



**REGIONE AUTÒNOMA DE SARDIGNA**  
**REGIONE AUTONOMA DELLA SARDEGNA**

ASSESSORADU DE SOS AFÀRIOS GENERALES, PERSONALE E REFORMA  
DE SA REGIONE  
ASSESSORATO DEGLI AFFARI GENERALI, PERSONALE  
E RIFORMA DELLA REGIONE  
*Direzione generale dell'innovazione e Sicurezza IT*

ASSESSORADU DE S'IGIENE E SANIDADE E DE S'ASSISTÈNZIA  
SOTZIALE  
ASSESSORATO DELL'IGIENE E SANITA' E DELL'ASSISTENZA SOCIALE  
*Direzione generale della sanità*

# TS-CNS

Realizzazione e diffusione della carta nazionale dei servizi con funzioni di  
tessera sanitaria

Documento:

**Manuale Operativo**

**Data:** 03 Marzo 2022  
**File:** TS-CNS-ManualeOperativo\_V01-02.doc  
**Versione:** 1.2

**Redazione:** Sardegna IT



Progetto cofinanziato dall'Unione Europea  
FESR - Fondo Europeo di Sviluppo Regionale 2014-2020



## Sommario

1.	Introduzione.....	5
1.1	STORIA DELLE VERSIONI E DELLE MODIFICHE .....	5
1.2	SCOPO E CAMPO DI APPLICAZIONE DEL DOCUMENTO .....	5
1.3	GLOSSARIO .....	5
1.3.1	Identificazione informatica .....	6
1.3.2	Carta Nazionale dei Servizi .....	6
1.3.3	Certificato Digitale .....	6
1.3.4	Certificatore .....	6
1.3.5	CRL .....	6
1.3.6	Ente Emittitore .....	6
1.3.7	Firma elettronica avanzata .....	7
1.3.8	Firma digitale .....	7
1.3.9	Manuale Operativo .....	7
1.3.10	PIN .....	7
1.3.11	PUK .....	8
1.3.12	Revoca di un Certificato .....	8
1.3.13	Sospensione di un Certificato .....	8
1.3.14	Titolare .....	8
1.3.15	TS-CNS .....	8
1.4	ACRONIMI .....	8
2.	Generalità.....	10
2.1	IDENTIFICAZIONE DEL DOCUMENTO .....	10
2.2	ENTE EMETTITORE .....	10
2.3	SPORTELLI DI ATTIVAZIONE .....	10
2.4	CONTATTI .....	10
2.5	TUTELA DEI DATI PERSONALI .....	11
3.	Ruoli previsti .....	12
3.1	ENTE EMETTITORE .....	12
3.2	PRODUTTORE .....	12
3.3	CERTIFICATORE .....	12
3.4	SPORTELLO DI ATTIVAZIONE .....	12
3.5	TITOLARE.....	13
4.	Obblighi e responsabilità .....	14
4.1	OBBLIGHI DEL TITOLARE.....	14



4.2	RESPONSABILITÀ .....	14
4.2.1	Responsabilità dell'Ente emettitore.....	14
4.2.2	Responsabilità del produttore.....	15
4.2.3	Responsabilità del certificatore .....	15
5.	Amministrazione del manuale operativo .....	16
5.1	PROCEDURE PER L'AGGIORNAMENTO .....	16
6.	Identificazione del titolare .....	17
6.1	IDENTIFICAZIONE DE VISU DEL TITOLARE .....	17
6.1.1	Soggetti abilitati ad effettuare l'identificazione .....	17
6.1.2	Procedure per l'identificazione.....	17
6.2	IDENTIFICAZIONE DEL TITOLARE TRAMITE CALL CENTER.....	18
6.3	IDENTIFICAZIONE INFORMATICA DEL TITOLARE.....	18
6.4	CASI PARTICOLARI .....	19
6.4.1	Minore.....	19
6.4.2	Minore emancipato.....	19
6.4.3	Tutelato .....	19
6.4.4	Identificazione in caso di delega.....	19
7.	Procedura per il rilascio del certificato di firma digitale .....	21
7.1	IDENTIFICAZIONE DEL RICHIEDENTE .....	21
7.2	RILASCIO DEL CERTIFICATO DI FIRMA DIGITALE .....	21
8.	Procedura per l'attivazione della TS-CNS in interoperabilità.....	22
8.1	IDENTIFICAZIONE DEL RICHIEDENTE .....	22
8.2	RILASCIO DELLE CREDENZIALI DI ATTIVAZIONE.....	22
9.	Operatività .....	23
9.1	EMISSIONE E SPEDIZIONE DELLE TS-CNS AI TITOLARI .....	23
9.1.1	Registrazione dei dati dei titolari.....	23
9.1.2	Generazione del certificato di autenticazione.....	23
9.1.3	Generazione del certificato di firma digitale .....	23
9.2	VALIDITÀ DEI CERTIFICATI.....	23
9.3	RICHIESTA CODICI SEGRETI.....	24
9.3.1	Documentazione necessaria.....	24
9.3.2	Procedura standard .....	24
9.3.3	Procedura in caso di interoperabilità.....	25
9.3.4	Procedura in caso di minore.....	26
9.3.5	Procedura in caso di tutelato.....	26



