Camera di Commercio Industria Artigianato Agricoltura di Taranto

Ente Emettitore CCIAA di Taranto

Carta Nazionale dei Servizi

Manuale Operativo - CA ArubaPEC

Codice documento: CNS-MOAR-CCIAA

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 : 06/04/11

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 accreditato Aruba PEC; la CNS è emessa dalla Camera di Commercio. 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 Aruba PEC nel ruolo di Certificatore, per i CDRL, 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:

- **Aruba PEC** Ente Certificatore - Certificati di Sottoscrizione - Manuale Operativo

- **Aruba PEC** 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 – Codice dell'amministrazione digitale come modificato dal Decreto Legislativo 4 aprile 2006, n. 159 e dal Decreto Legislativo 30 dicembre 2010, n.235 (nel seguito referenziato come CAD).

[2] Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 (nel seguito referenziato come TU).

[3] Decreto del Presidente del Consiglio dei Ministri 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.

[4] Decreto Legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali".

[5] Decreto del Presidente della Repubblica 2 marzo 2004, n. 117.

[6] Decreto interministeriale 9 dicembre 2004, Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi.

[7] “Linee guida per l’emissione e l’utilizzo della Carta Nazionale dei Servizi”, Ufficio Standard e tecnologie d’identificazione, CNIPA, Versione 3.0, 15 maggio 2006.

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 Aruba PEC – Servizio di Certificazione Digitale, Manuale Operativo

[14] Ente Certificatore Aruba PEC – Certificati di autenticazione per la CNS, Certificate Policy

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 30 marzo 2009 [3] e dal DPR 2 marzo 2004, n. 117 [5] 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.

Centri di Registrazione Locali [CDRL]
L'Ente Emettitore o altro Ente delegato dall'Ente Emettitore che svolge le attività necessarie al rilascio, da parte di quest'ultimo, dei certificati digitali, nonché alla consegna della CNS.

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. [1]

Certificatore Accreditato – cfr. [1]

Certificatore Qualificato – cfr. [1]

Chiave Privata e Chiave Pubblica – cfr. [1]

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

Dispositivo sicuro di firma
Il dispositivo sicuro di firma utilizzato dal Titolare è costituito da un microprocessore generalmente installato su un supporto di plastica (smart card) o all'interno di un lettore con interfaccia USB (token). 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. [1]

Firma elettronica avanzata – cfr. [1]

Firma elettronica qualificata – cfr. [1]

Firma digitale [digital signature] – cfr. [1]

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.

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.

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.

ODR – Operatore di Registrazione

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.

SSCD – Secure Signature Creation Device

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 accreditato Aruba PEC 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 Aruba PEC ed è riferita mediante URL all'interno del certificato di autenticazione 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 – CA ArubaPEC**" ed è caratterizzato dal codice documento: CNS-MOAR-CCIAA.

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 http://www.card.infocamere.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, 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	CAMERA DI COMMERCIO INDUSTRIA ARTIGIANATO E AGRICOLTURA TARANTO
Sede legale	Queste informazioni sono reperibili nel sito web della Camera di Commercio che adotta il presente manuale.
Rappresentante legale	
Direzione Generale	
N° telefono	
N° fax	
N° partita IVA	
Sede Operativa	
Sito web per i servizi di certificazione digitale:	http://www.card.infocamere.it

2.3 Contatto per utenti finali e comunicazioni

La Camera di Commercio è responsabile di questo documento. Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte all'indirizzo di seguito indicato:

InfoCamere S.C.p.a.

Corso Stati Uniti 14

35127 Padova

tel: +39 049 8288111

telefax: +39 049 8288406

Call Center Firma Digitale: 199.500.000

Web: http://www.card.infocamere.it

E-mail : firma@infocamere.it

2.4 Pubblicazione

2.4.1 Pubblicazione delle informazioni

Il presente Manuale Operativo è reperibile:

- in formato elettronico presso il sito web http://www.card.infocamere.it
- in formato cartaceo, disponibile sia presso la Camera di Commercio sia presso i Centri di Registrazione Locale.

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 [4].

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 i CDRL.

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 sono gratuite.

