

## **DECRETO MINISTERO DELL'INTERNO 2 agosto 2005**

*(pubblicato nella Gazzetta Ufficiale n. 187 del 12 agosto 2005)*

**MODIFICAZIONI AL DECRETO MINISTERIALE 19 LUGLIO 2000, RECANTE: "REGOLE TECNICHE E DI SICUREZZA RELATIVE ALLA CARTA D'IDENTITA' E AL DOCUMENTO D'IDENTITA' ELETTRONICI"**

Il Ministro dell'Interno

Visto l'art. 2 della legge 15 maggio 1997, n. 127, come modificato dall'art. 2, comma 4, della legge 16 giugno 1998, n. 191;

Visto il regio decreto 18 giugno 1931, n. 773, ed il regio decreto 6 maggio 1940, n. 635;

Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;

Vista la legge 9 ottobre 2002, n. 222;

Visto il decreto ministeriale 14 maggio 2003 e il decreto ministeriale 6 novembre 2004;

Considerato che la legge 31 marzo 2005, n. 43 ha disposto che dal 1° gennaio 2006 la carta d'identità su supporto cartaceo venga sostituita, all'atto della richiesta del primo rilascio o del rinnovo del documento, dalla carta d'identità elettronica;

Ravvisata, pertanto, la necessità e l'urgenza di apportare alcune modifiche al decreto del Ministro dell'interno in data 19 luglio 2000, modificato con decreto ministeriale 14 maggio 2003 e il decreto ministeriale 6 novembre 2003 recante regole tecniche e di sicurezza relative alla carta d'identità e al documento di identità elettronici, in attuazione delle disposizioni contenute nell'art. 7-vicies ter della legge n. 43 del 2005;

Tenuto conto delle indicazioni e delle proposte presentate dal Gruppo interministeriale di lavoro incaricato di collaborare alla realizzazione della fase di consolidamento e razionalizzazione della sperimentazione della carta d'identità elettronica, istituito con decreto ministeriale 25 gennaio 2004 in attuazione delle disposizioni contenute nell'art. 7-vicies ter della legge 31 marzo 2005, n. 43;

Tenuto conto delle direttive dell'Unione europea sul passaporto elettronico;

Decreta:

### **Art. 1.**

Il decreto del Ministro dell'interno 19 luglio 2000 di cui in premessa, é modificato come segue.

«All'art. 1 (Definizioni) - Sono modificate:

la lettera d-bis): per «porta applicativa» la porta di accesso, attraverso il backbone, ai domini applicativi del CNSD;

la lettera l): per «sito» sito web della carta d'identità elettronica accessibile all'indirizzo internet

www.servizidemografici.interno.it;

Sono aggiunte le lettere:

m) per «certificato qualificato» il certificato elettronico conforme ai requisiti di cui all'allegato I della direttiva n. 1999/93 CE, rilasciato da certificatori che rispondono ai requisiti di cui all'allegato II della medesima direttiva;

n) per «finalità istituzionali»: utilizzo della CIE per nome e per conto del Ministero dell'interno.

## **Art. 2.**

L'allegato B del decreto ministeriale 19 luglio 2000 del Ministro dell'interno é modificato come segue:

Il punto 4.3 é sostituito dal seguente:

4.3 - Microprocessore (fa riferimento all'art. 8, comma 1 del D.M.).

E' composto da un circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, e da un circuito integrato (chip), incastonati sulla scheda.

Per la CIE, é richiesta una memoria EEPROM dalla capacità non inferiore a 32KBytes.

In particolare per la CIE sono ammissibili tagli di memoria EEPROM da 32KBytes, 64KBytes, 66KBytes e 72KBytes.

Il coprocessore crittografico della CIE deve implementare almeno, per le operazioni di crittografia asimmetrica, l'algoritmo RSA a 1024 bit.

In particolare per la CIE sono ammissibili, per la crittografia asimmetrica, algoritmi RSA da 1024, 2048, o 3072 bit e algoritmi ellittici ECDSA con curve raccomandate da 224 a 283 bit.

