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

Ente Certificatore InfoCamere

Servizio di Certificazione Web Server

Manuale Operativo

Codice documento: INDI-MOWS

Funzione emittente	U. O. Firma Digitale
Redatto da	Fabio Uliano
Verificato da	Alfredo Esposito
Approvato da	Pio Barban

Nomefile:
INDI-MOWSv1r1

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 del Web Server.

Le indicazioni di questo documento hanno validità per le attività relative ad InfoCamere nel ruolo di Certificatore, per i soggetti richiedenti ed utilizzatori del servizio.
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 emessi durante la loro vigenza e fino alla prima scadenza degli stessi.

Il presente documento è denominato "**Servizio di Certificazione Web Server - Manuale Operativo**" ed è caratterizzato dal codice documento: **INDI-MOWS**.

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

L'*object identifier* (OID) di questo documento è il seguente: **1.3.76.14.1.1.7**
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 Web Server	1.3.76.14.1.1.7

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** :	04/07/2002
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione		

Versione/Release n° :	1.1	**Data Versione/Release** :	06/08/2004
Descrizione modifiche:	Vengono aggiornati i riferimenti al nuovo Codice in materia di protezione dei dati personali laddove precedentemente si indicavano gli articoli della ex. Legge 675/96		

Motivazioni :	Adeguamento del presente manuale operativo in seguito alla pubblicazione del Decreto Legislativo del 30 Giugno 2003, n° 196, Gazzetta Ufficiale, Serie Generale, n.174 del 29 Luglio 2003.

1.2 Termini e definizioni

Certificatore

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

Client

È l'applicativo software, in particolare un browser Web, utilizzato dall'utente che si connette ad un sito di un Web server certificato, con cui vuole instaurare una comunicazione sicura e protetta.

Firma Digitale

È 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 (cfr. D.P.R 28 Dicembre 2000, n. 445)

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#10

PKCS, acronimo di **P**ublic **K**ey **C**ryptography **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#10 definisce la struttura della richiesta per la certificazione della chiave pubblica di una coppia di chiavi asimmetriche.

Soggetto richiedente

È la persona fisica, l'ente di diritto privato o pubblico, proprietario o utilizzatore di un server Web, che richiede il servizio di certificazione per il proprio dominio Internet.

SSL

Acronimo di **S**ecure **S**ockets **L**ayer, è il protocollo che consente di stabilire una comunicazione autenticata e riservata tra le parti comunicanti, client e server.

Titolare

È il soggetto richiedente che abbia ottenuto la certificazione per il proprio dominio Internet.

Utente

È il soggetto terzo che instaura, generalmente tramite un browser o server Web, una comunicazione SSL con il Web server certificato.

Web server

È il software che consente di distribuire informazioni su Internet e riceve richieste da parte di un browser Web restituendo i dati richiesti.

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 riguardanti questo documento e il servizio in esso descritto è:

InfoCamere S.C.p.A.
Responsabile U.O. Firma Digitale
Corso Stati Uniti 14
35127 Padova

Telefono: 049 828 8111
Fax : 049 828 8406
Call Center: 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 del Web server viene fornito dall'Ente di Certificazione InfoCamere S.C.p.A. secondo le procedure e le condizioni stabilite nel presente Manuale Operativo.

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	**Codice Fiscale 02313821007 (già 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

Oggetto del servizio è la certificazione della chiave pubblica appartenente alla coppia di chiavi asimmetriche (chiave privata e chiave pubblica) generata dal Web server in uso o di proprietà dei soggetti richiedenti il servizio di certificazione per il proprio dominio Internet. La certificazione è rilasciata esclusivamente a Web Server dedicati, ovvero non saranno certificati Web server adibiti ad Hosting condiviso.

Con la certificazione del Web server è possibile instaurare una comunicazione sicura tra server e client basandosi sul protocollo SSL e garantendo al client l'identità del server comunicante, ovvero del dominio a cui ci si connette, e la riservatezza dei dati trasmessi.

In tal modo l'utente che si connette, tramite un browser Web (client), al dominio corrispondente ad un Web server certificato avrà la certezza dell'identità della parte comunicante, della riservatezza delle transazioni e dell'integrità dei dati.