9.3.6	<i>Procedura in caso di delega</i> .....	26
9.4	RILASCIO NUOVI CODICI SEGRETI .....	26
9.5	SOSPENSIONE DI UN CERTIFICATO .....	26
9.5.1	<i>Sospensione di un certificato tramite sito web</i> .....	27
9.5.2	<i>Sospensione di un certificato tramite Call center</i> .....	27
9.5.3	<i>Sospensione di un certificato tramite Sportello di attivazione</i> .....	27
9.6	RIATTIVAZIONE DI UN CERTIFICATO .....	27
9.6.1	<i>Riattivazione di un certificato tramite sito web</i> .....	27
9.6.2	<i>Riattivazione di un certificato tramite Sportello di attivazione</i> .....	28
9.7	REVOCA DI UN CERTIFICATO .....	28
9.7.1	<i>Revoca su iniziativa del titolare</i> .....	28
9.7.2	<i>Revoca su iniziativa dell'Ente Emittitore</i> .....	28
10.	Riferimenti normativi e tecnici .....	29
10.1.1	<i>Riferimenti normativi</i> .....	29
10.1.2	<i>Riferimenti tecnici</i> .....	29



## 1. Introduzione

### 1.1 Storia delle versioni e delle modifiche

Versione e data	1.2 del 03 marzo 2022
Descrizione modifiche	Adeguamento normativo, GDPR <ul style="list-style-type: none"> <li>• Eliminazione Paragrafo 5.2</li> </ul> Inserimento capitolo “8. Procedura per l'attivazione della TS-CNS in interoperabilità” Inserimento paragrafo “9.3.3 Procedura in caso di interoperabilità” <ul style="list-style-type: none"> <li>• Eliminazione servizio di “Riattivazione di un certificato tramite Call center” (ex paragrafo 8.6.2)</li> </ul> Aggiornamento paragrafi 9.5.1 “Sospensione di un certificato tramite sito web” e 9.6.1 “Riattivazione di un certificato tramite sito web”
Versione e data	1.1 dell'8 marzo 2012
Descrizione modifiche	§8.7.2 - Aggiunta di ulteriori motivi di revoca da parte dell'Ente emittitore
Versione e data	1.0 del 13 febbraio 2012
Descrizione modifiche	Primo rilascio

### 1.2 Scopo e campo di applicazione del documento

Il presente documento contiene le regole e le procedure operative che governano l'emissione della TS-CNS della Regione Autonoma della Sardegna e le procedure che il cittadino deve seguire in caso di malfunzionamento, smarrimento, furto o compromissione della sicurezza della TS-CNS.

Il presente documento ha valore per l'Ente emittitore, per il certificatore, per gli sportelli di attivazione e per i titolari.

Autore di questo documento è la Regione Autonoma della Sardegna, a cui spettano tutti i diritti previsti dalla legge. E' vietata la riproduzione anche parziale.

### 1.3 Glossario



### **1.3.1 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.

### **1.3.2 Carta Nazionale dei Servizi**

Il documento rilasciato su supporto informatico per consentire l'accesso per via telematica ai servizi erogati dalle pubbliche amministrazioni.

### **1.3.3 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.

### **1.3.4 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..

### **1.3.5 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.

### **1.3.6 Ente Emittitore**

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 Emittitore è svolto dalla Regione Autonoma della Sardegna.



### **1.3.7 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.

La firma elettronica avanzata soddisfa i seguenti requisiti:

- a) è connessa unicamente al firmatario;
- b) è idonea a identificare il firmatario;
- c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e
- d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

### **1.3.8 Firma digitale**

Un particolare tipo di firma qualificata basata su un sistema di chiavi crittografiche, una pubblica e una privata, correlate tra loro, che consente al titolare di firma elettronica tramite la chiave privata e a un soggetto terzo 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.