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 Emettitore per la richiesta della CNS;
2. non essere Titolare di una carta di identità elettronica; (dopo il 31/12/2011, art. 66, comma 8bis del CAD);
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 Emettitore 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 Emettitore ed il Certificatore accreditato non saranno tenuti a rispondere di quegli eventi a loro non direttamente imputabili, inclusi i danni che direttamente o indirettamente saranno riconducibili:

- all'inosservanza di questo manuale operativo;
- allo svolgimento di attività illecite;
- a comportamenti del fruitore di servizi di certificazione privi delle richieste misure di diligenza atte ad evitare danni a terzi;

e subiti dal Titolare, dal Richiedente, dagli Utenti o da terzi.

In nessun caso l'Ente Emettitore ed il Certificatore accreditato 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 versione 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 tempestivamente ai CDRL.

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.

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 [2]) 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. Il CDRL, 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, 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
- Cittadinanza
- Codice fiscale
- Indirizzo di residenza
- Indirizzo email
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente

- emittente e data di rilascio dello stesso

6. Operatività

Le operazioni necessarie per compiere le attività di emissione, revoca, sospensione, riattivazione e rinnovo dei Certificati sono descritte nei seguenti paragrafi.

6.1 Registrazione

L'emissione di certificati prevede una fase di registrazione dell'utente, previa identificazione: questa avviene presso l'Ente Emettitore o un suo CDRL. E' durante questo passaggio iniziale che i dati dell'utente vengono inseriti nel sistema in uso al Certificatore.

Registrato il futuro Titolare, sono previste due diverse modalità di rilascio certificati e consegna dei dispositivi. La prima (in seguito Caso A) prevede il rilascio dei certificati e la consegna al Titolare dei dispositivi subito dopo la registrazione: L'ODR avvierà la procedura di generazione delle coppie di chiavi e di emissione dei certificati in presenza del Richiedente, a seguito delle opportune verifiche.

Nella seconda modalità (Caso B) è prevista una separazione del momento dell'identificazione, che ha luogo in presenza del Richiedente, da quello della registrazione ed emissione della CNS e dei relativi certificati, effettuata in un secondo momento dagli ODR.

In ambedue le modalità la personalizzazione della CNS è effettuata dal Certificatore, attraverso il PIN consegnato al Richiedente dopo l'identificazione.

Il Caso B prevede che la CNS personalizzata venga consegnata al 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 l'Ente Emettitore o un suo CDRL.

1. Terminata l'identificazione, l'ODR registra il Titolare attivando la procedura di rilascio dei certificati.
2. la CNS viene automaticamente sbloccata con il PIN di default consentendo la generazione delle coppie di chiavi di crittografia. E' richiesto l'inserimento PIN del Titolare se questo è differente da quello di default.

3. L’ODR firma le richieste di certificazione della chiave pubblica del Richiedente utilizzando il proprio dispositivo, quindi le invia al Certificatore.
4. Effettuate le opportune verifiche e terminata la certificazione, 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

Gli ODR effettuano questa procedura presso i locali dell'Ente Emettitore o presso i CDRL.

1. L’ODR 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 delle coppie di chiavi di crittografia.
3. L’ODR, utilizzando il proprio dispositivo, firma le richieste di certificazione delle chiavi pubbliche corrispondenti alle coppie 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.

Adeguati sistemi di cifratura garantiscono la segretezza del PIN personale anche durante le fasi di personalizzazione della CNS. Il PIN è generato in modo casuale e conservato all'interno dei sistemi del Certificatore in modo protetto. Viene comunicato in modo sicuro (attraverso procedure automatiche di stampa e oscuramento su scratch card) solamente al 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

Le coppie di chiavi per l'Autenticazione e per la Firma Digitale sono generate attraverso le funzionalità messe a disposizione dalla CNS.

Le chiavi sono generate all’interno del dispositivo, la loro lunghezza è di 1024 bit.

Un'area protetta della smart card genera e custodisce le chiavi private impedendone l’esportazione. In caso di forzatura il sistema operativo del dispositivo protegge i dati al suo interno rendendo illeggibile la carta. L’utilizzo delle chiavi contenute nella CNS è subordinato all’autenticazione del Titolare via PIN segreto.

6.3 Emissione del certificato

I certificati vengono emessi in maniera automatica attraverso apposite applicazioni informatiche predisposte dal Certificatore le quali:

- Verificano la correttezza delle richieste di certificato, assicurandosi che:
  - siano presenti tutte le informazioni necessarie al rilascio, in forma completa e corretta;
  - siano valide e della lunghezza prevista le chiavi pubbliche che si intendono certificare;
  - il titolare sia in possesso delle relative chiavi private e le richieste siano autentiche.
- Generano e pubblicano i certificati nel registro.
- Memorizzano i certificati nella CNS.

