Camera di Commercio Industria Artigianato Agricoltura

Ente Emettitore CCIAA di Bolzano
Carta Nazionale dei Servizi
Manuale Operativo
Codice documento:

Redatto da

Verificato da

Approvato da

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** :	
Descrizione modifiche:	Nessuna		
Motivazioni :	Prima emissione		

Versione/Release n° :	2.0	**Data Versione/Release** :	
Descrizione modifiche:	Modificato riferimenti all'Ente Certificatore		
Motivazioni :	Aggiornamento		

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 InfoCert; la CNS è emessa dalla Camera di Commercio di Bolzano. 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 Camera di Commercio in qualità di Ente Emettitore, ad InfoCert 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:

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

1.3 Riferimenti normativi e tecnici

Riferimenti normativi

[1] Decreto Legislativo 7 marzo 2005, n.82 (G.U. n.112 del 16 maggio 2005) – Codice dell'amministrazione digitale (nel seguito referenziato come CAD)
[2] Decreto Legislativo 4 aprile 2006, n.159 (G.U. n.99 del 29 aprile 2006) - Disposizioni integrative e correttive al decreto legislativo 7 marzo 2005, n. 82, recante codice dell'amministrazione digitale.
[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
[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 InfoCert - Certificati di Sottoscrizione, Manuale Operativo, ICERT-INDI-MO

[14] Ente Certificatore InfoCert - Certificati di Autenticazione per la CNS, Certificate Policy, ICERT-INDI-CPCA-CNS

1.4 Definizioni

Vengono di seguito elencate le definizioni utilizzate nella stesura del presente documento. Per i termini definiti dal CAD [1], DPR 445/2000 [3], 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. [3]

Certificatore Accreditato – cfr. [3]

Certificatore Qualificato – cfr. [3]

Chiave Privata e Chiave Pubblica – cfr. [3]

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

Dati per la verifica della firma – cfr. [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 Emettitore

Ente responsabile della formazione e del rilascio della CNS.
E' 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. [3]

Firma elettronica avanzata – cfr. [3]

Firma elettronica qualificata – cfr. [3]

Firma digitale *[digital signature]* – cfr. [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 Emettitore 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 Emettitore 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 Emettitore o altro Ente delegato dall'Ente Emettitore, 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

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 InfoCert sono emessi su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte dell'Ente Emettitore 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. 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 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 Emettitore, del titolare e dell'utente;
- la policy applicata dall'Ente Certificatore 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.

La Certificate Policy [14] è pubblicata a cura dell'Ente Certificatore 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-XXX**.

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 Emettitore all'indirizzo http://www.camcom.bz.it.

2.2 Ente Emettitore

L'Ente Emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico la Camera di Commercio di Bolzano, 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 Emettitore sono i seguenti:

Tabella

Denominazione Sociale	
Sede legale	**xxxx**
Rappresentante legale	xxxx
Direzione Generale	**xxxx**
N° telefono	**xxxx**
N° fax	**xxxx**
N° Iscrizione Registro Imprese	**xxxx**
N° partita IVA	**xxxx**
Sito web	**xxxx**

Sito web per i servizi di certificazione digitale:	xxxx
Sede Operativa	**xxxx**

2.3 Contatto per utenti finali e comunicazioni

La Camera di Commercio diBolzano 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:

INSERIRE UN RIFERIMENTO DELLA CCIAA O DELL'ENTE CERTIFICATORE.

2.4 Pubblicazione

2.4.1 Pubblicazione delle informazioni

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso:
  - ➢ il sito web del Ente Emettitore (cfr. § 2.1)
  - ➢ il sito web del Certificatore www.firma.infocert.it
- in formato cartaceo, disponibile sia presso la Camera di commercio di Bolzano sia presso gli Uffici di Registrazione.

2.5 Tutela dei dati personali

Le informazioni relative al Titolare di cui l'Ente Emettitore 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 Emettitore in conformità con il Decreto Legislativo 30 giugno 2003, n.196 [5].

2.6 Tariffe

2.6.1 Rilascio e rinnovo del certificato

Sono previste tariffe riguardanti l'emissione e il rinnovo del Certificato di Autenticazione CNS. Tali tariffe sono funzione delle quantità trattate e delle specifiche normative che le regolamentano.
Le tariffe sono disponibili presso gli Uffici di Registrazione.

Il costo del lettore di smart card non è compreso in queste tariffe.