### **1.3.9 Manuale Operativo**

Il Manuale Operativo definisce le procedure che il Certificatore e l'Ente Emittitore applicano nello svolgimento del servizio di rilascio e gestione della TS-CNS e dei relativi Certificati.

### **1.3.10 PIN**

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



### **1.3.11 PUK**

Personal Unlocking Key - codice associato alla TS-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.

### **1.3.12 Revoca di un Certificato**

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

### **1.3.13 Sospensione di un Certificato**

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

### **1.3.14 Titolare**

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

### **1.3.15 TS-CNS**

E' la Carta nazionale dei servizi con funzionalità di Tessera sanitaria.

## **1.4 Acronimi**

AGID – Agenzia per l'Italia Digitale

CA – Certification Authority

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

MEF – Ministero Economia e Finanze

PIN – Personal Identification Number



## TS-CNS

*Realizzazione e diffusione della carta nazionale dei servizi  
con funzioni di tessera sanitaria*



Progetto cofinanziato dall'Unione Europea  
FESR - Fondo Europeo di Sviluppo Regionale 2014-2020

---

PUK – Personal Unblocking Key

TEAM - Tessera europea di assicurazione malattia

TS-CNS - Tessera sanitaria - Carta nazionale dei servizi



## 2. Generalità

### 2.1 Identificazione del documento

Questo documento è denominato “Tessera Sanitaria - Carta Nazionale dei Servizi - Manuale Operativo”.

La versione e la data di emissione sono riportate in calce ad ogni pagina.

Questo documento è distribuito in formato elettronico presso il sito web dell'Ente emittitore all'indirizzo <https://tscns.regione.sardegna.it/>

### 2.2 Ente emittitore

L'Ente emittitore è la Regione Autonoma della Sardegna, che è responsabile della sicurezza del circuito di emissione e rilascio della carta e della corretta gestione del ciclo di vita della carta stessa. La responsabilità di alcune delle attività può essere delegata dall'Ente emittitore a terzi, ma l'Ente emittitore rimane comunque responsabile del ciclo di vita della carta nel suo complesso.

### 2.3 Sportelli di attivazione

L'elenco degli sportelli di attivazione è pubblicato all'indirizzo <https://tscns.regione.sardegna.it/it/sportelli-di-attivazione> ed è mantenuto costantemente aggiornato dalla Regione Autonoma della Sardegna.

### 2.4 Contatti

Domande, osservazioni e richieste di chiarimento in ordine al presente Manuale Operativo dovranno essere rivolte ai seguenti riferimenti:

Telefono: **800336611**

Indirizzo e-mail: ***tesseractivizisardegna@regione.sardegna.it***

Indirizzo web: <https://tscns.regione.sardegna.it>



## 2.5 Tutela dei dati personali

I dati personali che entrano nella disponibilità dell'Ente emittitore e in conseguenza delle attività istituzionali connesse alla TS-CNS sono trattati in conformità al Regolamento europeo sulla protezione dei dati personali n. 2016/679 e del D.Lgs. 196/03 e ss.mm.

Si veda, al riguardo, l'Informativa Privacy relativa alla TS-CNS [13].



### **3. Ruoli previsti**

#### **3.1 Ente emittitore**

L'Ente emittitore è la Regione Autonoma della Sardegna, che è responsabile della sicurezza del circuito di emissione e rilascio della carta e della corretta gestione del ciclo di vita della carta stessa. La responsabilità di alcune delle attività può essere delegata dall'Ente emittitore a terzi, ma l'Ente emittitore rimane comunque responsabile del ciclo di vita della carta nel suo complesso.

#### **3.2 Produttore**

Il produttore, aggiudicatario di apposite gare ministeriali ad evidenza pubblica, provvede alla fornitura delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, predispone opportunamente gli spazi dedicati alla firma digitale, applica al supporto fisico l'artwork e gli elementi costanti.

#### **3.3 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.

#### **3.4 Sportello di attivazione**

Per la gestione del ciclo di vita delle TS-CNS l'Ente emittitore si avvale di Enti che gestiscono gli sportelli fisici di attivazione:

- Aziende sanitarie della Regione Sardegna
- Farmacie aderenti
- Uffici regionali abilitati

Eventuali nuovi Enti verranno inseriti nelle versioni successive del Manuale operativo.



---

L'elenco degli sportelli di attivazione è pubblicato all'indirizzo <https://tscns.regione.sardegna.it/it/sportelli-di-attivazione> ed è mantenuto costantemente aggiornato dalla Regione Autonoma della Sardegna.

