

**Caratteristiche fisiche e modalità
di gestione delle Tessere Sanitarie Carta
nazionale dei servizi (TS-CNS)**

-documento tecnico-

CARATTERISTICHE TECNICHE E MODALITÀ DI GESTIONE DELLA TESSERA SANITARIA TS-CNS.3

1.	CARATTERISTICHE FISICHE DELLE TS-CNS	3
2.	FRONTE TS-CNS STANDARD.....	3
3.	FRONTE TS-CNS CON CARATTERI DIACRITICI	4
4.	RETRO TS-CNS STANDARD.....	5
4.1.	<i>Bar Code</i>	5
4.2.	<i>Dati TEAM</i>	5
4.3.	<i>Dati TEAM con asterischi</i>	6
4.4.	<i>Banda magnetica presente sul retro delle TS-CNS</i>	7
5.	REGOLE DI GESTIONE DELLE TS-CNS	8
5.1.	<i>Produzione e distribuzione delle TS-CNS</i>	8
5.2.	<i>Ritiro e disattivazione delle TS-CNS</i>	9
6.	SERVIZI AUSILIARI	9

SPECIFICHE TECNICHE E DI GESTIONE DELLA COMPONENTE CNS DELLE TS-CNS..... 10

1.	CARATTERISTICHE TECNICHE DELLA COMPONENTE CNS	10
1.1.	<i>Caratteristiche del microprocessore della TS-CNS</i>	10
1.2.	<i>Personalizzazione File System della TS-CNS</i>	10
1.3.	<i>Answer to reset delle TS-CNS</i>	11
1.4.	<i>Certificato di autenticazione delle TS-CNS</i>	11
1.5.	<i>Software del microchip delle TS-CNS</i>	11
2.	I SERVIZI DI GESTIONE DEI CERTIFICATI DELLE TS-CNS (CERTIFICATION AUTHORITY).....	12
3.	SERVIZI OPERATIVI DI GESTIONE DELLE CNS	13

Caratteristiche tecniche e modalità di gestione della Tessera Sanitaria TS-CNS

Si riportano di seguito le caratteristiche tecniche e le regole di gestione della Tessera Sanitaria - Carta nazionale dei servizi (TS-CNS) di cui all'articolo 11, comma 15 del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122, in conformità con quanto previsto dall'Allegato B del decreto 11 marzo 2004 e successive modificazioni, e nelle more dell'emanazione dei decreti attuativi del comma 13 dell'articolo 50 del decreto legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e successive modificazioni.

Tali specifiche, stabilite di concerto fra il Ministero dell'economia e finanze, il Ministero della salute e la Presidenza del consiglio dei ministri Dipartimento per la digitalizzazione della pubblica amministrazione e l'innovazione tecnologica, sono in ogni caso riportate nel **capitolo II** "*Specifiche Tecniche e di gestione della componente CNS delle TS-CNS*" del presente documento.

1. Caratteristiche Fisiche delle TS-CNS

La TS-CNS ha le seguenti caratteristiche fisiche:

- formato Standard ISO 7810: 1995 e per i metodi di test ISO/IEC 10373: 1993;
- altezza: mm 53,98;
- larghezza: mm 85,60;
- spessore: mm 0,76;

Gli angoli sono arrotondati con un raggio di 3.18 mm con tolleranza di +/- 0.08 mm.

2. Fronte TS-CNS standard

Il fronte della TS-CNS riporta le informazioni anagrafiche nel loro formato originale, così come presenti negli archivi del Ministero dell'economia e finanze, nonché la replica della data di scadenza della TEAM, presente sul retro della Tessera Sanitaria, comunicata dalle ASL.

I dati riportati sul fronte delle Tessere Sanitarie hanno un formato Font «Verdana Bold True Type», stile normale, colore nero. La risoluzione di stampa è di massimo 300 dpi.

