CNS

Realizzazione e diffusione della carta nazionale dei servizi con Firma Digitale

Documento: **Manuale Operativo**

Data: 08/09/2023
File: 20230908_CNS_Cittadini - Manuale Operativo.doc
Versione: 1.3

Responsabile del documento:

GIANCARLA MASE'
15.09.2023 16:57:34 UTC

1. Introduzione

1.1 Storia delle versioni e delle modifiche

Versione e data	Descrizione modifiche
1.0 del 21/08/2012	Prima versione
1.1 del 3/12/2015	Durata certificati
1.2 del 10/05/2022	Aggiornamento CA
1.3 del 08/09/2023	Piccole modifiche di forma ai: P. 2; P. 4.1; P. 5.1; P. 7.1; P. 7.2; P. 8.1; P. 8.1.3; P. 9.6; P. 10. P. 3.1: aggiornamento dei riferimenti normativi. P. 3.3: inserita forma tabellare e aggiornamento definizioni e riferimenti normativi. P. 4.3: aggiornamento numeri di centralino e indirizzo email Aruba PEC, eliminato canale di contatto fax. P.9.7: aggiornamento del paragrafo.

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 dell'Università della Calabria (UNICAL).

La CNS è emessa dall'Università della Calabria ed i relativi certificati di autenticazione e di firma digitale sono sottoscritti dal Certificatore accreditato Aruba PEC o dal Certificatore accreditato Actalis a seconda dei casi.

Le indicazioni di questo documento hanno validità per le attività relative all'Università della Calabria in qualità di Ente Emettitore, ad Aruba PEC o Actalis 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** S.p.A. Manuale Operativo Certificati Qualificati - tempo per tempo vigente pubblicato all'indirizzo: https://www.pec.it/termini-condizioni.aspx
- **Actalis** S.p.A. Manuale Operativo Certificati Qualificati - tempo per tempo vigente pubblicato all'indirizzo: https://www.actalis.it/area-download.aspx

3. Riferimenti normativi e tecnici

3.1 Riferimenti normativi

1. Decreto Legislativo 7 marzo 2005, n.82 e s.m.i.– Codice dell'amministrazione digitale - (G.U. n.112 del 16 maggio 2005) nel seguito referenziato come “CAD”;
2. Decreto del Presidente della Repubblica 28 Dicembre 2000, n. 445 e s.m.i. – Testo Unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa (nel seguito referenziato come “TU”);
3. Decreto del Presidente del Consiglio dei Ministri 22 febbraio 2013 “Regole tecniche in materia di generazione, apposizione e verifica delle firme elettroniche avanzate, qualificate e digitali”;
4. Decreto Legislativo 30 giugno 2003, n. 196 e s.m.i. - Codice in materia di protezione dei dati personali;
5. Regolamento (UE) 2016/679 (“GDPR”) del Parlamento Europeo e del Consiglio del 27 aprile 2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE;
6. Decreto del Presidente della Repubblica 2 marzo 2004, n. 117 “Regolamento concernente la diffusione della carta nazionale dei servizi”;
7. 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”;
8. “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

9. Certificate Policy CNS di Aruba PEC ed Actalis
10. Aruba PEC S.p.A. Manuale Operativo Certificati Qualificati - tempo per tempo vigente pubblicato all'indirizzo: https://www.pec.it/termini-condizioni.aspx
11. Actalis S.p.A. Manuale Operativo Certificati Qualificati - tempo per tempo vigente pubblicato all'indirizzo: https://www.actalis.it/area-download.aspx
12. RFC 5280 (2002): "Internet X.509 Public Key Infrastructure Certificate and CRL Profile and Certificate Revocation List (CRL) Profile";
13. Information Technology – Open Systems Interconnection – The Directory: Authentication Framework; ITU-T Recommendation X.509 (2019) | ISO/IEC 9594-8

3.3 Definizioni ed acronimi

Vengono di seguito elencate le definizioni e gli acronimi utilizzati nella stesura del presente documento. Per i termini definiti dal CAD [1], DPR 445/2000 [2], dal DPCM 22 febbraio 2013 [3] e dal DPR 2 marzo 2004, n. 117 [5] si rimanda alle definizioni stabilite dagli stessi decreti.

