

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

Ente Certificatore InfoCamere
Certificati per CodeSigning RTRT
Manuale Operativo
Codice documento: ICCA-CS-RT

Redatto da	Alfredo Esposito InfoCamere Area Sistemi Sicurezza Informatica
Verificato da	Pio Barban InfoCamere Area Sistemi Sicurezza Informatica
Verificato da	Andrea Panichi Settore I.I.T.R. Direzione Generale O.S.I. Regione Toscana - Giunta Regionale
Approvato da	Simone Nasoni Direzione Prodotti e Servizi Applicativi
Approvato da	Domenico Fantasia Consulenza e Servizi Legali
Approvato da	Laura Castellani Settore I.I.T.R. Direzione Generale O.S.I. Regione Toscana - Giunta Regionale

Nome file: manualeoperativo_cs_0.32.sxw

Questa pagina è lasciata
intenzionalmente bianca

Indice

1.Introduzione al documento.....	5
1.1Novità introdotte rispetto alla precedente emissione.....	5
1.2Termini e definizioni.....	5
1.3Riferimenti.....	7
1.4Responsabile del Manuale Operativo.....	7
2.Caratteristiche del servizio.....	8
2.1Soggetto fornitore.....	8
2.1.1Oggetto del servizio.....	8
2.2Soggetti destinatari del servizio.....	9
2.3Responsabile del servizio.....	9
2.4Tempistica.....	9
3.Procedure operative.....	10
3.1Richiesta di certificazione.....	10
3.1.1Il modulo di richiesta.....	10
3.1.2Inoltro richiesta.....	10
3.1.3Generazione della coppia di chiavi ed emissione del certificato.....	10
3.1.4Modalità di generazione.....	11
3.1.5Caratteristiche della chiave pubblica certificata.....	11
3.1.6Formato del certificato e sua validità.....	11
3.2Invio del file p12 al richiedente la certificazione.....	11
3.3Rinnovo del certificato.....	11
3.4Revoca e sospensione del certificato.....	12
3.4.1Revoca.....	12
3.4.1.1Revoca su iniziativa del Certificatore.....	12
3.4.1.2Revoca su iniziativa della Regione Toscana.....	13
3.4.1.3Revoca su iniziativa del titolare.....	13
3.4.2Sospensione.....	13
3.4.3Pubblicazione e frequenza di emissione della CRL.....	13
3.4.4Tempistica.....	14
3.5Tariffe e condizioni.....	14
4.Condizioni Generali del contratto relativo al servizio di certificazione per la firma di oggetti Software.....	15
4.1Informativa Decreto Lgs. n. 196/03.....	15
4.2Oggetto del contratto	15
4.3Conclusione del contratto.....	16

4.4Utilizzo del certificato.....	16
4.5Obblighi e responsabilità del Soggetto richiedente o Titolare.....	16
4.6Obblighi e responsabilità del Certificatore.....	17
4.7Obblighi e responsabilità del Soggetto Terzo.....	17
4.8Modificazioni in corso di erogazione.....	18
4.9Comunicazioni.....	18
4.10Risoluzione del rapporto.....	18

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	0.32 BOZZA	Data Versione/Release :	26/04/2005
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione		

Il presente manuale ha lo scopo di descrivere le regole e le procedure operative adottate dalla struttura di certificazione digitale di InfoCamere per l'erogazione del servizio di certificazione per la firma di oggetti software.

Le indicazioni di questo documento hanno validità per le attività relative ad InfoCamere nel ruolo di Certificatore, nonché per i soggetti richiedenti e per i soggetti terzi.

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

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

Il presente documento è denominato "Certificati per CodeSigning RTRT - **Manuale Operativo**" ed è caratterizzato dal codice documento: **ICCA-CS-RT**.

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

L'object identifier (OID) di questo documento è il seguente: 1.3.76.14.1.1.12.5

Tale OID identifica:

InfoCamere	1.3.76.14
certification-service-provider	1.3.76.14.1
certificate-policy	1.3.76.14.1.1
Cliente Regione Toscana	1.3.76.14.1.1.12
manuale-operativo-Servizio di Certificazione CodeSign	1.3.76.14.1.1.12.5

Il manuale è pubblicato in formato elettronico sul sito Web del Certificatore, all'indirizzo <http://www.card.infocamere.it/doc/manuali.htm> e sul portale RTRT www.rtrt.it/servizi/PKI.

