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

Ente Certificatore InfoCamere

Servizio di Certificazione per la firma del Software

Manuale Operativo

Codice documento: INDI-MOCS

Funzione emittente	Area Sistemi e Sicurezza Informatica
Redatto da	Carolina Simonato
Verificato da	Alfredo Esposito
Approvato da	Pio Barban

Nomefile:
INDI-MOCSv1r0

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento

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 ee 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 "**Servizio di Certificazione per la firma del Software - Manuale Operativo**" ed è caratterizzato dal codice documento: **INDI-MOCS**.

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

L'*object identifier* (OID) di questo documento è il seguente: **1.3.76.14.1.1.5**
Tale OID identifica:

InfoCamere	1.3.76.14
Certification-Service-Provider	1.3.76.14.1
Certificate-policy	1.3.76.14.1.1
Manuale-Operativo – Servizio di Certificazione per la firma del Software	1.3.76.14.1.1.5

Il manuale è pubblicato in formato elettronico sul sito Web del Certificatore, all'indirizzo http://www.card.infocamere.it/doc/manuali.htm.

1.1 Novità introdotte rispetto alla precedente emissione

Versione/Release n° :	1.0	**Data Versione/Release** :	03/02/2003
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione		

1.2 Termini e definizioni

Certificato, Certificato Digitale, Certificato X.509

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del Soggetto titolare e la chiave pubblica certificata. Nel certificato compaiono altre informazioni tra cui:

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

Certificatore

È l'ente che fornisce il Servizio di Certificazione. Ai fini del presente documento Certificatore è InfoCamere S.C.p.A.

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.

Firma digitale

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 documenti informatici.

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 **P**rivacy **E**nhanced **M**ail, 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 **P**ublic **K**ey **C**riptography **S**tandards, 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.

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 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: 06 4428 5555 (lunedì – venerdì ore 8-20; sabato ore 8-14)

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**

2.2 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).

2.3 Soggetti destinatari del servizio

Il servizio di certificazione per la firma del software può essere richiesto da enti privati o pubblici, i quali vogliano 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.

2.4 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 1.3.

2.5 Tempistica

In presenza della completa e corretta documentazione richiesta dal presente Manuale Operativo e soddisfatte le condizioni in esso riportate, l'Ente di Certificazione InfoCamere, in caso di esito positivo delle verifiche effettuate, consentirà al richiedente di entrare in possesso della coppia di chiavi asimmetriche e del certificato relativo alla chiave pubblica della coppia una volta completato il pagamento 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 (§ 3.2.1) 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 o il form elettronico, e le password nelle modalità previste nel presente manuale operativo, nonché fornire i documenti aggiuntivi di seguito indicati.

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.Detto modulo dovrà essere inviato debitamente compilato, sottoscritto e munito degli eventuali timbri della struttura di appartenenza.

In particolare il modulo di richiesta dovrà essere sottoscritto:

a) dal legale rappresentante, in caso di società commerciali e altre persone giuridiche;
b) dal rappresentante, per altri enti di diritto privato;
c) dall'imprenditore titolare di partita I.V.A, per le imprese individuali;
d) dal rappresentante dell'ente o dai funzionari da questo espressamente delegati, per gli enti ed organismi pubblici.

3.1.2 La documentazione aggiuntiva

Unitamente al modulo di richiesta, il richiedente dovrà fornire la fotocopia di un suo documento di identificazione, valido e non scaduto, scelto tra i seguenti (cfr. art. 35 Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445):

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

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

Dovrà, inoltre, essere fornita la seguente documentazione di competenza a seconda della categoria di appartenenza:

a) certificato di attribuzione della partita I.V.A., per imprese non iscritte presso il Registro Imprese;
b) copia dell'atto costitutivo, per altri enti di diritto privato;
c) altra documentazione, in originale, idonea al conferimento dei poteri al soggetto incaricato della richiesta di certificazione secondo l'organizzazione interna della struttura di appartenenza, nel caso di enti ed organismi pubblici.

3.1.3 Inoltro richiesta

La documentazione prevista ai paragrafi 3.1.1 e 3.1.2 potrà essere consegnata ad un Incaricato del Certificatore o inviata a quest'ultimo in uno dei seguenti modi.

