

Decreto del Ministro dell'interno 19 luglio 2000

“Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.”¹

G.U. 21 luglio 2000, n. 169- S.O. n. 116

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;
- Visti il regio decreto 18 giugno 1931, n. 773 ed il regio decreto 6 maggio 1940, n. 635;
- Vista la legge 31 dicembre 1996, n. 675;
- Visto il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;
- Sentita l'Autorità per l'informatica nella pubblica amministrazione;
- Sentita la Conferenza Stato-città ed autonomie locali, che ha espresso il proprio avviso nella riunione del 22 giugno 2000;

DECRETA

Capo I - Principi generali

1. Definizioni.

1. Ai sensi del presente decreto si intende:

- a. per «D.P.C.M.»: il decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437;
- b. per «documento»: la carta d'identità elettronica e/o il documento d'identità elettronico di cui all'art. 2 del decreto del Presidente del Consiglio dei Ministri costituito dall'insieme del supporto fisico e dei supporti informatici;
b-bis) per «C.N.S.D.»: il Centro nazionale dei servizi demografici costituito con il decreto ministeriale 23 aprile 2002
- c. per «S.S.C.E.»: il sistema di sicurezza del circuito di emissione dei documenti;

¹ Decreto rettificato con il D.M. 6 novembre 2003 - “Rettifica al D.M. 19 luglio 2000 recante regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.” e modificato con il D.M. 2 agosto 2005 - “Modificazioni al D.M. 19 luglio 2000, recante: «Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici».”

- c-bis. per «I.N.A.»: l'Indice nazionale delle anagrafi istituito con legge 28 febbraio 2001, n. 26, per la fornitura dei servizi di convalida anagrafica durante l'emissione e l'uso del documento;
- c-ter. per «Backbone»: il backbone INA/SAIA di sicurezza e certificazione per l'accesso ai servizi di convalida e di aggiornamento dell'INA;
- d. per «S.A.I.A.»: il sistema predisposto dal Ministero dell'interno per l'accesso e l'interscambio anagrafico;
- d-bis. per «porta applicativa»: la porta di accesso, attraverso il backbone, ai domini applicativi del C.N.S.D.;
- e. per «Istituto»: l'Istituto Poligrafico e Zecca dello Stato;
- f. per «dati»: i dati identificativi della persona di cui all'art. 1, comma 1, lettera *d*) e gli altri elementi di cui all'art. 3, comma 1, lettere da *b*) ad *h*), del D.P.C.M.;
- g. per «carta-servizi»: l'insieme dei dati di cui alla precedente lettera *f*) - ad esclusione della fotografia e della firma - e delle informazioni amministrative di cui all'art. 1, comma 1, lettera *e*) e dell'art. 3, comma 4, del D.P.C.M.;
- h. per «codice cifrato»: la coppia di codici alfanumerici che identificano univocamente il microprocessore di ogni documento;
- i. per «cartellino elettronico»: la trasposizione, in formato digitale e cifrata, del cartellino cartaceo di cui all'art. 290 del *regio decreto 6 maggio 1940, n. 635*;
- i-bis. per «copia elettronica»: la copia del cartellino elettronico inviata dal S.S.C.E. al C.N.S.D. al momento dell'emissione del documento ed identificata mediante codice fiscale del titolare del documento, ID carta del documento, codice ISTAT del comune emittente;
- j. per «P.I.N.»: il numero identificativo personale necessario alla fruizione dei servizi che ne richiedono l'utilizzo;
- k. per «Comitato tecnico permanente» il Comitato istituito con decreto dirigenziale del Ministero dell'interno in data 20 marzo 2003 con il compito di stabilire la perfetta corrispondenza dei supporti fisici prodotti dall'Istituto alle caratteristiche indicate nell'allegato *B* al presente decreto, nonché l'idoneità tecnica e la compatibilità con il sistema di rete delle attrezzature da utilizzare per l'emissione della C.I.E.;
- l. per «sito»: sito web della carta d'identità elettronica accessibile all'indirizzo internet www.servizidemografici.interno.it;
- m. per «certificato qualificato»: il certificato elettronico conforme ai requisiti di cui all'allegato I della *direttiva 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.

2. Funzioni dei comuni.

1. Le funzioni di pertinenza dei comuni possono essere esercitate anche in forma associata.

2. I comuni, nel rispetto delle regole tecniche e di sicurezza di cui all'allegato *B* al presente decreto, predispongono in piena autonomia i servizi locali.

3. Modalità di connessione.

1. Le amministrazioni e gli enti che, ai sensi della normativa vigente e del D.P.C.M., esercitano funzioni e svolgono compiti nell'ambito delle procedure di produzione, trasmissione, formazione, rilascio, rinnovo, aggiornamento e relativa verifica dei documenti si connettono al S.S.C.E. con le modalità di cui all'allegato *B* e devono provvedere all'aggiornamento dell'I.N.A. e all'accesso ai servizi di convalida anagrafica tramite collegamento su backbone al C.N.S.D.

