MANUALE OPERATIVO

Emissione Carta Nazionale dei Servizi

CODICE DOCUMENTO 001
VERSIONE 1.0
DATA 19/09/2025

RegioneEmilia-Romagna

tinexta infocert

Sommario

Questa pagina è lasciata intenzionalmente bianca.

1 NOVITÀ INTRODOTTE RISPETTO ALLA PRIMA EMISSIONE

Campo	*Descrizione*
Versione:	1.0
Data Versione/Release:	16/07/2025
Descrizione modifiche:	Nessuna
Motivazioni:	Prima emissione

2 SCOPO E CONTENUTO 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 emessi dal Certificatore InfoCert, Trust Service Provider, su affidamento dell'Ente Emettitore.

Questo manuale indica, inoltre, le procedure da seguire in caso di smarrimento, furto o sospetta compromissione della carta.

Le indicazioni di questo documento hanno validità per le attività relative all'Ente Emettitore, per InfoCert nel ruolo di Certificatore, per gli Uffici di registrazione (RA), 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 alla seguente documentazione InfoCert, reperibile sul sito www.infocert.it/documentazione:

- Manuale Operativo Certificate Policy - Certificate Practice Statement (ICERT-INDI-MO);
- Manuale Operativo per il rilascio del certificato digitale di autenticazione (ICERT-INDI-MOCA);
- InfoCert Ente Certificatore - Certificati di Autenticazione per la Carta Nazionale dei Servizi - Certificate Policy (ICERT-INDI-CPCA-CNS).

3 RIFERIMENTI NORMATIVI

- D.P.R. n. 445/2000 Testo Unico del Documento Amministrativo e successive modifiche e integrazioni;
- Decreto Legislativo 7 marzo 2005, n. 82 (G.U. n.112 del 16 maggio 2005) – Codice dell'Amministrazione Digitale (nel seguito referenziato come CAD) e successive modifiche e integrazioni, comprese le sue Regole Tecniche e Linee Guida;
- Decreto del Presidente della Repubblica 2 marzo 2004, n. 117, Regolamento concernente la diffusione della carta nazionale dei servizi;
- Regolamento UE eIDAS (electronic IDentification Authentication and Signature) - n° 910/2014, come modificato dal Regolamento n. 1183/2024;
- Regolamento UE GDPR (General Data Protection Regulation) - n° 679/2016;
- **https://www.agid.gov.it/it/piattaforme/carta-nazionale-servizi.**

3.1 Definizioni e acronimi

Campo	Descrizione
AgID	Agenzia per l'Italia Digitale.
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.
Ente Emettitore	Ente responsabile della formazione e del rilascio della CNS. È la Pubblica Amministrazione che rilascia la CNS ed è responsabile della sicurezza del circuito di emissione e del rilascio della carta, garantendo la corretta gestione del ciclo di vita della CNS.
ERC	Emergency Request Code. Acronimo assegnato al codice di emergenza.
HTTPS	HyperText Transfer Protocol Secure
ISO	International Organization for Standardization.
IUT	Identificativo Univoco del Titolare, è un codice associato al Titolare che lo identifica univocamente presso il Certificatore. Il Titolare ha codici diversi per ogni ruolo per il quale può firmare.
LDAP	Lightweight Directory Access Protocol, protocollo utilizzato per accedere al registro dei certificati.
Lista dei Certificati Revocati o Sospesi (Certificate Revocation List – CRL)	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.
OCSP	Online Certificate Status Protocol.
OID	Object Identifier, è costituito da una sequenza di numeri, registrata secondo la procedura indicata nello standard ISO/IEC 6523, che identifica un determinato oggetto all'interno di una gerarchia.
PIN	Personal Identification Number, codice associato alla CNS, utilizzato dall'utente per accedervi alle funzioni. Altre funzioni installate sulla CNS richiedono PIN specifici della funzione.
PUK	Codice personalizzato per ciascuna CNS, utilizzato dal Titolare per riattivare il proprio dispositivo di firma in seguito al blocco dello stesso per errata digitazione del PIN. Altre funzioni installate sulla CNS richiedono PUK specifici della funzione.
RAO	Registration Authority Officer, 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.
Revoca o sospensione di un Certificato	Operazione con cui il Certificatore annulla la validità del certificato prima della naturale scadenza. Vedi Lista dei Certificati Revocati o Sospesi - CRL.
Richiedente - Subscriber	Soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS.
Titolare - Subject	Soggetto in favore del quale è rilasciata la CNS ed è identificato nel certificato digitale come il legittimo possessore della chiave privata, corrispondente alla chiave pubblica contenuta nel certificato stesso. Al Titolare stesso è attribuita la firma elettronica avanzata generata con la chiave privata della coppia.
Uffici di Registrazione (Registration Authority – RA)	Soggetto delegato che svolge le attività necessarie al rilascio dei certificati digitali e alla consegna della CNS.
Utente - Relying Party	Soggetto che riceve un certificato digitale e che fa affidamento sul certificato medesimo o sulla firma elettronica avanzata basata su quel certificato.

