Certificati SIAE Manuale Operativo

Ente Certificatore InfoCerte

Certificati per SIAE

Manuale Operativo

Codice documento: ICERT-INDI-SIAE

Versione 2.2

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento.....5
1.1 Novità introdotte rispetto alla precedente emissione.....5
1.2 Scopo e campo di applicazione del documento.....5
1.3 Riferimenti.....6
1.4 Definizioni 6
1.5 Acronimi e abbreviazioni.....8
2. Generalità.....9
2.1 Identificazione del documento.....9
2.2 Attori e Domini applicativi.....10
2.2.1 Certificatore.....10
2.2.2 Autorità di Registrazione.....10
2.2.3 Uffici di Registrazione.....10
2.2.4 CMS.....11
2.2.5 Richiedente/Titolare del certificato.....11
2.2.6 Utilizzatore.....11
2.2.7 Registro dei Certificati.....11
2.2.8 Applicabilità.....11
2.3 Contatto per utenti finali.....12
3. Regole Generali.....12
3.1 Obblighi e Responsabilità.....12
3.1.1 Obblighi del Certificatore 12
3.1.2 Obblighi degli Incaricati alla Registrazione.....12
3.1.3 Obblighi del CMS.....13
3.1.4 Obblighi dei Richiedenti/Titolari 13
3.1.5 Obblighi degli Utilizzatori.....13
3.2 Responsabilità.....14
3.2.1 Limitazioni di responsabilità del Certificatore.....14
3.2.2 Comunicazioni.....14
3.3 Pubblicazione 14
3.3.1 Pubblicazione di informazioni inerenti SIAE.....14
3.3.2 Pubblicazione dei certificati.....14
3.4 Tutela dei dati personali 14
4. Amministrazione del Manuale Operativo.....14
4.1 Procedure per l'aggiornamento.....14
4.2 Regole per la pubblicazione e la notifica.....15
4.3 Responsabile dell'approvazione 15
5. Identificazione.....15

5.1 Registrazione iniziale....15
5.2 Rinnovo delle chiavi e certificati....16
5.3 Richiesta di Revoca o di Sospensione....16
6. Operatività....17
6.1 Registrazione dei Richiedenti....17
6.1.1 Registrazione degli Richiedenti/ Titolari....17
6.1.2 Registrazione dei Responsabili CMS....18
6.2 Richiesta di certificazione per utenti SIAE....18
6.3 Emissione del certificato....19
6.3.1 Emissione del certificato SIAE e rilascio della carta di attivazione al Titolare....19
6.3.2 Emissione del certificato SIAE-CMS....20
6.3.3 Validità del certificato....20
6.4 Pubblicazione del certificato....20
6.5 Uso del Certificato....21
6.5.1 Certificato SIAE....21
6.5.2 Certificato SIAE-CMS....21
6.6 Revoca e sospensione di un certificato....21
6.6.1 Motivi per la revoca di un certificato....21
6.6.2 Procedura per la richiesta di revoca....22
6.6.3 Motivi per la Sospensione di un certificato....23
6.6.4 Pubblicazione e frequenza di emissione della CRL....23
6.6.5 Tempistica....23
6.7 Rinnovo del Certificato....23
6.8 Restituzione della Smart card a fine ciclo di vita o per sua rottura....24
6.9 Interruzione attività di biglietteria....24
6.10 Furto o smarrimento Smart card....24
6.11 Ritrovamento Smart card precedentemente denunciate....24
7. Gestione ed operatività della CA....24
7.1 Gestione della sicurezza....24
7.2 Gestione delle operazioni....25
7.2.1 Verifiche di sicurezza e qualità....25
7.3 Procedure di Gestione dei Disastri....25
7.4 Dati archiviati....25
7.4.1 Procedure di salvataggio dei dati....26
7.5 Chiavi del Certificatore....26
7.6 Sistema di qualità....26
7.7 Disponibilità del servizio....26
8. Appendice A: Profilo dei Certificati e delle CRL....27
A1. Certificato della CA "Servizi di Certificazione"....27
A2. Profilo del Certificato SIAE....28
A3. Profilo del Certificato SIAE-CMS....29
A3. Profilo della CRL....31

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	2.2	**Data Versione/Release** :	11/2/2008
Descrizione modifiche:	Correzioni		
Motivazioni :	Corrette alcune diciture e Inserita la possibilità di emettere il certificato CMS ad un dipendete generico SIAE. Modificato il numero della release		

Versione/Release n° :	1.1	**Data Versione/Release** :	23/1/2008
Descrizione modifiche:	Allungamento del periodo di validità del certificato		
Motivazioni :	La data di scadenza del certificato descritto in questo manuale è stata portata dal 1.2.2008 a Tre Anni.		

Versione/Release n° :	1.0	**Data Versione/Release** :	5/5/2007
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione InfoCert		

1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole che governano l'emissione e l'utilizzo dei **Certificati SIAE** sottoscritti dal Certificatore InfoCert nell'ambito della "Fornitura di servizi per l'emissione di certificati X.509 da utilizzare nelle smart card destinate ai sistemi di emissione dei biglietti" (Lettera 08/10/2002 Prot. SIAE 06/152).
Il manuale descrive le procedure operative adottate dal Certificatore stesso per il rilascio di certificati digitali da utilizzare con carte di attivazione nell'ambito esclusivo del "Sistema Informatico di Emissione dei Titoli di Accesso" (SIETA) e quelle per l'emissione e gestione dei certificati per i Responsabili del Card Management System SIAE (Certificati SIAE-CMS).

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

Per la compilazione del presente manuale operativo 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

[1] Decreto del Presidente della Repubblica 7 Aprile 2003, n.137 (G.U. n.138 del 17 Giugno 2003)Decreto del Presidente della Repubblica 7 Aprile 2003, n.137 (G.U. n.138 del 17 Giugno 2003)

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

[3] 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.

[4] 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)

[5] 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

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

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

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

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

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

[11] PKCS 12 v.1.0: Personal Information Exchange Syntax

[12] Decreto 13-Lug-2000 (GU 171 del 24 Lug 2000)

[13] Provvedimento Ag. delle entrate 23-Lug-2001 (Supplemento ordinario alla GU 212 del 12-Set-2001)

[14] Provvedimento 22 ottobre 2002 dell’Agenzia delle entrate (G. U. n. 258 del 4/11/2002)

[15] Decreto Legislativo 23 Gennaio 2002, n. 10 (G.U. n. 39 del 15 febbraio 2002)

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal DPR 445/2000 [1] e dal DPCM 8 febbraio 1999 [2] si riportano le definizioni stabilite dagli stessi decreti. 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 effettua tra Certification Authority appartenenti a domini diversi. In questo processo i certificatori si certificano l’un l’altro. Condizione necessaria affinché possa avvenire la *cross-certification* è che i certificatori accettino e condividano le regole dei rispettivi Manuali Operativi.

Autorità di Registrazione (RA)

L’entità cui è data la responsabilità di registrare gli utenti, controllarne l’identità, verificarne il possesso dei requisiti richiesti per ottenere il rilascio del certificato, verificare la titolarità dei dati presenti nella richiesta di certificazione e verificare il possesso, in caso di generazione delle chiavi da parte del Titolare, della chiave privata corrispondente a quella pubblica di cui è richiesta la certificazione.