1.2 Termini e definizioni

Chiave Privata e Chiave Pubblica – cfr. TU (Art. 22)

Dati per la creazione di una firma – cfr. TU

Dati per la verifica della firma – cfr. TU

Dispositivo sicuro per la creazione della firma – cfr. TU

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. TU

Firma elettronica avanzata – cfr. TU

Firma elettronica qualificata – cfr. TU

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

Lista dei Certificati Revocati o Sospesi

È 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 di revoca dei certificati revocati o sospesi (CRL), che viene poi pubblicata nel registro dei certificati.

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).

PEM

Acronimo di **Privacy Enhanced Mail**, è uno standard per la trasmissione di posta sicura sulla rete Internet che si basa su tecniche crittografiche e firma digitale per la protezione dei dati trasmessi.

PKCS#12

PKCS, acronimo di **Public Key Cryptography Standards**, è un insieme di standard per la crittografia a chiave pubblica sviluppati dai Laboratori RSA: definiscono la sintassi del certificato digitale e dei messaggi crittografati, in particolare il PKCS#12 descrive una sintassi per il trasferimento di informazioni d'identità personale, tra cui chiavi private e certificati digitali a chiave pubblica, garantendo riservatezza e integrità dei dati trasmessi.

Registro dei Certificati

Il Registro dei Certificati è un archivio pubblico che contiene:

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

Revoca o sospensione di un Certificato

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

RTRT

Acronimo di Rete Telematica Regionale Toscana.

Soggetto richiedente

È il soggetto, privato o pubblico, che richiede il servizio di certificazione per la firma di oggetti software.

Soggetto terzo

È la persona fisica che fa affidamento sul software firmato, scaricato dalla rete.

Titolare

È il soggetto richiedente che abbia ottenuto la certificazione delle chiavi utilizzate per firmare il software.

X.509

Standard per la definizione della struttura del formato dei certificati digitali di chiave pubblica. Definisce, inoltre, le caratteristiche di un'Infrastruttura a Chiave Pubblica (PKI).

1.3 Riferimenti

1. Contratto N° 6604 di Repertorio N° 2500 di Raccolta sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Imprese composto da InfoCamere (mandataria) e NETikos in data 25 Febbraio 2005
2. Progetto 240029 - Infrastruttura a chiave pubblica PKI -Reg. Toscana Linee guida per il profilo dei certificati

Riferimenti tecnici

3. RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile
4. RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)"
5. RFC 2527 (1999): "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework"
6. Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8

1.4 Responsabile del Manuale Operativo

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

InfoCamere S.C.p.A.
Responsabile Area Sistemi di Sicurezza informatica
Corso Stati Uniti 14
35127 Padova

Telefono: 049 828 8111
Fax : 049 828 8406
Call Center: 800-901906 (lunedì – venerdì ore 8-18)

Web: <http://www.card.infocamere.it>
e-mail: firma.digitale@infocamere.it

2. Caratteristiche del servizio

2.1 Soggetto fornitore

Il servizio di certificazione per la firma del software viene fornito dall'Ente di Certificazione InfoCamere S.C.p.A. secondo le procedure e le condizioni stabilite nel presente manuale e nelle Condizioni di Contratto ad esso allegate.

I dati del fornitore sono riportati nella seguente tabella:

Tabella 2.1

Denominazione Sociale	InfoCamere - Società Consortile di Informatica delle Camere di Commercio Italiane per azioni
Sede legale	Piazza Sallustio, 21 – 00187 Roma
Rappresentante legale	Dott. Giuseppe Pichetto In qualità di Presidente del Consiglio di Amministrazione
Direzione Generale	Via G.B. Morgagni, 30H – 00161 Roma
N° telefono	06-442851
N° fax	06-44285255
N° Iscrizione Registro Imprese	Trib. di Roma 1/95
N° partita IVA	02313821007
Sito web	Http://www.card.infocamere.it/
Sede Operativa	Corso Stati Uniti, 14 – 35127 Padova

2.1.1 Oggetto del servizio

Generalmente, la distribuzione di software sulla rete pone problemi di sicurezza sia da un punto di vista di integrità, sia per quanto riguarda l'origine dello stesso: il software, di cui non si conosce sempre con certezza la provenienza, viene filtrato da una serie di computer intermedi prima di raggiungere l'utente destinatario con il rischio di manipolazioni durante il suo percorso. Inoltre, sebbene milioni di utenti scarichino software ogni giorno senza incidenti, esiste un rischio potenziale (accidentale o intenzionale) di danneggiare i dati e i sistemi dei singoli utenti. L'utente utilizzatore spesso non ha modo di verificare la provenienza del software o se lo stesso ha subito modifiche durante il transito.