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. proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne

l'integrità e la riservatezza;
3. 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;
4. 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;
5. adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
6. utilizzare le chiavi e il certificato per le sole modalità previste nel presente Manuale Operativo;
7. inoltrare all'Ente Emittente senza ritardo la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
8. 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 di causare 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 Emettitore 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 della Camera di Commercio di Bolzano.

5. Identificazione e Autenticazione

Questo capitolo 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.

5.1 Identificazione ai fini del primo rilascio

L'Ente Emettitore, 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 § 5.1.1, 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 [3]) in corso di validità.

5.1.1 Soggetti abilitati ad effettuare l'identificazione

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

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

5.1.2 Procedure per l'identificazione

L'identificazione è effettuata da uno dei soggetti indicati al § 5.1.1 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.

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

5.1.2.1 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 Emettitore 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..

5.1.2.2 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 Emettitore 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

6. Operatività

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

6.1 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 sono previste due diverse modalità.

La prima modalità (nel seguito **Caso A**) consente al Titolare/Richiedente di concludere la procedura di certificazione entrando in possesso della CNS e del certificato di autenticazione CNS immediatamente dopo la registrazione: in questo caso il RAO avvierà la procedura di generazione della coppia di chiavi e, effettuate le opportune verifiche, di emissione del certificato in presenza del Richiedente/Titolare.

La seconda modalità (nel seguito **Caso B**) prevede una separazione tra la fase di identificazione, effettuata in presenza del Richiedente, Titolare del certificato, e quella di registrazione ed emissione della CNS e del certificato, che viene effettuata successivamente dai RAO.

In entrambi i casi la CNS viene personalizzata a cura del Certificatore con il PIN consegnato al Richiedente al momento dell'identificazione.
Nel **Caso B** la CNS personalizzata è consegnata al Richiedente (ora Titolare) in un secondo momento.

6.2 Rilascio del certificato

6.2.1 Caso A: Chiavi generate in presenza del Richiedente

Questa 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

6.2.2 Caso B: Chiavi generate dal Certificatore

Questa procedura viene effettuata dai RAO, presso i locali dell'Ente Emettitore o presso gli Uffici di Registrazione.

1. Il RAO seleziona i dati di registrazione di un Richiedente/Titolare e attiva la procedura di richiesta di certificato.
2. La procedura automatica sblocca la CNS con il PIN di default consentendo la generazione della coppia di chiavi di crittografia.
3. Il RAO, utilizzando il proprio dispositivo, firma la richiesta di certificazione della chiave pubblica corrispondente alla coppia di chiavi crittografiche generate all'interno della CNS 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/Titolare 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.

6.2.3 Generazione delle chiavi e protezione delle chiavi private

La coppia di chiavi per l'autenticazione è generata utilizzando le funzionalità offerte dalla 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.

6.3 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) si distinguono i due casi:
   - (*Caso A*): il Titolare è già in possesso del dispositivo sicuro di firma, quindi il punto precedente conclude la procedura di rilascio del certificato di autenticazione.

- (*Caso B*): il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato da un incaricato dell'Ufficio di Registrazione personalmente al Titolare.

6.3.1 Formato e contenuto del certificato

Il profilo minimo del certificato è riportato nella Policy

6.3.2 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.

6.3.3 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 Emettitore.
- su iniziativa del Certificatore.

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

L'Ente Emettitore, 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 revoca segreto (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.

6.3.4 Motivi per la revoca di un certificato

E' fatto obbligo di richiedere la revoca nel caso in cui si verifichino 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.

6.3.5 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 Emettitore
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 Emettitore, il quale richiede i dati necessari (la motivazione della revoca, il codice di revoca 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 Emettitore
L'Ente Emettitore 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).

6.3.6 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.

6.3.7 Procedura per la richiesta di sospensione

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

a. telefonando al Call Center dell'Ente Emettitore 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;
b. 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 Emettitore 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.

6.3.8 Pubblicazione e frequenza di emissione della CRL

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

6.4 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.firma.infocert.it).

7. Disponibilità del servizio

Gli orari di erogazione del servizio sono:

Servizio	Orario
Accesso all'archivio pubblico dei certificati ([1]) (comprende i certificati e le CRL)	Secondo quanto previsto nella Certificate Policy del Certificatore [14]
Revoca e sospensione dei certificati ([2])	Secondo quanto previsto nella Certificate Policy del Certificatore [14]
Altre attività: registrazione, generazione, pubblicazione, rinnovo ([3])	Lun – Ven: dalle 09:00 alle 18:00 Sabato: dalle 09:00 alle 12:00 Festività escluse

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

2 L'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.

3 L'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.