In particolare sul fronte sono riportati su 6 righe i seguenti dati:

- **Codice Fiscale:** il campo ha una lunghezza di 16 caratteri alfanumerico (dim. carattere 8 punti);
- **Data di Scadenza:** il campo nel formato GG/MM/AAAA ha una lunghezza 10 caratteri, compresa una barra obliqua tra ciascun gruppo (dim carattere 7);
- **Cognome:** il campo ha una lunghezza massima di 40 caratteri gruppo (dim carattere 7 punti);
- **Nome:** il campo ha una lunghezza massima di 35 caratteri gruppo (dim carattere 7 punti);
- **Sesso:** il campo ha una lunghezza di 1 carattere (dim. carattere 8 punti);
- **Comune di nascita:** il campo ha una lunghezza massima di 35 caratteri (dim. carattere 7 punti);

- **Provincia di nascita:** il campo ha una lunghezza di 2 caratteri (dim. carattere 8 punti);
- **Data di Nascita:** il campo nel formato GG/MM/AAAA (G: giorno; M: mese; A: anno) ha una lunghezza di 10 caratteri, compresa una barra obliqua tra ciascun gruppo (dim. carattere 7 punti);
- **Tre lettere in formato Braille standard a 6 punti:** il campo rappresenta la combinazione di 3 lettere del codice fiscale (le prime 2 che identificano il nome e il sedicesimo carattere del codice fiscale che ha la funzione di controllo dell'esatta trascrizione dei primi quindici caratteri) in formato braille, per agevolare i cittadini non vedenti nel riconoscimento tra più tessere in possesso della stessa persona nonché la direzione di utilizzo della stessa.



Si riporta di seguito il significato degli spazi riservati alle Regioni/Province Autonome sul fronte della TS-CNS:

- **A** - dicitura “Carta Regionale dei Servizi” o “Carta Provinciale dei Servizi”
- **B** - logo della Regione/Provincia autonoma
- **C** - logo della Regione/Provincia autonoma

I layout personalizzati delle Regioni / Province Autonome sono pubblicati sul sito del Sistema TS.

3. Fronte TS-CNS con caratteri diacritici

Nel caso in cui il nome e/o il cognome registrati negli archivi del Ministero dell'economia e finanze comprendano caratteri diacritici, ferme restando le diciture della TS-CNS di cui al precedente paragrafo 2, il cognome e nome dell'intestatario della TS sono riportati su due righe, tra loro incolonnate: la prima contenente il dato con i segni diacritici e la seconda la relativa traslitterazione.

Con riferimento alla descrizione della TS-CNS di cui al paragrafo 2 sono apportate le seguenti modificazioni:

- **Cognome:** le dimensioni dei caratteri sono 7 punti per il dato in caratteri diacritici e 5 punti per la relativa traslitterazione;
- **Nome:** le dimensioni dei caratteri sono 7 punti per il dato in caratteri diacritici e 5 punti per la relativa traslitterazione.

4. Retro TS-CNS standard

TESSERA EUROPEA DI ASSICURAZIONE MALATTIA

3 Cognome

4 Nome

5 Data di nascita

6 Numero di identificazione personale

7 Numero di identificazione dell'istituzione

8 Numero di identificazione della tessera

9 Scadenza

4.1. Bar Code

Il codice fiscale in modalità “BAR CODE” è riportato sul retro della tessera secondo lo standard di codifica 39 che risponde alle norme MIL-STD-1189 e ANSI MH 10.8M-1983.

4.2. Dati TEAM

Le TS-CNS riportano sul retro le seguenti informazioni in coerenza con lo standard europeo per la Tessera Europea di Assicurazione Malattia, in conformità alle caratteristiche dell'allegato 1 della decisione 190 del 18 giugno 2003 della Commissione Amministrativa della sicurezza sociale dei lavoratori migranti (CASSTM), pubblicata sulla Gazzetta Ufficiale dell'Unione europea del 27 ottobre 2003, n. L. 276 (formato Font «Verdana Bold True Type», stile normale, dimensione 8, colore nero).

- **Cognome;**
- **Nome;**
- **Data di nascita;**
- **Sigla di identificazione dello Stato che rilascia la tessera:** IT secondo il codice ISO 3166-1;
- **Numero di identificazione personale:** coincide con il codice fiscale riportato sul fronte;
- **Numero di identificazione dell'istituzione** costituito da:
 - il codice di sei caratteri di identificazione dell'istituzione: 500001.
 - la denominazione dell'istituzione (14 caratteri): recante la dicitura “SSN-MIN SALUTE”.