### **3.5 Titolare**

Il titolare della carta è l'utente utilizzatore della stessa come strumento di identificazione in rete e di sottoscrizione dei documenti informatici.



## **4. Obblighi e responsabilità**

### **4.1 Obblighi del titolare**

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

- fornire all'Ente emittitore o struttura delegata informazioni esatte e veritiere in fase di rilascio dei codici PIN e PUK;
- controllare la correttezza dei dati riportati sulla TS-CNS;
- custodire con la massima diligenza i codici riservati ricevuti al fine di preservarne la riservatezza;
- conservare con la massima diligenza la TS-CNS contenente le proprie chiavi private;
- conservare le informazioni di abilitazione all'uso delle chiavi private in luogo diverso da quello in cui è conservata la TS-CNS;
- richiedere il codice di sblocco (PUK) nell'apposita sezione del sito <https://tscns.regione.sardegna.it/articoli/recupero-puk>;
- conservare il codice di sblocco (PUK) con la massima diligenza in luogo sicuro e diverso da quello in cui è conservata la TS-CNS;
- adottare ogni altra misura atta ad impedire la perdita, la compromissione o l'utilizzo improprio della TS-CNS;
- adottare tutte le misure organizzative e tecniche idonee ad evitare danno ad altri;
- richiedere senza ritardi la sospensione e la revoca dei certificati nei casi previsti al § 8.5 e § 8.7.1.

### **4.2 Responsabilità**

#### **4.2.1 Responsabilità dell'Ente emittitore**

L'Ente emittitore è responsabile

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione (responsabilità delegata all'Agenzia delle Entrate);



- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione (responsabilità delegata all'Agenzia delle Entrate);
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione (responsabilità delegate all'Agenzia delle Entrate), attivazione e eventuale ritiro della carta (responsabilità delegate agli Sportelli di attivazione).

#### **4.2.2 Responsabilità del produttore**

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

#### **4.2.3 Responsabilità del certificatore**

Il certificatore è responsabile della generazione del certificato di autenticazione e di firma. Le informazioni anagrafiche trasmesse al certificatore dall'Agenzia delle Entrate, congiuntamente con le chiavi pubbliche generate in fase di personalizzazione, sono utilizzate dal certificatore per generare i certificati secondo le specifiche disponibili presso il sito di AgID.



## **5. Amministrazione del manuale operativo**

### **5.1 Procedure per l'aggiornamento**

Questo documento potrà essere variato per esigenze tecniche o per modifiche alle procedure descritte.

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

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 § 2.1 in formato elettronico.





## **6. Identificazione del titolare**

Questo capitolo descrive le procedure usate per:

- l'identificazione de visu del titolare al momento della richiesta di rilascio dei codici segreti della TS-CNS, dell'eventuale certificato di firma digitale e di rinnovo, sospensione e riattivazione di certificati;
- l'identificazione del titolare, nel caso di sospensione e riattivazione dei certificati tramite il Call center;
- l'identificazione informatica del Titolare, nel caso di richiesta del codice di sblocco (PUK), di rinnovo, sospensione e riattivazione dei certificati tramite il canale Internet.

### **6.1 Identificazione de visu del titolare**

L'Ente emittitore, direttamente o tramite un soggetto delegato, verifica con certezza l'identità del Richiedente prima di procedere al rilascio dei codici segreti della TS-CNS e del certificato di firma digitale, eventualmente richiesto.

#### **6.1.1 Soggetti abilitati ad effettuare l'identificazione**

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

- l'Ente emittitore, anche tramite suoi incaricati;
- l'Ente gestore degli sportelli di attivazione, anche tramite suoi incaricati.

#### **6.1.2 Procedure per l'identificazione**

L'identificazione è effettuata da uno dei soggetti indicati al § 3.4 ed è richiesta la presenza fisica del titolare.

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.

L'operatore di sportello inserisce sul CMS i dati necessari:

- numero del documento;
- tipo del documento;
- Ente emittente del documento;
- data di scadenza del documento.

Al momento dell'identificazione viene fornito al Richiedente un codice utente, che costituisce lo strumento di identificazione nel sistema di comunicazione sicuro tra Titolare e Certificatore, anche per il tramite delle strutture appositamente predisposte dall'Ente emittitore.

## **6.2 Identificazione del titolare tramite call center**

L'identificazione del titolare tramite call center avviene mediante codice fiscale e codice utente consegnato al titolare stesso in busta chiusa in occasione della prima identificazione de visu.