Carta di Attivazione
La Smart Card oggetto del provvedimento normativo di cui al riferimento 1.3.

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, tra le altre informazioni:
- il Certificatore che lo ha emesso
- il periodo di tempo in cui il certificato può essere utilizzato;
- alcuni campi (estensioni) che determinano caratteristiche aggiuntive al certificato.

Certificatore *[Certification Authority – CA]*
Il soggetto pubblico o privato che effettua la certificazione, rilascia il certificato della chiave pubblica, lo pubblica unitamente a quest'ultima, pubblica ed aggiorna le liste dei certificati sospesi e revocati.

Chiave Privata e Chiave Pubblica
La coppia di chiavi crittografiche asimmetriche, una privata ed una pubblica, correlate tra loro, da utilizzarsi nell'ambito dei sistemi di validazione o di cifratura di documenti informatici.

Card Management System (CMS)
È il sistema SIAE che provvede alla personalizzazione grafica ed elettrica delle smart card sulla base dei dati degli utenti richiedenti la carta di attivazione. E', inoltre, l'unico punto autorizzato ad inviare richieste di emissione, rinnovo, revoca e sospensione dei certificati SIAE all'Ente Certificatore InfoCert.

Dispositivo per la creazione della firma
Il programma informatico adeguatamente configurato (software) o l'apparato strumentale (hardware) usati per la creazione della firma elettronica

Dispositivo sicuro per la creazione della firma
E' un apparato elettronico in grado di conservare in modo protetto le chiavi private e di generare al suo interno firme digitali. 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]*
Il risultato della procedura informatica (validazione) basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al sottoscrittore tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

Help Desk SIAE
Punto di contatto per clienti SIAE, a cui i Titolari della carta di attivazione debbono rivolgersi per le richieste di revoca o sospensione dei propri certificati.

Incaricati alla Registrazione SIAE
Gli Incaricati alla Registrazione possono essere dipendenti SIAE, appartenenti a sue strutture distribuite sul territorio, oppure Mandatari, legati a SIAE da rapporti contrattuali esclusivi. Svolgono, principalmente, le seguenti attività:
- identificazione fisica degli utenti nelle modalità indicate nel presente manuale operativo (§ 5.1);
- inoltro dei dati del Richiedente per l'archiviazione nel sistema di data entry della Direzione Generale SIAE;
- consegna e "collaudo" della smart card in presenza dell'utente Titolare presso l'Ufficio di Registrazione.

Gli Incaricati alla Registrazione eseguono, in sostanza, tutte le operazioni preliminari di identificazione e raccolta dei dati relativi ai richiedenti la carta di attivazione.

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 *[digital time stamping]*

Il risultato della procedura informatica, con cui si attribuiscono, ad uno o più documenti informatici, una data ed un orario opponibili ai terzi.

Manuale Operativo

Il Manuale Operativo definisce le procedure che il Certificatore applica nello svolgimento del servizio e le regole che definiscono l'applicabilità del Certificato. Si tratta di un'equivalente dei documenti noti come CP (Certificate Policy) e CPS (Certification Practice Statement). Nella stesura del Manuale sono state seguite le indicazioni della letteratura internazionale [4] [5] [6].

Registration Authority Officer (RAO)

E' il responsabile dell'attivazione e gestione del CMS: è responsabile, inoltre, della sottoscrizione delle richieste di emissione e rinnovo dei certificati da inviare alla CA InfoCert.

Registro dei Certificati *[Directory]*

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.

Richiedente

Il Richiedente è la persona fisica che si reca personalmente presso gli Uffici di Registrazione e richiede il rilascio di una o più carte di attivazione per l'uso nell'ambito di SIETA, accettando le condizioni procedurali indicate nel presente manuale operativo. La smart card rilasciata contiene una coppia di chiavi asimmetriche la cui corrispondente chiave pubblica è certificata dal certificatore InfoCert.

Titolare di Biglietteria *[Subject /Subscriber]*

I titolari di Biglietteria sono persone che sono entrate in possesso della carta di attivazione secondo le modalità previste nel presente manuale operativo avendone fatto richiesta all'Agenzia delle entrate: risultano di conseguenza anche i titolari dei certificati a chiave pubblica in essa contenuti.

Utilizzatore o Utente Utilizzatore *[Relying Party]*

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

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.

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.

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.

PASSPHRASE/PIN – Personal Identification Number
Codice associato ad un dispositivo di firma, utilizzato dal Titolare per autenticarsi con lo stesso e ottenere l'accesso alle sue funzioni.

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

Codice di revoca
Codice riservato consegnato dalla SIAE ai Titolari per la loro identificazione in caso di richiesta telefonica all'Help Desk SIAE di revoca o sospensione.

2. Generalità

Un certificato digitale associa una chiave pubblica di crittografia ad un insieme di informazioni che identificano il soggetto possessore della corrispondente chiave privata, chiamato anche Titolare della coppia di chiavi asimmetriche (pubblica e privata). Il certificato è utilizzato da altri soggetti (gli Utilizzatori) per recuperare la chiave pubblica, contenuta e distribuita con il certificato, e verificare, tramite questa, la firma digitale creata con la corrispondente chiave privata.

Il certificato garantisce la corrispondenza tra la chiave pubblica e la persona Titolare: il grado di affidabilità di questa associazione dipende da diversi fattori: 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.

Il presente documento contiene le regole che governano l'emissione e l'uso dei **Certificati SIAE** e **SIAE-CMS** sottoscritti dal Certificatore InfoCert.

I **Certificati SIAE** sono rilasciati e gestiti dal Certificatore InfoCert previa registrazione dei Richiedenti secondo le procedure di identificazione stabilite da SIAE medesima.
Detti certificati sono rivolti principalmente all'uso nell'ambito dei protocolli S/MIME e SSL e utilizzabili esclusivamente in quello delle applicazioni funzionali al SIETA.
I certificati SIAE-CMS sono certificati memorizzati, insieme alle relative chiavi, in un file secondo le specifiche PKCS#12 e utilizzabili dal Responsabile CMS per la sottoscrizione delle richieste inviate dal CMS medesimo alla CA.

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.

2.1 Identificazione del documento

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

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

L'*object identifier* (OID) di questo documento è il seguente: **1.3.76.36.1.1.3.1**
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-SIAE	1.3.76.36.1.1.3.1

Questo documento è distribuito in formato elettronico presso il sito Web del Certificatore all'indirizzo: http://www.firma.infocert.it/doc/manuali.htm e sul sito di SIAE all'indirizzo http://www.siae.it/Erario.asp selezionando il link Biglietterie automatizzate e di li' Manuale Operativo Carta d'Attivazione.

2.2 Attori e Domini applicativi

2.2.1 Certificatore

InfoCert è il **Certificatore** che emette, pubblica nel registro e revoca i **Certificati SIAE** e **SIAE-CMS**, operando nelle modalità di seguito descritte.
I dati completi dell'organizzazione che svolge la funzione di Certificatore sono i seguenti:

Tabella 2

Denominazione Sociale	**InfoCert - Società per azioni**
Sede legale	**Via G.B. Morgagni 30H 00161 Roma**
Rappresentante legale	**Dott. Daniele Vaccarino** 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/
Sede Operativa	**Corso Stati Uniti, 14bis– 35127 Padova**

2.2.2 Autorità di Registrazione

Il ruolo di Autorità di Registrazione è svolto dalla SIAE.