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.
Agenzia per l'Italia Digitale - AgID	Ente Nazionale per la digitalizzazione della Pubblica Amministrazione (già DIGITPA e CNIPA).
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	L'Ente emettitore o altra struttura delegata dall'Ente emettitore che svolge le attività necessarie al rilascio, da parte di quest'ultimo, dei

Locale [CDRL]	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, o anche CA – Certification Authority	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 o Actalis S.p.A.
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.
Certificate Revocation List - Lista dei certificati revocati o sospesi [CRL]	È 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	È un codice segreto assegnato all’utente al momento del rilascio della CNS. Esso costituisce lo strumento di identificazione del Titolare all’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	È la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS. Ai fini del presente documento il ruolo di Ente Emettitore è svolto dall' Università della Calabria.
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.
Produttore	Il produttore è l'azienda che provvede alla fornitura ed inizializzazione delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS
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	È l'operazione con cui il Certificatore annulla definitivamente la validità del certificato prima della sua scadenza naturale.

Richiedente	È il soggetto fisico che richiede all'Ente emettitore il rilascio della CNS
Sospensione di un Certificato	È l'operazione con cui il Certificatore annulla temporaneamente la validità del certificato prima della sua scadenza naturale.
Titolare (Utente – Cittadino)	È il soggetto in favore del quale è rilasciata la CNS.

3.4 Acronimi

AgID – Agenzia per l'Italia Digitale

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

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 o Actalis su richiesta diretta del Titolare, successivamente all'identificazione fisica dello stesso da parte del Certificatore stesso quale struttura delegata dall'Ente Emettitore.
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 [10 o 11].

4.1 Identificazione del documento

Questo documento è denominato "**CNS Cittadini - Manuale Operativo**".

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

Questo documento è distribuito in formato elettronico presso il sito web dell'Ente emettitore (http://www.unical.it) e presso il sito web del Certificatore accreditato Aruba PEC (https://www.pec.it/termini-condizioni.aspx) o Actalis (Actalis S.p.A https://www.actalis.it/area-download.aspx).

4.2 Ente emettitore

L'Ente emettitore è, in generale, la Pubblica Amministrazione che rilascia la CNS, nel caso specifico l'Università della Calabria, 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 Manuale Operativo della CA interessata dovranno essere rivolte all'indirizzo di seguito indicato:

Aruba PEC S.p.A.
Via S. Clemente, 53
24036 Ponte San Pietro (BG)
Telefono (centralino): +39 0575 0505
Indirizzo web (informativo): www.pec.it
Indirizzo email (generale): CPS-requests@ca.arubapec.it

Actalis S.p.A.
Via S. Clemente, 53
24036 Ponte San Pietro (BG)
Telefono (centralino): +39 0575 050350
Indirizzo web (informativo): www.actalis.it
Indirizzo email (generale): info@actalis.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 Regolamento (UE) 2016/679 ed il D. Lgs. 30 giugno 2003, n. 196 integrato con le modifiche introdotte dal decreto legislativo 10 agosto 2018, n.101.

5. Ruoli previsti

5.1 Ente emettitore

L'Ente emettitore è l'Università della Calabria, 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 al Certificatore:

- Produzione e inizializzazione delle CNS
- Identificazione dei Titolari
- Registrazione dei Titolari
- Personalizzazione delle CNS
- Generazione dei certificati di Autenticazione e Firma Digitale
- Consegna della CNS e dei relativi codici di attivazione (PIN) e sblocco (PUK)

.
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 dell'Università della Calabria sono:

- STMicroelectronics SrL - Incard Division (https://www.st.com/)
- Idemia - Oberthur (https://www.idemia.com)

5.3 Certificatore

Il certificatore, Aruba PEC o Actalis, 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 l'utente 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
- 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 (responsabilità delegata al Certificatore Aruba PEC o Actalis);
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione (responsabilità delegata al Certificatore Aruba PEC o Actalis);
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione, attivazione e ritiro della carta (responsabilità delegata al Certificatore Aruba PEC o Actalis);

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 registrate dal Certificatore in fase di identificazione dei Titolari, congiuntamente con le chiave pubbliche generate in fase di personalizzazione delle CNS, sono utilizzate dal Certificatore per generare i certificati secondo le specifiche disponibili presso il sito di AgID. Il dettaglio della responsabilità del Certificatore è rinvenibile nei documenti del Certificatore [10 o 11].

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 ai contatti per gli utenti indicati al par 4.3.