## **6.3 Identificazione informatica del titolare**

L'identificazione informatica del titolare per l'accesso alla procedura web per la richiesta del codice PUK avviene tramite la TS-CNS.



L'identificazione informatica del titolare per l'accesso alla procedura web di sospensione e riattivazione della TS-CNS avviene mediante codice fiscale e codice utente consegnato al titolare stesso in busta chiusa in occasione della prima identificazione de visu.

## **6.4 Casi particolari**

### **6.4.1 Minore**

In caso di TS-CNS intestata ad un minore l'identificazione verrà effettuata nei confronti del genitore, che dovrà presentarsi allo sportello con un proprio documento di identità valido. La presenza allo sportello del minore non è necessaria. Al genitore verrà richiesto di firmare una dichiarazione di autocertificazione della potestà genitoriale.

Sulle TS-CNS intestate a minori non è consentita l'attivazione della firma digitale.

### **6.4.2 Minore emancipato**

In caso di TS-CNS intestata ad un minore emancipato l'identificazione avverrà secondo la procedura standard descritta al § 6.1.2. Inoltre il titolare dovrà dare evidenza all'operatore del suo stato (esibizione di un documento di identità da cui risulti il matrimonio, copia dell'atto giuridico comprovante lo status di minore emancipato o apposita autocertificazione).

Sulle TS-CNS intestate a minori emancipati non è consentita l'attivazione della firma digitale.

### **6.4.3 Tutelato**

In caso di TS-CNS intestata ad una persona sottoposta a tutela l'identificazione verrà effettuata nei confronti del rappresentante legale, che dovrà presentarsi allo sportello con un proprio documento di identità valido. La presenza allo sportello della persona sottoposta a tutela non è necessaria. Al rappresentante legale verrà richiesto di firmare una dichiarazione di autocertificazione del suo status.

Sulle TS-CNS intestate a persone sottoposte a tutela non è consentita l'attivazione della firma digitale.

### **6.4.4 Identificazione in caso di delega**

Esclusivamente nel caso in cui, per motivi di salute, il titolare non possa recarsi agli sportelli di attivazione per l'identificazione per un periodo superiore ai tre mesi, è possibile procedere alla



---

richiesta dei codici segreti per delega. Il delegato dovrà essere identificato secondo la procedura standard descritta al § 6.1.2 e dovrà inoltre portare con sé:

- una fotocopia di un documento di identità valido del delegante;
- una delega sottoscritta dal delegante;
- il certificato medico o analoga documentazione clinica idonea (il certificato medico deve essere generico e non deve indicare riferimenti inerenti alla patologia del titolare della TS-CNS).



## 7. Procedura per il rilascio del certificato di firma digitale

La TS-CNS viene fornita con installato il solo certificato di autenticazione; il titolare della TS-CNS, se maggiorenne, potrà richiedere senza oneri allo Sportello di attivazione, contestualmente alla richiesta dei codici segreti o successivamente, il rilascio anche di uno specifico certificato di firma digitale, da installare a bordo della TS-CNS.

Il certificato di autenticazione permette, ove previsto, l'accesso ai servizi presenti nei vari siti web; il certificato di firma digitale è utile per firmare digitalmente i file; la firma digitale ha infatti il valore legale di una firma autografa.

Il certificato di firma digitale verrà rilasciato dal certificatore Aruba PEC S.p.A. all'interno dell'appalto *Procedura aperta per la fornitura di software tipo Card Management System, servizi di manutenzione e servizi accessori, per la gestione della Tessera Sanitaria-Carta Nazionale dei Servizi*.

In ogni caso il richiedente dovrà essere identificato personalmente e dovrà inoltre firmare un modulo di richiesta del servizio al certificatore Aruba PEC.

L'operatore di sportello agirà in qualità di Operatore di registrazione del certificatore Aruba PEC.

Il certificato di firma digitale non potrà essere rilasciato a minori o tutelati.

### 7.1 Identificazione del richiedente

Si fa integrale riferimento a quanto riportato al § 6.1.

### 7.2 Rilascio del certificato di firma digitale

Il certificato di firma digitale viene rilasciato su richiesta del titolare della TS-CNS al momento del rilascio dei codici segreti o successivamente.



## **8. Procedura per l'attivazione della TS-CNS in interoperabilità**

Tramite l'interoperabilità applicativa con il sistema TS nazionale, gestito dal MEF, è possibile attivare una TS-CNS emessa da un'altra regione, differente dalla Regione Sardegna.

Il servizio può essere richiesto dai cittadini, esclusivamente presso gli sportelli di attivazione situati nelle Aziende Sanitarie e negli URP regionali. Non è possibile usufruire di tale servizio presso gli sportelli di attivazione delle Farmacie.

