CNS

Realizzazione e diffusione della carta nazionale dei servizi con Firma Digitale

Documento: **Manuale Operativo**

Data: 06/12/2018
File: 20181206_CNS_Ing-Arezzo_Manuale Operativo_v1.docx
Versione: 1.0

Firmato digitalmente da
beatrice benelli
CN = benelli beatrice
O = Ordine Ingegneri della Provincia di Arezzo/80008860514
C = IT

SASSETTI ANDREA
16.04.2019 08:03:54 UTC

1. Introduzione

1.1 Storia delle versioni e delle modifiche

Versione e data	1.0 del 06/12/2018
Descrizione modifiche	Prima emissione

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 del Ordine degli Ingegneri della Provincia di Arezzo(da qui in avanti Ordine)**.**

La CNS è emessa dal Ordineed i relativi certificati di autenticazione e di firma digitale sono sottoscritti dal Certificatore accreditato Aruba PEC.

Le indicazioni di questo documento hanno validità per le attività relative al Ordinein qualità di Ente Emettitore, ad Aruba PEC nel ruolo di Certificatore, 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

3. Riferimenti normativi e tecnici

3.1 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. DPCM 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

3.2 Riferimenti tecnici

8. Certificate Policy CNS (https://ca.arubapec.it/ARUBAPEC-CP-CNS-1.0.pdf)
9. Manuale Operativo - Servizio di Certificazione Digitale – (https://ca.arubapec.it/MOArubaPEC.pdf)
10. RFC 3280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile

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

3.3 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.

Identificazione informatica

La validazione dell'insieme di dati attribuiti in modo esclusivo ed univoco ad un soggetto, che ne consentono l'individuazione nei sistemi informativi, effettuata attraverso opportune tecnologie anche al fine di garantire la sicurezza dell'accesso.

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 Locale [CDRL]

L'Ente emettitore o altra struttura delegata dall'Ente emettitore che svolge le attività necessarie al rilascio, da parte di quest'ultimo, dei certificati digitali nonché alla consegna della CNS.

Certificato Digitale

Insieme di dati elettronici firmati dalla Certification Authority con la chiave privata di certificazione, che garantisce la corrispondenza tra il nome del soggetto certificato e la sua chiave pubblica. Il formato del certificato ed i dati ivi contenuti sono definiti dallo standard ITU-T X.509.

Certificatore

Il soggetto che presta servizi di certificazione delle firme elettroniche o che fornisce altri servizi connessi con queste ultime. Ai fini del presente documento il ruolo di Certificatore è svolto da Aruba PEC S.p.A.

Certificate Revocation List - Lista dei certificati revocati o sospesi

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.

Codice utente

E' un codice segreto assegnato all'utente al momento del rilascio della CNS.

Esso costituisce lo strumento di identificazione del Titolareall'interno del sistema che gestisce il ciclo di vita della CNS.

Tale codice è contenuto assieme a PIN e PUK all'interno della busta cieca consegnata al Titolare con la propria CNS.

Codici di sicurezza

La terna rappresentata da PIN, PUK e Codice Utente.

Ente Emettitore

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.

Ai fini del presente documento il ruolo di Ente Emettitore è svolto dal Ordine.

Firma elettronica avanzata

Insieme di dati in forma elettronica allegati oppure connessi a un documento informatico che consentono l'identificazione del firmatario del documento e garantiscono la connessione univoca al firmatario, creati con mezzi sui

quali il firmatario può conservare un controllo esclusivo, collegati ai dati ai quali detta firma si riferisce in modo da consentire di rilevare se i dati stessi siano stati successivamente modificati.

Firma digitale

Un particolare tipo di firma elettronica avanzata basata su un certificato qualificato e su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

IR

Incaricato alla Registrazione. Soggetto che esegue le funzioni di identificazione certa del Richiedente.

Manuale Operativo

Il Manuale Operativo definisce le procedure che l'Ente Emettitore applica nello svolgimento del servizio di rilascio e gestione della CNS e dei relativi Certificati.

PIN

Personal Identification Number – codice associato alla CNS e ai certificati digitali in essa contenuti, che deve essere utilizzato dal Titolare per accedere alle sue funzioni.