2.2.3 Uffici di Registrazione

Gli Uffici di Registrazione sono uffici autorizzati SIAE presso i quali gli Incaricati alla Registrazione effettuano l'**identificazione e registrazione degli utenti Richiedenti**.

Le seguenti attività sono invece svolte presso la sede del Titolare:

- distribuzione al Titolare del dispositivo di firma e della busta contenente il codice di attivazione, di sblocco e di richiesta di revoca/sospensione del certificato e contestuale collaudo delle funzionalità della carta.
- supporto al Titolare nel rinnovo della smart card e revoca/sospensione dei certificati.

2.2.4 CMS

E' l'area della Direzione Generale SIAE che provvede alla personalizzazione delle smart card e all'interfacciamento con la CA InfoCert per quanto riguarda le richieste di emissione, revoca, sospensione e rinnovo dei certificati.

Il CMS è tenuto a rispettare le modalità di comunicazione previste tra SIAE e InfoCert ed è responsabile del contenuto delle comunicazioni trasmesse da SIAE ad InfoCert.

Una o più persone fisiche ad esso appartenenti sono esplicitamente e formalmente incaricate da SIAE come responsabili della sottoscrizione delle richieste che il CMS invierà alla CA: ad ognuna di loro verrà rilasciato un certificato digitale personale SIAE-CMS memorizzato su file con cui firmare e convalidare le suddette richieste.

2.2.5 Richiedente/Titolare del certificato

I Titolari del certificato possono essere unicamente persone fisiche Titolari di una Biglietteria, o altre persone fisiche da questi delegati con atto notarile. Ad essi è attribuita una o più coppie di chiavi asimmetriche (di cui sono "titolari") la cui chiave pubblica è certificata dal Certificatore.

Le comunicazioni verso il Titolare saranno effettuate dal personale autorizzato SIAE, via posta elettronica all'indirizzo dichiarato dal Richiedente al momento della Registrazione.

2.2.6 Utilizzatore

L'Utilizzatore (o Utente Utilizzatore) è il soggetto che fa affidamento su un certificato digitale emesso dal Certificatore, nei termini del presente Manuale Operativo. Tale affidamento ha quale presupposto l'obbligo da parte dell'Utilizzatore di accedere al Registro dei Certificati del Certificatore per verificare l'esistenza del certificato e la sua validità, controllando tramite la CRL eventuali revoche o sospensioni.
Nello specifico dei **Certificati SIAE**, l'Utilizzatore è la SIAE stessa, con esclusione di eventuali ulteriori soggetti, per la verifica dei dati trasmessi dai Titolari.

2.2.7 Registro dei Certificati

Tutti i certificati emessi dal Certificatore sono pubblicati nel registro dei certificati come pure le relative liste di revoca e sospensione.
L'indirizzo e le modalità di accesso al registro sono descritte al § 6.4.

2.2.8 Applicabilità

In generale, un soggetto tramite sottoscrizione con la propria chiave privata, la cui corrispondente chiave pubblica sia stata certificata da una CA riconosciuta, assicura l'origine e l'integrità delle informazioni da lui trasmesse in rete, consentendo di individuare eventuali alterazioni da parte di terzi.
Affinché un Utilizzatore possa fare affidamento sulla firma ricevuta, il certificato corrispondente deve essere valido, cioè non scaduto, sospeso o revocato.

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.

L'ambito d'utilizzo del **Certificato SIAE** è limitato alle applicazioni funzionali all'esecuzione delle attività previste per il progetto SIETA.

Il **certificato SIAE-CMS** è utilizzabile esclusivamente per la firma delle richieste di certificazione, revoca o sospensione e rinnovo inviate alla CA InfoCert da parte del CMS.

2.3 Contatto per utenti finali

InfoCert è responsabile della definizione, pubblicazione ed aggiornamento di questo documento, previo accordo con la SIAE

Per questioni riguardanti questo documento ed il servizio descritto il punto di contatto è fornito dall'Help Desk SIAE.

3. Regole Generali

In questo capitolo sono descritte le condizioni generali secondo cui viene erogato il servizio di certificazione descritto in questo manuale.

3.1 Obblighi e Responsabilità

3.1.1 Obblighi del Certificatore

Il Certificatore è tenuto a:

1. Verificare la corretta provenienza delle richieste di certificazione, revoca/sospensione e rinnovo secondo le modalità concordate tra SIAE ed il Certificatore;
2. Verificare l'integrità della richiesta proveniente dal CMS SIAE, sulla base della firma digitale apposta dal Responsabile CMS, e la presenza delle informazioni necessarie alla certificazione;
3. Garantire l'associazione tra una chiave pubblica ed un utente Titolare o Responsabile CMS di cui è stata completata con successo la fase di registrazione e di identificazione;
4. non rendersi depositario di chiavi private corrispondenti ai Certificati SIAE o SIAE-CMS;
5. emettere e rinnovare un certificato secondo le presenti procedure e renderlo accessibile per via telematica;
6. revocare o sospendere un certificato dandone tempestiva pubblicità secondo le previsioni del presente Manuale Operativo (cfr. § 6.6);
7. proteggere accuratamente le proprie chiavi private mediante dispositivi hardware e software adeguati a garantire i necessari criteri di sicurezza;
8. gestire le operazioni e l'infrastruttura relativa al servizio di certificazione digitale secondo le regole e procedure descritte nel presente Manuale Operativo;
9. 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 [7].

3.1.2 Obblighi degli Incaricati alla Registrazione

Gli Incaricati alla Registrazione sopra definiti sono tenuti a:

1. verificare con certezza l'identità del Richiedente il certificato e provvedere alla registrazione dei suoi dati;
2. informare espressamente il richiedente la certificazione riguardo la necessità di protezione della segretezza della chiave privata e la conservazione e l'uso dei dispositivi di firma;
3. comunicare e trasmettere alla Direzione Generale SIAE tutti i dati e documenti acquisiti durante la registrazione del Richiedente allo scopo di attivare la procedura di emissione del certificato;

4. inoltrare alla Direzione Generale SIAE le richieste di revoca o di sospensione attivate dall'utente Titolare presso l'Ufficio di Registrazione;
5. effettuare tutte le operazioni relative al servizio di certificazione digitale, affidate all'Ufficio di Registrazione dal Certificatore, secondo le regole e procedure descritte nel presente Manuale Operativo;
6. 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.

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 del CMS

I responsabili della gestione del CMS sono tenuti a:

1. Garantire la correttezza del contenuto delle informazioni inserite nelle richieste di certificazione, revoca o sospensione e rinnovo inviate alla CA;
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 (Passphrase) utilizzato per l'abilitazione alle funzionalità del dispositivo di firma, in luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;
4. 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 [7];
5. Utilizzare le chiavi ed il certificato SIAE-CMS solo nelle modalità e per gli scopi previsti dal presente Manuale Operativo.