Eventuali deroghe a tale codifica possono essere concordate esclusivamente con il Min. Salute.

- **Scadenza:** la data di scadenza della TEAM, riportata anche sul fronte, è di 6 anni a partire dalla data di emissione della TS, salvo il caso in cui risulti che l'assistito abbia diritto all'assistenza sanitaria per un periodo inferiore, come rilevato dalle comunicazioni pervenute al Sistema TS dalla ASL di competenza.
- **Numero di identificazione della tessera** secondo le regole stabilite dall'European Committee for Standardization :

- Codice Tipo tessera: valore fisso 80 per Assistenza sanitaria;
- Codice Stato: valore fisso 380 per l'Italia;
- Codice Ente: codice regione preceduto da due zeri;
- Progressivo: progressivo regionale composto di nove caratteri;
- Check digit.

Il codice Regione, riportato nella tabella seguente, è relativo alla Regione della ASL di appartenenza dell'assistito, al momento dell'emissione della TS-CNS. La ASL di appartenenza, per i residenti italiani, coincide con la ASL di residenza.

Si riportano di seguito i codici della Regioni:

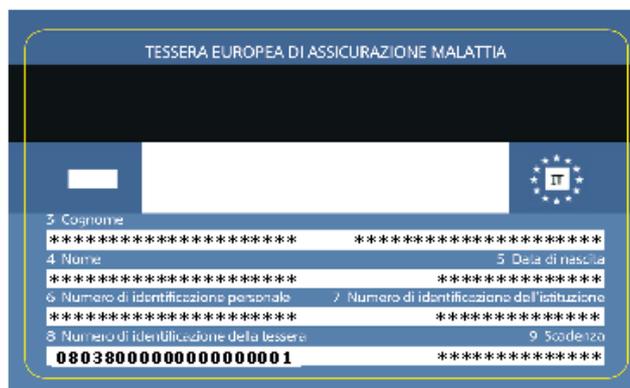
Regione	Codice
Piemonte	010
Val D'Aosta	020
Lombardia	030
Provincia Autonoma di Bolzano	041
Provincia Autonoma di Trento	042
Veneto	050
Friuli Venezia Giulia	060
Liguria	070
Emilia Romagna	080
Toscana	090
Umbria	100
Marche	110
Lazio	120
Abruzzo	130
Molise	140
Campania	150
Puglia	160
Basilicata	170
Calabria	180
Sicilia	190
Sardegna	200

Per i cittadini registrati nelle liste del SASN di Genova e Napoli e per quelli comunicati dal Ministero della Salute che non hanno la residenza in Italia, il Codice Ente assume i seguenti valori:

Altri Uffici del Ministero della Salute	Codice
SASN Genova	001
SASN Napoli	002
Ufficio rapporti internazionali per gli iscritti AIRE	003

4.3. Dati TEAM con asterischi

Nel caso in cui l'assistito non abbia diritto all'assistenza all'estero vengono inseriti asterischi in tutti i campi, ad eccezione del campo 8 relativo al numero identificativo della Tessera che deve essere regolarmente valorizzato.



4.4. Banda magnetica presente sul retro delle TS-CNS

La banda magnetica, di tipo HiCo con altezza mm. 12,75, rispetta le norme ISO Standard 7811-4: 1995 e 7811-7: 1995 e prevede le prime due tracce per codifica IATA/ABA e la terza traccia standard ISO 7811-5: 1995.

Sulla traccia 1 della banda magnetica sono registrate le seguenti informazioni, secondo la codifica IATA (International Air Transport Association):

- codice fiscale: 16 caratteri;
- cognome e nome: 60 caratteri (il cognome è separato dal nome con due spazi).

La codifica IATA è una codifica alfanumerica a 6 bit ASCII I con 1 bit di parità.

Le informazioni registrate nella traccia 1 sono precedute da un carattere denominato « START SENTINEL » (codifica ASCII: 1000101 e seguite da un carattere denominato END SENTINEL » (codifica ASCII; 0011111).

A chiusura delle traccia 1 è registrato un carattere di controllo LRC con il suo bit di parità. Il metodo di registrazione è l' « AIKEN » con densità 210 bpi.