3.1.3.1 Inoltro via posta elettronica

Il Soggetto richiedente potrà inviare il modulo di richiesta in formato elettronico, scaricandolo dal sito del Certificatore all'indirizzo http://www.card.infocamere.it/servizi/codesigning.htm.

Il modulo, debitamente compilato, ed i file contenenti la documentazione richiesta (§ 3.1.1 e 3.1.2) dovranno essere sottoscritti con firma digitale a valore legale da parte del Soggetto richiedente, in modo da poterne verificare la provenienza e l'integrità, e inviati come allegato tramite posta elettronica all'indirizzo **certificati.codesigning@infocamere.it**.
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 digitale 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.

3.1.3.2 Inoltro via Web

Il soggetto che effettua la richiesta di certificazione potrà alternativamente inviare i dati necessari alla sua identificazione compilando un apposito "form" elettronico presente sul sito del Certificatore all'indirizzo Internet http://www.card.infocamere.it/servizi/codesigning.htm
Il form riprodurrà gli stessi campi previsti dal modulo di richiesta e dovrà essere sottoscritto anche in questo caso con firma digitale del Soggetto richiedente dopo essere stato debitamente compilato.

In questo caso il richiedente dovrà comunicare la password prevista a protezione del file PKCS#12 tramite il form: tale password dovrà essere alfanumerica, compresa tra 8 e 16 caratteri. Al momento della sottomissione dei dati, verrà generata un ulteriore password da parte del Certificatore e comunicata in risposta all'utente.
L'utente dovrà annotare quest'ultima password e conservarla in modo protetto per poterla poi utilizzare come mezzo di autenticazione al momento dello scarico del file.
Sarà comunque necessario, per dar corso alla procedura di certificazione, inviare, contestualmente ai dati identificativi, la documentazione aggiuntiva di cui al punto 3.1.2, sottoscritta con firma digitale del Soggetto richiedente.

3.2 Generazione della coppia di chiavi ed emissione del certificato

InfoCamere, ricevuta la documentazione prevista ai punti 3.1.1 e 3.1.2, 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 inviatagli solo in seguito alla ricezione del pagamento per la stessa.

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 del completamento del pagamento per lo stesso.

Per informazioni sulle modalità di pagamento e sulle tariffe previste si rimanda ad apposito listino, come indicato al paragrafo 4.1.

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.

3.2.1 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.

3.2.2 Caratteristiche della chiave pubblica certificata

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

3.2.3 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 (si veda l'allegato A per la descrizione esemplificativa di contenuto ed estensioni di un certificato per la firma del software). Il certificato ha durata di un anno 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.

3.3 Invio del file p12 al richiedente la certificazione

Il file p12, contenente la chiave privata per la firma del software e la catena di certificazione per la validazione della firma medesima, verrà inviato al richiedente in una delle seguenti modalità, a seconda di quella seguita al momento della richiesta.

3.3.1 Invio tramite posta elettronica

Nel caso in cui la richiesta sia pervenuta via email, il Certificatore, effettuata la generazione del file PKCS#12, provvederà ad inviarlo come allegato via email **crittografata** all'indirizzo elettronico indicato nel modulo di richiesta compilato dal richiedente e da questo sottoscritto.

3.3.2 Scarico del file p12 da Web

Qualora la richiesta sia stata effettuata via Web, il Certificatore provvederà a notificare via email all'utente richiedente, all'indirizzo da lui dichiarato, l'avvenuta certificazione e ad indicare contestualmente l'indirizzo Internet da dove scaricare il file p12. Lo scarico di tale file, **in modalità protetta**, potrà avvenire in seguito all'identificazione dell'utente tramite inserimento di una userid e una password: la userid sarà costituita dall'indirizzo di email del Soggetto richiedente, mentre la password sarà quella generata dal Certificatore e trasmessa all'utente al momento della sottomissione dei suoi dati tramite form elettronico.
Avvenuto lo scarico del file p12, questo non sarà più disponibile per ulteriori successivi scarichi.

3.4 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.

3.5 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.

3.5.1 Revoca

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

- la chiave privata sia stata compromessa, ovvero sia venuta meno la segretezza della chiave, ovvero si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave;
- 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.