Modifiche minori comportano l'incremento del sotto-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 presente 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

Il presente Manuale Operativo viene approvato dal Responsabile dell'Università della Calabria, la Direzione Generale, come indicato in frontespizio

8. Identificazione del titolare

Questo capitolo descrive le procedure usate per:

- l'identificazione del Richiedente 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 del titolare

Aruba PEC o Actalis, in qualità di struttura delegata dall'Ente emettitore, verifica con certezza l'identità del Richiedente, prima di procedere al rilascio della CNS e dei relativi certificati di Autenticazione CNS e Firma Digitale, utilizzando una delle modalità riportate nel Manuale Operativo di Aruba PEC o Actalis.
Nello svolgimento di tale attività, il Certificatore opera in piena conformità al proprio Manuale Operativo [10 o 11].

8.1.1 Soggetti abilitati ad effettuare l'identificazione

In base a quanto descritto nel paragrafo precedente, e a quanto riportato all'interno del Manuale Operativo del Certificatore, l'identità del Richiedente può essere accertata da uno dei soggetti di seguito indicati quando applicabile:

- Il Certificatore, tramite suoi incaricati;
- Il CDRL, tramite i suoi incaricati;
- Pubblico Ufficiale.

8.1.2 Procedure per l'identificazione

L'identificazione è eseguita da Aruba PEC o Actalis o uno dei CDRL nominati avvalendosi di una delle modalità di identificazione riportate nel Manuale Operativo di Aruba PEC o Actalis.

L'elenco dettagliato dei documenti di riconoscimento accettati da Aruba PEC ed Actalis ai fini della corretta identificazione sono riportati nel Manuale Operativo del Certificatore così come richiamato sopra.

8.1.3 Richiesta di rilascio della CNS e dei Certificati

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

1. prendere visione del presente Manuale Operativo e della Certificate Policy [9], [10 o 11] e dell'eventuale ulteriore documentazione informativa;
2. seguire le procedure di identificazione adottate dal Certificatore come descritte nei paragrafi precedenti;
3. fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
4. sottoscrivere la richiesta di registrazione e prendere visione, accettandole, delle modalità di utilizzo della CNS.

8.1.4 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. 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.

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 e spedizione delle CNS seguono quanto descritto all'interno del Manuale Operativo Aruba PEC o Actalis [10 o 11].

9.2 Registrazione dei dati dei Titolari

Le attività relative alla registrazione dei dati dei Titolari seguono quanto descritto all'interno del Manuale Operativo Aruba PEC o Actalis [10 o 11].

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 all'interno del dispositivo sicuro e la loro lunghezza è di almeno 2048 bit.
In linea generale, tutte le attività relative alla generazione e protezione delle coppie di chiavi seguono quanto descritto all'interno del Manuale Operativo Aruba PEC o Actalis [10 o 11].

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 Aruba PEC o Actalis [10 o 11].

9.5 Validità dei Certificati

I certificati sono da considerarsi validi per **tre, cinque, sei anni** a partire dalla loro emissione o in caso di revoca/sospensione fino alla data di pubblicazione delle stesse, salvo specifici accordi tra le parti interessate.

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 o Actalis [10 o 11].

La pubblicazione del certificato all'interno della CRL attribuisce efficacia alla revoca o sospensione, 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.

Il Certificatore verifica il richiedente la revoca o sospensione, direttamente o attraverso personale delegato, autenticando il Titolare che richiede la revoca o la sospensione, e registrandone inoltre la motivazione della richiesta.

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.
È 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 Titolare 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 o Actalis [10 o 11].

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.
È 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 o Actalis [10 o 11].

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 o Actalis [10 o 11].

9.7 Attivazione della CNS

La procedura e le modalità di attivazione della CNS seguono quanto descritto all'interno del Manuale Operativo del Certificatore Aruba PEC o Actalis [10 o 11] e nelle guide online presenti nel sito del Certificatore Aruba PEC o Actalis.

10. Disponibilità del servizio

Di seguito si indicano le tempistiche di disponibilità dei servizi da parte delle CA:

Accesso all'archivio pubblico dei certificati:

- H24 secondo quanto previsto dal Manuale operativo del Certificatore [10 o 11].

Sospensione, Revoca e Riattivazione:

- H24 attraverso il sito web del Certificatore (cft. par. 4.3).