



Ente Emittitore Regione Toscana

**Carta Nazionale dei Servizi
Manuale Operativo**

Codice documento: CNS-MO-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 |



Questa pagina è lasciata
intenzionalmente bianca



Indice

| | |
|--|-----------|
| 1.Introduzione al documento..... | 5 |
| 1.1Novità introdotte rispetto alla precedente emissione..... | 5 |
| 1.2Scopo e campo di applicazione del documento..... | 5 |
| 1.3Riferimenti normativi e tecnici..... | 5 |
| 1.4Definizioni | 6 |
| 1.5Acronimi e abbreviazioni..... | 8 |
| 2.Generalità..... | 8 |
| 2.1Identificazione del documento..... | 9 |
| 2.2Ente Emittitore..... | 9 |
| 2.3Contatto per utenti finali e comunicazioni..... | 10 |
| 2.4Pubblicazione | 10 |
| 2.4.1Pubblicazione delle informazioni | 10 |
| 2.5Tutela dei dati personali | 10 |
| 2.6Tariffe..... | 10 |
| 2.6.1Rilascio e rinnovo del certificato..... | 10 |
| 2.6.2Revoca e sospensione del certificato..... | 10 |
| 2.6.3Accesso al certificato e alle liste di revoca..... | 10 |
| 3.Obblighi e Responsabilità..... | 11 |
| 3.1Obblighi dei Titolari..... | 11 |
| 3.2Responsabilità..... | 11 |
| 3.2.1Limitazioni di responsabilità..... | 11 |
| 4.Ammministrazione del Manuale Operativo..... | 11 |
| 4.1Procedure per l'aggiornamento..... | 11 |
| 4.2Responsabile dell'approvazione | 11 |
| 5.Operatività..... | 12 |
| 5.1Identificazione e Autenticazione..... | 13 |
| 5.2Identificazione ai fini del primo rilascio | 13 |
| 5.2.1Soggetti abilitati ad effettuare l'identificazione..... | 13 |
| 5.2.2Procedure per l'identificazione..... | 13 |
| 5.3Registrazione iniziale..... | 14 |
| 5.4Rilascio del certificato..... | 14 |
| 5.4.1Generazione delle chiavi e protezione delle chiavi private..... | 15 |
| 5.5Emissione del certificato..... | 15 |
| 5.5.1Formato e contenuto del certificato..... | 15 |
| 5.5.2Validità del certificato..... | 15 |
| 5.5.3Interdizione di una CNS..... | 15 |
| 5.5.4Motivi per la revoca di un certificato..... | 16 |
| 5.5.5Procedura per la richiesta di revoca..... | 16 |



| | |
|--|-----------|
| 5.5.6Motivi per la Sospensione di un certificato..... | 16 |
| 5.5.7Procedura per la richiesta di sospensione..... | 17 |
| 5.5.8Pubblicazione e frequenza di emissione della CRL..... | 17 |
| 5.6Rinnovo del Certificato..... | 17 |
| 6.Disponibilità del servizio..... | 18 |



1. Introduzione al documento

1.1 Novità introdotte rispetto alla precedente emissione

| | | | |
|-------------------------------|-----------------|--------------------------------|------------|
| Versione/Release n° : | 1.0 | Data Versione/Release : | 03/11/2005 |
| Descrizione modifiche: | Nessuna | | |
| Motivazioni : | Prima emissione | | |

1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole e le procedure operative che governano l'emissione della **Carta Nazionale dei Servizi (CNS) e dei relativi certificati** sottoscritti dal Certificatore InfoCamere; la CNS è emessa dalla Regione Toscana. Questo manuale indica inoltre le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta.

Le indicazioni di questo documento hanno validità per le attività relative alla Regione Toscana in qualità di Ente Emittitore, ad InfoCamere nel ruolo di Certificatore, per gli Uffici di Registrazione, per i soggetti incaricati ad effettuare l'identificazione/registrazione dei Titolari e/o a consegnare i dispositivi CNS ai medesimi, per gli stessi Titolari e per gli Utenti.

Per la compilazione di questo documento si è fatto riferimento ai seguenti documenti:

- **InfoCamere** Ente Certificatore - Certificati di Sottoscrizione - Manuale Operativo
- **InfoCamere** Ente Certificatore - Certificati di Autenticazione per la Carta Nazionale dei Servizi - Certificate Policy

L'autore del presente Manuale Operativo è la Regione Toscana, a cui spettano tutti i diritti previsti dalla legge. E' vietata la riproduzione anche parziale.