Il chip della CIE deve essere almeno a tecnologia contact, secondo lo standard ISO 7816.

In particolare per la CIE sono ammissibili sia la tecnologia contact che, in aggiunta a questa, la tecnologia contactless, eventualmente implementata su un secondo processore a bordo della CIE stessa, i cui standard di riferimento sono l'ISO 14443 per le proximity card e l'ISO 15693 per le vicinity card.

Il microprocessore a bordo della CIE deve quindi essere almeno conforme ai seguenti standard di riferimento:

ISO 7816-3

ISO 7816-4

ISO 7816-8.

Il microprocessore a bordo

della CIE deve inoltre:

- a. rispettare tutte le specifiche riportate nel presente documento;
- b. rispettare le specifiche del sistema operativo (APDU) pubblicate sul sito della Carta d'Identità Elettronica;
- c. aver superato i test di compatibilità predisposti dal Ministero dell'interno.

A tal fine ogni fornitore di chip dovrà realizzare e rendere disponibile al Ministero dell'interno un ambiente di test per il chip che consenta di verificare tutte le funzionalità richieste dal Ministero e dichiarate dal fornitore per il chip stesso, sia per le fasi di inizializzazione, sia per successive fasi di rilascio ed uso, nonché per installazione ed uso di firma elettronica. Tale ambiente sarà utilizzato dal laboratorio di sicurezza del CNSD per le verifiche del caso.

Il punto 4.4 é sostituito dal seguente:

4.4 Dati (fa riferimento all'art. 13, comma 1, lettera d) del D.M.).

Di seguito é riportato il formato elettronico dei dati previsti nella CIE.

| <b>Descrizione campo</b>  | <b>Tipo</b>         |
|---|---------------------|
| Numero assegnato al documento..   | in bianco           |
| Comune che emette il documento....  | carattere           |
| Data di emissione del documento...  | carattere data      |
| Data di scadenza del documento....  | carattere data      |
| Cognome....   | carattere           |
| Nome....  | carattere           |
| Data di nascita....   | carattere data      |
| Sesso....   | carattere (M/F)     |
| Statura (cm.)....   | carattere           |
| Codice fiscale....  | carattere           |
| Cittadinanza....  | carattere           |
| Comune/Stato estero di nascita....  | carattere           |
| Estremi atto di nascita....   | carattere           |
| Comune di residenza....   | carattere           |
| Indirizzo....   | carattere           |
| Firma del titolare....  | BMP JPG (fattore 5) |
| Eventuale annotazione in caso di non validità del documento per l'espatrio....  | Logico              |
| Fotografia 23 x 28 mm. - 200 dpi 16 MI di colori (a 24 bit)....   | BMP JPG (fattore 5) |
| Impronte digitali del dito indice di ogni mano 1 "x1" - 500 dpi - 256 liv. di grigio (ove, in una mano, l'impronta del dito indice non fosse disponibile si utilizzerà per la stessa, procedendo in successione: la prima impronta disponibile fra le dita: medio, anulare e mignolo).... | BMP WSQ             |
| Template impronte digitali....  | numerico            |

La dimensione, i formati di dettaglio ed i relativi livelli di protezione, dei vari campi indicati nella tabella, saranno definiti a seguito della elaborazione delle specifiche tecniche di dettaglio.

In particolare nella memoria del microprocessore della CIE sono ammissibili aree di memoria destinate alla memorizzazione delle impronte digitali, in associazione alle apposite sezioni previste per la memorizzazione dei template numerici delle impronte digitali.

Ai fini delle verifiche di validità dei dati e dei certificati memorizzati nella memoria del microprocessore per l'uso della CIE come strumento di accesso a servizi in rete, presso il CNSD risiedono la lista dei certificati CIE revocati (CRL) e i sistemi di convalida anagrafica dell'INA.

Tale lista dei certificati revocati (CRL) é resa disponibile dal CNSD attraverso servizi distribuiti di validazione dei certificati delle CIE (OCSP distribuito) per l'uso della CIE come strumento di accesso a servizi in rete.

