Il Ministro dell'interno,
il Ministro per l'innovazione e le tecnologie
ed
il Ministro dell'economia e delle finanze

Visto l'articolo 36, comma 5 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, recante testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa. (Testo A);

Visto il decreto del Presidente della repubblica 2 marzo 2004, n. 117, recante regolamento concernente la diffusione della carta nazionale dei servizi;

Visto il decreto del Presidente del Consiglio dei ministri del 22 ottobre 1999, n. 437, che ha istituito la carta d'identità elettronica;

Visto il decreto-legge 27 dicembre 2000, n. 392, convertito con legge 28 febbraio 2001, n. 26, che istituisce, all'art. 2-*quater*, l'Indice Nazionale delle Anagrafi (INA) presso il Ministero dell'Interno;

Visto il decreto legislativo 30 giugno 2003, n. 196, recante codice in materia di protezione dei dati personali;

Acquisito il parere della Conferenza Stato-città ed autonomie locali, ai sensi dell'articolo 9, comma 6, lettera b), del decreto legislativo 28 agosto 1997, n. 281, espresso nella riunione dell'8 luglio 2004;

Sentito il Garante per la tutela dei dati personali;

ADOTTANO

il seguente decreto

ART.1

(Oggetto)

1. Sono approvate le regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della carta nazionale dei servizi di cui all'allegato, che costituisce parte integrante del presente decreto.

Il presente decreto sarà pubblicato sulla Gazzetta Ufficiale della Repubblica Italiana

Roma, 29 DIC. 2004

IL MINISTRO DELL'INTERNO

IL MINISTRO PER L'INNOVAZIONE E LE TECNOLOGIE

IL MINISTRO DELL'ECONOMIA E DELLE FINANZE

Allegato

Regole tecniche e di sicurezza relative alle tecnologie e ai materiali utilizzati per la produzione della Carta nazionale dei servizi

Indice

1. Introduzione

1.1 Scopo del Documento

Il presente documento stabilisce l'architettura, i requisiti e le caratteristiche del circuito di emissione della Carta Nazionale dei Servizi, nel seguito CNS.

2. Definizioni

Carta d'Identità Elettronica	*Documento di riconoscimento personale a fini di Polizia rilasciato dal comune su supporto informatico* Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. All'esterno contiene gli elementi necessari per l'identificazione a vista. Acronimo **CIE**
Documento d'Identità Elettronica	*Documento analogo alla carta d'identità elettronica rilasciato dal comune fino al compimento del quindicesimo anno di età* Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. All'esterno contiene gli elementi necessari per l'identificazione a vista.
Carta Nazionale dei Servizi	*Documento informatico, rilasciato da una Pubblica Amministrazione, con la finalità di identificare in rete il titolare della carta* Utilizza una carta a microprocessore (smart card) in grado di registrare in modo protetto le informazioni necessarie per l'autenticazione in rete. Acronimo **CNS**
Caveau	*Locale protetto in cui sono conservate le smart card inizializzate in corso di lavorazione* E' un locale con caratteristiche di sicurezza fisica tali da impedire il furto delle smart card inizializzate o personalizzate, acceduto con procedure che assicurino la massima sicurezza e richiedano la presenza contemporanea del responsabile della sicurezza e del responsabile della sede.
Certificato di autenticazione	*L'attestato elettronico che garantisce l'autenticità del circuito che ha emesso la CNS.* Certificato X509 v3 della carta, rilasciato da un certificatore accreditato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002. Acronimo **Cda**
Certificato di firma	*L'attestato elettronico che collega i dati utilizzati per verificare la firma elettronica al titolare e conferma l'identità del titolare stesso* Si tratta di un certificato X509 v3, emesso da un certificatore accreditato ai sensi dell'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002, che può essere utilizzato per la verifica delle firme digitali emesse in aderenza alla vigente normativa.

Certificatore

Ente che presta servizi di certificazione delle informazioni necessarie per l'autenticazione o per la verifica delle firme elettroniche
Si tratta di enti abilitati a prestare servizi di certificazione in base all'articolo 5 del Decreto Legislativo n.10 del 23 gennaio 2002.
Acronimo **Ce**

Dati_processore

Dati univoci che identificano il processore
E' un file elementare che riporta alcuni dati univoci del processore.
Le informazioni che contiene sono numero seriale e data fabbricazione.

Ente emettitore

Ente responsabile della formazione e del rilascio della CNS.
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.
Acronimo **EE**

Fase di inizializzazione

Fase in cui vengono attivate le smart card che ospiteranno la CNS, eseguendo la generazione del file system e creando le condizioni per l'accesso "controllato" alle strutture interne.

Fase di personalizzazione

Fase in cui vengono inserite nella smart card le informazioni proprie dell'utente finale e quelle necessarie per usufruire dei servizi previsti.

Ministero dell'Interno CNSD

Centro Nazionale dei Servizi Demografici.

Il Ministero dell'Interno, con DM del 23 aprile 2002 ha costituito il Centro Nazionale dei Servizi Demografici, per gestire in modo integrato e razionale i flussi delle informazioni anagrafiche necessari al mantenimento dell'allineamento dei dati delle anagrafi comunali.
Gli enti emettitori si collegano su rete Internet o Rete unitaria al CNSD attraverso la porta applicativa.
Acronimo **CNSD**

Backbone

Il backbone INA/SAIA di sicurezza e certificazione per l'accesso ai servizi di convalida e di aggiornamento dell'INA

Ministero dell'Interno INA

Indice Nazionale delle Anagrafi.