Pubblico Ufficiale

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

PUK

Personal Unlocking Key - codice associato alla CNS e ai certificati digitali in essa contenuti, che deve essere utilizzato dal Titolare per riattivare il

dispositivo o un certificato in seguito al blocco dello stesso per una ripetuta errata digitazione del PIN.

Revoca di un Certificato

E' l'operazione con cui il Certificatore annulla definitivamente la validità del certificato prima della sua scadenza naturale.

Richiedente

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

Sospensione di un Certificato

E' l'operazione con cui il Certificatore annulla temporaneamente la validità del certificato prima della sua scadenza naturale.

Titolare (Utente - Ingegnere)

E' il soggetto in favore del quale è rilasciata la CNS.

3.4 Acronimi

CA – Certification Authority

CNIPA – Centro Nazionale per l'Informatica nella Pubblica Amministrazione

CNS – Carta Nazionale dei Servizi

CRL – Certificate Revocation List - Lista dei certificati revocati o sospesi

DIGITPA - Ente Nazionale per la digitalizzazione della Pubblica Amministrazione (ex CNIPA)

HTTP – Hyper Text Transfer Protocol

HTTPS – Hyper Text Transfer Protocol over Secure Socket Layer

PIN – Personal Identification Number

PUK – PIN Unblocking Key

4. 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 e di Firma Digitale sono rilasciati dal Certificatore accreditato Aruba PEC su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte dell'Ordine provinciale degli APPC di competenza.
I certificati di Autenticazione e di Firma Digitale sono rilasciati su dispositivo sicuro di firma conforme alla normativa in merito alla Firma Digitale.

Il presente documento contiene le procedure operative che si attuano per l'emissione delle CNS e dei relativi Certificati di Autenticazione e di Firma Digitale (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 [9].

4.1 Identificazione del documento

Questo documento è denominato "**CNS Ingegneri di Arezzo - Manuale Operativo**".

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 (https://www.ordineingegneriarezzo.it/)e presso il sito web del Certificatore accreditato Aruba PEC (www.pec.it).

4.2 Ente emettitore

L'Ente emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico l'**Ordine degli Ingegneri della Provincia di Arezzo**, ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta nonché della corretta gestione del ciclo di vita della CNS. La responsabilità di alcune delle attività può essere delegata dall'Ente emettitore a terzi, ma l'Ente emettitore rimane comunque responsabile del ciclo di vita della carta nel suo complesso.

4.3 Contatti

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

Aruba PEC S.p.A.
Via San Clemente 53

Ponte San Pietro (BG)

Telefono (centralino) :+39 05750504
Fax:+39 0575 862022
Indirizzo e-mail: assistenza@ca.arubapec.it
Indirizzo web (informativo): www.pec.it
Indirizzo web (assistenza): http://assistenza.aruba.it

4.4 Tutela dei dati personali

Le informazioni relative all'interessato 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 D.Lgs. 30 giugno 2003, n. 196 [4].

5. Ruoli previsti

5.1 Ente emettitore

L'Ente emettitore è l'Ordine, che è responsabile della sicurezza del circuito di emissione, del rilascio della carta e della corretta gestione del ciclo di vita della carta stessa.
L'Ente emettitore delega la responsabilità delle seguenti attività:

- Produzione e inizializzazione delle CNS
- Personalizzazione delle CNS
- Generazione dei certificati di Autenticazione e Firma Digitale

Al Certificatore.

La delega delle responsabilità delle seguenti attività:

- Identificazione dei Titolari
- Registrazione dei Titolari
- Consegna della CNS e dei relativi codici di attivazione (PIN) e sblocco (PUK)

è invece attribuita all'Ordine provinciale di competenza in cui risulta iscritto il professionista.
L'Ente emettitore rimane comunque responsabile del ciclo di vita della carta nel suo complesso.

5.2 Produttori

Il produttore è l'azienda che provvede alla fornitura ed inizializzazione delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, predispone opportunamente gli spazi dedicati alla firma digitale ed applica al supporto fisico l'artwork e gli elementi costanti.

I Produttori del circuito CNS per l'Ordine sono:

- STMicroelectronics Srl - Incard Division (http://www.incard.it)
- Oberthur (http://www.oberthur.com)

5.3 Certificatore

Il certificatore, Aruba PEC, è il soggetto che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche.

5.4 Titolare

Il titolare della carta è il professionista utilizzatore della stessa come strumento di identificazione in rete e di sottoscrizione dei documenti informatici.