2.3 Soggetti destinatari del servizio

Il servizio di certificazione può essere richiesto da soggetti privati, enti privati o enti pubblici, i quali siano legittimi proprietari di un dominio regolarmente registrato e 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, nonché quella relativa alla titolarità del dominio. Il richiedente dovrà, inoltre, garantire, dichiarandola per iscritto, l'univoca corrispondenza tra il dominio da certificare ed il Web server che lo "ospita".

InfoCamere effettuerà al riguardo le opportune verifiche in fase di richiesta del servizio e potrà negare l'emissione del certificato 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 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 esposte, l'Ente di Certificazione InfoCamere, in caso di esito positivo delle verifiche effettuate, consentirà al richiedente di entrare in possesso del certificato Web Server 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 certificazione di un dominio Internet si compone delle seguenti fasi:

1. richiesta del certificato
2. emissione del certificato

3.1 Richiesta del certificato

3.1.1 Il modulo di richiesta

Il soggetto richiedente dovrà inviare all'Ente Certificatore InfoCamere il modulo di richiesta, messo a disposizione da quest'ultimo, debitamente compilato, sottoscritto, e munito degli eventuali timbri della struttura di appartenenza.

In particolare il modulo di richiesta dovrà essere sottoscritto dal soggetto richiedente secondo la seguente casistica:

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

Nella richiesta dovrà essere esattamente indicato il nome del dominio per il quale si chiede la certificazione, il quale dovrà risultare inserito negli archivi esistenti nella rete Internet; qualora si tratti di domini di livello oltre il secondo sarà sufficiente verificare nei suddetti archivi la presenza del dominio principale.

Il modulo di richiesta è disponibile in formato elettronico sul sito http://www.card.infocamere.it/servizi/webserver.htm.

3.1.2 La documentazione aggiuntiva

Unitamente al modulo di richiesta, il soggetto richiedente dovrà fornire la fotocopia di un suo documento di identificazione, valido e non scaduto, scelto tra i seguenti qui di seguito indicati (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.

Al modulo di richiesta va, inoltre, allegata copia della documentazione comprovante la registrazione di un dominio Internet, ove presente e necessaria in base alle precedenti previsioni.

3.1.3 Il file CSR (Certificate Signing Request)

Oltre al modulo di richiesta e alla documentazione aggiuntiva deve essere inviato all'Ente Certificatore il file con la richiesta di certificazione contenente la chiave pubblica del server: tale file deve essere in formato PKCS#10 e codificato PEM. Le modalità per la generazione di tale file e i server supportati sono descritti al punto seguente.

3.1.3.1 Generazione del CSR

Il file CSR, contenente la richiesta di certificazione della chiave pubblica del Web server in formato PKCS#10, viene generato dallo stesso una volta creata la coppia di chiavi asimmetriche; tale file, oltre alle informazioni indicate qui di seguito, conterrà la firma del Web server generata con la chiave privata corrispondente alla chiave pubblica che si desidera certificare, in modo da fornire prova di possesso della medesima chiave privata.

Nel file CSR dovranno essere inserite almeno le seguenti informazioni negli appositi campi previsti dallo stesso standard PKCS#10 (indicati di seguito tra parentesi):

- il dominio del Web server da certificare (*Common Name*);
- la denominazione sociale del proprietario del dominio da certificare (*Organization*);
- l'unità organizzativa del proprietario del dominio all'interno dell'ente specificato al punto precedente (*Organizational Unit*);
- il codice del paese dell'ente proprietario del dominio (*Country*, es. Italia=IT);
- un indirizzo di posta elettronica di riferimento, da utilizzare per ricevere comunicazioni specifiche da parte dell'Ente Certificatore o suoi delegati (*E-mail address*).

Per completezza, possono essere eventualmente inseriti nella richiesta di certificazione PKCS#10 i seguenti attributi standard:

- *State or Province*;
- *Locality*.

con lo scopo di fornire indicazioni di carattere geografico relative al proprietario o legittimo utilizzatore del dominio da certificare.
Per ulteriori approfondimenti e chiarimenti sul significato ed uso di detti campi si faccia riferimento allo standard X.509 dell'ITU-T.

Le informazioni inserite nella richiesta PKCS#10, siano esse obbligatorie o opzionali, dovranno esattamente corrispondere a quelle inserite nel modulo di richiesta cartaceo o elettronico sottoscritto dal richiedente la certificazione.
Il Certificatore, in fase di istruttoria della documentazione inviata dal richiedente, provvederà anche al controllo di tale corrispondenza.

