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

Ente Certificatore InfoCamere

Certificati "Application to Application" RTRT

Manuale Operativo

Codice documento: ICCA-A2A-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_A2A_1.0.sxw

Questa pagina è lasciata
intenzionalmente bianca

Indice

1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione:

Versione/Release n° :	1.0	**Data Versione/Release**:	19/05/2005
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 l'autenticazione dei messaggi scambiati tra applicazioni operanti nell'ambito della Rete Telematica Regionale Toscana o funzionali alle attività istituzionali della Regione. Il servizio è compreso nelle attività previste dal contratto di servizio per la Regione Toscana.

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 "Certificati "Application to Application" RTRT"
Manuale Operativo" ed è caratterizzato dal codice documento: ICCA-A2A-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: **1.3.76.14.1.1.12.6**
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 "Application to Application"	1.3.76.14.1.1.12.6

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

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.

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

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.

RTRT

Acronimo di Rete Telematica Regionale Toscana.

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 Riferimenti

Riferimenti normativi

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

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

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

[4] DELIBERAZIONE 17 febbraio 2005 Regole per il riconoscimento e la verifica del documento informatico (Deliberazione n. 4/2005)

[5] Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004)

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

[7] Circolare AIPA/CR/22 del 26 Luglio 1999

[8] Legge 15 Marzo 1997, n. 59 (c.d. legge Bassanini)

[9] Legge 24 Dicembre 1993, n. 537

[10] Legge 23 Dicembre 1993, n. 547

[11] Contratto N° 6604 di Repertorio N° 2500 di Raccolta sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Impresa composto da Infocamere (mandataria) e NETikos in data 25 Febbraio 2005

[12] Progetto 240029 - Infrastruttura a chiave pubblica PKI -Reg. Toscana Linee guida per il profilo dei certificati

Riferimenti tecnici

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

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

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

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

[17] Applicazione Gestione Chiavi - Specifiche Revisione: 01 del 25 Marzo 2005

1.4 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: 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 Application to Application (nel seguito abbreviato in A2A) 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 responsabile di un Applicazione operante esclusivamente nell'ambito della Rete Telematica Regionale Toscana.
Regione Toscana può, sotto la sua completa responsabilità, richiedere un certificato per terze parti non facenti parte di RTRT da utilizzare esclusivamente per l'instaurazione di comunicazioni sicure con la Regione stessa.
Tale certificazione non si applica nelle relazioni tra terze parti che non fanno parte di RTRT, pertanto i certificati digitali rilasciati in base al presente Manuale Operativo non possono essere utilizzati nell'ambito di relazioni in cui non sia parte un soggetto appartenente a RTRT.

Con la certificazione dell'applicazione è possibile instaurare una comunicazione sicura tra applicazione e applicazione e garantendo alle parti l'identità dell'applicazione comunicante e la riservatezza dei dati trasmessi.

2.3 Soggetti destinatari del servizio

Il servizio di certificazione può essere richiesto dalla Regione Toscana e da altri enti pubblici che fanno parte di RTRT, i quali siano autorizzati all'acquisto dal responsabile del contratto [11] della Regione Toscana.
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 1.4.

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 A2A.

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'applicazione si compone delle seguenti fasi:

1. richiesta del certificato
2. emissione del certificato

3.1 Richiesta del certificato

La richiesta verrà inoltrata alla CA tramite l'Applicazione Gestione Chiavi messa a disposizione di RTRT dall'RTI nell'ambito delle attività previste dal contratto di servizio per la Regione Toscana.
La richiesta dovrà essere autenticata tramite firma elettronica avanzata, basata su certificati memorizzati in strutture PKCS#12 emessi dal certificatore InfoCamere ai soggetti che saranno stati indicati come referenti per ciascun Ente aderente a RTRT.
In alternativa le richieste potranno essere inviate come allegato di posta elettronica.

3.1.1 Il file CSR (Certificate Signing Request)

Deve essere inviato all'Ente Certificatore, il file firmato con la richiesta di certificazione contenente la chiave pubblica dell'applicazione: tale file deve essere in formato PKCS#10 e codificato PEM, imbustato in una struttura PKCS#7 Signed Data, firmata da uno dei referenti di cui al punto precedente.

Il file CSR, contenente la richiesta di certificazione della chiave pubblica dell'applicazione in formato PKCS#10, conterrà la firma dell'applicazione 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 nome dell'applicazione da certificare (Common Name);
- la dicitura fissa "Rete Telematica Regionale Toscana (Organization);
- l'ente responsabile dell'applicazione (Organizational Unit);
- la codifica fissa "IT" per il codice identificante il paese dell'ente proprietario del dominio (Country);
- 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:

- Locality.

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

3.1.2 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.
L'algoritmo di crittografia asimmetrica da utilizzare è l'RSA.

L'applicazione deve essere attivata ed eseguita in modo tale da prevenire l'eventuale compromissione, perdita, individuazione, modifica o utilizzo non autorizzato della chiave privata.
Il server su cui opera deve essere custodito in luogo protetto ad accesso controllato e deve, inoltre, dare adeguate garanzie di sicurezza logica, ovvero

- essere amministrato secondo procedure documentate;
- essere protetto da firewall;
- essere opportunamente configurato;
- essere conforme a quanto previsto dall'Allegato B "Diciplinare tecnico in materia di misure minime di sicurezza", del d.l.vo n. 196/2003.