3.5.1.1 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 la pubblicazione nella lista dei certificati revocati o sospesi. Il titolare potrà verificare la revoca del certificato al più tardi dopo 24 ore dalla notifica inviatagli dal Certificatore, tramite la funzionalità messa a disposizione da quest'ultimo sul proprio sito.

3.5.1.2 Revoca su iniziativa del titolare

Il soggetto titolare può richiedere la revoca telefonando al Call Center del Certificatore (numero 0644285555, orario 8-20 dal lunedì al venerdì, 8-14 il sabato), 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.

3.5.2 Sospensione

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

- è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
- il titolare 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 procedura riportata ai punti 3.5.1.1 e 3.5.1.2, specificando che la richiesta riguarda la sospensione del certificato.
Il titolare è tenuto comunque a sottoscrivere con firma digitale la richiesta di sospensione e ad inviarla al Certificatore nella modalità indicata al paragrafo precedente (richiesta di revoca).

3.5.3 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.
La CRL viene pubblicata giornalmente dal Certificatore ed emessa sempre integralmente. Ogni elemento della lista CRL contiene nell'apposita estensione la data e l'ora di richiesta della revoca o sospensione.

L'acquisizione e consultazione della CRL è a cura dei soggetti terzi, ovvero Titolari.

3.5.4 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.

4. Tariffe e condizioni

4.1 Tariffe

Sono previste tariffe e apposite modalità di pagamento per l'emissione e il rinnovo del certificato: le tariffe stabilite sono funzione delle quantità trattate e soggette all'andamento del mercato.
La revoca e la sospensione dei certificati sono gratuite.

Per ottenere informazioni al riguardo si prega di contattare l'Area Sistemi di Sicurezza informatica oppure il Call Center ai riferimenti riportati al paragrafo 1.3.

5. 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, dalle presenti Condizioni generali di contratto 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.

5.1 Informativa ex l. n. 675/96

InfoCamere S.C.p.A. titolare del trattamento dei dati forniti dal Soggetto richiedente 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. 10 della Legge 31.12.1996, n. 675, 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 richiedente sulla Richiesta sopra citata.

Il conferimento dei dati indicati nella richiesta è obbligatorio da parte del Soggetto richiedente ai fini dello svolgimento del servizio e della conclusione del contratto, ed un'eventuale rifiuto o un conferimento parziale comporterà l'impossibilità di concludere il contratto. 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 relativo la firma di oggetti Software.

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 Soggetto richiedente al momento dell'inoltro della Richiesta di certificazione per la firma di oggetti Software, nonché l'esito delle verifiche effettuate ai sensi del precedente punto 3.2., ad esclusione comunque della fotocopia del documento di identificazione

Previo consenso espresso del Soggetto richiedente, 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.

Il Soggetto richiedente o Titolare può esercitare in qualunque momento i diritti di cui all'art. 13 della legge n. 675/1996 contattando InfoCamere agli indirizzi indicati al precedente punto 1.3.

5.2 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.

5.3 Conclusione del contratto

Il contratto si considera perfezionato nel momento in cui InfoCamere riceve il modulo di richiesta debitamente sottoscritto, inoltrata secondo le modalità previste dal presente Manuale Operativo e completo della documentazione di cui al punto 3.1.2

InfoCamere non accetterà richieste inviate con modalità diverse da quelle indicate nel presente Manuale Operativo.

5.4 Durata del contratto e del certificato

L'erogazione del servizio disciplinata dal presente contratto ha durata pari a quella indicata nel certificato di chiave pubblica: tale durata è indicata nel campo "validità (validity)" dello stesso.

Prima della scadenza il Titolare può richiedere il rinnovo del certificato ai sensi del punto 3.4 del presente Manuale Operativo.

Il rinnovo comporta la proroga del contratto di erogazione del servizio fino alla scadenza o revoca del certificato rinnovato.

Un certificato scaduto non può essere rinnovato.

5.5 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.

5.6 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.

5.7 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 3.5 e seguenti del presente Manuale Operativo.

Il Certificatore non assume ulteriori obblighi rispetto a quelli previsti dalle presenti condizioni generali di contratto e dal presente Manuale Operativo.

InfoCamere, in particolare, pur fatto salvo il diritto di cui al punto 5.12, 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.