3.1.3.2 Caratteristiche della chiave pubblica da certificare

La lunghezza della chiave pubblica di cui si richiede la certificazione (e della corrispondente chiave privata) non deve essere inferiore ai 1024 bit allo scopo di fornire adeguate garanzie di sicurezza.

La certificazione della chiave pubblica può essere effettuata per ogni tipologia di Web server presente nel mercato, utilizzando gli algoritmi crittografici ammessi dal protocollo SSL e supportati dai browser Web più diffusi.

I Web server di cui si richiede la certificazione devono essere situati in luoghi protetti in modo tale da prevenire l'eventuale compromissione, perdita, individuazione, modifica o utilizzo non autorizzato della chiave privata del server.

Detto server deve, inoltre, dare adeguate garanzie di sicurezza logica, ovvero

- essere amministrato secondo procedure documentate;
- essere protetto da firewall;
- essere opportunamente configurato.

Il Certificatore esclude ogni responsabilità per il non rispetto delle condizioni di sicurezza sopra esposte.

3.1.4 Inoltro richiesta

La documentazione prevista ai paragrafi 3.1.1, 3.1.2 e 3.1.3 può essere inviata in uno dei seguenti modi.

3.1.4.1 Inoltro via posta ordinaria

Il soggetto richiedente invierà un plico con ricevuta di ritorno contenente il modulo di richiesta, la prescritta documentazione e il CD-ROM o dischetto floppy con il file contenente il CSR al seguente indirizzo:

InfoCamere S.C.p.A
Responsabile U.O Firma Digitale
Corso Stati Uniti 14
35127 Padova

3.1.4.2 Inoltro via posta elettronica

Il soggetto richiedente potrà inviare il modulo di richiesta in formato elettronico, compilando gli appositi campi di suddetto documento scaricabile dal sito http://www.card.infocamere.it/servizi/webserver.htm.

Il modulo debitamente compilato dovrà essere sottoscritto con firma digitale del soggetto richiedente.

Il modulo, la documentazione aggiuntiva, se in formato elettronico, e il file contenente il CSR, dovranno essere poi inviati come allegato tramite posta elettronica all'indirizzo certificati.webserver@infocamere.it.
Qualora i documenti aggiuntivi di cui al paragrafo 3.1.2, non fossero disponibili in formato elettronico, dovranno essere spediti via posta ordinaria all'indirizzo riportato al paragrafo 3.1.4.1.

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

3.1.4.3 Inoltro via Web

Il soggetto richiedente la certificazione del proprio dominio 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/webserver.htm e inviare contestualmente il CSR seguendo le istruzioni ivi riportate.
Il form suddetto riprodurrà gli stessi campi previsti dal modulo di richiesta e dovrà essere sottoscritto con firma digitale dopo essere stato debitamente compilato.

Sarà comunque necessario, per dar corso alla procedura di certificazione, inviare via posta ordinaria, ovvero via posta elettronica se disponibile in formato elettronico, la documentazione aggiuntiva di cui al punto 3.1.2.

3.2 Emissione del certificato

InfoCamere, ricevuta la documentazione prevista ai punti 3.1.1, 3.1.2 e 3.1.3, procederà alle opportune verifiche dei dati comunicati.

Nell'eventualità in cui vengano riscontrate mancanze nella documentazione inviata si darà tempestiva informazione al soggetto richiedente, con il quale saranno concordate le modalità per la sua integrazione.

InfoCamere verificherà inoltre l'effettiva presenza in rete del dominio da certificare.

Il Certificatore avvierà la procedura di verifica della documentazione inviatagli solo in seguito alla ricezione del pagamento per la stessa.

InfoCamere provvederà a comunicare al richiedente l'eventuale esito positivo delle verifiche di cui sopra, e metterà a disposizione il certificato richiesto a fronte del pagamento per lo stesso.

InfoCamere non darà corso all'emissione del certificato qualora i dati comunicati non risultino corretti o completi in base ai riscontri derivanti dalle verifiche poste in essere.

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

Il soggetto richiedente ha facoltà di mettere a disposizione sul proprio sito il certificato di chiave pubblica corrispondente alla chiave privata con cui l'Ente Certificatore InfoCamere sottoscrive i certificati Web server. Tale certificato è anche scaricabile dal sito del Certificatore alla voce "Prodotti e Servizi", seguendo le procedure indicate nel sito medesimo. Il prelievo e il successivo inserimento di tale certificato nella lista dei certificati di CA "trusted" gestita dai client e server degli utenti consentiranno di validare correttamente l'intera catena di certificazione (certificato di Web server e certificato di CA), permettendo così di verificare l'identità del Web server comunicante.