1.3 Riferimenti normativi e tecnici

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 **TU**};
- [4] Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004 (G. U. n. 98 del 27/04/2004);
- [5] Decreto Legislativo 30 giugno 2003, n. 196 (G.U. n. 174 del 29 luglio 2003);
- [6] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117 (G.U. n. 105 del 06/05/2004);
- [7] Regole tecniche per l'emissione della Carta Nazionale dei Servizi.

Riferimenti tecnici

- [8] Deliverable ETSI TS 102 042 "*Policy requirements for certification authorities issuing public key certificates*" – Aprile 2002;
- [9] RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile";
- [10] RFC 3161 (2001): " Internet X.509 Public Key Infrastructure Time Stamp Protocol (TSP)";



- [11]RFC 2527 (1999): “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”;
- [12]Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (1997) | ISO/IEC 9594-8;
- [13]Ente Certificatore InfoCamere - Certificati di Sottoscrizione, Manuale Operativo, ICCA-MO;
- [14]Ente Certificatore InfoCamere - Certificati di Autenticazione per la CNS, Certificate Policy, INDI-CPCA-CNS;
- [15]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.

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal DPR 137/2003, DPR 445/2000, dal DPCM 13 gennaio 2004 [4] e dal DPR 2 marzo 2004, n. 117 [6] si rimanda alle definizioni stabilite dagli stessi decreti. Dove appropriato viene indicato tra parentesi quadre il termine inglese corrispondente, generalmente usato nella pubblicistica, negli standard e nei documenti tecnici.

Accreditamento facoltativo

Il riconoscimento del possesso, da parte del certificatore che lo richieda, dei requisiti del livello più elevato, in termini di qualità e di sicurezza.

Carta Nazionale dei Servizi

Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

Certificato Elettronico, Certificato Digitale, Certificato X.509 [Digital Certificate]

Insieme di informazioni atte a definire con certezza la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica.

Nel certificato compaiono 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 al certificato.

Certificatore [Certification Authority – CA] – cfr. TU [3]

Certificatore Accreditato – cfr. TU [3]

Certificatore Qualificato – cfr. TU [3]

Chiave Privata e Chiave Pubblica – cfr. TU [3]

Codice di emergenza

Codice preimbastato consegnato dall'Ufficio di Registrazione al Titolare per l'autenticazione della richiesta di sospensione di un certificato.

Dati per la creazione di una firma – cfr. TU [3]

Dati per la verifica della firma – cfr. TU [3]

Dispositivo sicuro di firma

Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da una carta di plastica delle dimensioni di una carta di credito in cui è inserito un microprocessore. E' chiamato anche **carta a microprocessore** o **smart card**. Rispetta i requisiti di sicurezza richiesti dalla normativa vigente.

Ente Emittitore

Ente responsabile della formazione e del rilascio della CNS.

È la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del



circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.

Evidenza Informatica

Sequenza di simboli binari (bit) che può essere oggetto di una procedura informatica.

Firma elettronica – cfr. TU [3]**Firma elettronica avanzata – cfr. TU [3]****Firma elettronica qualificata – cfr. TU [3]****Firma digitale [*digital signature*] – cfr. TU [3]****Lista dei Certificati Revocati o Sospesi [*Certificate Revocation List – CRL*]**

E' una lista di certificati che sono stati resi "non validi" prima della loro naturale scadenza.

L'operazione è chiamata revoca se definitiva, sospensione se temporanea.

Quando un certificato viene revocato o sospeso il suo numero di serie viene aggiunto alla lista CRL, che viene quindi pubblicata nel registro dei certificati.

Marca temporale [*digital time stamping*]

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

Manuale Operativo

Il Manuale Operativo definisce le procedure che il Certificatore e l'Ente Emittitore applicano nello svolgimento del servizio di rilascio e gestione della CNS e del relativo Certificato.

Pubblico Ufficiale

Soggetto che, nell'ambito delle attività esercitate è abilitato in base alla legge di riferimento ad attestare l'identità di persone fisiche.

Registration Authority Officer

Soggetto incaricato a verificare l'identità e, se applicabile, ogni specifico attributo di un Titolare, nonché ad attivare la procedura di certificazione per conto del Certificatore.

Registro dei Certificati [*Directory*]

Il Registro dei Certificati è un archivio pubblico che contiene:

- i certificati validi emessi dal Certificatore per i quali i Titolari hanno richiesto la pubblicazione;
- la lista dei certificati revocati e sospesi (CRL).

Revoca o sospensione di un Certificato

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

Richiedente [*Subscriber*]

E' il soggetto fisico che richiede all'Ente Emittitore il rilascio della CNS.

Titolare [*Subject*]

E' il soggetto in favore del quale è rilasciata la CNS ed identificato nel certificato digitale come il legittimo possessore della chiave privata corrispondente alla chiave pubblica contenuta nel certificato stesso: al Titolare stesso è attribuita la firma elettronica avanzata generata con la chiave privata della coppia.