Oggetto del servizio è, dunque, la certificazione della chiave pubblica di una coppia di chiavi asimmetriche, generata dal Certificatore, la cui chiave privata è utilizzata per firmare digitalmente oggetti software.

Firmare digitalmente il software consente di assicurarne la provenienza e l'integrità, dando la possibilità ai soggetti terzi di:

- stabilire con certezza l'identità del firmatario e di conseguenza la provenienza dell'eseguibile scaricato;
- verificare l'integrità dell'oggetto firmato, determinando eventuali modifiche subite dal software, successive all'apposizione della firma;
- gestire accessi potenzialmente pericolosi da parte di software di terze parti (es. java applet) alle risorse locali del proprio sistema tramite la concessione dei privilegi richiesti dall'applicativo stesso (ad es. accessi in lettura e/o in scrittura al sistema locale).

2.2 Soggetti destinatari del servizio

Il servizio di certificazione per la firma del software oggetto del presente Manuale Operativo può essere richiesto dagli enti che fanno parte di RTRT, che vogliono garantire la provenienza e l'integrità del software da loro sviluppato e/o distribuito e che possano produrre una documentazione ufficiale che attesti l'identità o l'iscrizione presso pubblici registri o la fonte normativa, amministrativa o negoziale dei poteri del richiedente.

InfoCamere effettuerà al riguardo le opportune verifiche in fase di richiesta del servizio e potrà negare l'erogazione dello stesso in caso di falsità, incongruenze e difformità delle informazioni fornite.

2.3 Responsabile del servizio

Responsabile del servizio fornito è l'Ente Certificatore InfoCamere.

I riferimenti della persona da contattare per questioni riguardanti il servizio stesso sono riportati al paragrafo 1.4.

2.4 Tempistica

In presenza della completa e corretta documentazione richiesta dal presente Manuale Operativo e soddisfatte le condizioni in esso esposte, l'Ente di Certificazione InfoCamere, in caso di esito positivo delle verifiche effettuate, consentirà al richiedente di entrare in possesso del certificato CodeSigning una volta verificata la copertura contrattuale per la fornitura del servizio.

In caso di informazioni incomplete o inesatte InfoCamere contatterà il richiedente esponendo il problema riscontrato.

3. Procedure operative

La procedura per la generazione della coppia di chiavi asimmetriche per la firma di oggetti software e la certificazione della chiave pubblica della coppia si compone delle seguenti fasi:

1. richiesta di certificazione
2. generazione della coppia di chiavi asimmetriche ed emissione del certificato relativo alla chiave pubblica

3.1 Richiesta di certificazione

Il soggetto che effettua la richiesta potrà richiedere al Certificatore la generazione di una coppia di chiavi asimmetriche e la certificazione della corrispondente chiave pubblica per firmare software a nome:

1. dell'intera organizzazione di appartenenza;
2. di singole sotto unità organizzative dell'ente di appartenenza.

Dovranno essere forniti al Certificatore, in una delle modalità indicate nel seguito, tutti i dati necessari all'identificazione dell'ente richiedente: quest'ultimo dovrà inoltre definire una password che il Certificatore utilizzerà a protezione del file contenente la coppia di chiavi e il certificato di chiave pubblica da quest'ultimo generati: nel caso di richiesta di certificazione per più sotto unità organizzative dovranno essere definite password diverse per ciascuna unità.

Per dar corso alla procedura di certificazione, sarà necessario comunicare al Certificatore tutti i dati richiesti per l'identificazione (compilando l'apposito modulo di richiesta) e le password nelle modalità previste nel presente manuale operativo.