5.8 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)

5.9 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 5.10, alle specifiche tecniche del Servizio ed alle previsioni del Manuale Operativo per sopravvenute esigenze tecniche, legislative e gestionali.
Le modifiche di cui al precedente comma potranno comportare modificazione di prezzi, tariffe e condizioni contrattuali.
Il Titolare che non accetti le modifiche potrà, nei 30 giorni successivi alla data in cui esse sono state portate a sua conoscenza, recedere dal contratto richiedendo 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.

5.10 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.

5.11 Diritto di recesso

Il Titolare, entro il termine di 10 giorni lavorativi a decorrere dalla conclusione del contratto, ha il diritto di recedere dal contratto a mezzo lettera raccomandata a.r. da comunicarsi con le modalità stabilite al punto 5.10, 1° comma.

5.12 Risoluzione del rapporto

Il presente contratto si risolve automaticamente, con conseguente interruzione del Servizio, in caso di revoca del certificato, come disciplinata ai punti da 3.5. a 3.5.1.2. del presente Manuale Operativo nonché in caso di esito negativo delle verifiche di cui al punto 3.2. dello stesso.
In caso di mancato o non corretto adempimento di quanto previsto ai punti 5.5. e 5.6 del presente Manuale Operativo il Certificatore avrà facoltà, ai sensi dell'art. 1456 codice civile, di risolvere il presente contratto revocando il certificato della chiave pubblica emessa, a mezzo comunicazione da inviarsi tramite raccomandata a.r. al Titolare.
In tutti i casi di presunta violazione da parte del Titolare delle previsioni contenute nel presente Manuale Operativo, InfoCamere si riserva l'obbligo di sospendere cautelativamente l'erogazione del Servizio, attraverso la sospensione del certificato.

ALLEGATO A

Formato del Certificato per la firma del SoftWare

Di seguito un esempio di profilo del Certificato per la firma del Software.

Attributo/Estensioni	Valore/Informazione
Version	Version 3
SerialNumber	Numero intero
Signature	sha1-with-rsa-encryption
Issuer	
Country Name	IT
Organization Name	InfoCamere ScpA
Organizational Unit Name	Ente Certificatore del Sistema Camerale
Common Name	InfoCamere Servizi di Certificazione
Validity	1 anno
Subject	*Esempio:*
Country Name	IT
Organization Name	Denominazione sociale dell'Organizzazione
Organizational Unit Name	Unità Organizzativa all'interno dell'Organizzazione
Common Name	***Ente a nome del quale viene firmato il SW (*)***
E-mail Address	email@esempio.it
State or Province	Triveneto
Locality	Trento
Serial number	Codice fiscale dell'Organizzazione
SubjectPublicKeyInfo	Algoritmo: rsa-encryption Lunghezza della chiave: RSA 1024 bit
AuthorityKeyIdentifier	(non critica) valore SHA-1 della chiave pubblica: 0x847bef62 2ede74e5 111f7539 fbbc2f1b 9cb63255
BasicConstraints	(non critica) cA=FALSE
KeyUsage	(non critica) Digital Signature
SubjectAltName	(non critica)
RFC Name	*indirizzo email di riferimento dell'utente richiedente (email@esempio.it)*
URI	Indirizzo ldap dell'entry in cui è memorizzato il certificato per la firma del software all'interno del directory dell'ente certificatore
IssuerAltName	(non critica)
RFC Name	servizi.certificazione@infocamere.it
URI	Indirizzo ldap dell'entry in cui è memorizzato il certificato di chiave pubblica di CA corrispondente alla chiave privata con cui il certificatore ha sottoscritto il certificato per la firma del software

CertificarePolicies PolicyIdentifier PolicyQualifier: cPSuri	(non critica) OID=1.3.76.14.1.1.5 http://www.card.infocamere.it/doc/manuali.htm
CRLDistributionPoints	(non critica) Indirizzo ldap dell'entry del directory del Certificatore in cui è memorizzata la lista dei certificati revocati
Extended Key Usage:	Code Signing
Subject Key Identifier	(non critica) valore SHA-1 della chiave pubblica

(*) L'ente a nome del quale viene firmato il SW può coincidere con l'Organization o con l'Organization Unit, ovvero rappresentare una ulteriore suddivisione organizzativa all'interno di quest'ultima.