6. Obblighi e responsabilità

6.1 Obblighi del titolare

Il titolare della CNS ha l'obbligo e la responsabilità di:

- garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ente emettitore, o struttura delegata, per la richiesta della CNS
- non essere titolare di una carta d'identità elettronica; (dopo il 31/12/2011, art 66, comma8-bis del CAD);
- proteggere e conservare la propria CNS con la massima accuratezza al fine di garantire la riservatezza delle chiavi private in essa custodite;
- 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;
- 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;
- proteggere e conservare il Codice utente utilizzato per la sospensione, riattivazione e revoca della CNS;
- adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della chiave privata e della CNS;
- utilizzare le chiavi e il certificato per le sole modalità previste nel presente Manuale Operativo;
- richiedere immediatamente la revoca delle certificazioni relative alle chiavi contenute nella CNS al verificarsi di quanto previsto nel presente Manuale Operativo;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

6.2 Responsabilità

6.2.1 Responsabilità dell'Ente emettitore

L'Ente emettitore è responsabile

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione in base ai dati forniti dall'Ordine degli Ingegneri di Arezzo;
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione in base ai dati forniti dall'Ordine degli Ingegneri di Arezzo;
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione, attivazione e ritiro della carta (responsabilità delegata al Certificatore Aruba PEC e, limitatamente alla consegna della CNS e alla produzione della relativa documentazione, all'Ordine degli Ingegneri di Arezzo);

6.2.2 Responsabilità del produttore

Il produttore deve garantire la sicurezza del circuito di produzione rispettando le normative esistenti.

6.2.3 Responsabilità del certificatore

Il certificatore è responsabile della generazione del certificato di autenticazione CNS e di Firma Digitale. Le informazioni anagrafiche raccolte dal Certificatore in fase di identificazione dei Titolari da parte del Ordine degli Ingegneri di Arezzo, congiuntamente con le chiavi pubbliche generate in fase di personalizzazione delle CNS, sono utilizzate dal Certificatore per generare i certificati secondo le specifiche disponibili presso il sito di DigitPA.

7. Amministrazione del manuale operativo

7.1 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.

Eventuali errori, imprecisioni o suggerimenti possono essere segnalati al contatto per gli utenti indicato al par 4.3.

Modifiche minori comportano l'incremento del sottonumero 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.

Il Manuale è pubblicato in conformità a quanto indicato al par. 4.1 in formato elettronico.

7.2 Responsabile dell'approvazione

Questo Manuale Operativo viene approvato dal Consiglio dell'Ordine degli Ingegneri della Provincia di Arezzo.

Ordine degli Ingegneri della Provincia di Arezzo,
Via Petrarca, 21
Citta: Arezzo
CAP: 52100
Tel: 0575 27730
Indirizzo e-mail: info@ordineingegneriarezzo.it
Indirizzo pec: ordingar@pec.aruba.it
Indirizzo web: www.ordineingegneriarezzo.it

8. Identificazione titolare

Questo capitolo descrive le procedure usate per:

- l'identificazione del Richiedente (Professionista) al momento della richiesta di rilascio della CNS e dei relativi certificati di Autenticazione CNS e Firma Digitale
- l'autenticazione del Titolare, nel caso di rinnovo, revoca e sospensione di certificati di Autenticazione CNS e Firma Digitale

8.1 Identificazione De-Visu

Il Certificatore Aruba PEC, in qualità di struttura delegata dall'Ente emettitore, per il rilascio della CNS e dei relativi certificati di Autenticazione CNS e Firma Digitale, verifica con certezza l'identità del Richiedente.

8.1.1 Soggetti abilitati ad effettuare l'identificazione

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

- Il Certificatore, anche tramite suoi incaricati (CDRL o IR);
- Il CDRL, anche tramite suoi incaricati
- Pubblico Ufficiale.

8.1.2 Procedure per l'identificazione

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 del DPR 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.

Per lo svolgimento di tale attività, l'identificazione del titolare (Ingegnere), vincolante ai fini del rilascio della CNS, viene effettuata dall'incaricato dell'Ordine degli Ingegneri della Provincia di Arezzo (IR) presso il quale il titolare dovrà recarsi per il ritiro della CNS preventivamente prodotta e rilasciata dalla CA Aruba PEC.
Per ulteriori dettagli si rimanda alla procedura ampiamente descritta al capitolo 10.