3.1.1 Il modulo di richiesta

Il modulo di richiesta è disponibile in formato elettronico sul sito del Certificatore all'indirizzo <http://www.card.infocamere.it/servizi/codesigning.htm>.

3.1.2 Inoltro richiesta

La documentazione prevista al paragrafo 3.1.1 potrà essere consegnata ad un Incaricato del Certificatore o inviata a quest'ultimo via posta elettronica.

Il modulo, debitamente compilato, dovrà essere sottoscritto con firma digitale a valore legale da parte di un rappresentante dell'ente richiedente (precedentemente accreditato ufficialmente presso InfoCamere dalla Regione Toscana), in modo da poterne verificare la provenienza e l'integrità, e inviati come allegato tramite posta elettronica all'indirizzo certificati.codesigning@infocamere.it.

InfoCamere darà conferma dell'accettazione della tramite l'invio di un'email firmato. Il certificato allegato all'email sarà successivamente utilizzato per crittografare gli ulteriori messaggi del richiedente al Certificatore.

Dopo l'accettazione, il richiedente dovrà inviare un nuovo messaggio ad InfoCamere. Nel corpo del messaggio di posta elettronica dovrà essere specificata una password alfanumerica, di almeno 8 caratteri, a protezione del file .p12: l'email dovrà essere **sottoscritto con firma elettronica avanzata del Soggetto richiedente** e inviato all'indirizzo sopra indicato **crittografato** in modo da garantire la riservatezza della password indicata.

InfoCamere non darà corso alla procedura di certificazione finché non avrà ricevuto la documentazione completa indicata nei paragrafi precedenti.

3.1.3 Generazione della coppia di chiavi ed emissione del certificato

InfoCamere, ricevuta la documentazione prevista, procederà alle opportune verifiche dei dati comunicati.

Nell'eventualità in cui vengano riscontrate mancanze nella documentazione inviata, ovvero non siano rispettate le modalità di invio indicate, si darà tempestiva informazione al Soggetto richiedente, con il quale saranno concordate le modalità per la sua integrazione.

Il Certificatore avvierà la procedura di verifica della documentazione inviata solo in seguito alla verifica della copertura contrattuale della richiesta.

InfoCamere provvederà, poi, a comunicare al richiedente l'eventuale esito positivo delle verifiche di cui sopra, e gli consentirà di entrare in possesso del file contenente la chiave privata per la firma del software e il certificato relativo alla chiave pubblica della coppia a fronte della verifica della sussistenza delle condizioni contrattuali.

InfoCamere non darà corso alla generazione della coppia di chiavi e all'emissione del certificato qualora i dati comunicati non risultino corretti o completi in base ai riscontri derivanti dalle verifiche poste in essere.

3.1.4 Modalità di generazione

Il Certificatore, verificate la completezza e correttezza della documentazione richiesta, provvederà alla generazione della coppia di chiavi, privata e pubblica, e alla successiva certificazione della chiave pubblica della coppia.

La chiave privata e la catena di certificazione verranno memorizzati in un file in formato PKCS#12, codificato PEM, protetto dalla password stabilita dal Soggetto richiedente.

3.1.5 Caratteristiche della chiave pubblica certificata

La lunghezza della chiave pubblica certificata (e della corrispondente chiave privata) è di 1024 bit.

3.1.6 Formato del certificato e sua validità

Il certificato emesso dall'Ente Certificatore è conforme al formato standard X.509 v3, per quanto riguarda gli attributi in esso presenti e il relativo utilizzo.

Il certificato ha durata di tre anni dal momento dell'emissione, con possibilità di rinnovo.

Gli obblighi e i diritti dell'Ente Certificatore e dei Soggetti titolari che scaturiscono dal presente Manuale e dalle Condizioni di contratto si intendono riferiti al periodo di validità del certificato emesso.

3.2 Invio del file p12 al richiedente la certificazione

Il Certificatore, effettuata la generazione del file PKCS#12, contenente la chiave privata per la firma del software e la catena di certificazione per la validazione della firma medesima, provvederà ad inviarlo come allegato via email **crittografata** all'indirizzo elettronico indicato nel modulo di richiesta compilato dal richiedente e da questo sottoscritto.

In alternativa il file potrà essere recapitato dall'Incaricato che ha ricevuto la richiesta.

3.3 Rinnovo del certificato

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

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

Il certificato emesso può essere rinnovato.