3.1.4 Obblighi dei Richiedenti/Titolari

Il Richiedente/Titolare è tenuto a:

1. Garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ufficio di Registrazione e, tramite questi, 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 alle funzionalità del dispositivo sicuro di firma in luogo sicuro e diverso da quello in cui è custodito il dispositivo medesimo;
4. proteggere e conservare il codice di revoca per le richieste di revoca o sospensione del proprio certificato;
5. proteggere e conservare il codice da utilizzare per lo sblocco (PUK) della carta di attivazione in luogo sicuro e diverso da quello in cui è custodito il dispositivo medesimo;
6. adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e del proprio dispositivo sicuro di firma;
7. utilizzare personalmente il dispositivo sicuro di firma non cedendolo o dandolo in uso a terzi;
8. utilizzare le chiavi e il certificato per le sole modalità e con i limiti di utilizzo previsti nel presente Manuale Operativo (cfr. § 2.2.8);
9. inoltrare senza ritardo all'Ufficio competente SIAE la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto al § 6.6.1;
10. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.1.5 Obblighi degli Utilizzatori

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

1. controllare la validità del certificato prima di usare la chiave pubblica in esso contenuta. La validità del certificato viene accertata controllando che questo non sia scaduto, ovvero revocato o sospeso;

2. conoscere l'ambito di utilizzo del certificato, le limitazioni di responsabilità e i limiti di indennizzo del Certificatore, riportati nel presente Manuale Operativo;
3. utilizzare i dati contenuti nel registro dei certificati 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 Utilizzatore è l'unico responsabile per utilizzi del certificato difformi da quanto indicato nel presente Manuale Operativo.

3.2 Responsabilità

3.2.1 Limitazioni di responsabilità del Certificatore

Il Certificatore, fatto salvo i casi di dolo e colpa grave, non assume responsabilità per danni diretti ed indiretti subiti dagli utenti o da terzi in conseguenza ad un utilizzo improprio dei certificati disciplinati dal presente manuale operativo.
SIAE, nel ruolo di Autorità di Registrazione, è l'unica responsabile per quanto riguarda la corretta identificazione degli utenti richiedenti, nonché della conservazione dei loro dati anagrafici. Sarà inoltre responsabilità della SIAE il contenuto ed il corretto inoltro, secondo le modalità convenute, delle richieste di certificazione, di revoca e sospensione e di rinnovo dei certificati che perverranno al Certificatore.

3.2.2 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

3.3 Pubblicazione

3.3.1 Pubblicazione di informazioni inerenti SIAE

Il presente Manuale Operativo è reperibile in formato elettronico presso il sito web del Certificatore ed presso il sito SIAE indicati al § 2.1

3.3.2 Pubblicazione dei certificati

I certificati e le liste di revoca e sospensione sono pubblicati nel registro dei certificati accessibile con protocollo LDAP all'indirizzo: **ldap://ldap.InfoCert.it**
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 SIAE e il Certificatore vengono in possesso nell'esercizio delle proprie tipiche attività, sono da considerarsi riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (chiave pubblica, certificato, date di revoca e di sospensione del certificato).

1. In particolare i dati personali vengono trattati da SIAE e dal Certificatore in conformità a quanto previsto dal D.Lgs 196/2003 e dal regolamento contenente le misure minime di sicurezza per la loro protezione, DPR 318/99 Errore: sorgente del riferimento non trovata.

4. Amministrazione del Manuale Operativo

4.1 Procedure per l'aggiornamento

Sentita la SIAE, 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, tipografiche o altre di carattere minore 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 e sul sito SIAE all'indirizzo riportato al § 2.1.

4.3 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Responsabile dell'Area Sicurezza dei Sistemi Informativi di InfoCert, sentito anticipatamente il parere della SIAE.

5. Identificazione

Questo capitolo descrive le procedure usate per l'identificazione degli utenti in relazione al rilascio, rinnovo, revoca e sospensione dei Certificati SIAE e SIAE-CMS.

5.1 Registrazione iniziale

Identificazione dei Richiedenti la carta di attivazione
SIAE, avvalendosi di personale appartenente alle proprie strutture o esplicitamente autorizzato, verifica l'identità del richiedente la carta di attivazione al momento della sua registrazione.
La procedura di identificazione comporta che il Richiedente sia fisicamente presente davanti ad un incaricato SIAE presso un suo Ufficio di Registrazione; l'incaricato addetto alla registrazione verifica l'identità del richiedente attraverso il controllo di un documento di riconoscimento in corso di validità.

I documenti di riconoscimento accettati da SIAE per l'identificazione del richiedente sono:

- carta di identità
- passaporto
- patente di guida rilasciata da una Prefettura

Il Richiedente, Titolare di Biglietteria, dovrà inoltre presentare il tesserino che riporti il suo codice fiscale.
Se il Richiedente è persona differente dal Titolare di Biglietteria, deve presentare procura autenticata da un Notaio o altro pubblico ufficiale che attesti l'autorizzazione ad operare per nome e per conto del Titolare di Biglietteria. Il nome, cognome e codice fiscale del Titolare devono essere desumibili dai documenti presentati al momento dell'identificazione (tra quelli previsti) e dal tesserino codice fiscale.

L'addetto al riconoscimento provvederà a registrare i dati del Richiedente e del Titolare di Biglietteria in un archivio centrale presso la Direzione Generale SIAE, in modo tale che possa essere poi avviata da parte del CMS la personalizzazione della smart card e la certificazione della chiave pubblica contenuta in essa da parte di InfoCert.
Sulla base delle dichiarazioni del richiedente, verrà generato il certificato digitale secondo il profilo descritto al § A2.

Al momento della registrazione viene consegnato al Richiedente una copia del modulo di richiesta sottoscritto dall'addetto alla registrazione.
Al momento della consegna della carta di attivazione, viene fornito al Titolare un codice segreto di revoca, che costituisce lo strumento di autenticazione nel sistema di comunicazione tra Help Desk SIAE e Titolare.

Identificazione dei Responsabili SIAE-CMS
SIAE dovrà comunicare formalmente, per iscritto, al Certificatore il nome e i dati del Responsabile CMS cui dovrà essere rilasciato il certificato SIAE-CMS.

La procedura di identificazione prevede che il Responsabile nominato dalla SIAE si presenti fisicamente ad un incaricato della CA, addetto alla registrazione, che ne verificherà l'identità controllando un documento di riconoscimento in corso di validità tra quelli previsti.
I documenti di riconoscimento accettati per l'identificazione sono i medesimi indicati per il riconoscimento dei richiedenti la carta di attivazione, ossia:

- **carta di identità**
- **passaporto**
- **patente di guida rilasciata dalla Prefettura.**

Il Richiedente dovrà, inoltre, presentarsi munito del tesserino codice fiscale.

5.2 Rinnovo delle chiavi e certificati

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "*validity"* (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.

Rinnovo Certificati SIAE
Salvo i casi di smarrimento, furto o rottura della smart card, in prossimità della scadenza, il CMS provvederà a generare una nuova carta con a bordo una nuova coppia di chiavi e un nuovo certificato.

La richiesta di rinnovo del Certificato SIAE, relativamente alle procedure di identificazione, segue le stesse procedure del primo rilascio.

Rinnovo Certificati SIAE-CMS
Le richieste di rinnovo di Certificati SIAE-CMS dovranno essere comunicate, per iscritto, al Certificatore InfoCert da parte della Direzione SIAE prima della scadenza del certificato medesimo.
Con suddetta comunicazione la Direzione sarà inoltre tenuta a confermare, tramite sottoscrizione, il persistere della validità dei dati comunicati ai fini della prima emissione.