Possono presentarsi due casi:

(a) il Titolare risulta già in possesso del dispositivo sicuro di firma: il passaggio precedente termina la procedura di validazione dei Certificati.

(b) il dispositivo sicuro di firma, inizializzato e protetto dal PIN, viene consegnato al Titolare da un incaricato del CDRL oppure spedito allo stesso per posta.

6.3.1 Formato e contenuto dei certificati di autenticazione e firma digitale

Di seguito è riportato il profilo minimo del certificato di Autenticazione CNS:

```
Certificate:
Data:
      Version: 3 (0x2)
      Serial Number:
            60:e0:eb:19:5d:1a:ea:d8:f4:23:a1:30:68:08:8d:c8
      Signature Algorithm: sha1WithRSAEncryption
      Issuer:   C=IT,   O=ArubaPEC   S.p.A.,   OU=Certification   AuthorityB,
      CN=ArubaPEC S.p.A. NG CA
2
      Validity
            Not Before: Feb 10 00:00:00 2011 GMT
            Not After : Feb 9 23:59:59 2014 GMT
      Subject:
CN=AAAAAA00A00A000A/7000000820691652.Dmx4NnOV3jvfQ0Rs99R/IDrnqy0=/serialNumber
=IT:AAAAAA00A00A000A,   GN=NomeTest201102100001,   SN=CognomeTest201102100001,
O=ArubaPEC S.p.A., OU=ArubaPEC
S.p.A., C=IT
      Subject Public Key Info:
            Public Key Algorithm: rsaEncryption
                  Public-Key: (1024 bit)
                  Modulus:
                        00:e1:52:ce:bc:03:4f:73:59:e8:46:40:8e:24:13:
                        c7:4e:1c:68:1d:de:81:20:4a:9a:14:c2:29:cb:7e:
                         . . .
                        04:d7:2c:58:61:8f:a8:c3:4b:16:cb:48:74:1f:58:
                        28:00:ee:e0:a5:4c:d2:1c:e6:de:7d:92:eb:fb:b0:
                        87:89:62:26:46:26:0e:cd:83
                  Exponent: 65537 (0x10001)
      X509v3 extensions:
```

```
            X509v3 Certificate Policies:
                 Policy: 1.3.76.16.2.1
                   User Notice:
                     Explicit    Text:    Identifies    X.509    authentication
certificates issued for the italian National Service Card (CNS) project in
according to the italian regulation
                 Policy: 1.3.6.1.4.1.29741.1.1.2
                   CPS: https://ca.arubapec.it/cps.html
           X509v3 CRL Distribution Points:
                 Full Name:
URI:http://onsitecrl.arubapec.trustitalia.it/ArubaPECSpACertificationAuthority
B/LatestCRL.crl
           X509v3 Key Usage: critical
                 Digital Signature, Key Encipherment
           X509v3 Authority Key Identifier:
                 keyid:F2:FF:63:40:1C:11:42:FD:CC:DF:F1:59:F6:6E:E8:99:87:31:47
                 :79

           X509v3 Subject Key Identifier:
                 70:7A:8F:5C:A7:71:BD:BA:9B:02:05:01:AF:5F:17:43:F5:98:63:13
           X509v3 Subject Alternative Name:
                 email:support@ca.arubapec.it
           Authority Information Access:
                 OCSP - URI:http://ocsp.arubapec.trustitalia.it

           X509v3 Extended Key Usage:
                 TLS  Web  Client  Authentication,  Microsoft  Smartcardlogin,  E-
                 mail Protection
     Signature Algorithm: sha1WithRSAEncryption
         80:8c:65:67:f7:50:10:32:22:60:87:b1:8d:6c:8e:3f:5f:97:
         22:ae:77:6f:e0:93:03:f7:00:52:df:4a:eb:9c:c8:e9:2b:ee:
          . . .
         d8:70:48:d8:cf:c3:43:5e:01:9b:22:c9:6c:f1:49:87:da:76:
         da:17:b1:d5:73:15:79:4e:e9:83:b3:fe:e6:ba:96:20:59:cb:
         2f:d3:8f:61:76:f0:42:f6:21:2e:c8:1d:e4:a0:7f:d8:b4:3b:
         91:8a:ed:8a
```