Uffici di Registrazione [*Registration Authority – RA*]

L'Ente Emittitore o altro Ente delegato dall'Ente Emittitore, previa stipula di accordi di servizio con il Certificatore, svolge le attività necessarie al rilascio, da parte di quest'ultimo, del certificato digitale, nonché alla consegna della CNS.

Utente [*Relying Party*]

Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma elettronica avanzata basata su quel certificato.



1.5 Acronimi e abbreviazioni

CNS – Carta Nazionale dei Servizi

CRL – Certificate Revocation List

Lista dei certificati revocati o sospesi.

DN – Distinguished Name

Identificativo del Titolare di un certificato di chiave pubblica; tale codice è unico nell'ambito degli utenti del Certificatore.

ETSI – European Telecommunications Standards Institute

IETF - Internet Engineering Task Force

IETF è una comunità aperta ed internazionale di progettisti di rete, operatori, venditori e ricercatori coinvolti nell'evoluzione dell'architettura Internet e delle normali operazioni su Internet.

ISO - International Organization for Standardization

Fondata nel 1946, l'ISO è un'organizzazione internazionale costituita da organismi nazionali per la standardizzazione.

ITU - International Telecommunication Union

Organismo intergovernativo mediante il quale le organizzazioni pubbliche e private sviluppano le telecomunicazioni. L'ITU fu fondato nel 1865 e diventò l'ente regolatore per gli standard nelle telecomunicazioni.

IUT – Identificativo Univoco del Titolare

E' un codice associato al Titolare che lo identifica univocamente presso il Certificatore; il Titolare ha codici diversi per ogni ruolo per il quale può firmare.

LDAP – Lightweight Directory Access Protocol

Protocollo utilizzato per accedere al registro dei certificati.

OID – Object Identifier

E' costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.

PIN – Personal Identification Number

Codice associato alla CNS, utilizzato dall'utente per accedervi alle funzioni. Altre funzioni installate sulla CNS richiedono PIN specifici della funzione.

PUK

Codice personalizzato per ciascuna CNS, utilizzato dal Titolare per riattivare il proprio dispositivo di firma in seguito al blocco dello stesso per errata digitazione del PIN. Altre funzioni installate sulla CNS richiedono PUK specifici della funzione.

RAO - Registration Authority Officer

RRC

Acronimo di Revocation Request Code, nome assegnato in precedenza al codice di emergenza e ancora utilizzato per chiarezza e continuità.

2. Generalità

Un certificato digitale è l'associazione tra una chiave pubblica di crittografia ed un insieme di informazioni che identificano il soggetto che possiede la corrispondente chiave privata, chiamato anche Titolare della coppia di chiavi asimmetriche (pubblica e privata). Il certificato è utilizzato da altri soggetti (gli Utenti) per ricavare la chiave pubblica, contenuta e distribuita con il certificato, e verificare, tramite questa, il possesso della corrispondente chiave privata, identificando in tal modo il Titolare della stessa.

Il certificato garantisce la corrispondenza tra la chiave pubblica ed il Titolare. Il grado di affidabilità



di questa associazione è legato a diversi fattori, quali, ad esempio, la modalità con cui il Certificatore ha emesso il certificato, le misure di sicurezza adottate e le garanzie offerte dallo stesso, gli obblighi assunti dal Titolare per la protezione della propria chiave privata.

A tale proposito i certificati di Autenticazione CNS emessi dall'Ente Certificatore InfoCamere sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte dell'Ente Emittitore o di altro soggetto da questi delegato, e rilasciati su dispositivo sicuro di firma (Smart card).

Il presente documento contiene le procedure operative che si attuano per l'emissione delle CNS e dei relativi Certificati di Autenticazione (in seguito anche chiamati più brevemente **Certificati**) sottoscritti dal Certificatore InfoCamere. Esso indica inoltre le procedure da seguire in caso di smarrimento, furto o timore di compromissione della CNS.

Informazioni riguardanti in modo più specifico l'Ente Certificatore InfoCamere sono presenti nel documento [14] Certificate Policy. In quest'ultimo documento vengono inoltre specificati:

- gli ambiti di utilizzo del certificato CNS;
- il formato del certificato CNS;
- gli obblighi e le responsabilità dell'Ente Certificatore, dell'Ente Emittitore, del titolare e dell'utente;
- la policy applicata dall'Ente Certificatore InfoCamere per quanto riguarda:
 - l'identificazione e l'autenticazione dei richiedenti il certificato CNS;
 - la revoca e la sospensione del certificato CNS;
 - il rinnovo del certificato CNS;
 - l'emissione della CRL o di altre modalità di notifica della validità dei certificati;
- la gestione della sicurezza e il livello di servizio dell'Ente Certificatore InfoCamere.