5.3 Richiesta di Revoca o di Sospensione

Revoca/Sospensione Certificati SIAE
L'Help Desk SIAE, unico punto di contatto per il Titolare ai fini della richiesta di revoca o sospensione, si accerta dell'identità del richiedente e delle motivazioni della richiesta di revoca o di sospensione.
Il Titolare, che richiede la revoca o sospensione del certificato via telefono, dovrà fornire per il suo riconoscimento la password (codice di revoca) consegnata al momento del rilascio della smart card.

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

Revoca/Sospensione Certificati SIAE-CMS
Anche ai fini della Revoca/Sospensione dei Certificati SIAE-CMS, la Direzione SIAE dovrà inviare per iscritto la richiesta di revoca/sospensione al Certificatore, indicandone il motivo e la data di decorrenza. In caso di sospensione dovrà essere anche specificato il periodo durante il quale il certificato rimarrà sospeso.
Tale richiesta dovrà essere inviata al Certificatore opportunamente sottoscritta

6. Operatività

Questo capitolo descrive le operazioni necessarie per compiere le attività di registrazione di un Richiedente la carta di attivazione e del/i Responsabili CMS, nonché quelle di richiesta, emissione, pubblicazione, revoca, sospensione e rinnovo di un Certificato SIAE e SIAE-CMS.

6.1 Registrazione dei Richiedenti

6.1.1 Registrazione degli Richiedenti/ Titolari

I passi principali che un utente deve effettuare per ottenere la carta di attivazione sono i seguenti:
a) fornire all'Ufficio di Registrazione tutte le informazioni personali necessarie alla sua identificazione certa e alla registrazione dei suoi dati, in particolare dovranno essere forniti i dati da inserire nel certificato (come indicato nel modulo di richiesta);
b) firmare il modulo di richiesta contenente i dati di registrazione, a conferma della veridicità degli stessi, e per espressa accettazione del contratto di adesione al servizio offerto da SIAE e del presente manuale operativo, previa visione del contenuto di questi documenti.

La carta di attivazione sarà consegnata direttamente al Titolare dagli incaricati dell'identificazione dei Richiedenti.

In dettaglio, la procedura di Registrazione si articola nei seguenti passi:

1) l'Incaricato alla Registrazione, prima di iniziare il rapporto contrattuale con il Titolare, lo informa sui termini e sulle condizioni contrattuali riguardanti l'uso del Certificato;
2) il Richiedente fornisce tutte le informazioni personali necessarie alla identificazione e registrazione, e che verranno inserite nel certificato (cfr. § 6.1.1.1).
3) l'Incaricato alla Registrazione si accerta personalmente dell'identità del Richiedente che si deve presentare di persona presso l'ufficio munito del documento d'identità previsto (cfr. § 5.1);
4) il Richiedente, presa visione del contratto di adesione al servizio di SIAE e del presente manuale operativo, sottoscrive la richiesta di registrazione e certificazione completa dei dati ivi riportati.

6.1.1.1 Informazioni che il Richiedente deve fornire

Le informazioni di registrazione dell'utente Richiedente comprendono le informazioni obbligatorie che devono comparire nel certificato ed altre informazioni necessarie a gestire il rapporto tra SIAE e l'utente stesso.

Sono considerate obbligatorie le seguenti informazioni:
- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- I riferimenti del documento utilizzato per l'identificazione, quali: tipo e numero, ente che lo ha emesso e data di rilascio.

- Indirizzo di posta elettronica.

6.1.2 Registrazione dei Responsabili CMS

La procedura di Registrazione dei Responsabili CMS si articola nei seguenti passi:

a) fornire all'Ufficio di Registrazione InfoCert tutte le informazioni personali necessarie alla sua identificazione certa e alla registrazione dei suoi dati, in particolare dovranno essere forniti i dati da inserire nel certificato (come indicato nel modulo di richiesta);
b) firmare il modulo di richiesta contenente i dati di registrazione, a conferma della veridicità degli stessi, e per espressa accettazione del presente manuale operativo, previa visione del contenuto di questo documento.

In particolare:

1) l'Incaricato alla Registrazione InfoCert informa il Responsabile CMS sui termini e sulle condizioni riguardanti l'uso del Certificato SIAE-CMS;
2) il Responsabile CMS fornisce tutte le informazioni personali necessarie alla identificazione e registrazione, e che verranno inserite nel certificato (cfr. § 6.1.2.1).
3) l'Incaricato alla Registrazione InfoCert si accerta personalmente dell'identità del Responsabile CMS che si deve presentare di persona presso l'ufficio di registrazione munito di un documento d'identità tra quelli previsti;
4) il Responsabile, presa visione del presente manuale operativo e della relazione contrattuale in essere tra InfoCert e SIAE, sottoscrive la richiesta di registrazione e certificazione completa dei dati ivi riportati.

6.1.2.1 Informazioni che il Responsabile CMS deve fornire

Le informazioni per la registrazione del Responsabile CMS comprendono quelle obbligatorie che devono comparire nel certificato ed altre informazioni necessarie a gestire il rapporto tra InfoCert e CMS. I dati devono corrispondere a quelli comunicati ad InfoCert da parte della Direzione SIAE.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Codice fiscale
- Indirizzo di residenza
- I riferimenti del documento utilizzato per l'identificazione, quali: tipo e numero, ente che lo ha emesso e data di rilascio.
- Indirizzo di posta elettronica.

6.2 Richiesta di certificazione per utenti SIAE

Completata la fase di Registrazione, la richiesta di certificazione della chiave personale di firma viene effettuata dal CMS sulla base delle informazioni archiviate nel DB presso la Direzione Generale SIAE.
Il CMS verifica la presenza di richieste pendenti nell'archivio e a fronte di ciascuna domanda procede alla personalizzazione delle Smart card. Al termine della personalizzazione grafica della carta, il CMS, dopo aver instaurato un collegamento protetto con la Certification Authority, provvede a generare a bordo della Smart card la coppia di chiavi asimmetriche e ad inviare la richiesta di certificazione della chiave pubblica alla CA.

La richiesta di certificazione è sottoscritta dal responsabile del CMS od altro incaricato dipendente della SIAE a garanzia della sua autenticità e integrità.

6.3 Emissione del certificato

6.3.1 Emissione del certificato SIAE e rilascio della carta di attivazione al Titolare

L'emissione del certificato viene effettuata dal Certificatore secondo i seguenti passi:

1. viene verificata la correttezza della richiesta di certificato controllando:
   - la provenienza (sono accettabili solo richieste provenienti dal CMS SIAE);
   - l'integrità e la presenza di tutte le informazioni necessarie al rilascio del certificato;
   - che la chiave pubblica contenuta nella richiesta di certificazione sia una chiave valida e della lunghezza prevista;
2. si procede alla generazione del certificato
3. il certificato viene pubblicato nel registro dei certificati,
4. il certificato emesso viene inviato al CMS, tramite un canale sicuro, il quale provvede a scaricarlo nella smart card completandone la personalizzazione.