4 PARTECIPANTI E RESPONSABILITÀ

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

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

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

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, le procedure da seguire in caso di smarrimento, furto o sospetta compromissione della CNS, ed è liberamente disponibile sul sito dell'Ente Emettitore.

4.1 Ente Emettitore

L'Ente Emettitore è, in generale, 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. I dati completi dell'organizzazione, che svolge la funzione di Ente Emettitore, sono i seguenti:

Campo	*Descrizione*
Denominazione Sociale	Regione Emilia-Romagna
Sede legale	Viale Aldo Moro, 52 - 40127 Bologna (BO)
Rappresentante legale	Il Presidente de Pascale Michele
Numero verde	800662200
PEC	urp@postacert.regione.emilia-romagna.it
N° Codice Fiscale	**80062590379**
N° partita IVA	02086690373
Sito web	www.regione.emilia-romagna.it
Sito web per i servizi di certificazione digitale	https://salute.regione.emilia-romagna.it/siseps/convezione-cns/
Supporto e assistenza	Lepida ScpA - smartcard@progetto-sole.it

4.2 Certification Authority – Autorità di Certificazione

La Certification Authority (CA) è il soggetto terzo e fidato che emette, pubblica nel registro e revoca i certificati.

I dati completi dell'organizzazione che svolge la funzione di CA sono i seguenti:

Campo	*Descrizione*
Denominazione Sociale	InfoCert S.p.A. Società Soggetta alla Direzione ed al coordinamento di Tinexta S.p.A.
Sede legale	Piazzale Flaminio 1/B, 00196 – Roma (RM)
Sedi operative	Via Giandomenico Romagnosi 4, 00196 – Roma (RM) Via Fernanda Wittgens 2, 20123, Milano (MI) Piazza Luigi da Porto 3, 35131, Padova (PD)
Call center	Consultare il link https://help.infocert.it/contatti/ per maggiori dettagli
Rappresentante legale	Danilo Cattaneo in qualità di Amministratore Delegato
Numero di telefono	+39 06 836691
N° Codice Fiscale	07945211006
N° partita IVA	07945211006
Sito web	https://www.firma.infocert.it - https://www.infocert.it

4.3 Ufficio di Registrazione - RA

L'Ente Emettitore si può avvalere di un'altra organizzazione per le attività necessarie al rilascio dei certificati digitali, nonché alla consegna della CNS.

L'Ente Emettitore ha delegato InfoCert che, a sua volta, si può avvalere di altri soggetti che operano sotto la sua supervisione.

Questi soggetti delegati vengono denominati "Registration Authority" (RA).

I rapporti tra InfoCert, Ente Emettitore e RA sono definiti da appositi accordi di servizio e convenzioni.

4.4 Richiedente – Subscriber

È il soggetto fisico che richiede all'Ente Emettitore il rilascio della CNS e può coincidere con il Titolare.

4.5 Titolare – Subject

Il titolare è il soggetto in favore del quale è rilasciata la CNS ed è identificato nel certificato digitale come il legittimo possessore della chiave privata, corrispondente alla chiave pubblica, contenuta nel certificato stesso.