Il punto 6 é sostituito dal seguente:

#### 6. Servizi erogabili (fa riferimento all'art. 5 del D.M.).

Le tipologie dei servizi erogabili possono, in sostanza, ricondursi a due: servizi standard, che non necessitano di essere installati sul documento e servizi qualificati che richiedono l'installazione.

Nel caso dei servizi standard si accede al servizio con il semplice riconoscimento tramite digitazione di PIN o inserimento di altre quantità di sicurezza. I servizi standard vengono erogati in piena autonomia dalle amministrazioni interessate.

Richiedono invece l'installazione sulla carta, quei servizi (detti qualificati) che necessitano di informazioni aggiuntive da memorizzare sul microprocessore. L'installazione dei servizi qualificati é effettuata presso i Comuni, con l'eccezione del servizio di firma digitale disciplinata dal decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, che deve essere effettuata utilizzando un certificatore accreditato ai sensi del medesimo decreto.

Il Ministero dell'interno, conformemente alla normativa vigente in materia, genera direttamente certificati qualificati per la firma digitale dei pubblici ufficiali. Tali certificati, installati all'interno della CIE, ai sensi dell'art. 29-quinquies del decreto del Presidente della Repubblica, 28 dicembre 2000, n. 445, possono essere utilizzati esclusivamente per lo svolgimento di attività istituzionali. Nella CIE può comunque essere inserito almeno un ulteriore certificato qualificato per la firma digitale, rilasciato al titolare per l'utilizzo al di fuori delle finalità istituzionali.

Ai Comuni spetta l'attività di sportello di registrazione per le attività di riconoscimento certo del titolare. I Comuni garantiranno quindi la correttezza delle generalità del soggetto per il quale, direttamente, ovvero ai sensi dell'art. 2, comma 1, del presente decreto, richiederanno al certificatore accreditato, con le modalità stabilite dal Ministero dell'interno, il rilascio di un certificato qualificato.

In caso di smarrimento o furto della CIE, il titolare segnala l'episodio attenendosi alle modalità vigenti in materia.

Conseguentemente, il Comune dovrà provvedere direttamente e tempestivamente, ovvero ai sensi dall'art. 2, comma 1, del presente decreto, a richiedere la revoca del certificato di firma digitale al

certificatore che lo ha emesso.

Nei certificati qualificati rilasciati ai titolari per l'utilizzo della firma digitale al di fuori delle finalità istituzionali, non devono essere inseriti titoli, ruoli, appartenenza ad organizzazioni o altri dati la cui presenza non é obbligatoria, ai sensi delle norme che regolano il rilascio dei certificati qualificati per la firma digitale.

Il Ministero dell'interno fornisce ai Comuni le quantità di sicurezza necessarie per l'inserimento nella CIE degli elementi inerenti il servizio qualificato di firma digitale. L'inserimento nella CIE dei certificati di firma digitale e delle relative quantità di sicurezza effettuata ai sensi del presente paragrafo non deve essere tale da alterare i profili di protezione utilizzati per la certificazione di sicurezza dei supporti informatici della CIE, ai sensi dell'art. 52, comma 3, del decreto del Presidente del Consiglio dei Ministri, 13 gennaio 2004.

Il punto 6.1 Le liste dei servizi e la lista delle carte interdette (black-list), é sostituito dal seguente:

6.1 Le liste dei servizi e la lista delle carte interdette (black-list).

Le liste dei servizi sono indispensabili per poter procedere all'installazione dei servizi qualificati sulla carta. Solo i servizi presenti in tale lista possono essere installati sulla carta.

Le liste dei servizi contengono almeno le seguenti informazioni:

Identificativo del servizio

Formato della struttura dati da creare sulla carta (se presente)

Chiave di autenticazione del server erogatore (Spub)

Spazio richiesto in EEPROM (memoria) del microcircuito

Informazioni descrittive del servizio.