	In attuazione alla legge 28 febbraio 2001, n. 26, il Ministero dell'Interno rende disponibile il collegamento telematico al backbone INA/SAIA di sicurezza e certificazione, per la convalida delle informazioni anagrafiche dei cittadini. Acronimo **INA**
PIN	*Personal Identification Number* E' il codice utilizzato per svolgere operazioni privilegiate sulla CNS
PIN_firma digitale	*PIN utilizzato per l'attivazione della funzione di firma digitale* E' il PIN necessario al titolare per farsi installare da un certificatore il servizio di firma digitale.
PIN_personalizzazione	*PIN utilizzato per la personalizzazione della CNS* E' il PIN che consente l'accesso alle strutture interne della smart card prima della sua personalizzazione.
PIN_utente	*PIN utilizzato per l'accesso alle funzioni della CNS* E' il PIN, necessario al titolare per attivare le operazioni di autenticazione in rete, che viene consegnato dall'ente emettitore con meccanismi di sicurezza.
Produttore	*Azienda che esegue le fasi di produzione secondo gli standard della CNS* E' l'azienda che provvede alla fornitura e/o inizializzazione delle carte a microprocessore con un chip compatibile con quello previsto dalla CNS, predispone opportunamente gli spazi dedicati alla carta sanitaria (Netlink), alla firma digitale ed applica al supporto fisico l'artwork e gli elementi costanti. Acronimo **Pr**

3. Le caratteristiche delle carte

3.1 Utilizzo della CNS

La CNS è uno strumento di autenticazione in rete. Tutte le CNS dovranno essere predisposte per operare come carta sanitaria in conformità alle specifiche definite nel paragrafo **6.3**.

La CNS deve essere predisposta per ospitare il servizio di firma digitale, fornendo al titolare la possibilità di sottoscrivere documenti elettronici.

3.2 Struttura delle informazioni nel microprocessore

La successiva tabella definisce la struttura dei dati registrati nella memoria riscrivibile (EEPROM) del microcircuito.

Fornito da: indica il soggetto che fornisce l'informazione (proprietario del dato).

Predisposto da: indica il soggetto responsabile della predisposizione della struttura nel file system della carta destinata a contenere il dato.

Scritto da: indica il soggetto responsabile dell'inserimento del dato nella CNS.

Elemento	*Fornito da*	*Predisposto da*	*Scritto da*	*Descrizione*
MF	-	Pr		E' il *Master File* della struttura di memorizzazione. Corrisponde alla directory radice di un ordinario sistema operativo.
DF0	-	Pr		*Dedicated file* (directory) dove vengono memorizzate le informazioni prodotte durante la fase di inizializzazione della carta.
DF1	-	Pr		Dedicated file (directory) dove vengono memorizzate le informazioni raccolte durante la fase di personalizzazione della carta.
DF2	-	Pr/EE		Dedicated file (directory) dove vengono installati i servizi che necessitano, per il loro funzionamento, di una struttura dati riservata nella memoria riscrivibile (EEPROM) del microcircuito.
PIN	EE	EE	EE	E' il PIN utente richiesto per usare la chiave privata K_{pri} per le operazioni di autenticazione in rete. Questo codice deve essere consegnato dall'ente emettitore o centro servizi di rilascio, con garanzia di segretezza, al titolare della CNS.
PUK	EE	EE	EE	E' il PUK utente richiesto per sbloccare la carta nel caso non si disponga del PIN. Questo codice deve essere consegnato dall'ente emettitore, con garanzia di segretezza, al titolare della CNS.
K_{pri}		EE		Chiave presente internamente alla carta, congiuntamente a K_{pub}. Essa è invisibile all'esterno, ma utilizzabile per le operazioni di cifra richieste durante l'operazione di strong authentication. Il microcircuito deve essere provvisto di un motore crittografico interno (crypto-engine), al fine di rendere più rapide tali operazioni.
Id_Carta	-	EE/Ce	EE/Ce	E' il numero identificativo della carta che contiene informazioni sull'Ente emettitore e il numero progressivo dell'emissione presso tale Ente.
Cda	Ce	EE	EE	E' il certificato, rilasciato dall'ente di certificazione iscritto all'albo, che garantisce la validità del legame tra la componente pubblica, K_{pub}, ed il titolare della CNS.
Carta sanitaria	Pr	Regione/Salute	Regione/Salute	E' lo spazio dedicato ad ospitare la carta sanitaria. Fornito da PR, viene predisposto e scritto dalle regioni ovvero dal Ministero della Salute.
Firma digitale	Pr	Ce	Ce	E' il Dedicated file destinato a ospitare le informazioni per la firma digitale.
PIN_SO	EE	EE	EE	E' il PIN di Security Officer che può essere utilizzato per l'installazione della firma digitale eventualmente rilasciato da EE all'utente per poter installare tale servizio.
Dati_personali	EE	EE	EE	E' un file elementare che contiene i dati personali dell'individuo.
Memoria_residua	EE	EE	EE	E' l'ammontare dello spazio totale previsto per i servizi decurtato dello spazio utilizzato da quelli già installati.

Tabella 1 – struttura dei dati e matrice delle responsabilità

Le altre informazioni presenti nel file system hanno un impiego analogo a quello della Carta d'Identità Elettronica.
Il file elementare dei dati personali è codificato secondo le modalità previste per la Carta d'Identità Elettronica con le definizioni specifiche seguenti:

Dato	MOV	Dimensione Max	Descrizione
Emettitore	M	4	Indicazione dell'emettitore
Data di emissione del documento	M	8	Formato GGMMAAAA
Data di scadenza del documento	M	8	Formato GGMMAAAA
Cognome	M	26	
Nome	M	26	
Data di Nascita	M	8	Formato GGMMAAAA
Sesso	M	1	'M' maschile, 'F' femminile
Statura (cm)	O	0	Presente per compatibilità CIE
Codice fiscale	M	16	
Cittadinanza (codice)	O	0	Presente per compatibilità CIE
Comune di Nascita	M	4	
Stato estero di Nascita	O	0	Presente per compatibilità CIE
Estremi atto di nascita	O	0	Presente per compatibilità CIE
Comune di residenza al momento dell'emissione	M	4	
Indirizzo di residenza	O	80	
Eventuale annotazione in caso di non validità del documento per l'espatrio	V	0	Presente per compatibilità CIE

Tabella 2- Definizione Dati Personali

I campi obbligatori (M), opzionali (O) e vuoti (V) sono indicati nella colonna MOV.