Sono possibili le seguenti operazioni:

- Attivazione TS-CNS di altra regione, anche per delega
- Richiesta duplicati PIN e PUK di TS-CNS di altra regione, già attivata
- Revoca della TS-CNS di altra regione per i motivi previsti

Il sistema CMS regionale dispone inoltre di alcuni servizi di interoperabilità, per cui è possibile ricevere richieste dal sistema TS nazionale presso sportelli di attivazione dislocati in altre regioni italiane, al fine di:

- recuperare credenziali PIN e PUK per l'attivazione o la richiesta di duplicati per TS-CNS di cittadini sardi,
- revocare il certificato della TS-CNS per i motivi previsti

E' consentita la richiesta per delega, secondo i casi descritti nel paragrafo § 9.7

### **8.1 Identificazione del richiedente**

Si fa integrale riferimento a quanto riportato al § 6.1.

### **8.2 Rilascio delle credenziali di attivazione**

Le credenziali di attivazione verranno rilasciate in due parti:

- la prima parte dei codici PIN, PUK del titolare della TS-CNS al momento dell'attivazione su supporto cartaceo e la seconda parte via email, comunicata in fase di attivazione.



## 9. Operatività

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

### 9.1 Emissione e spedizione delle TS-CNS ai titolari

Tutte le attività del processo di emissione delle TS-CNS sono sotto la responsabilità dell'Agenzia delle Entrate, che ha appaltato tali attività tramite SOGEI.

#### 9.1.1 Registrazione dei dati dei titolari

Ai fini dell'emissione del certificato CNS i dati dei titolari vengono trasmessi da SOGEI al Certificatore col formato descritto nel documento *Formati di interscambio dei flussi informativi con i Card Management System delle Regioni/Province Autonome* consultabile all'indirizzo <http://www.sistemats.it>.

#### 9.1.2 Generazione del certificato di autenticazione

L'attività di generazione del certificato di autenticazione standard CNS viene svolta dal certificatore secondo quanto previsto nel proprio documento *Manuale Operativo - Servizio di Certificazione Digitale - Revisione 2.5* [11].

#### 9.1.3 Generazione del certificato di firma digitale

Un'apposita funzionalità del Card Management System, che crea l'area di firma nella TS-CNS, richiede alla CA l'emissione del certificato e lo carica nella stessa area di firma.

Relativamente al certificato di firma digitale si rimanda al *Manuale Operativo - Servizio di Certificazione Digitale - Revisione 2.5* [11].

### 9.2 Validità dei certificati

Il certificato di autenticazione contenuto nella TS-CNS ha una validità pari alla validità della TS-CNS, cioè di sei anni ad esclusione del caso in cui la tessera sanitaria ha una validità inferiore.



### **9.3 Richiesta codici segreti**

All'atto della spedizione al titolare la TS-CNS è immediatamente utilizzabile come tessera sanitaria, TEAM e tesserino di codice fiscale. Il certificato di autenticazione a bordo della TS-CNS è rilasciato in stato attivo. La funzionalità CNS della TS-CNS può essere utilizzata solo richiedendo i codici segreti presso gli sportelli di attivazione.

Allo sportello verrà consegnata al titolare una busta oscurata pre-stampata contenente all'interno il codice PIN e il codice utente che verranno associati alla TS-CNS durante l'operazione di consegna.

#### **9.3.1 Documentazione necessaria**

L'identificazione verrà effettuata presso gli sportelli di attivazione come descritto al § 6.1, che riporta anche la documentazione necessaria nel caso standard e nei casi particolari. In ogni caso dovrà essere esibita allo sportello di attivazione la TS-CNS per cui vengono richiesti i codici segreti.

#### **9.3.2 Procedura standard**

L'operatore di sportello, dopo aver proceduto all'identificazione del richiedente nelle modalità previste al § 6.1, compie le seguenti operazioni:

1. invita il cittadino a leggere l'informativa per la tutela dei dati personali affissa presso lo sportello;
2. accede al CMS identificandosi mediante la propria smart card, se non ancora operativo sul sistema;
3. richiede al cittadino di esprimere verbalmente la volontà di procedere con l'attivazione della carta;
4. richiede al cittadino la TS-CNS e la inserisce nel lettore di smart card collegato al computer;
5. esegue una verifica dell'identità del cittadino confrontando i dati del documento di identità con i dati riportati sul certificato pubblico contenuto nella TS-CNS: nel caso i dati non coincidano interrompe l'operazione e invita il cittadino a recarsi presso lo sportello competente dell'Agenzia delle Entrate;
6. prende una busta PIN pre-stampata a caso tra quelle assegnategli e inserisce sul CMS il codice della busta riportato esternamente leggendolo mediante il lettore di codice a barre o inserendo manualmente il numero corrispondente;