Esistono due tipologie di liste dei servizi:

La lista dei servizi nazionali (mantenuta da SSCE)

Le liste dei servizi comunali (mantenute dai Comuni).

La lista nazionale presso il SSCE e le liste comunali interoperano secondo modalità e standard specifici. La lista nazionale contiene l'elenco dei servizi nazionali e l'elenco dei servizi ultracomunali.

Per servizi ultracomunali si intendono quelli che un Comune rende disponibili al di fuori della sua competenza territoriale.

Il software di sicurezza rilasciato ai comuni, al fine dell'installazione dei servizi, deve interoperare sia con la lista nazionale sia con l'eventuale lista comunale.

La predisposizione e la gestione della lista dei servizi comunali é affidata alla responsabilità del

comune.

La predisposizione e la gestione della lista dei servizi nazionali é affidata al SSCE. Le amministrazioni centrali che intendono offrire servizi qualificati devono richiedere una autorizzazione al Dipartimento della Funzione Pubblica specificando i motivi per cui si ritiene necessario utilizzare questa tipologia di servizio, le modalit  di installazione ovvero aggiornamento (nel caso si tratti di un servizio gi  esistente) e, in caso di parere favorevole, presentare al SSCE un documento in cui si evidenzia:

la descrizione del servizio da erogare;

le modalit  tecniche attraverso le quali sar  garantito il servizio;

l'organizzazione a supporto del sistema di erogazione del servizio.

Ai fini delle verifiche di validit  delle CIE come strumento di accesso a servizi in rete, presso il CNSD risiedono la lista dei certificati CIE revocati (CRL) e i sistemi di convalida anagrafica dell'INA.

Tale lista dei certificati revocati (CRL) é resa disponibile dal CNSD attraverso servizi distribuiti di validazione dei certificati delle CIE (OCSP distribuito) per l'uso della CIE come strumento di accesso a servizi in rete.

Il punto 6.2 - Modalit  di riconoscimento in rete, é sostituito dal seguente:

#### 6.2 - Modalit  di riconoscimento in rete.

In considerazione dell'architettura definita per la carta d'identit  elettronica e dell'utilizzo della componente microchip per il riconoscimento in rete della carta nei confronti di un server applicativo che eroga dei servizi, la soluzione che si é scelta é quella della Strong Authentication che richiede l'utilizzo di funzioni tipiche di una Public Key infrastructure, basata sul sistema di Certification Authority presso SSCE. La verifica dello stato di revoca o sospensione dei certificati emessi da tale sistema di CA, é resa disponibile dal CNSD attraverso servizi distribuiti di validazione dei certificati delle CIE (OCSP distribuito), mentre la convalida anagrafica dei dati é resa disponibile attraverso i servizi di convalida anagrafica del CNSD.

Il punto 6.2.1 Crypto Middleware ed API PKCS11, é sostituito dal seguente:

#### 6.2.1 Crypto Middleware ed API PKCS11.

Il Cripto Middleware é costituito dalle applicazioni (piattaforme) che il Ministero dell'interno mette a disposizione dei Client, che operano su reti aperte, per gestire i servizi di cifratura/decifratura, verifica dello stato dei certificati e convalida anagrafica. Orientativamente, tali piattaforme svolgono le seguenti funzioni:

Richiesta di certificazione di chiavi pubbliche  
Richiesta di revoca certificati  
Accesso ai servizi di OCSP distribuito di interrogazione dello stato di un certificato;

Accesso ai servizi di convalida anagrafica dei dati anagrafici presenti sulla CIE;

Parsing dei Certificati Digitali

Costruzione di strutture PKCS7

Interfaccia ad alto livello verso le funzioni di cifratura.

Queste piattaforme, a loro volta, poggiano su strati software, o API, che le isolano dai dispositivi di cifratura, tipicamente le Smart Card.

Le API più comunemente usate sono le PKCS11, le cui caratteristiche salienti sono:

Consentire ai Crypto Middleware di prescindere dai dispositivi che memorizzano chiavi e sviluppano crittografia Fornire ai Crypto Middleware una interfaccia standard Rendere portabili le applicazioni negli ambienti in cui la crittografia é trattata con queste API.