A tal fine il Certificatore informerà il titolare via e-mail, con un preavviso di almeno 30 giorni, della imminente scadenza del certificato e della possibilità di rinnovarlo con le modalità indicate nella comunicazione stessa e qui di seguito sinteticamente riportate.

In ogni caso il titolare che intende rinnovare il suo certificato deve richiedere l'emissione di un nuovo certificato prima della scadenza di quello in suo possesso.

La richiesta di rinnovo dovrà contenere una dichiarazione con la quale il titolare, sotto la propria responsabilità, confermi al Certificatore il permanere del possesso dei requisiti richiesti per la prima emissione del certificato. Con il processo di rinnovo verrà generata una nuova coppia di chiavi per la firma del software.

Oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà effettuare una nuova richiesta di certificazione nelle modalità precedentemente descritte dal presente manuale operativo.

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

3.4 Revoca e sospensione del 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.

3.4.1 Revoca

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.

Il Certificatore può eseguire la revoca del certificato su propria iniziativa, su richiesta del titolare o su richiesta della Regione Toscana. La revoca va richiesta nel caso si verifichino le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia venuta meno la segretezza della medesima, ovvero si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata stessa;
- il titolare non riesce più ad utilizzare il certificato in suo possesso;
- si verifica un cambiamento dei dati presenti nel certificato;
- termina il rapporto tra il titolare e il Certificatore;
- viene verificata una sostanziale condizione di non rispetto del presente Manuale Operativo;
- vi sia un provvedimento dell'Autorità Giudiziaria.

3.4.1.1 Revoca su iniziativa del Certificatore

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

1. il Certificatore comunica al titolare l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza;
2. la procedura di revoca del certificato viene completata con l'inserimento dello stesso nella lista dei certificati revocati o sospesi. Il titolare potrà verificare la revoca del certificato, di cui è proprietario o utilizzatore, al più tardi dopo 24 ore dalla notifica da parte del Certificatore medesimo tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito.

3.4.1.2 Revoca su iniziativa della Regione Toscana

La richiesta di revoca su iniziativa della Regione Toscana deve essere effettuata secondo la seguente modalità:

1. La Regione richiede per iscritto al Certificatore la revoca del certificato compilando e firmando (anche digitalmente) l'apposito modulo messo a disposizione dal Certificatore stesso sul proprio sito e presso gli Uffici di Registrazione, fornendo la motivazione della richiesta, allegando la relativa documentazione, se presente, e specificando gli estremi del certificato comunicati dal Certificatore al momento dell'emissione del certificato.
2. il Certificatore, verificata l'autenticità della richiesta, la comunica al Titolare, secondo le modalità di comunicazione stabilite all'atto della Identificazione e procede alla revoca del certificato, inserendolo nella lista di revoca e sospensione da lui gestita.

3.4.1.3 Revoca su iniziativa del titolare

Il soggetto titolare può richiedere la revoca telefonando al Call Center del Certificatore, fornendo la motivazione della revoca, i propri dati identificativi e gli estremi del certificato da revocare (numero seriale del certificato).

Il Certificatore, in attesa di ricevere la richiesta di revoca sottoscritta da parte del titolare del certificato, lo sospenderà sulla base delle informazioni fornite dal Call-Center.

La richiesta di revoca sottoscritta con firma digitale da parte del titolare dovrà essere inviata via e-mail all'indirizzo certificati.codesigning@infocamere.it.

3.4.2 Sospensione

Il Certificatore può eseguire la sospensione del certificato su propria iniziativa, su richiesta del titolare o della Regione Toscana. La sospensione va richiesta nel caso in cui si verificano le seguenti condizioni:

- è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il titolare o il Certificatore acquisiscono elementi di dubbio sulla validità del certificato;
- si presenta la necessità di un'interruzione della validità del certificato.

Per le modalità operative si osserva la stessa procedura prevista per la revoca, specificando che la richiesta riguarda la sospensione del certificato ed indicando la durata della sospensione.

3.4.3 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 (Directory LDAP) all'indirizzo indicato nell'estensione "CRL Distribution Point" presente nel certificato.

Per la Regione Toscana il Certificatore pubblica una CRL dedicata.