Sulla traccia 2 della banda magnetica delle TS-CNS è registrato con codifica ABA (American Bankers Association) lo stesso codice fiscale registrato in traccia 1, convertito in forma numerica, ovvero, in accordo con le Regioni, il numero di identificazione della tessera. Per quanto attiene alla transcodifica dei caratteri alfanumerici, ciascun carattere è sostituito da un numero di due cifre, in base alle corrispondenze qui indicate:

Zero =00	C=13	0=25
1=01	D=14	P=26
2=02	E=15	Q=27
3=03	F=16	R=28
4=04	G=17	S=29
5=05	H=18	T=30
6=06	I=19	U=31
7=07	J=20	V=32
8=08	K=21	W=33
9=09	L=22	X=34

A=11	M=23	Y=35
B=12	N=24	Z=36

La codifica ABA è una codifica esclusivamente numerica a 4 bit BCD con 1 bit di parità.

- Il **codice fiscale** registrato in traccia 2 ha una lunghezza di 32 cifre numeriche ed è preceduto da un carattere denominato « START SENTINEL » (codifica BCD: 01011) e seguito da un altro carattere denominato « END SENTINEL » (codifica BCD: 11111);
- il **numero identificativo tessera**, registrato in traccia 2 in alternativa a codice fiscale, ha una lunghezza di 20 cifre numeriche ed è preceduto da un carattere «START SENTINEL» (codifica BCD: 01011) e seguito da un altro carattere denominato «END SENTINEL» (codifica BCD:11111).

A chiusura della traccia 2 è registrato un carattere di controllo LRC con il suo bit di parità. Il metodo di registrazione è l' « AIKEM » con densità di 75 bpi.

La terza traccia è riservata ad uso futuro a discrezione dell' Agenzia delle Entrate.

5. Regole di gestione delle TS-CNS

In quanto Tessere Sanitarie valgono, per le TS-CNS, le modalità di gestione previste dai decreti attuativi del citato articolo 50 con le seguenti precisazioni collegate alla natura di "SMART CARD" delle TS-CNS.

5.1. Produzione e distribuzione delle TS-CNS

Le TS-CNS vengono prodotte e distribuite, in sostituzione delle TS, nei seguenti casi:

- a scadenza delle TS;
- in caso di variazione anagrafica che abbia determinato una modifica del codice fiscale, cognome o nome in Anagrafe Tributaria, in quanto le precedenti TS sono da considerare scadute;
- su esplicita richiesta della Regione/Provincia Autonoma, in cui sia stata completata la sostituzione delle TS con le TS-CNS. E' infatti consentito per tali Regioni/Province Autonome specificare, in sede di aggiornamento dei dati sanitari di cui al comma 9 del citato *articolo 50*, la tipologia di tessera sanitaria da emettere;
- in caso di richiesta di duplicato nelle Regioni/Province Autonome, in cui sia stata completata la sostituzione delle TS con le TS-CNS.

Sono considerate Regioni/Province Autonome in cui sia stata completata la sostituzione delle TS con le TS-CNS, quelle Regioni/ Province Autonome che hanno ottenuto dal Ministero dell'Economia e delle finanze:

- l'autorizzazione alla richiesta di adesione al comma 11 dell'articolo 50 del decreto legge 30 settembre 2003, n. 269, convertito, con modificazioni, dalla legge 24 novembre 2003, n. 326, e successive modificazioni;
- il riconoscimento del completamento della sostituzione delle TS, in scadenza a partire dal 1° gennaio 2011, con le TS-CNS, ex articolo 11, comma 15 del decreto-legge 31 maggio 2010, n. 78, convertito, con modificazioni, dalla legge 30 luglio 2010, n. 122.

Allo scopo di garantire il processo di emissione delle TS-CNS, le Regioni/Province Autonome comunicano l'avvenuto trasferimento di competenza sanitaria dell'assistito al Sistema TS

esclusivamente dopo aver espletato le procedure amministrative di raccordo con la Regione/Provincia Autonoma di provenienza.