Completata la personalizzazione della smart card presso il CMS, quest'ultimo provvede a predisporre una lettera di accompagnamento che riporta:

a) PIN e PUK;
b) una password per le comunicazioni vocali di supporto/revoca/sospensione della smart card.

La smart card, insieme alla lettera di accompagnamento, viene spedita in busta chiusa e cieca con raccomandata assicurata all'ufficio SIAE competente per la consegna al legittimo Titolare. Il punto periferico SIAE provvederà a contattare il Titolare per consegnargli di persona la carta e per verificarne le funzionalità nonché i valori dei contatori in essa contenuti (che saranno annotati dall'addetto SIAE in un opportuno libretto fiscale).

Il Titolare dovrà sottoscrivere e rilasciare all'addetto SIAE un modulo che attesti l'avvenuto recapito e attivazione della smart card.

6.3.1.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni fornite dal Richiedente e contenute nella richiesta inviata dal CMS alla CA. Il formato del certificato è descritto dettagliatamente al § A.2

Il Distinguished Name del Certificato, cioè il nome univoco del Titolare del Certificato definito secondo lo standard X.500, è composto come da tabella seguente:

Nome Campo (sigla)	Valore o Contenuto
`Country Name (C)`	`"IT"` (indica lo stato `"ITALIA"`)
`Organization Name (O)`	Assume il valore fisso "**SIAE/SIETA – USO INTERNO**".
`Organizational Unit Name (Ou)`	*Nome della ditta/codice fiscale della ditta*
`Common Name (CN)`	*Cognome/Nome/CodiceFiscale del titolare*
`E-mail Address (mail)`	Indirizzo di posta elettronica del Titolare
`Given Name (G)`	Nome del Titolare (da documento di riconoscimento)
`Surname (s)`	Cognome del Titolare (da documento di riconoscimento)
`SerialNumber (SN)`	Codice identificativo del sistema del Titolare/Numero Seriale Smart card

Esempio:

```
C=IT,
O=SIAE/SIETA – USO INTERNO,
Ou=Giochi e Scommesse S.r.l/0123456789abcdef,
Cn=ROSSI/GIOVANNI/RSSGNN60T25G224N
```

```
E-mail = g.rossi@miaposta.it,
g=GIOVANNI,
s=ROSSI,
sn=00000001/A00000001
```

6.3.2 Emissione del certificato SIAE-CMS

Completata la fase di Registrazione, la generazione della coppia di chiavi è effettuata, in un secondo momento, dal Certificatore in locali sicuri: il Certificatore provvederà a generare contestualmente la richiesta di certificazione ed emettere il relativo certificato.
La coppia di chiavi ed il certificato verranno memorizzati in un file in formato p12 protetto tramite una passphrase.

Il file p12 e la relativa password di attivazione verranno inviati al responsabile CMS o altro incaricato dipendente della SIAE per posta ordinaria in busta sigillata e con ricevuta di ritorno, all'indirizzo da questi dichiarato in fase di registrazione.

Il Certificatore provvederà poi a cancellare le chiavi create e i relativi codici di attivazione.

6.3.2.1 Formato e contenuto del certificato

Il certificato viene generato con le informazioni fornite dal Responsabile CMS in fase di registrazione.
Il formato del certificato è descritto dettagliatamente al § A3

Il Distinguished Name del Certificato, cioè il nome univoco del Titolare del Certificato definito secondo lo standard X.500, è composto come da tabella seguente:

Nome Campo (sigla)	Valore o Contenuto
Country Name (C)	IT (indica lo stato "ITALIA")
Organization Name (O)	Assume il valore fisso "SIAE/SIETA – USO INTERNO".
Organizational Unit Name (Ou)	Assume il valore fisso "Card Management System
Common Name (CN)	Cognome/Nome/CodiceFiscale del titolare
E-mail Address (mail)	Indirizzo di posta elettronica del Titolare

Cognome e Nome del Titolare dovranno essere desumibili da documento di riconoscimento.

6.3.3 Validità del certificato

I certificati SIAE e SIAE-CMS emessi fino al 1/2/2008 hanno una validità di due anni, mentre quelli emessi successivamente hanno una validità di tre anni a partire dalla data di emissione ovvero fino alla data di pubblicazione della loro revoca o sospensione se precedentemente effettuate.

6.4 Pubblicazione del certificato

Dopo l'emissione del certificato, il Certificatore lo pubblica nel Registro dei Certificati all'indirizzo **ldap://ldap.InfoCert.it.**

6.5 Uso del Certificato

6.5.1 Certificato SIAE

Il certificato SIAE e la relativa firma elettronica devono essere utilizzati unicamente nell'ambito delle applicazioni informatiche funzionali all'esecuzione delle attività interne alla SIAE previste dalle norme che regolamentano i sistemi di emissione titoli d'accesso (gestite mediante progetto SIETA a cura della SIAE).

6.5.2 Certificato SIAE-CMS

L'ambito d'utilizzo di tale certificato e della relativa firma elettronica è limitato esclusivamente alla sottoscrizione delle richieste che il sistema CMS invia alla CA InfoCert, allo scopo di assicurarne l'autenticità e l'integrità.

6.6 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.

6.6.1 Motivi per la revoca di un certificato

Certificato SIAE
Il Certificatore può eseguire la revoca del certificato su propria iniziativa, su richiesta esplicita della Direzione Generale SIAE o su richiesta del Titolare inoltrata al Certificatore tramite il CMS di SIAE.

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 sicuro 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 sicuro di firma in suo possesso (perdita del PIN, guasto del dispositivo, ecc.);
- viene restituita la carta di attivazione al termine del suo utilizzo ai fini di un rinnovo della stessa;
- si verifica un cambiamento dei dati del Titolare presenti nel certificato;
- si verifica un'interruzione dell'attività di biglietteria;
- termina il rapporto tra il Titolare e SIAE;
- viene verificata una sostanziale condizione di non conformità del presente Manuale Operativo.

Per alcuni dei casi di revoca citati, quali "Restituzione della smart card per fine ciclo di vita o per rottura", "Furto o Smarrimento Smart card", "Interruzione attività di biglietteria", sono indicate nel seguito anche le procedure operative che il Titolare dovrà seguire a completamento dell'operazione di revoca.

Certificato SIAE-CMS
Il Certificatore può eseguire la revoca del certificato SIAE-CMS su propria iniziativa o su richiesta esplicita della Direzione Generale SIAE.

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 alterato o rubato il dispositivo di firma che contiene la chiave;
  - sia venuta meno la segretezza della chiave o del suo codice di attivazione (Passphrase);
  - si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave;
- il Responsabile CMS non riesce più ad utilizzare il dispositivo di firma in suo possesso (perdita della Passphrase, corruzione del dispositivo, ecc.);
- viene verificata una sostanziale condizione di non conformità del presente Manuale Operativo.

6.6.2 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del richiedente.

Certificato SIAE

Nel caso di revoca di un certificato SIAE, sono previsti i seguenti casi:

- **Revoca su iniziativa del Titolare**

L'utente Titolare può richiedere la revoca telefonando al Call Center di SIAE e identificandosi fornendo il proprio codice segreto consegnato assieme alla carta di attivazione

Per effettuare la richiesta l'utente dovrà comunicare, inoltre, i propri dati identificativi, e la motivazione della revoca. 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).