Il titolare è tenuto a:

- garantire la correttezza, la completezza e l'attualità delle informazioni fornite all'Ente Emettitore o ai suoi delegati per la richiesta della CNS;
- proteggere e conservare le proprie chiavi private con la massima accuratezza al fine di garantirne l'integrità e la riservatezza;
- proteggere e conservare il codice di attivazione (PIN) utilizzato per l'abilitazione delle funzionalità della CNS, in un luogo sicuro e diverso da quello in cui è custodito il dispositivo stesso;
- 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;
- inoltrare all'Ente Emettitore o al Certificatore, senza ritardo, la richiesta di revoca o sospensione dei certificati al verificarsi di quanto previsto nel presente Manuale Operativo;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri.

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

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

5 OPERATIVITÀ

5.1 Identificazione

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 modalità di identificazione LiveID o *de visu* prevede un incontro di persona tra il Richiedente e uno dei soggetti abilitati a eseguire il riconoscimento, che provvede ad accertare la sua identità mediante l'esibizione in originale di uno o più documenti in corso di validità.

Il Richiedente deve essere in possesso anche del Codice Fiscale, la cui esibizione può essere richiesta dal soggetto abilitato ad eseguire il riconoscimento.

La procedura di identificazione comporta che il Richiedente sia riconosciuto personalmente, attraverso il controllo di uno dei seguenti documenti:

- Carta d'identità;
- Passaporto;
- Patente di guida.

Ove possibile potranno essere utilizzati, in conformità con quanto previsto nei Manuali Operativi di InfoCert, ulteriori strumenti di riconoscimento che non prevedano la presenza fisica del Titolare presso gli uffici di registrazione. L'Ente Emettitore ritiene idonee tutte le modalità di identificazione che sono ammissibili nell'ambito del rilascio di una Firma Elettronica Qualificata.

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

1. L'Ente Emettitore, anche tramite suoi Incaricati o Delegati;
2. il Certificatore, anche attraverso i propri Uffici di registrazione (RA).

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

- prendere visione della documentazione di cui alla sezione 2 del presente documento;
- fornire tutte le informazioni necessarie alla identificazione, corredate, ove richiesto, da idonea documentazione;
- sottoscrivere la richiesta di registrazione, con firma autografa o digitale, e prendere visione, accettandole, delle modalità di utilizzo della CNS.

Dopo il rilascio del Certificato viene inviata al Richiedente una busta virtuale cifrata contenente un codice segreto di emergenza (ERC), che consente la revoca o la sospensione del Certificato stesso.

Nella richiesta di registrazione sono contenute le informazioni che devono comparire nel certificato e quelle che consentono di gestire in maniera efficace il rapporto tra l'Ente Emettitore ed il Richiedente/Titolare.

Il modulo di richiesta deve essere sottoscritto dal Richiedente/Titolare.

Sono considerate obbligatorie le seguenti informazioni:

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

5.2 Registrazione dei dati del Titolare della CNS

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

La registrazione iniziale è effettuata presso l'Ente Emettitore o una RA.

Durante questo passaggio iniziale i dati del Titolare vengono inseriti nel sistema in uso al Certificatore.

Conclusasi la fase di registrazione iniziale, per il rilascio dei certificati digitali e la consegna della CNS verrà generata la coppia di chiavi sul dispositivo CNS e, dopo le opportune verifiche, verrà emesso il Certificato. Successivamente, il dispositivo verrà consegnato al Titolare. La CNS viene personalizzata, a cura del Certificatore, con il PIN consegnato al Richiedente attraverso la busta virtuale cifrata inviata all'indirizzo e-mail indicato al momento della registrazione.

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

5.3 Generazione delle chiavi e protezione delle chiavi private

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

Le chiavi sono generate all'interno del microprocessore e veicolate dalla smart card o dal token USB.