Oltre alla definizione dei dati personali compatibili con una struttura dati della CIE, in base a quanto riportato nel Decreto del Presidente della Repubblica concernente regolamento recante disposizioni per la diffusione e uso della Carta Nazionale dei servizi, si intende:

per dati identificativi della persona, i dati anagrafici e il codice fiscale;

per dati anagrafici, il nome, il cognome, il sesso, la data, il luogo di nascita e il comune di residenza al momento dell'emissione.

3.3 Materiali e Standard di Riferimento

La CNS, non presenta particolari restrizioni per quanto riguarda la struttura del supporto fisico. Va comunque rilevato che devono essere fatti salvi i vincoli imposti dagli standard internazionali sulle smart card, con particolare riferimento alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO)/IEC 7816-1-2.

Le dimensioni nominali dovranno essere di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810: 1995 per la carta di tipo ID-1. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.
Lo spessore della CNS, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

Inoltre, poiché la carta CNS deve essere predisposta per ospitare la firma digitale, valgono le norme vigenti in materia.

3.3.1 Il layout della carta

Sulla carta deve essere presente la scritta Carta Nazionale dei Servizi ed il nome della pubblica amministrazione che l'ha emessa.

3.3.2 I dati

I dati da stampare sulla CNS e l'eventuale loro memorizzazione sul microchip sono decisi e disposti dall'Ente emettitore che la rilascerà. Sulla CNS non devono essere presenti dei dati utilizzabili in alcun modo per il riconoscimento a vista del titolare, come per esempio la fotografia.

3.3.3 Struttura del certificato di autenticazione e interoperabilità con la CIE

La struttura del certificato di autenticazione, interoperabilità con la CIE e le relative modalità di aggiornamento sono definite nell'allegato 2.

3.3.4 Microcircuito

E' richiesta una memoria EEPROM dalla capacità non inferiore a 32 KB.

Il microprocessore deve essere conforme agli standard della serie ISO/IEC 7816 di pertinenza e comunque deve rispettare le specifiche del sistema operativo (APDU) pubblicate sul sito del Centro Nazionale per l'Informatica nella Pubblica Amministrazione e sul sito della Carta d'Identità Elettronica.

3.3.5 Interdizione della carta

Le procedure da seguire per l'interdizione della CNS sono contenute nel manuale operativo pubblicato dall'Ente emettitore.

Le liste di revoca dei certificati di autenticazione sono gestite dal corrispondente certificatore accreditato secondo le stesse modalità già in atto per la firma digitale.

4. Il circuito di emissione

Possono emettere la CNS tutte le Pubbliche Amministrazioni

La Pubblica Amministrazione che intende emettere la CNS è responsabile:

- della correttezza dei dati identificativi memorizzati nella carta e nel certificato di autenticazione,
- della correttezza del codice fiscale memorizzato nella carta e riportato nel certificato di autenticazione,
- della sicurezza delle fasi di produzione, inizializzazione, distribuzione ed aggiornamento/ritiro della carta.

Secondo il dettato dell'articolo 8 del decreto del Presidente della Repubblica 2 marzo 2004, n. 117, recante regolamento concernente la diffusione della carta nazionale dei servizi, è cura dell'Ente emettitore inviare i dati identificativi al Ministero dell'interno, CNSD per l'eventuale aggiornamento dell'INA, con modalità e formati definiti da apposita circolare del Ministero dell'interno.

4.1 Modello del circuito di emissione

Di seguito sono illustrate le attività funzionali da realizzare per emettere le carte CNS. Tali attività non sono descritte in modo temporale e l'Ente emettitore potrà definire quelle modifiche che ne rendono più semplice l'attuazione. In ogni caso rimangono di responsabilità esclusiva dell'Ente emettitore il riconoscimento e il rilascio delle CNS.

Fase	Attività	Descrizione
1	Individuazione servizi ed infrastruttura	L'ente emettitore analizza ed individua i servizi da rendere disponibili in rete mediante CNS. Valuta le possibilità di mercato offerte per la fornitura delle smart card e decide se far fronte in maniera autonoma all'emissione della CNS, ovvero utilizzare servizi di strutture delegate. Eventualmente stipula accordi con le Regioni per la predisposizione delle carte con le funzionalità di tessera sanitaria.
2	Avviamento del processo di emissione	L'ente emettitore avvia la produzione di un lotto di CNS, si dota eventualmente di tutte le risorse hw e sw necessarie all'emissione della CNS tenendo conto delle direttive e delle norme vigenti, commissiona al produttore individuato la fornitura dei lotti di CNS inizializzate.
3	Produzione delle CNS	Il produttore esegue le fasi di produzione ed inizializzazione seguendo le specifiche definite nel presente documento e nel sito del Centro Nazionale per l'Informatica nella Pubblica Amministrazione Le carte sono consegnate in modalità protetta all'ente emettitore.
4	Registrazione degli utenti	L'ente emettitore identifica, attraverso un documento di riconoscimento, il cittadino ed attiva la procedura di emissione CNS o in maniera autonoma o rivolgendosi a strutture delegate.
5	Verifica dati identificativi	L'ente emettitore effettua la verifica della correttezza dei dati identificativi collegandosi, direttamente o tramite struttura delegata, con il CNSD del Ministero dell'Interno fatto salvo quanto previsto dall'articolo 9 del Decreto del Presidente della Repubblica concernente regolamento recante disposizioni per la diffusione e uso della carta nazionale dei servizi .
6	Generazione del certificato Cda	Un certificatore accreditato, scelto dall'Ente emettitore rilascia il certificato che attesta l'autenticità delle informazioni associate ai dati di autenticazione. L'eventuale colloquio tra l'ente emettitore ed il certificatore avviene in modalità protetta.
7	Personalizzazione della CNS	L'ente emettitore, tramite strutture proprie o esterne, esegue la personalizzazione della CNS, inserendo i dati personali del cittadino ed il certificato di autenticazione, stampa gli stessi sulla carta, produce il PIN ed il PUK necessari all'utilizzo della CNS in rete ed il PIN necessario per l'eventuale installazione della firma digitale.
8	Consegna della CNS	L'ente emettitore, tramite strutture proprie o esterne, consegna la CNS al titolare. L'ente emettitore illustra al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di problemi. Fornisce al titolare un numero telefonico per l'assistenza (call center) ed il numero telefonico per la sospensione o revoca.
9	Gestione della CNS	L'ente emettitore provvede alla gestione delle CNS emesse predisponendo le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza. Per le funzioni di gestione delle carte l'ente può avvalersi di strutture delegate. L'eventuale software consegnato al cittadino deve garantire l'interoperabilità con la CIE.
10	Ritiro della CNS	La CNS può essere ritirata per rinnovo a seguito di problemi di funzionamento della smart card o dopo aver raggiunto il naturale termine di scadenza. L'ente emettitore è responsabile del suo ritiro prima dell'emissione di una nuova carta o del suo rinnovo