8.2 Richiesta di rilascio della CNS e dei Certificati

I passi principali a cui il Richiedente (Ingegnere) deve attenersi per ottenere una CNS con certificato di autenticazione e Firma Digitale sono:

- prendere visione del presente Manuale Operativo e della Certificate Policy [8], [9] e dell'eventuale ulteriore documentazione informativa;
- seguire le procedure di identificazione adottate dal Certificatore come descritte nei paragrafi che seguono;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione e prendere visione, accettandole, delle modalità di utilizzo della CNS;

8.2.1 Informazioni che il richiedente deve fornire

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nei Certificati e quelle che consentono di gestire in maniera efficace il rapporto tra l'Ente Emettitore ed il Richiedente/Titolare (professionista). Il modulo di richiesta deve essere sottoscritto dal Richiedente/Titolare (professionista).

Sono considerate obbligatorie le seguenti informazioni:

- Cognome e Nome
- Data e luogo di nascita
- Cittadinanza
- Codice fiscale
- Indirizzo di residenza
- Indirizzo e mail
- Estremi del documento di riconoscimento presentato per l'identificazione, quali tipo, numero, ente emittente e data di rilascio dello stesso.
- Estremi di iscrizione all'albo:
    - Sezione di appartenenza
    - Settore di appartenenza
    - Titolo
    - Numero di iscrizione
    - Data di iscrizione

La fase di registrazione delle informazioni necessarie all'emissione del certificato di autenticazione e di Firma Digitale, viene eseguita dal titolare (Ingegnere) attraverso un opportuna pagina della CA dedicata alle convezioni Aruba PEC.

Per ulteriori dettagli si rimanda alla procedura ampiamente descritta10 al paragrafo che segue.

9. Operatività

Questo capitolo descrive le operazioni relative all'emissione, attivazione, sospensione, revoca e rinnovo dei certificati contenuti a bordo della CNS.

9.1 Emissione e spedizione delle CNS ai titolari

Tutte le attività relative al processo di emissione delle CNS seguono quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

Per ciò che riguarda la consegna della CNS questa, dopo il rilascio ed unitamente alla busta cieca contenente i codici di attivazione pin puk, viene inizialmente spedita presso l'Ordine provinciale in cui risulta iscritto il professionista.

Successivamente, l'Ordine provinciale provvederà al riconoscimento del professionista e successiva consegna della CNS e busta pin puk.

9.2 Registrazione dei dati dei Titolari

Le attività relative alla registrazione dei dati dei Titolari seguono quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

9.3 Generazione e protezione delle coppie di chiavi

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 direttamente all'interno del dispositivo sicuro e la loro lunghezza è di almeno 1024 bit.
In linea generale, tutte le attività relative alla generazione e protezione delle coppie di chiavi seguono quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

9.4 Rilascio dei certificati di Autenticazione e di Firma Digitale

Una volta completata la fase di creazione delle coppie di chiavi, si procede automaticamente all'emissione dei Certificati 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 la lunghezza delle chiavi pubbliche che si intendono certificare sia conforme alla normativa;
    - 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.

In linea generale, tutte le attività relative legate alla generazione dei Certificati seguono quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

9.5 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.

9.6 Interdizione di una CNS

L'interdizione definitiva (revoca) o temporanea (sospensione) di una CNS si attua revocando o sospendendo i Certificati corrispondenti alle chiavi private in essa custodite.
In entrambi i casi, dal momento in cui la variazione di stato del certificato viene pubblicata nella CRL, il certificato oggetto di sospensione/revoca non è più riconosciuto come valido.

La **revoca** consiste nel blocco definitivo dell'operatività del certificato mentre la **sospensione** è un blocco temporaneo del certificato che può quindi essere **riattivato** o definitivamente revocato.

I certificati revocati o sospesi sono inseriti nella CRL (una lista di revoca e sospensione) firmata dal Certificatore e pubblicata secondo le modalità e la periodicità stabilite nel Manuale Operativo di Aruba PEC [9].

E' la pubblicazione del certificato all'interno della CRL a dar efficacia alla revoca o sospensione, invalidando l'utilizzo delle corrispondenti chiavi private da quel momento in poi.
La revoca o sospensione dei Certificati di **autenticazione CNS** può avvenire:

- su richiesta del Titolare;
- su iniziativa del Ordine (Ente Emettitore);
- su iniziativa del Certificatore.