Di seguito è riportato il profilo minimo del certificato di firma digitale:

```
Certificate:
    Data:
        Version: 3 (0x2)
        Serial Number:
            34:c2:0f:71:d9:a6:58:ec:3c:80:81:3f:d4:80:ee:e2
        Signature Algorithm: sha256WithRSAEncryption
        Issuer:   C=IT,   O=ArubaPEC   S.p.A.,   OU=Certification   AuthorityC,
        CN=ArubaPEC S.p.A. NG
CA 3
        Validity
            Not Before: Feb 10 00:00:00 2011 GMT
            Not After : Feb 9 23:59:59 2014 GMT
        Subject:   C=IT,   O=non   presente,   OU=Certification   Authority,
CN=CognomeTest201102100001
NomeTest201102100001/serialNumber=IT:AAAAAA00A00A000A,
GN=NomeTest201102100001,
SN=CognomeTest201102100001/dnQualifier=10269710/title=sig
```

```
        Subject Public Key Info:
             Public Key Algorithm: rsaEncryption
                  Public-Key: (1024 bit)
                  Modulus:
                       00:af:24:ff:f4:16:c3:b3:8e:2d:75:f4:7b:1b:df:
                        . . .
                       7d:e3:5b:07:e7:80:12:7e:ea:40:b9:01:eb:42:e5:
                       46:c5:f8:f4:02:3d:df:5d:47
                  Exponent: 65537 (0x10001)
        X509v3 extensions:
             X509v3 Key Usage: critical
                  Non Repudiation
             X509v3 Subject Key Identifier:
                  90:12:0A:E8:C7:5C:A8:F7:F1:D2:EA:BE:9F:B3:06:C4:0D:1B:B6:C3
             X509v3 Certificate Policies:
                  Policy: 1.3.6.1.4.1.29741.1.1.1
                    CPS: https://ca.arubapec.it/cps.html
             X509v3 CRL Distribution Points:

                  Full Name:
                    URI:
http://onsitecrl.arubapec.trustitalia.it/ArubaPECSpACertificationAuthorityC/La
testCRL.crl

             qcStatements:
                 0!0......F..0......F.....0......F..
             X509v3 Subject Alternative Name:
                 email:support@ca.arubapec.it
             X509v3 Authority Key Identifier:
                 keyid:F0:C0:45:B1:B6:35:B4:EA:5F:29:FA:83:03:4A:DC:2F:F5:B3:7D:
                 E8

             Authority Information Access:
                 OCSP - URI:http://ocsp.arubapec.trustitalia.it

   Signature Algorithm: sha256WithRSAEncryption
       43:3c:14:29:fd:dc:e8:c6:a3:49:5c:5f:dc:00:d8:f3:a2:b1:
       . . .
       d5:ef:ca:1c:2d:21:0c:b7:36:73:13:91:1c:7c:32:e8:66:f2:
       5c:ae:64:ce
```

6.3.2 Validità dei certificati

I certificati sono da considerarsi validi per tre anni a partire dalla loro emissione o in caso di revoca/sospensione fino alla data di pubblicazione delle stesse.

6.3.3 Interdizione di una CNS

Tramite revoca si attua l'interdizione definitiva della CNS mentre attraverso la sospensione si dà luogo ad una interdizione temporanea. In entrambi i casi, dal momento in cui viene eseguita l'operazione il certificato non viene più riconosciuto come valido.

I certificati revocati o sospesi sono inseriti nella CRL (una lista di revoca e sospensione) firmata dal Certificatore e pubblicata secondo la periodicità stabilita nel registro dei certificati.

E' la pubblicazione della revoca e della sospensione nella CRL ha dar loro efficacia, invalidando l'utilizzo delle corrispondenti chiavi private da quel momento in poi. La revoca o sospensione dei certificati può avvenire:

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

E' il Certificatore a verificare il richiedente la revoca o sospensione. L'Ente Emettitore, direttamente o attraverso personale delegato, autentica il Titolare che richiede la revoca o la sospensione registrandone inoltre la motivazione.

6.3.4 Motivi per la revoca di un certificato

E' da richiedersi la revoca nel caso in cui si verifichino le seguenti condizioni:

- una o più chiavi private risultano compromesse come nei casi di seguito riportati:

  - . furto o smarrimento CNS;
  - . cessata segretezza di una o entrambe le chiavi private e/o del codice di attivazione che ne consente l'accesso;
  - . qualsivoglia evento compromettente l' affidabilità delle chiavi private;

- impossibilità da parte del Titolare di utilizzo della CNS (come in caso di guasto del dispositivo);

- cambiamento dei dati Titolare all'interno dei Certificati;

- verificata non conformità al presente Manuale Operativo.