La CRL viene pubblicata in modo programmato **almeno** ogni giorno.

L'acquisizione e consultazione della CRL è a cura degli utenti, ovvero Titolari. 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.

3.4.4 Tempistica

Il tempo di attesa tra la richiesta di revoca o di sospensione e l'effettiva pubblicazione della CRL contenente il certificato revocato è al massimo di 24 ore.

3.5 Tariffe e condizioni

Le tariffe per la prima emissione e per il rinnovo dei certificati sono stabilite dal Contratto N° 6604 di Repertorio N° 2500 di Raccolta sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Imprese composto da InfoCamere (mandataria) e NETikos in data 25 Febbraio 2005.

La revoca e la sospensione dei certificati sono gratuite.

4. Condizioni Generali del contratto relativo al servizio di certificazione per la firma di oggetti Software

La presente sezione disciplina e regola il rapporto contrattuale intercorrente tra InfoCamere ed il Titolare a cui è stato erogato il servizio di certificazione per la firma di oggetti Software, nonché gli obblighi e le modalità di utilizzazione per coloro che verificano la firma di oggetti Software.

La fornitura di tale servizio al Titolare e le modalità di verifica da parte del Soggetto Terzo è regolata e disciplinata esclusivamente dal presente Manuale Operativo, dalle norme di legge vigenti, dal contratto di servizio [1] e dalla richiesta di certificazione inoltrata e debitamente sottoscritta dal Soggetto richiedente.

Il Soggetto richiedente, prima dell'inoltro della richiesta di cui al precedente punto 3.1, è tenuto a leggere attentamente ed approvare le previsioni del Manuale Operativo. Pari obbligo incombe al Soggetto Terzo che procede alla verifica di un certificato digitale.

I contratti stipulati per l'erogazione dei servizi di certificazione per la firma di oggetti Software sono sottoposti alla legge italiana.

4.1 Informativa Decreto Lgs. n. 196/03

InfoCamere S.C.p.A. titolare del trattamento dei dati forniti dall'Utente Titolare mediante la compilazione della Richiesta di cui al punto 3.1.1. del presente Manuale Operativo, informa lo stesso, ai sensi e per gli effetti di cui all'art. 13 del Decreto Legislativo 30.06.2003, n. 196, che i predetti dati personali saranno trattati, con l'ausilio di archivi cartacei e di strumenti informatici e telematici idonei a garantire la massima sicurezza e riservatezza.

Per "dati forniti" si intendono quelli forniti dal Titolare sulla Richiesta sopra citata.

Il conferimento dei dati indicati nella richiesta è obbligatorio da parte del titolare ai fini dello svolgimento del servizio, ed un'eventuale rifiuto o un conferimento parziale comporterà l'impossibilità di fornire il servizio richiesto. Parte di essi, appositamente indicati nella richiesta, verranno pubblicati nel certificato, comunicati e diffusi, anche in Paesi al di fuori dell'Unione Europea, attraverso l'inserimento nel certificato digitale.

I dati forniti verranno trattati al fine di fornire il Servizio previsto nel presente contratto e potranno essere comunicati alle società che forniscono consulenza ed assistenza tecnica al Certificatore.

In particolare, InfoCamere si riserva, su richiesta espressa da parte di terzi, di comunicare la documentazione fornita dal Titolare al momento dell'inoltro della Richiesta di emissione del certificato nonché quella relativa all'esito delle verifiche effettuate ai sensi dei precedenti punti 3.1.

Previo consenso espresso dell'Utente Titolare, i dati forniti potranno essere comunicati ad altri soggetti che offrono beni o servizi con i quali InfoCamere S.C.p.A. abbia stipulato accordi commerciali, utilizzati per lo svolgimento di ricerche di mercato, per proposte commerciali su prodotti e servizi di InfoCamere e/o di terzi, per l'invio di materiale pubblicitario e per altre comunicazioni commerciali.

L'Utente Titolare può esercitare in qualunque momento i diritti di cui all'art. 7 del Decreto Legislativo 30.06.2003, n. 196 contattando InfoCamere agli indirizzi indicati al precedente punto 1.3.