La Certificate Policy [14] è pubblicata a cura dell'Ente Certificatore Infocamere ed è riferita mediante URL all'interno del certificato CNS stesso. Essa consente sia ai Richiedenti che agli Utenti di valutare le caratteristiche e l'affidabilità del servizio di certificazione.

2.1 Identificazione del documento

Questo documento è denominato “**Carta Nazionale dei Servizi - Manuale Operativo**” ed è caratterizzato dal codice documento: **CNS-MO-RT**.

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

Questo documento è distribuito in formato elettronico presso il sito Web dell'Ente Emittitore all'indirizzo <http://www.rtrt.it/servizi/PKI>

2.2 Ente Emittitore

L'Ente Emittitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico la Regione Toscana, ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS. I dati completi dell'organizzazione che svolge la funzione di Ente Emittitore sono i seguenti:

Tabella

| Denominazione Sociale | Regione Toscana |
|--|---|
| Sede legale | Via Cavour 18, Firenze |
| Rappresentante legale | Claudio Martini |
| N° telefono | 055/4382111 |
| N° fax | 055/4383049 |
| N° partita IVA | 01386030488 |
| Sito web | www.regione.toscana.it |
| Sito web per i servizi di certificazione digitale: | http://www.rtrt.it/servizi/PKI |
| Sede Operativa | Via di Novoli 26, Firenze |



2.3 Contatto per utenti finali e comunicazioni

La Regione Toscana è responsabile della definizione, pubblicazione ed aggiornamento di questo documento.

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo e alla persona di seguito indicate:

Regione Toscana
Responsabile Settore Infrastrutture e Tecnologie per lo sviluppo della Amministrazione Elettronica
Via di Novoli 26
50127 Firenze

Telefono: 055/4383219

Fax : 055/4383195

Call Center: 800-901906 (lunedì – venerdì ore 8-18)

Web: <http://www.rtrt.it/servizi/PKI>

e-mail: cns.rt.info@regione.toscana.it

Le comunicazioni verso il Richiedente saranno effettuate, ai sensi dell'art. 14 DPR 445/2000 [3] via posta elettronica all'indirizzo dichiarato dal Richiedente medesimo al momento della Identificazione.

2.4 Pubblicazione

2.4.1 Pubblicazione delle informazioni

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web del Ente Emittitore (cfr. § 2.1);
- in formato cartaceo, disponibile sia presso la Regione Toscana sia presso gli Uffici di Registrazione.

2.5 Tutela dei dati personali

Le informazioni relative al Titolare di cui l'Ente Emittitore viene in possesso nell'esercizio delle sue attività, sono da considerarsi, salvo espresso consenso, riservate e non pubblicabili, con l'eccezione di quelle esplicitamente destinate ad uso pubblico (es. chiave pubblica, certificato, date di revoca e di sospensione del certificato).

In particolare i dati personali vengono trattati dall'Ente Emittitore in conformità con il Decreto Legislativo 30 giugno 2003, n.196 [5].

2.6 Tariffe

2.6.1 Rilascio e rinnovo del certificato

Le tariffe sono regolamentate dal contratto [15].

2.6.2 Revoca e sospensione del certificato

La revoca e sospensione del Certificato è gratuita.

2.6.3 Accesso al certificato e alle liste di revoca

L'accesso al registro dei certificati pubblicati e alla lista dei certificati revocati o sospesi è libero e gratuito.



3. Obblighi e Responsabilità

3.1 Obblighi dei Titolari

Il Titolare è tenuto a:

1. garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ente Emittente per la richiesta della CNS;
2. **non essere Titolare di una carta di identità elettronica (CIE)**;
3. proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
4. proteggere e conservare il codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità della CNS, in luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;
5. proteggere e conservare il codice di sblocco (PUK) utilizzato per la riattivazione della CNS in luogo protetto e diverso da quello in cui è custodito il dispositivo stesso;
6. adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
7. utilizzare le chiavi e il certificato per le sole modalità previste nel presente Manuale Operativo;
8. inoltrare all'Ente Emittente senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
9. adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

3.2 Responsabilità

3.2.1 Limitazioni di responsabilità

L'Ente Emittente ed il Certificatore in nessun caso risponderanno di eventi ad essi non imputabili ed in particolare di danni subiti dal Titolare, dal Richiedente, dagli Utenti o da qualsiasi terzo causati direttamente o indirettamente dal mancato rispetto da parte degli stessi delle regole indicate nel presente Manuale Operativo ovvero dalla mancata assunzione da parte di detti soggetti delle misure di speciale diligenza idonee ad evitare la causazione di danni a terzi che si richiedono al fruitore di servizi di certificazione, ovvero dallo svolgimento di attività illecite.

