emergenza. Nell'impossibilità di identificare con certezza il Titolare si potrà procedere con una sospensione del Certificato in attesa della corretta identificazione del richiedente (ad esempio mediante richiesta di revoca formulata per iscritto). Nel caso di richiesta di revoca tramite il Call Center, il Titolare dovrà inviare via fax la richiesta di revoca firmata, corredata da una fotocopia, anch'essa firmata, di un documento di identità in corso di validità.

Revoca su iniziativa del Certificatore

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

1. il Certificatore comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza; la procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

6.4.3 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 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.

6.4.4 Procedura per la richiesta di sospensione

La richiesta di sospensione viene effettuata dai soggetti e secondo le modalità indicate per la richiesta di revoca, **specificando,** in tal caso, anche **la durata del periodo di sospensione.**

La procedura di sospensione è attivabile anche via Internet, dal sito del Certificatore.

Alla scadenza di tale periodo, alla sospensione seguirà o una revoca definitiva oppure la ripresa di validità del certificato.

6.4.5 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).

6.4.6 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 giorno.
L'acquisizione e consultazione della CRL è a cura degli Utenti. La CRL è emessa sempre integralmente.
Il Certificatore si riserva la possibilità di pubblicare separatamente altre CRL, sottoinsiemi della CRL più generale, allo scopo di alleggerire il carico di rete. La CRL da consultare per lo specifico certificato è indicata nel certificato stesso insieme alle informazioni sul protocollo da utilizzare.
Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di richiesta della revoca o sospensione.
Il formato della CRL è conforme allo standard X.509 V3.

6.4.7 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.

6.5 Rinnovo del Certificato

Il certificato ha validità di tre anni dalla data di emissione.
La procedura di rinnovo richiede la generazione di una nuova coppia di chiavi: la richiesta di un nuovo certificato deve essere avviata prima della scadenza dello stesso.
La nuova coppia di chiavi è generata all'interno della carta a microprocessore; l'emissione e la pubblicazione del certificato seguono il procedimento descritto in caso di nuova richiesta.

Le modalità per effettuare la procedura di rinnovo del certificato sono indicate dal Certificatore nel proprio sito (http://www.firma.infocert.it).

7. Gestione ed operatività della CA

7.1 Gestione della 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.

7.2 Gestione delle operazioni

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

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.

7.2.1 Verifiche di sicurezza e qualità

Le procedure operative e di sicurezza del Certificatore sono soggette a controlli periodici legati sia alla verifiche ispettive interne di conformità alle modalità operative previste dallo standard ISO 9001 sia a verifiche di auditing interno. Tali verifiche mirano a controllare 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.

7.3 Procedure di Gestione dei Disastri

Il Certificatore ha adottato le procedure necessarie a garantire la continuità del servizio anche in situazioni di elevata criticità, utilizzando componenti ridondanti e sistemi di riserva.
In caso di disastro le operazioni verranno riprese usando le copie di backup dei dati e dei sistemi crittografici contenenti le chiavi di certificazione.

7.4 Dati archiviati

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

- dati di registrazione dei titolari delle chiavi;
- certificati emessi, sospesi e revocati;
- associazione tra codice identificativo del Titolare e dispositivo di firma;
- dati di sessione al sistema e ai servizi e altri dati necessari a tracciare le operazioni rilevanti ai fini della sicurezza.

L'accesso ai dati contenuti nei diversi archivi è consentito solo a personale opportunamente abilitato, garantendo la riservatezza e l'integrità dei dati.

7.4.1 Procedure di salvataggio dei dati

Il salvataggio 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 a personale opportunamente abilitato. 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.

7.5 Chiavi del Certificatore

Le chiavi di certificazione sono generate a bordo di un apposito hardware crittografico con caratteristiche di sicurezza conformi ad un accreditamento ITSEC E3. La chiave di certificazione utilizzata per firmare i Certificati di Autenticazione è un chiave RSA di lunghezza 2048 bit.

7.6 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.

7.7 Disponibilità del servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati (1) (comprende i certificati e le CRL)	Dalle 00:00 alle 24:00 7 giorni su 7
Revoca e sospensione dei certificati (1)	Dalle 00:00 alle 24:00 7 giorni su 7
Altre attività: registrazione, generazione, pubblicazione, rinnovo (2)	Lun – Ven: dalle 09:00 alle 18:00 Sabato: dalle 09:00 alle 12:00 Festività escluse

(1) Il servizio potrà non essere disponibile nella fascia oraria indicata per fermi di manutenzione o per cause di forza maggiore.
(2) L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono avere diversi orari di sportello. In ogni caso il Certificatore garantisce l'erogazione del proprio servizio negli orari sopra riportati.

8. Appendice A: Modalità operative in caso di Identificazione da parte di Pubblico Ufficiale

8.1 A.1: Modalità operative in caso di Identificazione da parte di Pubblici Ufficiali in Italia

Alla data, la procedura di rilascio del certificato in caso di identificazione da parte di Pubblici Ufficiali in Italia non è ancora predisposta.

8.2 A.2: Modalità operative in caso di Identificazione da parte di Pubblici Ufficiali all'estero

Alla data, la procedura di rilascio del certificato in caso di identificazione da parte di Pubblici Ufficiali all'estero non è ancora predisposta.