- **Revoca su iniziativa del Certificatore**

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

1. il Certificatore comunica al CMS 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).

SIAE provvederà a notificare l'avvenuta revoca al Titolare e ad aggiornare lo stato dello stesso nei suoi archivi.

- **Revoca su iniziativa di SIAE**

La richiesta di revoca su iniziativa di SIAE viene effettuata con la seguente modalità:

1. SIAE richiede, tramite il CMS al Certificatore la revoca del certificato specificando i dati del Titolare del certificato;
2. il Certificatore, verificata l'autenticità della richiesta, procede alla revoca del certificato fornendo poi un riscontro a SIAE medesima.

   SIAE provvederà a notificare l'avvenuta revoca al Titolare e ad aggiornare lo stato dello stesso nei suoi archivi.
   Il Certificatore potrà procedere ad una sospensione del Certificato qualora vi siano carenze nella richiesta che non consentano di procedere alla revoca.

Certificato SIAE-CMS

- **Revoca su iniziativa del Certificatore**

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

1. il Certificatore comunica alla Direzione 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).

- **Revoca su iniziativa della Direzione SIAE**

La richiesta di revoca su iniziativa della Direzione SIAE viene effettuata con la seguente modalità:

1. La Direzione SIAE richiede la revoca del certificato telefonando all Call Center del Certificatore (numero 0644285555, orario 8-20 dal lunedì al venerdì, 8-14 il sabato), fornendo la motivazione della revoca, i dati identificativi del Responsabile CMS Titolare del certificato e gli estremi del certificato da revocare (numero seriale del certificato);
2. Il Certificatore, in attesa di ricevere la richiesta di revoca del certificato sottoscritta da parte della Direzione SIAE, lo sospenderà sulla base delle informazioni fornite dal Call-Center.

   La richiesta di revoca, sottoscritta con firma digitale, dovrà essere inviata via e-mail all'indirizzo supporto.firma.digitale@InfoCert.it, ovvero inviata per posta ordinaria, ugualmente sottoscritta, al responsabile Area Sistemi Sicurezza Informatica di InfoCert.

6.6.3 Motivi per la Sospensione di un certificato

Il Certificatore può eseguire una sospensione del certificato (SIAE o SIAE-CMS), per un periodo di tempo determinato, nel caso in cui venga effettuata una richiesta di revoca di cui non è possibile accertarne l'autenticità.
Alla sospensione seguirà o una revoca definitiva oppure, alla scadenza del periodo, la ripresa di validità del certificato.
La sospensione viene effettuata inserendo i dati che identificano il Certificato da sospendere nella lista di revoca e sospensione (CRL).

6.6.4 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 Utilizzatori. La CRL è emessa sempre integralmente.
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 descritto al § A.3

6.6.5 Tempistica

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

6.7 Rinnovo del Certificato

Il certificato ha validità di tre anni dalla data di emissione e non è previsto rinnovo se non col le modalità di seguito riportate.

Certificato SIAE
La procedura di rinnovo richiede la generazione di una nuova coppia di chiavi su una nuova carta a microprocessore e la certificazione della corrispondente chiave pubblica.
L'emissione e la pubblicazione del certificato segue il procedimento descritto in caso di nuova richiesta: SIAE consegnerà la nuova smart card al Titolare nella modalità prevista per il primo rilascio, avvalendosi degli uffici periferici autorizzati.

Certificato SIAE-CMS
Le richieste di rinnovo di Certificati SIAE-CMS dovranno essere comunicate, per iscritto, al Certificatore InfoCert da parte della Direzione SIAE prima della scadenza del certificato medesimo.

Con suddetta comunicazione la Direzione sarà inoltre tenuta a confermare, tramite sottoscrizione, il persistere della validità dei dati comunicati ai fini della prima emissione.

6.8 Restituzione della Smart card a fine ciclo di vita o per sua rottura

La modalità di restituzione della smart card si articola secondo i seguenti passi:

1. L'ufficio SIAE provvede a verificare, salvo il caso di rottura della SC, i montanti dei due contatori presenti sulla carta restituita dal Titolare ed a compilare un apposito modulo di restituzione, che verrà sottoscritto dallo stesso Titolare e dall'Incaricato del punto periferico;
2. L'ufficio periferico registra l'evento e spedisce alla Direzione Generale la carta restituita;
3. L'ufficio CMS provvede a segnalare tempestivamente alla CA la restituzione della carta, al fine della revoca del certificato;
4. In caso di carta ancora funzionante, l'ufficio CMS conserva presso un apposito armadio le carte restituite per un periodo di 10 anni; in caso di carta difettosa, queste verranno restituite alla ditta produttrice per la verifica di eventuali tentativi di violazione.

6.9 Interruzione attività di biglietteria

Nel caso di cessione a terzi delle apparecchiature o di cessazione dell'attività dovranno essere effettuate le seguenti operazioni:

1. Il titolare comunicherà all'ufficio SIAE di competenza l'interruzione dell'attività;
2. L'ufficio SIAE provvede a recarsi presso il sistema di biglietteria per prendere nota dei montanti dei due contatori presenti sulla carta restituita dal titolare della biglietteria e a compilare l'apposito modulo di restituzione, sottoscritto dal titolare della biglietteria e dallo stesso punto periferico. L'addetto SIAE provvede anche all'aggiornamento del **libretto fiscale**.
3. L'ufficio periferico SIAE spedirà alla Direzione Generale SIAE, presso l'ufficio CMS, la carta restituita, che dovrà essere conservata presso il medesimo ufficio per 10 anni;
4. L'ufficio SIAE provvederà a segnalare tempestivamente alla CA la restituzione della carta al fine della revoca del certificato.

6.10 Furto o smarrimento Smart card

In caso si furto o smarrimento della smart card, l'utente titolare dovrà procedere in due passi successivi:

1. Denunciare all'autorità preposta il furto o lo smarrimento della carta e contattare l'Help Desk SIAE per comunicare l'accaduto e richiedere la revoca del certificato, dopo essersi autenticato tramite la password ottenuta in fase di rilascio della smart card;
2. L'utente titolare dovrà poi recarsi presso l'ufficio SIAE di competenza per dichiarare l'accaduto, fornendo copia della denuncia effettuata presso le autorità competenti, e sottoscrivere l'apposito modulo (utilizzato anche per la restituzione della smart card)

6.11 Ritrovamento Smart card precedentemente denunciate

In caso di ritrovamento a seguito di precedente smarrimento, la SC dovrà essere restituita alla SIAE, in quanto non riattivabile, secondo le modalità previste al paragrafo § 6.8; il ritrovamento dovrà essere comunicato anche alle autorità presso le quali si era presentata precedente denuncia di smarrimento.

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 per la certificazione di qualità (ISO 9001) sia a verifiche 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.

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 SIAE 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
Registrazione dei richiedenti. (2)	Orario di sportello degli uffici SIAE
Servizio di certificazione su richiesta del CMS.	Lun – Sab: dalle 06:00 alle 24:00

(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 SIAE che possono avere diversi orari di sportello. In ogni caso il Certificatore garantisce l'erogazione del servizio di certificazione negli orari sopra riportati.