Le TS-CNS non vengono prodotte per:

- i nuovi nati, ai quali viene inviata una TS con validità per tutto il primo anno di vita laddove non sia pervenuta nel frattempo la richiesta di iscrizione alla ASL di competenza. In caso di emissione della TS, la TS-CNS viene comunque prodotta all'atto dell'iscrizione del nuovo nato al SSN salvo diversa indicazione della ASL;
- gli assistiti che hanno diritto ad un periodo di assistenza sanitaria inferiore ai 30 gg; in sostituzione le ASL rilasceranno agli interessati l'apposito certificato cartaceo sostitutivo della TS, ai sensi del DM 30 giugno 2004, attuativo del comma 6 del citato articolo 50;
- gli assistiti con periodo di assistenza tra i 30gg ed i 180 gg ai quali viene inviata automaticamente una TS;
- gli assistiti per i quali la Regione/Provincia Autonoma abbia effettuato una esplicita richiesta di emissione della TS in luogo della TS-CNS.

E' infatti consentito alle Regioni/Province Autonome, in sede di aggiornamento dei dati sanitari di cui al comma 9 del citato *articolo 50*, richiedere la transitoria emissione di una TS in luogo della TS-CNS.

5.2. Ritiro e disattivazione delle TS-CNS

La Regione/Provincia Autonoma, in qualità di ente emittitore, provvede **all'immediata disattivazione della TS-CNS**, attraverso la revoca del certificato in essa contenuto, non appena acquisite le informazioni:

- di **decesso** dell'assistito. Analogamente a quanto disposto per le Tessere Sanitarie, la carta deve essere restituita a cura degli eredi presso la propria ASL o presso un qualsiasi ufficio dell'Agenzia delle Entrate;
- di **restituzione** o richiesta di **duplicato**.

La Regione/Provincia Autonoma, allo scopo di garantire l'accesso in rete ai servizi erogati dalla Pubblica Amministrazione ai cittadini, provvede **alla disattivazione della TS-CNS**, attraverso la revoca del certificato in essa contenuto, al **ritiro e distruzione delle TS-CNS disattivate** nei seguenti casi:

- in sede di rilascio delle credenziali personali di utilizzo della nuova TS-CNS, emessa a seguito di **variazione anagrafica per un assistito già in possesso di TS-CNS**;
- in sede di rilascio delle credenziali personali di utilizzo della nuova TS-CNS emessa a seguito di **sostituzione a scadenza di una precedente TS-CNS**.

6. Servizi Ausiliari

Il Sistema TS pone a disposizione delle strutture di sicurezza delle Amministrazioni Pubbliche appositi servizi di tipo "booleano" (risposta si/no) per la verifica della validità delle tessere sanitarie.

Specifiche Tecniche e di Gestione della componente CNS delle TS-CNS

1. Caratteristiche tecniche della componente CNS

In relazione alle specifiche tecniche e alle modalità di produzione e gestione della componente CNS, le TS-CNS sono conformi alla normativa vigente ed alle relative regole tecniche emanate da DigitPA in particolare da riferire ai seguenti dispositivi vigenti:

- Decreto 9 dicembre 2004 “*Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta Nazionale dei Servizi*”;
- Documentazione DigitPA sulle CNS dal titolo “*Carta Nazionale dei Servizi – CNS - File System*”;
- Documentazione DigitPA sulle CNS dal titolo “*CNS - Carta Nazionale dei Servizi Functional Specification*”;
- Documentazione DigitPA sulle CNS dal titolo “*Profilo di certificato digitale per l’autenticazione mediante Carta Nazionale dei Servizi (CNS)*” ;
- Documentazione Netlink pubblicata da DigitPA sulle CNS dal titolo “*NetLink - Dati PDC*”, “*NetLink - Specifiche PDC*”, “*Netlink - Gestione del Serial Number delle carte sanitarie*”, “*NetLink - Specifiche HPC*”.

Quanto descritto nei paragrafi successivi é esclusivamente attinente alle scelte tecniche operate sulla TS-CNS in coerenza con tali disposizioni.