Il punto 6.2.2 Processo di Strong Authentication, é sostituito dal seguente:

6.2.2 Processo di Strong Authentication.

Questo processo consente l'identificazione da remoto della carta, la sua verifica e la convalida dei dati anagrafici ad essa associati, per la fruizione dei servizi erogati da una applicazione residente presso una Pubblica Amministrazione Centrale.

Orientativamente, i passi previsti dalla procedura sono:

1. L'applicazione client stabilisce la comunicazione con l'applicazione server.
2. L'applicazione server richiede all'applicazione client il file «C Carta» contenente il certificato (ID Carta più la chiave pubblica Kpub della carta).
3. L'applicazione client interroga la carta e legge tale file mediante i comandi APDU SELECT FILE (C Carta), READ BINARY.
4. L'applicazione client invia il file «C Carta» al server.
5. L'applicazione server verifica la validità del certificato mediante SSCEpub ed estrae da esso ID Carta e Kpub.
6. L'applicazione server accede ai servizi di OCSP distribuito resi disponibili dal CNSD per verificare lo stato del certificato ricevuto.
7. L'applicazione server, quando abilitata dal Ministero dell'interno, accede ai servizi di convalida anagrafica resi disponibili dal CNSD per associare l'ID carta con i dati anagrafici del cittadino.
8. L'applicazione server genera una stringa di challenge e la invia al client rimanendo in attesa della risposta.
9. L'applicazione client seleziona Kpri mediante il comando MSE (Manage Security Environment). In tal modo Kpri é attivata e verrà usata in tutte le successive operazioni di cifratura effettuate dalla carta. Mediante il comando PSO (Perform Security Operation) la

carta esegue la cifratura del challenge usando Kpri precedentemente attivata, e restituisce all'applicazione client la stringa ottenuta.

La chiave privata che é stata generata dalla carta in fase di inizializzazione, risulta invisibile dall'esterno e comunque impossibile estrarla dalla carta.

10. Il client invia al server in attesa il challenge firmato ricevuto dalla carta.
11. L'applicazione server verifica la stringa ricevuta e la confronta con il challenge precedentemente generato.

Se tale confronto ha esito positivo la carta é autenticata. A questo proposito é necessario che l'algoritmo di verifica, residente sul server, sia compatibile con quello usato dalla carta per cifrare il challenge.

Il punto 6.2.3 Comandi di gestione utilizzati dalla Strong Authentication, é sostituito dal seguente:

#### 6.2.3 Comandi di gestione utilizzati dalla Strong Authentication.

La norma ISO 7816 parte 4 e parte 8 definisce, oltre alla struttura del File System, anche i comandi per interagire a livello applicativo. Tali comandi sono chiamati APDU (Application Protocol Data Unit). L'insieme delle APDU della CIE é pubblicato sul sito del CNSD, insieme alle librerie di gestione di tali APDU.

Il punto 6.4 Strong Authentication lato Server, é sostituito dal seguente:

#### 6.4 Strong Authentication lato Server.

Quanto affermato nei precedenti paragrafi é un solido punto di partenza per risolvere il problema della autenticazione forte in rete per quanto concerne il Client e la CIE. é ora necessario definire la componente server del processo di autenticazione.

La figura [4] illustra i componenti che intervengono nel processo di autenticazione. (*omissis*)

Il punto 7.4.1.1 é sostituito dal seguente:

#### 7.4.1.1 Sottofase di compilazione.

Il Comune riceve i «documenti in bianco» da parte della Prefettura;

Tramite il software di sicurezza, le informazioni del titolare sono riportate dal Comune nel sistema.

I dati sono quelli indicati in dettaglio al paragrafo 4.4.

La fotografia può essere catturata direttamente, tramite videocamera digitale o digitalizzata per mezzo di uno scanner, in conformità alle norme ICAO sui formati di memorizzazione dei dati

biometrici.