Tabella 3 – Funzioni relative all'emissione e gestione della CNS

Nei successivi paragrafi si descrivono le attività di maggiore complessità.

4.1.1 Attività di produzione

Il processo di produzione prevede la produzione della carta plastica e la sua inizializzazione tramite la generazione del file system e la creazione delle condizioni per controllare l'accesso ai file.

L’operazione di Inizializzazione è finalizzata a produrre in maniera sicura delle carte che siano pronte ad essere personalizzate, ossia risultino in uno stato definito “Attivate”.

4.1.2 Attività di registrazione

Consiste nell’identificazione del titolare attraverso un documento di riconoscimento valido.
Al momento della registrazione, il cittadino deve dichiarare di non possedere la Carta d’Identità Elettronica.

4.1.3 Verifica dei dati identificativi ed allineamento anagrafi

Prima di personalizzare la CNS l’ente emettitore verifica i dati identificativi, direttamente o tramite struttura delegata, mediante il sistema informativo del Ministero dell’Interno – Centro Nazionale dei Servizi Demografici fatto salvo quanto previsto dall’articolo 8 del decreto del Presidente della Repubblica 2 marzo 2004, n. 117.

4.1.4 Generazione del certificato di autenticazione

Le informazioni anagrafiche ottenute in fase di registrazione congiuntamente con la chiave pubblica generata in fase di personalizzazione, sono utilizzate dal Certificatore per generare il certificato di autenticazione, secondo le specifiche definite in un apposita circolare del Dipartimento dell’Innovazione e Tecnologie e disponibili presso il sito del Centro Nazionale per l’Informatica nella Pubblica Amministrazione.

4.1.5 Attività di personalizzazione

La personalizzazione delle carte ed il loro rilascio è condotta dagli enti emettitori per mezzo di loro strutture o strutture esterne.
Nel corso dell’attività di personalizzazione, vengono inserite le informazioni utente necessarie per l’identificazione in rete e per gli altri servizi previsti.
Viene inoltre generato il PIN utente ed il PUK, utilizzabile per lo sbocco della carta nel caso di iterata digitazione errata del PIN. Il PIN ed il codice PUK sono stampati in buste retinate atte a garantire la riservatezza di tali informazioni.

4.1.6 Attività di rilascio

In questa fase la CNS viene consegnata al titolare dopo averne verificata l’identità, unitamente alla busta contenente il PIN ed il codice PUK. L’ente emettitore deve illustrare al titolare le modalità di uso della carta e le procedure che dovranno essere utilizzate in caso di anomalie o disservizi. Deve fornire al titolare un numero telefonico per l’assistenza ed il numero telefonico per la sospensione o revoca.

4.2 Modalità di connessione al Centro Nazionale dei Servizi Demografici

L'interconnessione al CNSD è realizzata attraverso la porta applicativa di accesso ai servizi del CNSD.

L'interconnessione al CNSD avverrà su backbone INA/SAIA attraverso la porta applicativa di accesso del CNSD secondo le seguenti modalità:

- tramite la Rete Unitaria della Pubblica Amministrazione (RUPA);
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite rete Internet.

Le modalità di interconnessione al CNSD, al fine della verifica (fatto salvo quanto previsto all'articolo 9 del decreto del Presidente della Repubblica concernente regolamento recante disposizioni per la diffusione e uso della carta nazionale dei servizi) dei dati identificativi dovranno essere conformi a quanto definito dal decreto del Ministro dell'interno 19 luglio 2000 e successive modifiche contenente regole tecniche e di sicurezza relative alla carta d'identità ed al documento di identità elettronici.

4.3 La gestione della CNS

L'ente emettitore è responsabile della gestione del circuito di emissione che a lui fa capo. L'ente dovrà definire le procedure di gestione, personalizzazione e rilascio delle carte CNS e descriverle in un apposito manuale operativo accessibile al pubblico.

L'ente emettitore predispone altresì, eventualmente avvalendosi di terzi, le strutture per l'assistenza agli utenti, la gestione dei malfunzionamenti e l'eventuale sostituzione o rinnovo delle carte in scadenza.

L'ente emettitore che emette carte CNS è responsabile di definire un servizio di "contact center" per l'assistenza, nonché la revoca o sospensione della CNS.

L'ente emettitore può procedere al rinnovo della CNS a seguito di problemi di funzionamento della smart card, di furto, smarrimento o per il fatto che questa ha raggiunto il naturale termine di scadenza, in tal caso è responsabile della revoca automatica della CNS prima dell'emissione di una nuova carta o del suo rinnovo.