L'Ente Emittente ed il Certificatore non saranno altresì responsabili di qualsiasi inadempimento o comunque di qualsiasi evento dannoso determinato da caso fortuito o da eventi di forza maggiore.

4. Amministrazione del Manuale Operativo

4.1 Procedure per l'aggiornamento

L'Ente Emittente si riserva di apportare variazioni al presente documento per esigenze tecniche o per modifiche alle procedure intervenute a causa di norme di legge o regolamenti.

Errori, aggiornamenti o suggerimenti di modifiche possono essere comunicati al contatto per gli utenti indicato al § 2.3.

Correzioni editoriali e tipografiche e altre modifiche minori comportano l'incremento del numero di release del documento, mentre variazioni con un impatto significativo sugli utenti (come ad esempio modifiche rilevanti alle procedure operative) comportano l'incremento del numero di versione del documento. In ogni caso il manuale sarà prontamente pubblicato e reso disponibile secondo le modalità previste.

Ogni modifica tecnica o procedurale a questo manuale operativo verrà prontamente comunicata agli Uffici di Registrazione.

Il Manuale è pubblicato in conformità a quanto indicato al § 2.4.1 in formato elettronico.

4.2 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Responsabile del Contratto [15] della Regione Toscana.



5. Operatività

Questo capitolo descrive le operazioni necessarie per compiere le attività di emissione, revoca, sospensione e rinnovo di un Certificato di Autenticazione CNS.

Il ciclo di vita della CNS è regolato dalle regole tecniche del decreto 9 Dicembre 2004. Questo regolamento impone alcuni ulteriori vincoli di sicurezza sulla gestione delle smartcard. E' necessario, sostanzialmente, tenere traccia delle carte nel loro percorso che va dalla produzione al rilascio. Questo vincolo impone che sia necessario tenere traccia delle smart-card CNS in relazione al loro stato:

- smartcard bianca¹: prepersonalizzata ovvero con file system completo ma senza certificato di autenticazione CNS e altri dati del titolare a bordo;
- smartcard pronta: personalizzata ovvero assegnata ad un titolare (completa di certificato e strutture dati);
- smartcard fallite: smartcard che per qualsiasi motivo non siano utilizzabili (es. la procedura di personalizzazione non è andata a buon fine, carta malfunzionante ecc...).

Queste smartcard, opportunamente suddivise per categoria (le tipologie di cui sopra) sono custoditi in un apposito armadio accessibile con chiave.

I prelievi di carte sono riportati su un apposito registro conservato anch'esso nell'armadio.

L'emissione delle carte avverrà **sempre** online, cioè alla presenza del titolare e con la contestuale consegna della smart card e della busta discreta contenente i codici di accesso.

Gli uffici di registrazione della Regione Toscana delegati ad emettere CNS (intesi come sedi fisiche) sono i seguenti:

- Uffici centrali della Regione Toscana (Firenze);
- Uffici Infocamere presso le Camere di Commercio;
- Uffici di Netikos;
- Uffici di registrazione mobili, costituiti dal personale Netikos, attrezzati con PC portatili adeguati all'emissione, collegamento ad Internet via modem, opportune misure di sicurezza per il trasporto delle smart card da emettere e quelle eventualmente fallite, registro delle carte emesse.

La procedura di emissione CNS proposta prevede:

- 1) Se il numero \mathcal{N} di richiedenti la CNS è inferiore o uguale a 10 sarà applicabile la procedura descritta nel seguito presso gli Uffici di Registrazione "fissi", se invece il numero di richiedenti la CNS è superiore a 10 sarà applicabile la procedura tramite gli Uffici di Registrazione mobili presso la sede dell'Ente richiedente;
- 2) Il Raggruppamento verifica preventivamente che i richiedenti siano presenti negli elenchi nominativi che ciascun ente dovrà precedentemente fornire;
- 3) Quindi i richiedenti si recheranno, dopo essersi prenotati mediante call center o addetto principale alla Registrazione, presso l'Ufficio di Registrazione e nel giorno per cui si sono prenotati ($\mathcal{N} \leq 10$) oppure, nel giorno di presenza dell'Ufficio di Registrazione mobile, nel locale predisposto dall'Ente ($\mathcal{N} > 10$), dove un RAO effettuerà tutte le registrazioni ed emissioni con conseguente consegna della busta discreta (codice di emergenza, pin, puk) e della smart card CNS.