4.2 Oggetto del contratto

Oggetto del contratto è la prestazione da parte di InfoCamere del servizio di certificazione della chiave pubblica corrispondente alla coppia di chiavi (privata e pubblica) generata dal Certificatore. La chiave privata della coppia è utilizzata per firmare digitalmente oggetti software. Al fine di erogazione del servizio, InfoCamere provvede ad effettuare le verifiche e i controlli stabiliti dal

presente Manuale Operativo ed, in caso di esito positivo degli stessi, a generare, in favore del Soggetto richiedente, la coppia di chiavi asimmetriche certificando la relativa chiave pubblica.

4.3 Conclusione del contratto

Le attività regolate dal presente Manuale Operativo sono regolate dal Contratto N° 6604 di Repertorio N° 2500 di Raccolta sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Imprese composto da InfoCamere (mandataria) e NETikos in data 25 Febbraio 2005.

4.4 Utilizzo del certificato

Il certificato digitale rilasciato in base al presente Manuale Operativo può essere utilizzato unicamente per i fini dichiarati nello stesso.

Il Titolare assume ogni eventuale responsabilità, nei confronti di InfoCamere e dei terzi, per utilizzi difformi del certificato.

Il certificato digitale disciplinato dal presente Manuale Operativo ha come esclusivo utilizzo quello di consentire al titolare di garantire al Soggetto terzo la provenienza del Software scaricato e l'integrità dell'oggetto digitalmente firmato così come indicato al punto 2.2 del presente Manuale Operativo. Il certificato non dovrà essere utilizzato per finalità diverse da quella dichiarata nel campo "Extended Key Usage".

In particolare, il certificato digitale di cui al presente Manuale Operativo non è utilizzabile per dare indicazioni sulla titolarità del diritto d'autore sugli oggetti software firmati digitalmente.

4.5 Obblighi e responsabilità del Soggetto richiedente o Titolare

Il Soggetto richiedente o Titolare è tenuto a:

- fornire al Certificatore tutte le informazioni necessarie per la richiesta del servizio, garantendo la correttezza e completezza delle stesse;
- proteggere e conservare la chiave privata e il certificato relativo alla corrispondente chiave pubblica con la massima diligenza al fine di garantirne l'integrità e la riservatezza;
- richiedere tempestivamente la revoca o la sospensione dei certificati nei casi previsti dal presente manuale operativo;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- ferme restando le ipotesi di revoca e sospensione previste nel presente Manuale Operativo, informare il Certificatore delle variazioni dei propri recapiti e degli altri dati necessari per la prestazione del servizio;
- non utilizzare il certificato per fini non previsti nel presente Manuale Operativo.

Il Soggetto richiedente o Titolare si obbliga a non firmare oggetti software che:

- siano in contrasto o violino diritti di proprietà intellettuale, segreti commerciali, marchi, brevetti o altri diritti di proprietà di terzi;
- abbiano contenuti diffamatori, calunniosi o minacciosi;
- contengano materiale pornografico, osceno o comunque contrario alla pubblica morale;
- contengano virus, worm, Trojan Horse o, comunque, altre caratteristiche di contaminazione o distruttive; in ogni caso siano in contrasto alle disposizioni normative e/o regolamentari applicabili.

Il Soggetto richiedente è responsabile della veridicità dei dati comunicati nel modulo di richiesta per la fornitura del servizio relativo alla firma di oggetti software.

Qualora lo stesso abbia, anche attraverso l'utilizzo di documentazione non vera, agito in modo tale da compromettere il processo di identificazione e le relative risultanze indicate nel certificato, egli sarà

considerato responsabile di tutti i danni derivanti ad InfoCamere e/o a terzi dall'inesattezza delle informazioni contenute nel certificato, con obbligo di garantire e manlevare InfoCamere per eventuali richieste di risarcimento danni.

Il Titolare è altresì responsabile dei danni derivanti ad InfoCamere e/o a terzi nel caso di ritardo di attivazione da parte sua delle procedure previste dai Manuali Operativi per la revoca e/o la sospensione del certificato.

Il Titolare si impegna a manlevare InfoCamere da qualsiasi responsabilità nei confronti dei terzi per danni derivanti dalla mancata attuazione da parte sua delle misure di sicurezza adottabili in base allo stato delle conoscenze scientifiche e tecnologiche al momento della violazione.