Ai sensi degli articoli 2 e 8 del decreto Presidente della Repubblica 2 marzo 2004, n. 117, recante regolamento concernente la diffusione della carta nazionale dei servizi l'ente emettitore ha la facoltà di procedere di propria iniziativa alla revoca della CNS; in tal caso ha l'obbligo di avvertire il titolare esplicitando le motivazioni della revoca.

Il Centro Nazionale per l'informatica nella Pubblica Amministrazione rende disponibile, secondo le modalità descritte sul sito, il software di supporto all'uso della CNS da parte dei cittadini e delle amministrazioni (librerie dei metacomandi, CSP e PKCS#11).

Gli enti che erogano servizi accessibili tramite CNS, dovranno consentire l'utilizzo degli stessi mediante CIE, secondo quanto previsto al punto 4 del decreto del Ministro dell'interno del 19 luglio 2000, e successive modifiche, concernente regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.

4.4 Requisiti per la partecipazione al circuito di emissione della CNS

4.4.1 Produttori

Ai fini della sicurezza dell'intero circuito di emissione, i fornitori di smart card che intendono offrire i propri servizi agli enti emettitori per le fasi di inizializzazione delle smart card, devono rispettare le specifiche previste nel presente documento.
In particolare, i fornitori sono vincolati al rispetto delle specifiche del sistema operativo (APDU) e della struttura interna della carta (file system) pubblicate sul sito del Centro Nazionale per l'informatica nella pubblica amministrazione e sul sito della Carta d'Identità Elettronica.
Ogni consegna di lotti di CNS dovrà essere accompagnata da distinta cartacea o elettronica, da consegnare all'ente emettitore richiedente, dalla quale si evinca il numero di CNS inizializzate ed i relativi numeri seriali.

4.4.2 Enti emettitori

Per quanto riguarda gli enti emettitori, essi devono rispettare caratteristiche di qualità e di affidabilità tali da garantire la sicurezza dell'intero circuito.
In particolare devono:

- Definire le procedure del sistema di emissione e gestione della CNS in modo conforme alle specifiche di qualità previste dalla norma ISO 9000/2000;
- realizzare l'analisi del rischio e delle misure di sicurezza nella gestione dell'intero ciclo di vita della CNS,
- soddisfare i requisiti minimi di sicurezza riportati nel capitolo 5,
- definire modalità di interazione con i produttori ed i certificatori che forniscano adeguate garanzie di affidabilità e sicurezza,
- predisporre un manuale operativo che evidenzi le procedure seguite per la gestione di tutte le fasi del processo di emissione e di gestione della CNS,
- predisporre un manuale utente che illustri le modalità d'uso della CNS, i modi per usufruire dei servizi in rete e le procedure da seguire in caso di smarrimento, furto o timore di compromissione della carta,
- organizzarsi in modo da costituire il riferimento per ogni problema di funzionalità, disponibilità o sicurezza del circuito di emissione, rendendo disponibile un recapito telefonico costantemente attivo,
- predisporre il piano della sicurezza relativo all'intero circuito di emissione.

L'ente emettitore può avvalersi di servizi di terzi per lo svolgimento delle funzioni di emissione della CNS o di parte di esse, purché questi assicurino il rispetto dei requisiti di cui ai precedenti punti.
L'ente emettitore mantiene la responsabilità della sicurezza del circuito di emissione e del rispetto delle normative vigenti in merito alla tutela dei dati personali.

4.4.3 Certificatori

Possono operare come emettitori dei certificati di autenticazione della CNS esclusivamente i certificatori accreditati di cui all'articolo 5 del Decreto Legislativo 23 gennaio 2002, n.10.
Tali soggetti devono operare in aderenza alle vigenti norme che regolano l'emissione e la gestione dei certificati qualificati.
I certificatori che rilasciano certificati di autenticazione CNS sono iscritti in un elenco consultabile in via telematica, tenuto dal Dipartimento per l'Innovazione e le Tecnologie.

5. Misure di sicurezza

Vengono illustrati di seguito i criteri di sicurezza che dovranno essere seguiti nel circuito di emissione della CNS.

Va osservato che il modello adottato permette diverse soluzioni organizzative. Infatti, in funzione delle strategie e dalle scelte di mercato dell'ente emettitore, le strutture schematizzate che concorrono alla produzione e gestione della CNS possono far capo ad un diverso numero di organizzazioni non escludendosi il caso che una stessa organizzazione gestisca l'intero ciclo di vita della CNS.

Poiché le misure di sicurezza non possono prescindere dall'organizzazione, vengono fornite delle indicazioni di carattere generale che devono poi essere calate nell'effettivo contesto operativo. Anche per quanto concerne le soluzioni individuate, sarà compito dell'Ente emettitore definire quelle possibili varianti che consentano una maggiore flessibilità, pur mantenendo equivalenti i requisiti di sicurezza esposti. Pertanto le misure esposte in questo paragrafo devono essere considerate delle linee guida nell'attuazione operativa da parte di ciascuna amministrazione. L'Ente emettitore, peraltro, può adempiere a tali requisiti utilizzando fornitori già in possesso di idonea certificazione o accreditamento nazionale o internazionale.

Ai fini della sicurezza del circuito, l'intero ciclo di vita della CNS deve essere opportunamente tracciato, dal momento di inizio della produzione della carta, fino al ritiro della CNS. Ciascuna attività elementare (produzione, inizializzazione, registrazione, emissione del certificato, personalizzazione, ecc.) deve essere registrata in appositi registri che devono essere sottoscritti con firma dal responsabile dell'attività e conservati in modo protetto.

Di seguito si riportano le misure di sicurezza relative al processo produttivo, ossia alle fasi di produzione, inizializzazione e personalizzazione.