7. utilizza la specifica funzionalità del CMS, che accede al PUK della carta senza visualizzarlo e modifica il codice PIN della TS-CNS assegnandogli il valore contenuto nella busta;
8. richiede al cittadino se è interessato ad attivare, gratuitamente, il certificato di firma digitale; in caso affermativo stampa il relativo modulo di richiesta, lo fa firmare dal cittadino e genera il certificato di firma digitale mediante l'opportuna funzionalità del CMS;
9. consegna al cittadino la busta cieca contenente il codice PIN e il codice utente;
10. riceve l'eventuale modulo di richiesta del lettore di TS-CNS, che viene fornito gratuitamente dalla Regione Sardegna ad ogni nucleo familiare, consegna il lettore al cittadino e registra l'operazione sul CMS;
11. consegna al cittadino l'informativa relativa alle operazioni svolte.

Le modalità operative utilizzate assicurano che nessuno, nemmeno l'operatore di sportello, possa conoscere il codice PIN se non aprendo la busta cieca.

### **9.3.3 Procedura in caso di interoperabilità**

L'operatore di sportello, dopo aver proceduto all'identificazione del richiedente nelle modalità previste al § 6.1, compie le operazioni di cui al § 9.3.2, fino al punto 3, poi prosegue come di seguito:

4. esegue una verifica dell'identità del cittadino confrontando i dati del documento di identità con i dati riportati sulla TS-CNS: nel caso i dati non coincidano interrompe l'operazione e invita il cittadino a recarsi presso lo sportello competente dell'Agenzia delle Entrate;
5. utilizza la specifica funzionalità del CMS, che permette di inserire i dati del cittadino e della TS-CNS e di fare la richiesta in interoperabilità al sistema TS nazionale dei codici di attivazione PIN e PUK della TS-CNS del cittadino, sia nel caso di attivazione che di richiesta duplicati PIN e PUK;
6. Stampa il relativo modulo con la prima parte dei codici PIN e PUK richiesti e lo consegna al cittadino, mentre il CMS invierà all'email richiesta la seconda parte dei codici PIN e PUK;
  - a. Nel caso di delega, il delegato dovrà anche firmare il modulo rilasciato.

Le modalità operative utilizzate assicurano che nessuno, nemmeno l'operatore di sportello, possa conoscere i codici PIN e PUK completi.



### **9.3.4 Procedura in caso di minore**

L'operatore di sportello compie le operazioni di cui al § 9.3.2 saltando le operazioni previste ai punti 5 e 8.

### **9.3.5 Procedura in caso di tutelato**

L'operatore di sportello compie le operazioni di cui al § 9.3.2 saltando le operazioni previste ai punti 5 e 8.

### **9.3.6 Procedura in caso di delega**

L'operatore di sportello compie le operazioni di cui al § 9.3.2 saltando le operazioni previste ai punti 5 e 8.

## **9.4 Rilascio nuovi codici segreti**

Qualora il cittadino smarrisca la busta PIN, ne dimentichi il contenuto e non abbia richiesto o non ricordi il codice di sblocco (PUK) non potrà utilizzare la funzionalità CNS della TS-CNS.

Il cittadino potrà recarsi presso uno sportello di attivazione e richiedere il rilascio di una nuova busta PIN. L'operazione è del tutto analoga a quella prevista al § 9.3 nel caso di prima richiesta codici segreti.

## **9.5 Sospensione di un certificato**

La sospensione consiste nel blocco temporaneo della carta, che può essere riattivata successivamente oppure definitivamente revocata. La sospensione viene richiesta in caso di sospetto furto, smarrimento o compromissione della segretezza dei codici riservati.

Il Titolare può richiedere la sospensione della TS-CNS tramite sito web, chiamando il Call center o recandosi presso uno sportello di attivazione.



### **9.5.1 Sospensione di un certificato tramite sito web**

Il Titolare può richiedere la sospensione tramite una pagina apposita del sito web del progetto, previa autenticazione nell'area riservata, inserendo il codice fiscale e il codice utente (contenuto nella busta consegnatagli all'attivazione della carta).