4.6 Obblighi e responsabilità del Certificatore

InfoCamere è tenuta a:

- verificare che la richiesta di certificazione sia autentica;
- generare la coppia di chiavi certificando la chiave pubblica nelle modalità previste dal presente Manuale Operativo;
- informare i soggetti richiedenti in modo compiuto e chiaro sulla procedura di certificazione;
- revocare o sospendere il certificato nei casi previsti al punto 3.4 e seguenti del presente Manuale Operativo.

Il Certificatore non assume ulteriori obblighi rispetto a quelli previsti dal Contratto N° 6604 di Repertorio N° 2500 di Raccolta sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Imprese composto da InfoCamere (mandataria) e NETikos in data 25 Febbraio 2005 e dal presente Manuale Operativo.

InfoCamere, in particolare, pur fatto salvo il diritto di cui al punto 4.11, in considerazione dell'oggetto del servizio di certificazione, relativo unicamente all'attestazione della provenienza dell'oggetto software certificato, non assume alcuna responsabilità sulle informazioni ed i dati informatici contenuti nello stesso.

Il Certificatore non presta alcuna garanzia sul funzionamento e sulla sicurezza degli oggetti software certificati e scaricati dal Soggetto Terzo.

In nessun caso il Certificatore potrà essere considerato responsabile nei confronti del Soggetto richiedente, del Titolare e/o dei Soggetti terzi per i danni costituiti da lucro cessante, perdita di opportunità commerciali o di risparmi, perdita di interesse, perdita di efficienza amministrativa, danni all'immagine o perdita di reputazione commerciale.

In ogni caso, il danno complessivo risarcibile da InfoCamere al Titolare del certificato per la firma di oggetti Software non potrà superare un importo pari al costo del certificato stesso.

4.7 Obblighi e responsabilità del Soggetto Terzo

Il Soggetto terzo che utilizza un oggetto software firmato è tenuto a verificare la validità della firma apposta sullo stesso; in particolare, nel caso il Browser non sia configurabile per effettuare il controllo automatico della lista di revoca, il Soggetto terzo dovrà provvedere a tale verifica tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito.

Il Soggetto terzo deve quindi:

- verificare le informazioni contenute nel certificato di chiave pubblica;
- verificare la data di scadenza del certificato;
- verificare lo stato del certificato (revocato o sospeso)

4.8 Modificazioni in corso di erogazione

Il Certificatore si riserva il diritto di effettuare modifiche, che saranno efficaci nei confronti del Titolare dopo 30 giorni dalla comunicazione presso il recapito di cui al successivo punto 4.9, alle specifiche tecniche del Servizio ed alle previsioni del Manuale Operativo per sopravvenute esigenze tecniche, legislative e gestionali.

Il Titolare che non accetti le modifiche potrà, entro 30 giorni successivi alla data in cui esse sono state portate a sua conoscenza, recedere dal contratto provvedendo a richiedere la revoca del certificato emesso in suo favore e specificando la volontà di recesso.

Dalla data del recesso il Titolare è obbligato a non utilizzare la coppia di chiavi fornite dal Certificatore.

4.9 Comunicazioni

Ogni comunicazione scritta dovrà essere inviata al Contatto per gli utenti finali del Certificatore.

L'indirizzo email indicato dal Richiedente ai sensi del presente Manuale Operativo dovrà intendersi come suo indirizzo elettronico ai sensi dell'art. 14, 1° comma del T.U., e tutte le comunicazioni saranno a lui validamente inviate presso lo stesso.

4.10 Risoluzione del rapporto

Il rapporto si risolve automaticamente, con conseguente interruzione del Servizio, in caso di revoca del certificato, come disciplinata ai punti da 3.4. a 3.4.1.3. del presente Manuale Operativo nonché in caso di esito negativo delle verifiche di cui al punto 3.2. dello stesso.

Il Certificatore, inoltre, ha facoltà, ai sensi dell'art. 1456 codice civile, di risolvere il presente rapporto, revocando il certificato emesso, a mezzo comunicazione inviata al Titolare qualora quest'ultimo si sia reso inadempiente ad una delle obbligazioni previste a suo carico ai punti 4.4 e 4.5 del presente Manuale Operativo.

In tutti i casi sopra previsti, il Certificatore potrà cautelativamente sospendere l'erogazione del Servizio, attraverso la sospensione del certificato.