1.1. Caratteristiche del microprocessore della TS-CNS

Il microprocessore della TS/CNS possiede i seguenti requisiti minimi:

- almeno 64k byte di memoria EEPROM;
- coprocessore crittografico;
- crittografia asimmetrica RSA con chiavi a 1024 e 2048 bit;
- possibilità di generare chiavi RSA all’interno del chip;
- crittografia simmetrica DES;
- crittografia simmetrica 3DES con chiavi ad almeno 128 bit;
- funzione di hashing SHA-1, SHA-256 (tali funzioni possono essere assicurate in alternativa dalle librerie software PKCS#11 e MS CSP della TS/CNS)
- conformità con la normativa vigente per la firma digitale;
- capacità di ritenzione dei dati di almeno 10 anni;
- numero di cicli R/W in EEPROM maggiore di centomila;
- interfaccia duale (a contatti e contact-less);
- conformità alla norma ISO 7816 secondo quanto previsto dal documento DigitPA “*CNS - Carta Nazionale dei Servizi Functional Specification*” per l’interfaccia a contatti;
- conformità alla norma ISO 14443 part 1-4 in modalità Type A oppure Type B per l’interfaccia contact-less;
- velocità di trasmissione ISO 14443 selezionabile fino ad almeno 424 kbit/s
- supporto protocolli T=0 e/o T=1
- rispetto delle specifiche del sistema operativo (APDU) pubblicate sul sito di DigitPA.

1.2. Personalizzazione File System della TS-CNS

La personalizzazione del File System eseguita dal Ministero economia e finanze sulle TS-CNS riguarda:

- inserimento dei dati anagrafici come da specifiche CNS;

- inserimento della chiave e del certificato di autenticazione conformemente alle specifiche CNS;
- predisposizione dei DF per firma digitale (DF_DS) e per dati di servizio aggiuntivi (DF2) come da specifiche pubblicate da DigitPA;
- predisposizione della struttura NetLink completa, come da specifiche Netlink pubblicate da DigitPA, in cui saranno creati, vuoti, i seguenti file:
 -
 - EF.NKAP (Dati amministrativi protetti)
 - EF.NKEF (Dati di emergenza a lettura libera)
 - EF.NKEP (Dati di emergenza protetti)
 - EF.NKPP (Puntatori a eventi sanitari)

I file EF.NKAF contengono la personalizzazione del nome e del cognome dell'intestatario e la opportuna formattazione degli ulteriori campi previsti.

Viene garantita alle Regioni la possibilità di attivare in proprio i servizi di firma digitale (DF_DS) secondo le specifiche di certificazione della carta (microchip), nonché i servizi aggiuntivi (DF2).

1.3. Answer to reset delle TS-CNS

L'Answer To Reset (ATR) è il messaggio con il quale la carta (più precisamente il microchip) risponde al precedente segnale di reset che il computer cui è collegato il lettore invia per attivare il microchip. In altri termini è il meccanismo attraverso il quale si avvia il colloquio tra computer e sistema operativo della Carta.

Il valore dell'ATR è univoco per ogni diverso microchip e consente di riconoscere le librerie crittografiche collegate.

Il valore dell'ATR è disponibile sul sito Sistema TS.

1.4. Certificato di autenticazione delle TS-CNS

Il microchip della TS-CNS contiene un certificato digitale di autenticazione emesso da un Certificatore accreditato secondo le modalità previste dalla normativa vigente per le CNS.

Il certificato di autenticazione ha la stessa validità prevista dalla data di scadenza della Tessera Sanitaria in cui è inserito.

Il profilo del certificato contiene i seguenti valori fissi, comunicati dalla Regione/Provincia Autonoma:

- nel campo Issuer:
 - attributo "OU": "Servizi di certificazione";
 - attributo "CN": "Regione <Nome Regione> – CA Cittadini".
- Sono inoltre valorizzati, a partire dal 2010, i seguenti attributi del campo Subject:
 - attributo "GN": "Given Name" che deve corrispondere al nome proprio del soggetto
 - attributo "SN": "Surname" che deve corrispondere al cognome del soggetto.
- in conformità a quanto riportato sul layer della carta e sulla traccia 1 della banda magnetica.