Il RAO aggiornerà il proprio registro delle carte prese in carico segnalando quelle emesse e quelle fallite.

E' compito del RAO l'inserimento nella maschera di registrazione delle informazioni obbligatorie:

OU=Regione Toscana

¹ con la personalizzazione grafica della Regione Toscana



Le smartcard fallite saranno raccolte presso l'Ufficio di Registrazione collocato presso la Regione da dove saranno inviate mensilmente ad Infocamere per essere verificate e distrutte.

5.1 Identificazione e Autenticazione

Questa sezione descrive le procedure usate per:

- l'identificazione del Richiedente al momento della richiesta di rilascio della CNS e del relativo certificato di Autenticazione CNS;
- l'autenticazione del Titolare, nel caso di rinnovo, revoca e sospensione di certificati di Autenticazione CNS.

5.2 Identificazione ai fini del primo rilascio

L'Ente Emittitore, direttamente o tramite un soggetto delegato, verifica con certezza l'identità del Richiedente prima di procedere al rilascio della CNS e del relativo certificato di Autenticazione CNS richiesto.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente da uno dei soggetti di cui al § 5.2.1, che ne verifica l'identità attraverso il controllo della carta d'identità o di un documento ad essa equipollente (cfr. art. 35 comma 2 del TU [3]) in corso di validità.

5.2.1 Soggetti abilitati ad effettuare l'identificazione

L'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati:

1. L'Ente Emittitore, anche tramite suoi Incaricati;
2. L'Ufficio di Registrazione, anche tramite suoi Incaricati.

5.2.2 Procedure per l'identificazione

L'identificazione è effettuata da uno dei soggetti indicati al § 5.2.1 ed è richiesta la presenza fisica del Richiedente.

Il soggetto che effettua l'identificazione ne verifica l'identità tramite il riscontro con uno dei seguenti documenti, valido e non scaduto, secondo quanto previsto dall'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, tra cui il tesserino di riconoscimento rilasciato dalla Regione Toscana.

Al momento dell'identificazione viene fornito al Richiedente un codice segreto di emergenza (RRC), che costituisce lo strumento di autenticazione nel sistema di comunicazione sicuro tra Certificatore e lo stesso Titolare.

5.2.2.1 Richiesta di rilascio della CNS e del certificato

I passi principali a cui il Richiedente deve attenersi per ottenere una CNS ed certificato di Autenticazione CNS sono:



- a) prendere visione del presente Manuale Operativo e della Certificate Policy [14] e dell'eventuale ulteriore documentazione informativa;
- b) seguire le procedure di identificazione adottate dall'Ente Emittitore come descritte nei paragrafi che seguono;
- c) fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- d) sottoscrivere la richiesta di registrazione e prendere visione, accettandole, delle modalità di utilizzo della CNS.

5.2.2.2 Informazioni che il Richiedente deve fornire

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra l'Ente Emittitore ed il Richiedente/Titolare. Il modulo di richiesta deve essere sottoscritto dal Richiedente/Titolare.

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome;
- Data e luogo di nascita;
- Codice fiscale;
- Indirizzo di residenza;
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso.

5.3 Registrazione iniziale

Per procedere all'emissione del certificato per la CNS è necessario eseguire una procedura di registrazione, successiva all'identificazione, durante la quale i dati dei Titolari vengono memorizzati negli archivi del Certificatore.

La registrazione iniziale è effettuata presso un Ufficio di Registrazione.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e la consegna della CNS si attiva la la procedura di certificazione.

5.4 Rilascio del certificato

La procedura prevede la presenza del Richiedente/Titolare in possesso della CNS presso un Ufficio di Registrazione .

1. Il RAO, contestualmente all'identificazione, registra il Titolare e attiva la procedura di rilascio di certificato;
2. La procedura automatica sblocca la CNS con il PIN di default consentendo la generazione della coppia di chiavi di crittografia. Nel caso in cui la CNS abbia un PIN differente da quello di default, la procedura richiede l'inserimento del PIN da parte del Titolare;
3. Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica del Richiedente e la invia al Certificatore;
4. Terminata la procedura di certificazione con le adeguate verifiche, la procedura automatica personalizza la CNS inserendo il PIN già consegnato al Richiedente in fase di identificazione.

La segretezza del PIN personale durante le fasi di personalizzazione della CNS è garantita da adeguati sistemi di cifratura. Tale codice PIN, generato in modo casuale, è conservato in modo protetto all'interno dei sistemi del Certificatore, e viene comunicato secondo procedure sicure (procedure automatiche con imbustamento in busta chiusa) al solo Titolare. La CNS così personalizzata con la coppia di chiavi generate è protetta da tale PIN personale.