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

3.1.3 Inoltro richiesta

La richiesta è inoltrata tramite l'Applicazione Gestione Chiavi sopra citata oppure come allegato ad un messaggio di posta elettronica all'indirizzo citato al § 1.4.

3.1.4 Emissione del certificato

InfoCamere, verificata la provenienza, l'integrità e le autorizzazioni del mittente della busta crittografica, e verificata la sussistenza delle condizioni contrattuali, provvederà a comunicare al richiedente l'eventuale esito positivo di dette verifiche, e metterà a disposizione il certificato richiesto.
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.

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 A2A. 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 applicazione e certificato di CA), permettendo così di verificare l'identità dell'applicazione comunicante.

3.2 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 profilo del certificato è riportato nel documento [2].
Il certificato ha durata di tre anni 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.

Per i certificati A2A il rinnovo consiste in una nuova emissione. Il Certificatore informerà il titolare via e-mail, con un preavviso di almeno 30 giorni, della imminente scadenza del certificato e della

necessità di richiederne uno nuovo per garantire la continuità del servizio, con le modalità indicate nella comunicazione stessa e qui di seguito sinteticamente riportate.

La nuova richiesta sarà effettuata secondo le stesse modalità della prima.
Il Certificatore procederà alla generazione di un nuovo certificato nelle modalità previste per la prima emissione, ferma restando la verifica della sussistenza delle condizioni contrattuali.

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 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 inoltra la richiesta di revoca tramite l'Applicazione Gestione Chiavi, firmata con firma elettronica avanzata di un referente autorizzato.

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 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 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.

3.5 Tariffe e condizioni

3.5.1 Tariffe

Le tariffe per la prima emissione e per il rinnovo dei certificati sono stabilite dal contratto di servizio tra InfoCamere e Regione Toscana.

La revoca e la sospensione dei certificati sono gratuite.

4. Condizioni Generali del contratto relativo al servizio di certificazione A2A

La presente sezione disciplina e regola il rapporto contrattuale intercorrente tra InfoCamere ed il Titolare del certificato A2A, nonché gli obblighi e le modalità di utilizzazione per coloro che verificano il certificato A2A.
La fornitura del servizio di certificazione A2A da parte di InfoCamere al Titolare ed agli Utenti è regolata e disciplinata esclusivamente dal presente Manuale Operativo, dalle norme di legge vigenti, dalla richiesta inoltrata dal Titolare e dal contratto di servizio con la Regione Toscana.
Il Titolare, prima dell'inoltro della richiesta di cui alla sezione 3.1, è tenuto a leggere attentamente 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 A2A 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 A2A nonché quella relativa all'esito delle verifiche effettuate ai sensi dei precedenti punti 3.1.4.
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 servizio

Oggetto del servizio è la prestazione da parte di InfoCamere del servizio di certificazione della chiave pubblica generata dal responsabile dell'applicazione 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.

4.3 Conclusione del contratto

Le attività regolate dal presente Manuale Operativo sono regolate dal Contratto [1] tra RTI e Regione Toscana.

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, 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 stabilito dal presente Manuale Operativo richiamato nell'estensione CertificatePolicy del certificato e non dovrà essere utilizzato per finalità diverse da quella dichiarata.
E' fatto divieto di utilizzare il certificato digitale per applicazioni che trattino 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.

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 di certificato, garantendo la correttezza e completezza delle stesse;
- proteggere e conservare le chiavi private 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;
- utilizzare il certificato digitale rilasciato da InfoCamere in base al presente Manuale Operativo unicamente per l'applicazione corrispondente al nome 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.
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 Server su cui opera l'applicazione per la quale è stato rilasciato il certificato digitale. InfoCamere non potrà essere considerata responsabile, ed il soggetto Titolare si impegna a manlevarla, per eventuali danni derivanti dalla mancata attuazione da parte di quest'ultimo 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;

- verificare che il richiedente la certificazione abbia titolo e sia contrattualmente autorizzato alla richiesta nonché che possegga la chiave privata della cui corrispondente chiave pubblica si richiede la certificazione;
- emettere il certificato rispettando il formato indicato nel presente manuale;
- revocare o sospendere il certificato nei casi previsti dal presente Manuale Operativo.

InfoCamere, inoltre, pur facendo salvo il diritto di cui al punto 4.11, in considerazione dell'oggetto del servizio di certificazione non assume alcuna responsabilità sulle informazioni ed i dati informatici trattati dall'applicazione certificata.

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 A2A 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 A2A non potrà superare un importo pari al costo del certificato stesso.

4.7 Obblighi e responsabilità dell'Utente

L'utente che riceve un applicazione firmata è tenuto a verificare la validità del certificato di chiave pubblica corrispondente alla firma controllando la lista di revoca relativa.
Il controllo di cui al comma precedente può essere effettuato automaticamente.

In particolare, l'utente deve:
- verificare le informazioni contenute nel certificato relative alla chiave pubblica della coppia di chiavi utilizzata;
- verificare la data di scadenza del certificato;
- verificare lo stato del certificato (se è valido, se è stato 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 cessare qualsiasi utilizzo del certificato A2A rilasciato in base al presente Manuale Operativo.

4.9 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.

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.
Inoltre, il rapporto si risolve automaticamente in caso di cessazione di efficacia del contratto sottoscritto tra Regione Toscana ed il Raggruppamento Temporaneo di Impresa [11].
In tutti i casi sopra previsti, il Certificatore potrà cautelativamente sospendere l'erogazione del Servizio, attraverso la sospensione del certificato.