### **9.5.2 Sospensione di un certificato tramite Call center**

Il Titolare può richiedere la sospensione chiamando il numero verde dedicato 800336611, spiegando il motivo della richiesta. Al Titolare verranno richiesti i dati anagrafici (nome, cognome, codice fiscale) e il codice utente (contenuto nella busta consegnatagli all'attivazione della carta).

### **9.5.3 Sospensione di un certificato tramite Sportello di attivazione**

Il Titolare può richiedere la sospensione presso uno sportello di attivazione, spiegando il motivo della richiesta.

L'operatore, dopo aver proceduto all'identificazione del richiedente nelle modalità previste al § 6.1, provvede a sospendere la validità dei certificati a bordo della carta.

## **9.6 Riattivazione di un certificato**

La riattivazione consiste nel ripristino delle funzionalità della TS-CNS, temporaneamente disabilitate in seguito alla sua sospensione.

Il Titolare può richiedere la riattivazione della TS-CNS tramite sito web o recandosi presso uno sportello di attivazione.

La riattivazione di una carta viene richiesta dal Titolare in seguito al venir meno delle ragioni che avevano portato alla sua sospensione.

### **9.6.1 Riattivazione di un certificato tramite sito web**

Il Titolare potrà richiedere la riattivazione tramite pagina apposita del sito web del progetto, previa autenticazione nell'area riservata, inserendo il codice fiscale e il codice utente (contenuto nella busta consegnatagli all'attivazione della carta).



## **9.6.2 Riattivazione di un certificato tramite Sportello di attivazione**

Il Titolare può richiedere la riattivazione presso uno sportello di attivazione.

L'operatore, dopo aver proceduto all'identificazione del richiedente nelle modalità previste al § 6.1, provvede a riattivare i certificati a bordo della carta.

## **9.7 Revoca di un certificato**

La revoca consiste nel blocco definitivo della carta, che rende inutilizzabili i certificati presenti sulla carta e la funzionalità CNS della tessera sanitaria, che conserva solamente le sue funzionalità "a vista".

### **9.7.1 Revoca su iniziativa del titolare**

Il titolare deve richiedere la revoca in caso di:

- compromissione della segretezza dei codici riservati;
- smarrimento o furto del dispositivo di firma;
- errore o variazione dei dati del titolare presenti nel certificato (nome, cognome, codice fiscale).

Dopo la revoca il titolare può richiedere la riemissione della TS-CNS.

Il Titolare può richiedere la revoca solo presso uno sportello di attivazione, spiegando il motivo della richiesta (malfunzionamento, furto, smarrimento...). In caso di furto o smarrimento deve presentare all'operatore copia della relativa denuncia o una autocertificazione.

L'operatore, dopo aver proceduto all'identificazione del richiedente nelle modalità previste al § 6.1 e aver riscontrato il problema segnalato, procede alla revoca della TS-CNS.

### **9.7.2 Revoca su iniziativa dell'Ente Emittitore**

L'Ente emittitore richiede la revoca in caso di errori nei dati anagrafici riportati sulla TS-CNS, mancato recapito della TS-CNS, decesso del titolare o cessato diritto all'assistenza sanitaria.



## 10. Riferimenti normativi e tecnici

### 10.1.1 Riferimenti normativi

1. D.Lgs. 7 marzo 2005, n.82 – Codice dell'amministrazione digitale
2. Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno.
3. DPR 28 Dicembre 2000, n. 445 - Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa
4. DPCM 30 marzo 2009 - Regole tecniche in materia di generazione, apposizione e verifica delle firme digitali e validazione temporale dei documenti informatici.
5. Regolamento europeo n. 2016/679 sulla protezione dei dati personali e D.Lgs. 196/03 e ss.mm.
6. DPR 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. DM 20 giugno 2011 - Modalità di assorbimento della Tessera Sanitaria nella Carta nazionale dei servizi
9. “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

### 10.1.2 Riferimenti tecnici

10. Aruba PEC - Certification Practice Statement ([https://www.pec.it/documents/tc-files/en/02\\_QualifiedCertificatesOperatingManual.pdf](https://www.pec.it/documents/tc-files/en/02_QualifiedCertificatesOperatingManual.pdf))
11. Aruba PEC - Manuale Operativo - Servizio di Certificazione Digitale - (<https://ca.arubapec.it> nella sezione dedicata al “[Manuale Operativo del Servizio di Certificazione per Firma Digitale](#)”)



12. Aruba PEC - Piano per la Sicurezza del Servizio di Certificazione Digitale – revisione 1.1 – Documento Interno
13. Regione Autonoma della Sardegna - TS-CNS Informativa Privacy