6.3.5 Procedura per la richiesta di revoca

Sono previste diverse procedure per l'attivazione della revoca, a seconda che sia il Titolare, il Certificatore o l'Ente Emettitore a richiederla.

Revoca su iniziativa del Titolare

Il Titolare può richiedere la revoca:

1. via help desk, che si occuperà di riconoscere il titolare nel sistema e compilerà un modulo con le informazioni: nome, cognome, codice fiscale, motivazione.
2. spedendo un fax all'Ente Emettitore, specificando nome, cognome, codice fiscale, codice utente e allegando copia del documento di identità.
3. recandosi direttamente presso l'Ente Emettitore competente.

Revoca su iniziativa del Certificatore
Il Certificatore, fatta eccezione per i casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di revocare il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi revocato.

Revoca su iniziativa dell'Ente Emettitore
L'Ente Emettitore, eccetto casi di motivata urgenza, comunica in anticipo al Titolare l'intenzione di revocare il certificato, specificandone il motivo e la data di decorrenza. Il certificato viene inserito nella CRL e da quel momento è da considerarsi revocato.

6.3.6 Motivi per la Sospensione di un certificato

Il certificatore sospende un certificato a seguito della richiesta del Titolare o perché lo ritiene opportuno, e comunque nel caso in cui:

- sia stata richiesta la revoca di un certificato ma non vi sia stato il tempo per verificarne l'autenticità;
- una delle parti nutra un ragionevole dubbio sulla validità del certificato;
- sia necessaria un'interruzione della validità del certificato.

6.3.7 Procedura per la richiesta di sospensione

Il Titolare può richiedere la sospensione attraverso una delle seguenti modalità:

- telefonando al Call Center dell'Ente Emettitore e fornendo le informazioni previste per la sospensione: nome, cognome, codice fiscale, tipologia dispositivo, motivazione della richiesta, codice utente;
- attraverso la compilazione di un form sul sito web contenente: nome, cognome, codice fiscale, motivazione della richiesta, codice utente;
- recandosi direttamente presso l'Ente Emettitore competente.

6.3.8 Procedura di richiesta di riattivazione

La richiesta di riattivazione è possibile solamente nei casi in cui un certificato è stato precedentemente sospeso. Il titolare del certificato sospeso ha due diverse modalità di riattivazione a sua disposizione:

- attraverso il sito web www.card.infocamere.it , ovvero compilando l'apposito form contenente codice utente e codice fiscale;
- comunicando i propri dati anagrafici (nome, cognome, codice fiscale) e il codice utente all'addetto dell'help desk, che procede con la riattivazione.
- recandosi direttamente presso l'Ente Emettitore competente.

6.3.9 Pubblicazione e frequenza di emissione della CRL

Pubblicazione,frequenza e tempistiche della CRL sono riportate nella certificate policy [14] del Certificatore.

6.4 Rinnovo del Certificato

Il campo "validity period" (periodo di validità) e i relativi attributi "not after" (non dopo il) e "not before" (non prima del) contengono l'indicazione dell' intervallo temporale all'interno del quale un certificato è da considerarsi valido. La procedura di rinnovo richiede la generazione di due nuove coppie di chiavi; la richiesta di rinnovo va effettuata prima dello scadere dei certificati. Le procedure di rinnovo certificati sono pubblicate sul sito www.card.infocamere.it.

7. Disponibilità del servizio

<u>Orari di erogazione del servizio</u>

Accesso all'archivio pubblico dei certificati:

- H24 secondo quanto previsto dal Manuale operativo del Certificatore.

Sospensione e Riattivazione:

- H24 attraverso il sito web www.card.infocamere.it
- Attraverso il servizio di help desk dalle ore 8 alle ore 20 (lun.-ven), dalle ore 9 alle 13 (sab) esclusi i festivi
- Presso la Camera di Commercio secondo gli orari indicati nel suo sito web

Revoca:

- Attraverso il servizio di help desk dalle ore 8 alle ore 20 (lun.-ven), dalle ore 9 alle 13 (sab) esclusi i festivi
- Presso la Camera di Commercio secondo gli orari indicati nel suo sito web

Registrazione, generazione, pubblicazione:

- Presso la Camera di Commercio secondo gli orari indicati nel suo sito web

Rinnovo:

- H24 attraverso il sito web www.card.infocamere.it.