5.4.1 **Generazione delle chiavi e protezione delle chiavi private**

La coppia di chiavi per l'autenticazione è generata utilizzando le funzionalità offerte dal processore della CNS.

Le chiavi sono generate all'interno della smart card, la lunghezza delle chiavi è di 1024 bit.

La chiave privata del Titolare è generata e memorizzata in un'area protetta della smart card che ne impedisce l'esportazione. Il sistema operativo del dispositivo, inoltre, in caso di forzatura della protezione rende illeggibile la carta, a protezione dei dati in essa contenuti.

Per utilizzare la chiave privata a bordo della CNS il possessore deve autenticarsi correttamente fornendo il proprio PIN segreto.

5.5 **Emissione del certificato**

L'emissione del certificato di Autenticazione CNS viene effettuata in modo automatico dalle procedure del Certificatore secondo i seguenti passi:

- 1) viene verificata la correttezza della richiesta di certificato controllando che:
 - il Richiedente/Titolare sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
 - la chiave pubblica che si intende certificare sia una chiave valida e della lunghezza prevista;
 - la richiesta sia autentica e il Titolare possieda la corrispondente chiave privata;
- 2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta;
- 3) si procede alla generazione del certificato e a pubblicarlo nel registro dei certificati;
- 4) il certificato viene memorizzato all'interno della CNS dispositivo sicuro di firma del Titolare.

5.5.1 **Formato e contenuto del certificato**

Il profilo minimo del certificato è riportato nella Policy del Certificatore.

5.5.2 **Validità del certificato**

Il certificato ha validità di tre anni a partire dalla data di emissione ovvero fino alla data di pubblicazione della sua revoca o sospensione se precedentemente effettuate.

5.5.3 **Interdizione di una CNS**

L'interdizione della CNS si attua tramite la revoca (interdizione definitiva) o la sospensione (interdizione temporanea) del relativo certificato che 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.

La revoca o sospensione del certificato può avvenire:

- su richiesta del Titolare;
- su iniziativa dell'Ente Emittitore;
- su iniziativa del Certificatore.

Il Certificatore verifica la provenienza della richiesta di revoca o di sospensione.

L'Ente Emittitore, direttamente o tramite strutture all'uopo delegate, autentica il Titolare richiedente la revoca o sospensione e si accerta delle motivazioni della stessa.

Se la richiesta viene effettuata per telefono, il Titolare (per la sola sospensione) si autentica fornendo il codice di emergenza (RRC), consegnato assieme al certificato che si intende sospendere.



Se la richiesta viene fatta presso l'Ufficio di Registrazione, l'autenticazione del Titolare avviene con le modalità previste per l'identificazione.

5.5.4 Motivi per la revoca di un certificato

E' fatto obbligo di richiedere la revoca nel caso in cui si verificano le seguenti condizioni:

- la chiave privata sia stata compromessa, ovvero sia presente uno dei seguenti casi:
 - sia stato smarrita o rubata la CNS;
 - sia venuta meno la segretezza della chiave privata o del codice di attivazione per accedervi;
 - si sia verificato un qualunque evento che abbia compromesso il livello di affidabilità della chiave privata;
- il Titolare non riesce più ad utilizzare la CNS in suo possesso (es: guasto del dispositivo sicuro);
- si verifica un cambiamento dei dati del Titolare presenti nel certificato;
- viene verificata una sostanziale condizione di non conformità del presente Manuale Operativo.

5.5.5 Procedura per la richiesta di revoca

La richiesta di revoca viene effettuata con modalità diverse a seconda del richiedente. Sono previsti i seguenti casi:

Revoca su iniziativa del Titolare

L'utente Titolare può richiedere la revoca:

1. telefonando al Call Center dell'Ente Emittitore;
2. tramite l'Ufficio di Registrazione presso cui è stato registrato.

Il Titolare deve richiedere la revoca tramite l'Ufficio di Registrazione o tramite il Call Center dell'Ente Emittitore, il quale richiede i dati necessari (la motivazione della revoca, il codice di emergenza del certificato (RRC)) ed effettua tutte le verifiche del caso, quindi procede a richiedere la revoca al Certificatore.

Il richiedente è tenuto a sottoscrivere la richiesta di revoca e consegnarla all'Ufficio di Registrazione o inviarla direttamente al Call Center dell'Ente per lettera o per fax, corredata di una fotocopia di un documento di identità in corso di validità.

Nell'impossibilità di identificare con certezza il Titolare si potrà procedere con una sospensione del Certificato in attesa della corretta identificazione del richiedente (ad esempio mediante richiesta di revoca formulata per iscritto).