Le chiavi del soggetto possono essere:

- chiavi asimmetriche RSA con lunghezza non inferiore a 2048 bits;
- chiavi asimmetriche EC su una delle curve ellittiche previste dal documento ETSI TS 119 312 - Cryptographic Suites di lunghezza non inferiore a 256 bit.

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

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

5.4 Emissione del certificato

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

1) viene verificata la correttezza della richiesta del certificato, controllando che:

- il Richiedente/Titolare sia stato correttamente registrato e siano state fornite tutte le informazioni necessarie al rilascio del certificato;
- la chiave pubblica che si intende certificare sia una chiave valida e della lunghezza prevista;
- la richiesta sia autentica e il Titolare possieda la corrispondente chiave privata;

2) viene controllata la validità della firma dell'incaricato che ha convalidato la richiesta;

3) si procede alla generazione del certificato e alla sua pubblicazione nel registro dei certificati;

4) il certificato viene memorizzato all'interno della CNS come dispositivo sicuro di firma del Titolare.

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

5.5 Interdizione di una CNS

L'interdizione della CNS si attua tramite la revoca (interdizione definitiva) o la sospensione (interdizione temporanea) del relativo certificato, che ne tolgono la validità e rendono non validi gli utilizzi della corrispondente chiave privata effettuati successivamente al momento di revoca o sospensione. I certificati revocati o sospesi sono inseriti in una lista di revoca e sospensione (CRL) firmata dal Certificatore e pubblicata ogni 24 ore nel registro pubblico dei certificati. Quest'ultimo è accessibile, con protocollo "LDAP" o "HTTPS", all'indirizzo indicato all'interno del certificato stesso. Oltre alla pubblicazione della CRL nei registri pubblici, il Certificatore mette a disposizione un servizio "OCSP" per la verifica online dello stato del certificato. L'URL del servizio è indicato nel certificato. Il servizio è disponibile 24 ore al giorno, 7 giorni alla settimana.

La revoca e la sospensione di un certificato hanno efficacia dal momento di pubblicazione della lista e comportano l'invalidità dello stesso e degli utilizzi della corrispondente chiave privata, effettuati successivamente a tale momento.

La revoca o sospensione del certificato può avvenire:

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

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

L'Ente Emettitore, direttamente o tramite il Certificatore, verifica l'identità del Titolare

richiedente la revoca o sospensione e si accerta delle motivazioni della stessa.

La richiesta viene effettuata sul sito www.infocert.it, in un'apposita sezione. Il Titolare (per la sola sospensione) si autentica fornendo il codice di emergenza segreto (ERC), consegnato assieme al certificato che si intende sospendere.

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

È fatto obbligo di richiedere la revoca nel caso in cui si verifichino le seguenti condizioni:

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

5.6 Procedura per la richiesta di revoca

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

- **Revoca su iniziativa del Titolare**

L'utente Titolare richiede la revoca tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della revoca e il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la revoca al Certificatore.

Nell'impossibilità di identificare con certezza il Titolare si potrà procedere con una sospensione del Certificato, in attesa della corretta identificazione del Richiedente attraverso un form presente sul sito del Certificatore nella pagina relativa all'assistenza.

- **Revoca su iniziativa del Certificatore**

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

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

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

- **Revoca su iniziativa dell'Ente Emettitore**

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

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

5.7 Procedura per la richiesta di sospensione

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

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

Il Titolare richiede la sospensione tramite l'Ufficio presso cui è stato registrato, il quale, ottenuti i dati necessari (la motivazione della sospensione e il codice di emergenza del certificato) ed effettuate tutte le verifiche del caso, procede ad inoltrare la richiesta di sospensione al Certificatore.

Alla scadenza dei periodi indicati, se non viene riattivato, il certificato passa in stato "revocato".

5.8 Rinnovo del certificato

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

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

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

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

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

Le modalità operative per effettuare la procedura di rinnovo del certificato sono indicate dal Certificatore nel proprio sito.

Il Certificato e il dispositivo possono essere rinnovati una sola volta. Dopo il primo rinnovo, si dovrà procedere ad una nuova emissione del Certificato e del dispositivo.