Anche per digitalizzare la firma del titolare può essere utilizzato uno scanner oppure può essere catturata direttamente tramite tavoletta grafica.

Per l'impronta digitale, il Comune deve utilizzare un lettore di impronte digitali (live scan);

Generazione della coppia di chiavi Kpub e Kpri (della carta) necessarie per garantire l'autenticazione in rete della carta e generazione del PIN utente per la protezione dei dati personali. é ammissibile per la CIE un ulteriore PIN per abilitare le operazioni di crittografia asimmetrica che utilizzano la Kpri della carta per l'autenticazione in rete. La generazione di queste chiavi avviene all'interno del microprocessore.

Cifratura simmetrica dei dati almeno a 128 bit. La cifratura viene eseguita automaticamente dal software di sicurezza. La cifratura é indispensabile per proteggere i dati durante la trasmissione al SSCE utilizzando la Kpub-enc del SSCE stesso con una chiave di trasporto almeno da 128 bit generata in maniera dinamica sessione per sessione;

Apposizione del bollo elettronico del Comune, per mezzo della Kpri-aut (Comune). L'apposizione di tale bollo garantisce il mittente al SSCE;

Invio della richiesta di emissione carta d'identità al SSCE per via telematica.

Il punto 8.4 é sostituito dal seguente:

#### 8.4. Procedure per l'installazione della firma digitale.

Per l'installazione del servizio qualificato di firma digitale, i Comuni che intendono erogare questo servizio, ne danno comunicazione al Ministero dell'interno, entro il 30 giugno o il 31 dicembre di ogni anno unitamente al piano dei fabbisogni di supporti informatici della CIE, trasmettendo copia del contratto pubblico, stipulato con il certificatore, prescelto, accreditato ai sensi del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445, contenente l'indicazione delle regole tecniche necessarie per erogare il servizio di firma digitale.

Il Ministero dell'interno, esaminata la documentazione predetta, approva il piano dei fabbisogni e la conformità delle regole tecniche a quanto stabilito per il circuito di emissione e trasmette tali informazioni, entro novanta giorni, dalla ricezione, all'Istituto Poligrafico e Zecca dello Stato per la predisposizione della fase di inizializzazione in maniera conforme alle regole tecniche ricevute.

Per quanto concerne le CIE già inizializzate al 1° gennaio 2006, i Comuni installano il servizio di firma digitale attenendosi alle specifiche regole tecniche di sicurezza, emanate dal Ministero dell'interno e pubblicate sul sito.

Il punto 8.5. é sostituito dal seguente:

## 8.5 Impronte digitali.

Nella memoria del microchip della CIE sono installati i template numerici delle impronte digitali del titolare della carta.

Il template é una rappresentazione numerica di un elemento biometrico (in questo caso l'impronta di due dita) e viene utilizzato ai fini di riconoscimento dell'impronta originale pur non consentendone una sua qualsivoglia ricostruzione. Tale riconoscimento non presuppone la presenza di nessuna banca dati avvenendo il confronto direttamente tra il template memorizzato sulla CIE e quello generato durante la fase di lettura da parte dello specifico reader utilizzato dalla postazione client che richiede il servizio. Nessuna traccia dell'operazione rimane sul client o sul server. Un simile confronto garantisce, per i servizi che lo richiedano, la presenza fisica del titolare della CIE.

Al fine di evitare qualsivoglia possibilità di manipolazione successiva, lo spazio dedicato alla memorizzazione del template, dopo la sua installazione, viene reso non riscrivibile. Più in dettaglio, durante la fase di installazione, le impronte assunte tramite lettori sono trasformate in template secondo lo specifico algoritmo fornito dal Ministero dell'interno e memorizzate nell'area dedicata assieme ad un progressivo che può variare da zero a nove in funzione delle dita utilizzate per l'assunzione dell'impronta. Anche la fase di installazione delle impronte non comporta la memorizzazione di dati sulle postazioni dei Comuni emettitori.