5.1 Sicurezza delle fasi di lavorazione della carta

Durante l'intero processo di lavorazione, le strutture interne della smart card devono essere protette mediante opportuni codici (PIN, codici di trasporto, ecc.) finalizzati a consentire al solo personale autorizzato la modifica di tali strutture.

I codici di protezione devono essere generati in modo casuale, quindi trasmessi e memorizzati in forma cifrata, con modalità tale da rendere possibile il loro utilizzo esclusivamente agli apparati preposti alla lavorazione della carta.

Questi apparati devono inoltre poter operare unicamente sotto il controllo di operatori muniti di opportuna smart card personale (smart card operatore, di seguito specificata) ovvero di altri sistemi di accesso individuale di paragonabile sicurezza.

Il sistema di sicurezza che governa il processo produttivo (fasi di produzione, inizializzazione e personalizzazione) deve assicurare:

- l'autenticazione certa dell'operatore,
- la registrazione di tutte le operazioni effettuate e dei dati utili alla tracciatura del processo,

- la protezione delle informazioni di tracciatura in modo tale da garantirne l'integrità e non ripudio.

5.1.1 Conservazione e trasporto delle carte

Quando le carte non sono in lavorazione, devono essere conservate in locali (di tipo caveau) in grado di assicurare adeguati livelli di sicurezza. Ogniqualvolta le carte devono transitare tra siti diversi, devono utilizzare un trasporto con regolare bolla di consegna che deve essere verificata dal responsabile della Sicurezza della sede di arrivo.

5.1.2 Gestione degli scarti

Ogni lavorazione deve tenere traccia degli eventuali scarti ed i moduli utilizzati per tracciare le attività devono riportare sia il numero delle smart card utili, sia il numero degli scarti non utilizzabili. Sia le smart card utili che le non utilizzabili devono essere conservate nel Caveau. Al centro di emissione devono pervenire sia le smart card utili che gli scarti in modo da poter verificare la corrispondenza con il numero delle carte complessive previste. La distruzione degli scarti può essere effettuata solo da un'apposita commissione con procedura verbalizzata.

5.1.3 Generazione delle chiavi

Il software presente sul sistema di personalizzazione dovrà provvedere a tale operazione in modalità sicura.
A tal fine il sistema dovrà leggere l'identificativo della carta ed accedere all'archivio cifrato contenente i PIN di personalizzazione.
A questo punto sarà possibile attivare la generazione delle coppie di chiavi RSA relative all'autenticazione ed eventualmente alla firma digitale.
Durante questa operazione saranno creati i PIN utente di attivazione delle relative chiavi private.
Tali PIN dovranno essere memorizzati in un archivio cifrato.

5.1.4 Tracciatura delle operazioni

Tutte le operazioni di inizializzazione dovranno essere tracciate in appositi registri elettronici o cartacei. I registri dovranno essere conservati per un periodo non inferiore a 10 anni. In particolare, il registro di entrate/uscite delle smart card dovrà essere compilato per ogni singolo movimento con data ed ora e firmato sia dal Responsabile della Sicurezza, sia dal Responsabile della fase produttiva.

5.1.5 Protezione delle informazioni di tracciatura

Occorrerà predisporre un archivio protetto in grado di contenere tutti i record relativi alle carte prodotte, cifrati con la chiave crittografica presente nella smart card operatore.

La chiave utilizzata per proteggere tali record dovrà essere tenuta in modalità "memorizzazione protetta" all'interno della smart card dell'operatore.

5.1.6 Gestione della smart card dell'operatore

La Smart Card Operatore deve essere generata, attraverso l'uso di software dedicato di generazione, mediante una procedura che assicuri la massima sicurezza del processo. In fase di generazione della carta, saranno registrate su di essa le informazioni di sicurezza (chiavi crittografiche) necessarie per l'accesso ai file protetti e la firma elettronica dei record di tracciatura.
Tale Smart Card dovrà essere consegnata al responsabile del processo produttivo, od a persona da lui delegata, e conservata in cassetta di sicurezza all'interno di un locale accessibile solo dal responsabile della sicurezza.
L'apertura della cassetta di sicurezza contenente tale smart card di firma dovrà avvenire con una procedura che preveda la presenza congiunta del responsabile della sicurezza e del responsabile della smart card.
Ogni accesso alla cassetta contenente la smart card dovrà essere documentato firmando opportuni registri.

5.1.7 Protezione dei flussi di dati

I flussi informativi che durante il processo produttivo si generano tra la struttura di registrazione, il certificatore e la struttura di personalizzazione, devono utilizzare esclusivamente canali sicuri, utilizzanti sistemi di cifratura simmetrica con chiavi di lunghezza almeno pari a 128 bit.

Nel caso di utilizzo di una sessione SSL, dovranno essere impiegati sia i meccanismi di autenticazione del server, sia quelli relativi alle postazioni client.

5.1.8 Misure organizzative

Dovranno essere previste opportune misure organizzative finalizzate a gestire in modo efficace la sicurezza dei siti.
In particolare, dovrà essere presente in ogni sito una opportuna organizzazione della sicurezza che deve prevedere almeno un Responsabile di Sicurezza per turno che risponderà al Responsabile della Sicurezza dell'Organizzazione.

I responsabili della sicurezza dovranno garantire il rispetto di tutte le procedure e le norme previste dalle organizzazioni.

5.2 Misure di sicurezza fisiche

Si riportano di seguito le protezioni minimali, di tipo fisico, che dovranno essere adottate dai centri di produzione, inizializzazione e personalizzazione coinvolti nel processo di emissione della CNS.

5.2.1 Esterno dello stabilimento

L'esterno dello stabilimento deve essere recintato e controllato tramite telecamere.
I cancelli devono essere sempre chiusi e gli utenti, i fornitori e gli spedizionieri non devono avere accesso ai locali interni se non dopo essersi presentati alla reception per il riconoscimento.