La revoca o sospensione dei Certificati di **Firma Digitale** presenti nella CNS può avvenire:

- su richiesta del Titolare;
- su iniziativa dell'Ordine provinciale di competenza;
- su iniziativa del Certificatore.

E' il Certificatore a verificare il richiedente la revoca o sospensione. Il Certificatore, direttamente oattraverso personale delegato, autentica il Titolare che richiede la revoca o la sospensioneregistrandone inoltre la motivazione.

9.6.1 Revoca dei Certificati

Sono previste diverse procedure per l'attivazione della revoca, a seconda che sia il Titolare, il Certificatore o l'Ente Emettitore a richiederla.
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 dei codici si attivazione (PIN) o sblocco (PUK) che ne consentono l'accesso;
- qualsivoglia evento compromettente l' affidabilità delle chiavi private;

- impossibilità da parte del professionista di utilizzo della CNS (come in caso di guasto del dispositivo);
- variazioni dei dati del Titolare riportati all'interno dei Certificati;
- verificata non conformità al presente Manuale Operativo.

La procedura e le modalità di richiesta di revoca dei Certificati sono conformi a quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

9.6.2 Sospensione dei Certificati

Sono previste diverse procedure per l'attivazione della sospensione, a seconda che sia il Titolare, il Certificatore o l'Ente Emettitore a richiederla.
E' utile richiedere la sospensione nel caso in cui si verifichino le seguenti condizioni:

- 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.

La procedura e le modalità di richiesta di sospensione dei Certificati sono conformi a quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

9.6.3 Riattivazione dei Certificati

La riattivazione consiste nel ripristino delle funzionalità del certificato ed è attuabile solo per quei certificati che siano stati precedentemente sospesi.
La procedura e le modalità di richiesta di riattivazione dei Certificati sono conformi a quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC [9].

10. Procedura di richiesta, produzione e rilascio CNS

Questo capitolo descrive nel dettaglio la procedura usata per il rilascio delle CNS con certificato di autenticazione e Firma Digitale per l'Ordine degli Ingegneri della Provincia di Arezzo.

10.1 Richiesta CNS

Di seguito è descritta una proposta di flusso di rilascio per la Carta dell'Iscritto:

1. L'iscritto si reca all'Ordine munito di un apposito Modulo di Richiesta dei Certificati precompilato
2. L'iscritto effettua il pagamento e procede alla sottoscrizione di un apposito Modulo di Richiesta dei Certificati dinnanzi all'Operatore di Registrazione
3. L'Operatore di Registrazione (ad esempio segreteria dell'Ordine), colleziona i dati necessari per l'evasione delle richieste in un file CSV e raccoglie le fotografie dell'iscritto
4. L'Operatore di Registrazione invia un archivio contenente tutte le richieste e le immagini delle fotografie ad una casella dedicata e concordata con la Certification Authority
5. La Certification Authority procede all'evasione delle richieste contenute nel CSV e produce le card
6. La Certification Authority, terminata la lavorazione del lotto, procede con l'invio di una PEC allegando il file degli esiti
7. La Certification Authority invia all'Ordine una spedizione contenente:

   a. Il set delle Carte personalizzate graficamente ed elettricamente

   b. Il set delle scratch card PIN PUK personalizzate graficamente ed elettricamente

c. Un plico contenente i lettori USB (opzionale)

8. L’Ordine, ogni 60 giorni, invia gli originali dei Moduli di Registrazione compilati e sottoscritti alla Certification Authority..

11. Disponibilità del servizio

Orari di erogazione del servizio

Accesso all'archivio pubblico dei certificati:

- H24 secondo quanto previsto dal Manuale operativo del Certificatore.

Sospensione e Riattivazione:

- H24 attraverso il sito web del Certificatore
- Attraverso il servizio di help desk dalle ore 8 alle ore 18 (lun.-ven) esclusi i festivi

Revoca:

- Attraverso il servizio di help desk dalle ore 8 alle ore 18 (lun-ven) esclusi i festivi

Registrazione, generazione, pubblicazione:

- H24 attraverso sito web del Certificatore dedicato al progetto CNS per gli Ingegneri di Arezzo.