1.5. Software del microchip delle TS-CNS

Il microchip delle TS/CNS è utilizzabile con le seguenti componenti software per sistema operativo Windows XP o superiore nelle versioni a 32 e 64 bit e per sistema operativo Windows 2003 server o superiore nelle versioni a 32 e 64 bit:

1. Libreria Microsoft Cryptographic Service Provider (CSP) conforme alle specifiche PC/SC e CryptoAPI di Microsoft;
2. Libreria crittografica di sistema PKCS#11;
3. Tool di gestione del PIN utente di autenticazione e di firma, per le funzioni di modifica e sblocco.

Per le componenti di cui ai punti 2, 3 la TS-CNS è utilizzabile anche con i sistemi operativi Mac OS X, nelle versioni a 32 e 64 bit, e per almeno due delle distribuzioni Linux di maggiore diffusione nelle versioni a 32 e 64 bit.

Le librerie precedentemente citate possono essere scaricate dal Portale Sistema TS per garantire al titolare l'utilizzo della componente CNS delle TS-CNS da qualsiasi postazione di lavoro connessa ad internet per l'accesso ai servizi in rete.

Verranno fornite alle Regioni le librerie per la generazione delle chiavi e per la personalizzazione del DF_DS mediante interfaccia PKCS#11, con facoltà di fornirle a certificatori terzi per l'erogazione di servizi di firma digitale e di firma elettronica qualificata.

2. I servizi di gestione dei certificati delle TS-CNS (Certification Authority)

I servizi di Certification Authority (CA) sono erogati in conformità a quanto previsto dalla normativa e dalle regole tecniche vigenti per l'emissione di certificati digitali di autenticazione per CNS.

Il certificatore, a seguito degli accordi contrattualmente assunti dal Ministero economia e finanze:

- emette un certificato di C.A. personalizzato per la Regione/Provincia Autonoma, come indicato al paragrafo precedente;
- eroga servizi pubblici di verifica dello stato (valido, revocato o sospeso) dei certificati di autenticazione, con disponibilità 24 ore al giorno e 7 gg su 7, indipendentemente dal soggetto che richiede tale verifica, mediante:
 - pubblicazione di CRL (Certificate Revocation List, RFC 5280) mediante protocollo HTTP e, ove disponibile, LDAP;
 - servizio di validazione on-line conforme alle specifiche OCSP (Online Certificate Status Protocol, RFC 2560).
- garantisce prestazioni adeguate per l'utilizzo delle CRL.

Le informazioni per l'accesso ai suddetti servizi sono contenute nel certificato di autenticazione.

Le TS-CNS vengono inviate ai cittadini con certificato di autenticazione in stato "attivo".

Il certificatore eroga servizi di revoca, sospensione e riattivazione dei certificati digitali di autenticazione nelle seguenti modalità:

- on-line tramite il proprio Portale;
- scambio flussi secondo gli standard di comunicazione pubblicati sul sito Sistema TS nelle more di una standardizzazione da parte di DigitPA. Fino all'adeguamento ai

citati standard le specifiche di interazione con i certificatori potranno essere concordate direttamente dalla Regione/Provincia Autonoma.

I servizi di certification authority indicati sono forniti per l'intero periodo di validità dei certificati emessi.

3. Servizi operativi di gestione delle CNS

Il Certificato di Autenticazione delle TS-CNS, in combinazione con il PIN utente, è utilizzato ai fini del riconoscimento in rete del titolare, consentendo l'accesso ai servizi on-line erogati dall'Ente emettitore e, più in generale, dalle Pubbliche Amministrazioni.

Una corretta gestione delle CNS richiede che vengano assicurate le attività operative relative al rilascio delle credenziali personali (PIN/PUK), alle richieste di revoca, sospensione e riattivazione del certificato.

Le Regioni/Province Autonome, in qualità di ente emettitore, predispongono e pubblicano sui propri siti le istruzioni e le modalità operative inerenti i servizi per il rilascio delle credenziali personali (PIN/PUK) di utilizzo delle TS-CNS, dei casi in cui i certificati sono soggetti a sospensione/revoca oltre che le modalità con cui lo stesso titolare può richiedere tali prestazioni.

In caso di richiesta di sospensione/revoca il certificatore inserisce la CNS in una lista di revoca o sospensione (CRL - CSL) firmata dal Certificatore e pubblicata con periodicità prestabilita nel registro dei certificati.