Nel caso di ingresso automezzi, il personale addetto alla reception deve avvertire il Responsabile di Sicurezza e/o il magazziniere, i quali ricevono all'esterno gli automezzi dopo che il personale addetto alla reception ha azionato il pulsante di apertura cancelli che si richiuderà automaticamente dopo un tempo predeterminato.

5.2.2 Uffici non inerenti la produzione o la personalizzazione

I dipendenti facenti capo a tali uffici devono avere a disposizione un badge di ingresso con accesso limitato ad aree ben definite.
Tali uffici non hanno particolari policy di sicurezza ma devono essere protetti da intrusioni esterne tramite sensori alle finestre.
Gli impianti di sicurezza devono essere attivati dopo l'orario di chiusura e disattivati prima dell'orario di apertura degli uffici.
Nel caso in cui si debba protrarre l'orario di chiusura o anticipare l'orario di apertura, si dovrà necessariamente avvertire il Responsabile di Sicurezza che opererà di conseguenza.

5.2.3 Guardiola di ingresso e controllo degli ingressi

Per accedere all'edificio deve essere necessario superare una bussola di sicurezza.
Dovrà essere previsto un servizio di guardiania che consentirà l'accesso ai reparti e/o agli uffici solo dopo le operazioni di riconoscimento e/o registrazione.
L'ingresso dovrà essere suddiviso tra:

1) Dipendenti con badge nominativi il cui passaggio è registrato dalla bussola e dal sistema di monitoraggio basato su telecamere.
2) Visitatori che si qualificano al citofono e accedono alla hall tramite la bussola operata dalla guardiola.

La qualificazione e la registrazione in guardiola dei visitatori deve basarsi su un documento di identità valido, di cui deve essere prodotta una fotocopia che sarà archiviata per un anno. Il personale addetto alla reception dovrà avvertire il dipendente a cui il visitatore fa riferimento. Questi dovrà prendere in consegna il visitatore, che verrà munito di un badge personale che verrà restituito alla fine della visita. Su

apposito registro verrà registrato l’orario di ingresso e di uscita che verrà firmato dal dipendente con funzione di accompagnatore.

6. Servizi erogabili

6.1 La firma digitale

La CNS deve essere predisposta per le funzionalità di firma digitale.
La predisposizione della firma digitale può avvenire con due diverse modalità:

a) l'ente responsabile della certificazione delle chiavi di firma è stabilito dall'ente emettitore nell'ambito del circuito di emissione;
b) il titolare della CNS può scegliere il Certificatore responsabile dell'erogazione dei servizi suddetti tra quelli accreditati o notificati secondo la normativa vigente.

Nel caso a) è compito dell'ente emettitore, o di struttura da questi delegata, predisporre una procedura atta a far sì che il titolare della CNS possa disporre della firma digitale al momento del rilascio della carta o in una fase successiva.

Nel caso b) deve essere consegnata al cittadino, nel momento del rilascio della CNS, una busta contenente il PIN utilizzabile per l'installazione della firma digitale sulla carta. Il titolare della CNS può successivamente richiedere l'installazione della firma digitale rivolgendosi ad uno dei certificatori accreditati o notificati secondo la normativa vigente.
Più in dettaglio, il titolare della CNS, provvisto di un documento di identità e ricordando il PIN rilasciato dall'ente emettitore per l'attivazione del servizio di firma digitale, si reca presso un Certificatore che procede ad impostare la smart card in modo che possa essere utilizzata per i processi di firma. Si rileva che la presenza del PIN dedicato all'installazione della firma digitale si rende necessaria per attivare i diritti di scrittura sulla directory dedicata ad ospitare tale servizio. Nel caso in cui l'ente emettitore attivi delle convenzioni con i certificatori di firma, non si esclude la possibilità che lo stesso ente emettitore svolga le funzioni di registration authority per le fasi di identificazione del cittadino.
La predisposizione della smart card per la firma digitale può avvenire utilizzando altre procedure che garantiscano l'aggiornamento del file system in conformità alla certificazione di sicurezza ISO/IEC 15408 (Common Criteria), ITSEC o equivalente della stessa smart card.

6.1.1 I certificati della CNS

La CNS contiene un certificato di autenticazione della carta utilizzato per tutte le funzioni di riconoscimento in rete e che, in combinazione con il PIN utente, permette l'utilizzo dei servizi in rete da parte del titolare. Tra le informazioni, il certificato contiene anche, nel campo common name, il codice fiscale del titolare.
La CNS, nel caso in cui venisse installato il servizio di firma digitale, contiene un certificato di firma digitale conforme al D.P.R. 445/2000 e successive modificazioni.

6.2 Pagamenti informatici

Attraverso opportuni protocolli d'intesa tra le Pubbliche Amministrazioni, le banche e le poste, è possibile utilizzare la CNS per funzioni di pagamento tra privati e Pubbliche Amministrazioni.

In tal caso le banche e le poste renderanno disponibile il software per la gestione delle funzioni di pagamento, specifico per la CNS.

6.3 La carta sanitaria

L'installazione facoltativa della componente sanitaria (Netlink) sulla CNS avviene in due fasi distinte:

- inizializzazione della CNS a cura dei produttori;
- formazione della CNS e caricamento dei dati sanitari.

Nella prima fase i produttori, delegati dall'Ente emettitore, predispongono le strutture dati sanitarie (secondo le specifiche Netlink), compilano i file elementari che non contengono dati specifici del cittadino e caricano le quantità di sicurezza derivate dalle chiavi di gruppo fornite dal Ministero della Salute.
I produttori devono garantire la segretezza delle chiavi di gruppo, conservandole in dispositivi che ne consentano l'utilizzo al fine di inizializzare le carte, ma ne impediscano la lettura o l'esportazione. L'Ente emettitore renderà disponibili, in modo sicuro, le chiavi di gruppo ai produttori previa autorizzazione del Ministero della Salute. Quest'ultimo ha il compito di definire le modalità di consegna e di conservazione delle quantità di sicurezza e la conseguente tracciatura.