8. Appendice A: Profilo dei Certificati e delle CRL

A1. Certificato della CA "Servizi di Certificazione"

Di seguito il profilo del certificato della CA "Servizi di Certificazione", relativo alla CA che firma i Certificati SIAE.
Il certificato è conforme allo standard 'X.509 v3 (ISO 9594-8).

Attributo	Valore/Informazione
Version	Version 3
SerialNumber	Numero intero
Signature	sha1-with-rsa-encryption
Issuer Country Name Organization Name Serial Number Organizational Unit Name Common Name	 IT INFOCERT SPA 07945211006 Ente Certificatore InfoCert Servizi di Certificazione
Validity	12 anni
Issuer Country Name Organization Name Serial Number Organizational Unit Name Common Name	 IT INFOCERT SPA 07945211006 Ente Certificatore InfoCert Servizi di Certificazione
SubjectPublicKeyInfo	Algoritmo: rsa-encryption Lunghezza della chiave: RSA 2048 bit
Estensione	**Valore/Informazione**
BasicConstraints	(non critica) cA=TRUE
KeyUsage	(critica) keyCertSign + cRLSign
CertificatePolicies	(non critica) policyIdentifier oid=2.5.29.32.0 (Any policy)
cRLDistributionPoints	(non critica) ldap://ldap.infocert.it/cn%3dInfoCert%20Servizi%20di%20Certificazione,ou%3dEnte%20Certificatore,o%3dINFOCERT%20SPA,c%3dIT?certificateRevocationList
Subject Key Identifier	(non critica) valore SHA-1 della chiave pubblica: 0x4168e4ff c764e314 437f35c7 ec8f6039 673d3fa6

A2. Profilo del Certificato SIAE

Di seguito il profilo del Certificato SIAE.

Il certificato è conforme allo standard X.509 v3 (ISO 9594-8).

Attributo/Estensioni	**Valore/Informazione**
Version	Version 3
SerialNumber	Numero intero
Signature	sha1-with-rsa-encryption
Issuer Country Name Organization Name Serial Number Organizational Unit Name Common Name	 IT INFOCERT SPA 07945211006 Ente Certificatore InfoCert Servizi di Certificazione
Validity	3 anni
Subject Country Name Organization Name Organizational Unit Name Common Name E-mail Address Given Name Surname Serial Number	*Esempio:* IT SIAE/SIETA – USO INTERNO GIOCHI e SCOMMESSE Srl/0123456789abcdef FERRARI/GIOVANNI/FRRGNN50D16H501D GIOVANNI.FERRARI@POSTALIBERA.IT GIOVANNI FERRARI *00000001/A00000001* *Nota:* *1) per la OU si tratta della Ragione sociale/Parita Iva oppure Codice Fiscale* *2) per il Serial Number si tratta della Codice Sistema/SmartCard Serial Number*
SubjectPublicKeyInfo	Algoritmo: rsa-encryption Lunghezza della chiave: RSA 1024 bit
AuthorityKeyIdentifier	(non critica) valore SHA-1 della chiave pubblica: 0x4168e4ff c764e314 437f35c7 ec8f6039 673d3fa6
BasicConstraints	(non critica) cA=FALSE
KeyUsage	(non critica) NonRepudiation+DigitalSignature+ keyEncipherment+DataEncipherment
subjectAltName RFC Name	(non critica) *indirizzo email dell'utente, esempio:* GIOVANNI.FERRARI@POSTALIBERA.IT
issuerAltName RFC Name	(non critica) firma.digitale@infocert.it
certificarePolicies policyIdentifier policyQualifier: cPSuri policyQualifier: userNotice	(non critica) OID=1.3.76.36.1.1.3.1 http://www.firma.infocert.it/doc/manuali.htm explicitText=Questo certificato deve essere adoperato solo nell'ambito SIETA
cRLDistributionPoints	(non critica) ldap://ldap.infocert.it/cn%3dInfoCert%20Servizi%20di%20Certificazione,ou%3dEnte%20Certificatore,o%3dINFOCERT%20SPA,c%3dIT?certificateRevocationList
Extended Key Usage:	E-mail protection, Client Authorisation
Subject Key Identifier	(non critica)

	valore SHA-1 della chiave pubblica

A3. Profilo del Certificato SIAE-CMS

Di seguito il profilo del Certificato SIAE-CMS.
Il certificato è conforme allo standard X.509 v3 (ISO 9594-8).

Attributo/Estensioni	Valore/Informazione
Version	Version 3
SerialNumber	Numero intero
Signature	sha1-with-rsa-encryption
Issuer Country Name Organization Name Serial Number Organizational Unit Name Common Name	 IT INFOCERT SPA 07945211006 Ente Certificatore InfoCert Servizi di Certificazione
Validity	3 anni
Subject Country Name Organization Name Organizational Unit Name Common Name E-mail Address	*Esempio:* IT SIAE/SIETA - USO INTERNO Card Management System COGNOME/NOME/CODICE FISCALE NOME.COGNOME@EMAIL.IT
SubjectPublicKeyInfo	Algoritmo: rsa-encryption Lunghezza della chiave: RSA 1024 bit
AuthorityKeyIdentifier	(non critica) valore SHA-1 della chiave pubblica: 0x4168e4ff c764e314 437f35c7 ec8f6039 673d3fa6
BasicConstraints	(non critica) cA=FALSE
KeyUsage	(non critica) DigitalSignature
subjectAltName RFC Name	(non critica) *indirizzo email dell'utente, esempio:* NOME.COGNOME@EMAIL.IT
issuerAltName RFC Name	(non critica) firma.digitale@infocert.it
certificarePolicies policyIdentifier policyQualifier: cPSuri policyQualifier: userNotice	(non critica) OID=1.3.76.36.1.1.3.1 http://www.firma.infocert.it/doc/manuali.htm **explicitText=Questo certificato deve essere adoperato solo per la sottoscrizione di richieste di certificati da parte del responsabile CMS SIAE.**
cRLDistributionPoints	(non critica) ldap://ldap.infocert.it/cn%3dInfoCert%20Servizi%20di%20Certificazione,ou%3dEnte%20Certificatore,o%3dINFOCERT%20SPA,c%3dIT?certificateRevocationList
Key Identifier	(non critica) valore SHA-1 della chiave pubblica

A3. Profilo della CRL

Le CRL, pubblicate all'indirizzo definito nell'estensione dei certificati: "cRLDistributionPoints", seguono lo standard X.509 V2 Certificate Revocation Lists (CRLs) come definito in RFC 2459 [X].

Attributo/Estensioni	Valore/Informazione
Version	Version 2
Signature	sha1-with-rsa-encryption
Issuer Country Name Organization Name Serial Number Organizational Unit Name Common Name	 IT INFOCERT SPA 07945211006 Ente Certificatore InfoCert Servizi di Certificazione
thisUpdate	data e ora (GMT) di emissione della attuale CRL
nextUpdate	data e ora (GMT) di emissione della prossima CRL
revokedCertificates	*è la lista dei certificiati revocati o sospesi per ogni certificato sono presenti i campi:* CertifcatesSerialNumber Time reasonCode (optional)
authorityKeyIdentifier	(non critica) valore SHA-1 della chiave pubblica del Certificatore: 0x847bef62 2ede74e5 111f7539 fbbc2f1b 9cb63255
CRL number	(non critica) numero intero (progressivo della CRL)