Revoca su iniziativa del Certificatore

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

il Certificatore comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza; la procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

Revoca su iniziativa dell'Ente Emittitore

L'Ente Emittitore attiva una richiesta di revoca con la seguente modalità:

comunica al Titolare anticipatamente, salvo casi di motivata urgenza, l'intenzione di revocare il certificato, fornendo il motivo della revoca e la data di decorrenza; la procedura di revoca del certificato viene poi completata con l'inserimento nella lista dei certificati revocati o sospesi (CRL).

5.5.6 Motivi per la Sospensione di un certificato

Il Certificatore esegue la sospensione del certificato su propria iniziativa o su richiesta del Titolare.



La sospensione deve essere effettuata nel caso si verifichino le seguenti condizioni:

1. è stata effettuata una richiesta di revoca senza la possibilità di accertare in tempo utile l'autenticità della richiesta;
2. il Titolare o il Certificatore acquisiscano elementi di dubbio sulla validità del certificato;
3. è necessaria un'interruzione della validità del certificato.

5.5.7 Procedura per la richiesta di sospensione

Il Titolare deve richiedere la sospensione con una delle seguenti modalità:

1. telefonando al Call Center dell'Ente Emittitore e fornendo le informazioni previste per la revoca e **la durata del periodo di sospensione**. In assenza del codice RRC e solo nel caso in cui si tratti di una richiesta di sospensione per compromissione di chiave, il Call Center, verificato il numero telefonico di provenienza della chiamata, attiva una **sospensione immediata** del certificato in attesa della richiesta scritta del Titolare;
2. tramite l'Ufficio di Registrazione, il quale richiede i dati necessari ed effettua tutte le verifiche del caso, quindi procede a richiedere la sospensione al Certificatore.

Il Titolare è tenuto a sottoscrivere la richiesta di sospensione e consegnarla all'Ufficio di Registrazione o inviarla direttamente al Certificatore.

Qualora il Certificatore, direttamente o tramite un Ufficio di Registrazione, non riceva la richiesta sottoscritta entro 10 giorni solari dalla richiesta di sospensione, il certificato verrà riattivato.

La richiesta di sospensione da parte del Certificatore o dell'Ente Emittitore viene effettuata secondo le modalità indicate per la richiesta di revoca, specificando, in tal caso, anche la durata del periodo di sospensione.

Alla scadenza di tale periodo, alla sospensione seguirà o una revoca definitiva oppure la ripresa di validità del certificato.

5.5.8 Pubblicazione e frequenza di emissione della CRL

Pubblicazione e frequenza della CRL e la relativa tempistica sono descritte nella certificate policy [14] del Certificatore.

5.6 Rinnovo del Certificato

Il certificato contiene al suo interno l'indicazione del periodo di validità nel campo "*validity period*" (periodo di validità) con gli attributi "*not after*" (non dopo il) e "*not before*" (non prima del).

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

Il certificato ha validità di tre anni dalla data di emissione.

La procedura di rinnovo richiede la generazione di una nuova coppia di chiavi: la richiesta di un nuovo certificato deve essere avviata prima della scadenza dello stesso.

La nuova coppia di chiavi è generata all'interno della CNS; l'emissione e la pubblicazione del certificato seguono il procedimento descritto in caso di nuova richiesta.

Le modalità operative per effettuare la procedura di rinnovo del certificato sono indicate dal Certificatore nel proprio sito (http://www.card.infocamere.it/servizi/servizi_home.htm).



6. Disponibilità del servizio

Gli orari di erogazione del servizio sono:

| Servizio | Orario |
|--|--|
| Accesso all'archivio pubblico dei certificati ⁽²⁾ (comprende le CRL) | Secondo quanto previsto nella <i>Certificate Policy</i> del Certificatore [14] |
| Revoca e sospensione dei certificati ⁽³⁾ | Secondo quanto previsto nella <i>Certificate Policy</i> del Certificatore [14] |
| Altre attività: registrazione, generazione, pubblicazione, rinnovo ⁽⁴⁾ | Lun – Ven: dalle 09:00 alle 18:00 Sabato: dalle 09:00 alle 12:00 Festività escluse |

2Il servizio potrà non essere disponibile nella fascia oraria indicata per fermi di manutenzione o per cause di forza maggiore.

3L'attività di revoca svolta presso gli Uffici di Registrazione può avere diversi orari di sportello. In ogni caso il Certificatore garantisce l'erogazione del proprio servizio negli orari riportati nella *Certificate Policy*.

4L'attività di registrazione viene svolta presso gli Uffici di Registrazione che possono avere diversi orari di sportello. In ogni caso il Certificatore garantisce l'erogazione del proprio servizio negli orari sopra riportati.