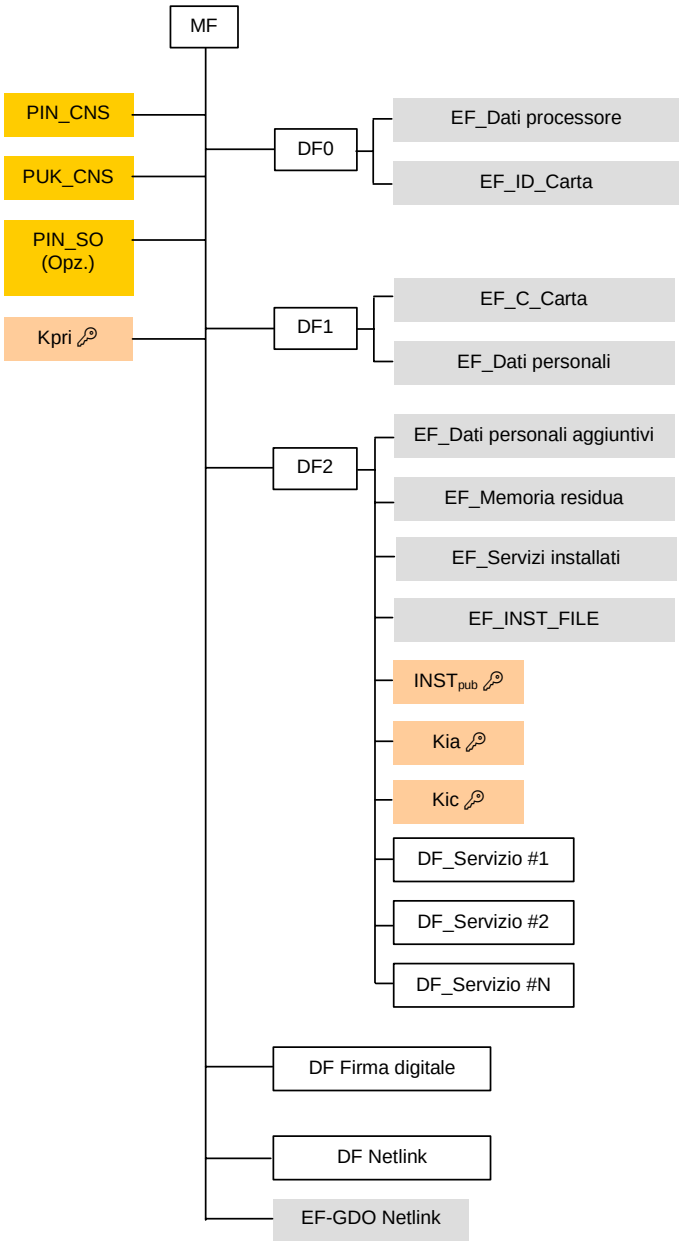
Per la gestione della seconda fase (personalizzazione e caricamento dei dati sanitari), le Regioni possono costituire Centri Servizi Regionali omologati per il territorio di competenza.
La realizzazione della seconda fase può avvenire secondo le modalità che sono di seguito brevemente descritte e che possono essere liberamente scelte dagli enti emettitori:

- si utilizza un Centro Servizi Regionale il quale, per gli Enti emettitori che effettuano questa scelta, effettua la fase di formazione della CNS, l'installazione dei dati sanitari ed eventualmente il rilascio;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale; in questo caso durante la fase di formazione sono installati i dati sanitari tramite collegamento con le ASL con cui gli Enti Emettitori hanno stabilito una opportuna convenzione;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS oppure si avvalgono di un Centro Servizi diverso da quello Regionale e, dopo la fase di formazione e prima del rilascio ai cittadini, inviano i lotti di CNS al Centro Servizi Regionale affinché possano essere caricati i dati sanitari;
- gli Enti emettitori gestiscono autonomamente la formazione della CNS predisponendo le strutture dati secondo quanto specificato in questo paragrafo e la rilasciano senza dati sanitari; i cittadini si recano presso gli sportelli delle amministrazioni competenti con cui l'ente emettitore avrà preventivamente stabilito accordi.

7. Bibliografia di Riferimento

- Schema per il circuito di emissione della Carta di Identità elettronica,
  Roma 22 dicembre 1999 – AIPA /Associazioni dei fornitori – Gruppo di lavoro Carta d'Identità Elettronica;
- Processo di autenticazione in rete. Roma 22 dicembre 1999 – AIPA /Associazioni dei fornitori – Gruppo di lavoro Carta d'Identità Elettronica;
- ISO/IEC 9594-8:2001 per il formato dei Certificati Digitali, le estensioni e le policy;
- ISO/IEC 10118-3:1998 per la funzione di Hash SHA-1;
- PKCS#11 per l'interfacciamento delle smart card.
- ISO/IEC 7816-1-2-3-4-5-6-7-8-9-10 per la parte relativa al microchip.
- Allegato tecnico al Protocollo d'intesa per la realizzazione dei progetti Carta d'Identità Elettronica e Carta Nazionale dei servizi – 13 maggio 2003.

8. ALLEGATO 1 – Struttura del file system



ALLEGATO 2 - Struttura del certificato di autenticazione, interoperabilità con la CIE e relative modalità di aggiornamento

La struttura del certificato di autenticazione è definita dal CNIPA e pubblicata sul sito internet del medesimo Centro nazionale.
Le relative modalità d'uso per l'interoperabilità con la CIE sono definite dal CNIPA in accordo con il Ministero dell'Interno e sono pubblicate sul medesimo sito internet.