A supporto di tali attività le Regioni/Province Autonome, come previsto dalle regole tecniche emanate da DigitPA, si avvalgono della infrastruttura di gestione del ciclo di vita delle CNS, denominata **Card Management System** (di seguito CMS), che prevede il trattamento di specifici flussi di dati in ingresso e in uscita, necessari alla gestione delle banche dati delle CNS.

Per quanto attiene allo scambio di informazioni con i certificatori ed il Sistema TS sono previsti i seguenti flussi:

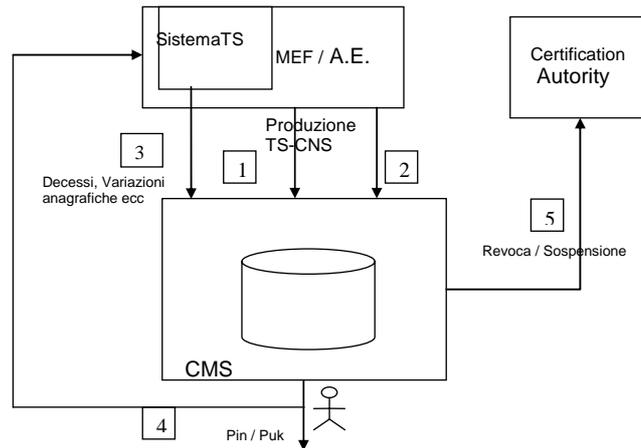
a) in ingresso al CMS:

- Flusso 1 - dati anagrafici degli assistiti utilizzati dal Produttore per la produzione e personalizzazione delle TS-CNS;
- Flusso 2 - dati inerenti i Certificati e le relative credenziali personali (PIN/PUK) associati alle TS-CNS prodotte;
- Flusso 3 - proveniente dal SistemaTS e contenente:
 - le informazioni inerenti le richieste di produzione delle TS-CNS al Produttore per nuovo assistito, riemissione a scadenza, richieste di duplicati, e riemissione per variazioni anagrafiche nonché le informazioni relative a decessi, restituzioni e mancati recapiti;
 - le informazioni relative alle precedenti TS-CNS nei casi di riemissione per variazioni anagrafiche;

b) in uscita dal CMS:

- Flusso 4 - fornitura verso SistemaTS dell'avvenuta consegna dei PIN/PUK ai Titolari delle TS-CNS (tale informazione consente di instradare su un canale privilegiato di produzione le eventuali richieste di sostituzione delle TS-CNS);
- Flusso 5 - inoltro delle richieste di revoca o sospensione verso le C.A.

I tracciati standard dei flussi precedentemente indicati sono consultabili nel sito del Sistema TS.



Tutti i flussi in ingresso vengono instradati ai CMS locali dal Sistema TS via FTP (H24) ed applicano modalità di crittografia e firma digitale dei dati al fine di garantire la provenienza e riservatezza.

Nelle more dell'adeguamento dei CMS a tale standard le specifiche di interazione tra i CMS ed i certificatori potranno essere concordate direttamente dalla Regione/Provincia Autonoma.

Tenuto conto dell'esigenza di garantire i servizi ai cittadini che si trasferiscono in altra Regione/Provincia Autonoma diversa dall'ente emittitore della TS-CNS in loro possesso, tutti i CMS devono prevedere, nelle more dell'emanazione di standard da parte di DigitPA, le seguenti funzionalità le cui specifiche di interfaccia sono pubblicate sul sito del Sistema TS:

- inoltro, verso la Regione/Provincia Autonoma ente emittitore della TS-CNS, della richiesta di rilascio delle credenziali personali (PIN/PUK), ovvero, di revoca, sospensione e/o riattivazione del certificato;
- restituzione, verso la Regione/Provincia Autonoma richiedente, delle credenziali personali (PIN/PUK), ovvero dell'esito delle richieste revoca, sospensione e/o riattivazione dei certificati inoltrate in modo automatico alle CA competente.

Nelle more di tali adeguamenti tecnici dei CMS già operativi le operazioni verranno svolte manualmente dalla Regione/Provincia Autonoma avendo la stessa ricevuto le richieste da altre Regioni/Province Autonome sull'indirizzo PEC pubblicato sul Sistema TS.