3.2.1 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 Web server).

Il certificato ha durata di un anno dal momento dell'emissione, salvo possibilità di rinnovo.

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

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.

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. Dovrà, inoltre, provvedere ad inviare una nuova richiesta PKCS#10 di rinnovo per il certificato in questione.
Il Certificatore verificherà la veridicità delle dichiarazioni fornite dal titolare.

Oltre la data di scadenza non sarà possibile effettuare il rinnovo ma si dovrà procedere alla generazione di un nuovo certificato nelle modalità previste per la prima emissione.

La chiave privata di firma di cui sia scaduto il certificato della relativa chiave pubblica, non può essere più utilizzata.

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

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 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 Web Server, 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 del titolare

Il soggetto titolare segnala la necessità di revocare il certificato Web server, telefonando al Call Center del Certificatore (numero 0644285555, orario 8-20 dal lunedì al venerdì, 8-14 il sabato) e fornendo la motivazione della revoca, nonché i propri dati identificativi e gli estremi del certificato da revocare (numero seriale del certificato).

Il richiedente è tenuto a sottoscrivere la richiesta di revoca e inviarla al Certificatore: la revoca verrà effettivamente evasa una volta giunta la richiesta sottoscritta da parte del titolare del certificato Web server.
Il Certificatore, in attesa di ricevere la documentazione completa, sospenderà il certificato.

3.4.2 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 3.4.1.1 e 3.4.1.2, specificando che la richiesta riguarda la sospensione del certificato.

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 Web server.
La CRL viene pubblicata in modo programmato 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 la sua realizzazione tramite pubblicazione della CRL 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'Unità Organizzativa Firma Digitale oppure il Call Center ai riferimenti riportati al paragrafo 1.3.

5. Condizioni Generali del contratto relativo al servizio di certificazione Web Server

La presente sezione disciplina e regola il rapporto contrattuale intercorrente tra InfoCamere ed il Titolare del certificato Web Server, nonché gli obblighi e le modalità di utilizzazione per coloro che verificano il certificato Web Server.

La fornitura del servizio di certificazione Web Server da parte di InfoCamere al Titolare ed agli Utenti è regolata e disciplinata esclusivamente dal presente Manuale Operativo, dalle norme di legge vigenti e dalla richiesta inoltrata dal Titolare.

Il Titolare, 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 è in capo agli Utenti del relativo certificato.

I contratti stipulati per l'erogazione del servizi di certificazione Web Server sono sottoposti alla legge italiana.

5.1 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 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 Web Server.

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 Web Server nonché quella relativa all'esito delle verifiche effettuate ai sensi del precedente punto 3.2.

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.

5.2 Oggetto del servizio

Oggetto del contratto è la prestazione da parte di InfoCamere del servizio di certificazione della chiave pubblica generata dal Web Server su cui risiede il dominio da certificare. Al fine di detta certificazione, InfoCamere provvede alla effettuazione delle verifiche e dei controlli stabiliti dal presente Manuale Operativo ed, in caso di esito positivo degli stessi, all'emissione in favore del Titolare di un certificato digitale associato alla chiave pubblica sottoposta a certificazione.

5.3 Conclusione del contratto

Il contratto si considera perfezionato nel momento in cui InfoCamere riceve la richiesta di certificazione del Web Server, inoltrata secondo le modalità previste dal presente Manuale Operativo e completa della documentazione di cui al punto 3.1.2.

InfoCamere non accetterà richieste inviate con modalità diverse da quelle indicate.

5.4 Durata del contratto e del certificato

Il contratto di certificazione ha durata pari a quella del certificato digitale di Web Server indicata nel campo "validità (validity)" dello stesso.

Prima della scadenza il Titolare può richiedere il rinnovo del certificato ai sensi del punto 3.3. del presente Manuale Operativo.

Il rinnovo comporta la proroga del contratto di certificazione 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, ed InfoCamere non assume alcuna responsabilità, salvo il caso di dolo o colpa grave, per utilizzi difformi.

In particolare, il certificato digitale disciplinato dal presente Manuale Operativo ha quale esclusivo utilizzo quello di "Web Server Authentication", così come indicato nel campo "Extended Key Usage" dello stesso, e non dovrà essere utilizzato per finalità diverse da quella dichiarata.

E' fatto divieto di utilizzare il certificato digitale Web Server su domini su cui risiedano dati informatici:

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

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 di certificato, garantendo la correttezza e completezza delle stesse;
- proteggere e conservare le chiavi private del Web server 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;
- installare il certificato digitale rilasciato da InfoCamere in base al presente Manuale Operativo unicamente sul Web Server corrispondente al dominio indicato nel medesimo certificato;
- 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.

Il soggetto richiedente o titolare è responsabile della veridicità dei dati comunicati nella richiesta di registrazione, con particolare riferimento alla titolarità del dominio.

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 soggetto Titolare è unico responsabile della sicurezza informatica del Web Server per il quale è stato rilasciato il certificato digitale, e 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;
- verificare che il richiedente la certificazione sia titolare e/o legittimo possessore del dominio sul quale è attestato il Web Server della cui chiave pubblica si richiede la certificazione;
- emettere il certificato rispettando il formato indicato nel presente manuale;
- revocare o sospendere il certificato nei casi previsti al punto 3.4. e seguenti del presente Manuale Operativo.

InfoCamere non assume alcuna responsabilità circa i collegamenti a domini esterni a quello riportato sul modulo di richiesta.

InfoCamere, inoltre, pur facendo salvo il diritto di cui al punto 5.12, in considerazione dell'oggetto del servizio di certificazione, che è relativo unicamente all'attestazione di titolarità del dominio residente sul Web server certificato, non assume alcuna responsabilità sulle informazioni ed i dati informatici contenuti nello stesso.

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

In particolare, il Certificatore non presta alcuna garanzia sul corretto funzionamento e sulla sicurezza dei macchinari hardware e dei software utilizzati dai richiedenti il certificato e dagli utilizzatori dello stesso, su usi diversi del certificato Web Server rispetto a quelli previsti dal presente Manuale Operativo, sul regolare e continuativo funzionamento di linee elettriche e telefoniche nazionali e/o internazionali, su disservizi e/o ritardi dovuti a malfunzionamento o blocco del sistema informativo derivanti da cause non imputabili ad InfoCamere stessa.

In nessun caso il Certificatore potrà essere considerato responsabile nei confronti del Richiedente, del Titolare e/o degli Utenti 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 Web Server non potrà superare un importo pari al costo del certificato stesso.

5.8 Obblighi e responsabilità dell'Utente

L'utente che si connette ad un dominio per il quale è stato rilasciato un certificato Web Server è tenuto a verificare la validità dello stesso controllando la lista di revoca relativa tramite la funzionalità messa a disposizione dal Certificatore sul proprio sito.
Il controllo di cui al comma precedente può essere effettuato automaticamente tramite apposita configurazione, secondo la procedura descritta sul sito Internet del Certificatore, del software Browser utilizzato per accedere al dominio certificato.
In particolare, l'utente deve:

- verificare le informazioni contenute nel certificato relative alla chiave pubblica della coppia di chiavi utilizzata per la certificazione del Web Server;
- verificare la data di scadenza del certificato;
- verificare lo stato del certificato (se è valido, se è stato revocato o sospeso);
- verificare che il dominio del sito a cui si è connesso corrisponda a quello indicato nel certificato Web Server.

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 con effetto immediato 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 il certificato Web Server provvedendo alla sua rimozione dal dominio certificato.

5.10 Comunicazioni

Ogni comunicazione scritta dovrà essere inviata al Contatto per gli utenti finali del Certificatore.
L'indirizzo e-mail 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 3.4. a 3.4.1.2. 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 contratto, 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 5.5. e 5.6 del presente Manuale Operativo.
In tutti i casi sopra previsti, il Certificatore potrà cautelativamente sospendere l'erogazione del Servizio, attraverso la sospensione del certificato.

ALLEGATO A

Formato del Certificato Web server

Di seguito un esempio di profilo del Certificato Web server.

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	Informatica Triveneto S.p.A
Organizational Unit Name	Direzione Tecnologie Informatiche
Common Name	www.esempio.it
E-mail Address	email@esempio.it
State or Province	Triveneto
Locality	Trento
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) KeyEncipherment
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 server 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 server
CertificarePolicies	(non critica)

PolicyIdentifier PolicyQualifier: cPSuri	OID=1.3.76.14.1.1.7 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:	Web server authentication
Subject Key Identifier	(non critica) valore SHA-1 della chiave pubblica