4. Misure di sicurezza.

1. Ai fini della produzione, del rilascio, dell'aggiornamento e del rinnovo dei documenti, il trattamento dei dati, da parte delle amministrazioni e degli enti indicati dall'art. 3, comma 1, è effettuato nel rispetto dell'art. 15 della *legge 31 dicembre 1996, n. 675* e delle disposizioni di cui al *decreto del Presidente della Repubblica 28 luglio 1999, n. 318*, nonché delle ulteriori prescrizioni tecniche descritte nell'allegato *B*.

5. Servizi e modalità di autenticazione.

1. Ai sensi dell'art. 3, comma 4, e dell'art. 7, comma 1, del D.P.C.M. tutti i servizi che non implicano la memorizzazione dei dati sui documenti sono predisposti in piena autonomia dalle amministrazioni. Le modalità di autenticazione in rete per l'accesso ai servizi da parte del titolare del documento sono definite nell'allegato *B*.
2. Per i servizi che richiedono la memorizzazione di dati sui documenti è necessaria l'installazione degli stessi da parte del comune e, qualora relativi a dati sensibili, la richiesta dell'interessato.
3. I servizi nazionali che richiedono la memorizzazione di dati sui documenti sono predisposti con le modalità e nel rispetto delle regole tecniche di cui all'allegato *B*.

Capo II - Regole tecniche di base

5-bis. Diffusione della documentazione.

1. Tutta la documentazione ufficiale, normativa e tecnica, relativa alla carta d'identità elettronica è pubblicata sul sito.

5-ter. C.N.S.D. e software di sicurezza.

1. Il C.N.S.D., con le modalità di cui all'allegato *B*, rende disponibile:
 - il software della porta applicativa di accesso al backbone, ai fini dell'utilizzazione dei servizi dell'I.N.A. da parte degli Enti emettitori;
 - il software di supporto all'uso in rete del documento, ai cittadini, ai comuni e alle amministrazioni ed enti interessati;
 - il servizio di convalida INA dell'ID carta, attraverso backbone, direttamente dall'INA o dalle anagrafi comunali;
 - le specifiche del file system del documento a chi ne faccia motivata richiesta;
 - un servizio di certificazione dei server che erogano servizi tramite il documento. Tale servizio è reso disponibile direttamente dal Ministero dell'interno e attraverso strutture dallo stesso riconosciute.

6. S.S.C.E. e software di sicurezza.

1. In attuazione dell'art. 8, commi 1 e 4, del D.P.C.M. il Ministero dell'interno - Dipartimento della pubblica sicurezza, mette a disposizione delle questure e dei comuni l'infrastruttura organizzativa, informatica e di rete del Centro elaborazioni dati della Polizia scientifica per la realizzazione, la gestione e la manutenzione del S.S.C.E., nonché fornisce ai comuni un *software* di sicurezza finalizzato a garantire l'integrità, l'accessibilità e la riservatezza delle informazioni nelle fasi di compilazione, rilascio, aggiornamento, rinnovo e verifica dei documenti.
2. Ai sensi dell'art. 6, comma 1, del D.P.C.M. le questure, nei casi previsti dallo stesso articolo, procedono all'interdizione dell'operatività del documento secondo le modalità descritte nell'allegato *B*.
3. Le questure, ai sensi dell'art. 290 del *regio decreto 6 maggio 1940, n. 635*, conservano il cartellino elettronico, a cui accedono in via esclusiva, relativo ai documenti rilasciati dai comuni della stessa provincia.

6-bis. Utilizzo delle infrastrutture di servizio C.N.S.D. e S.S.C.E. da parte di altri circuiti di emissione.

1. Il supporto informatico del documento ne rende possibile l'utilizzo, con le modalità di cui all'allegato *B*, da parte di altri circuiti di emissione.
2. Le modalità di accesso e di utilizzo delle infrastrutture di servizio C.N.S.D e S.S.C.E. devono di volta in volta essere concordate con il Ministero dell'interno.

7. Supporto fisico.

1. Il supporto fisico del documento è costituito da una carta plastica conforme alle norme ISO/IEC 7816-1, 7816-2 e ISO/ID-001 ed è integrato dai supporti informatici di cui all'art. 8.
2. Il supporto fisico è stampato con le tecniche tipiche della produzione di carte valori ed è dotato degli elementi fisici di sicurezza atti a consentire il controllo dell'autenticità del documento visivamente e mediante strumenti portatili e di laboratorio.
3. Il documento ha le caratteristiche grafiche di cui al modello approvato con il presente decreto e di cui all'allegato A.

8. Supporti informatici.

1. Il supporto fisico di cui all'art. 7 è dotato di una banda ottica per la memorizzazione, con modalità informatiche di sicurezza, dei dati riportati graficamente sul documento, nonché di un microprocessore per la memorizzazione della carta-servizi e per le operazioni connesse alle procedure di identificazione in rete del titolare del documento. Gli *standard* internazionali, le caratteristiche tecniche e l'architettura logica dei predetti supporti informatici sono conformi alle specifiche indicate nell'allegato B.

8-bis. Comitato tecnico permanente.

1. È istituito un Comitato tecnico permanente cui sono affidati i seguenti compiti:
 - definire e aggiornare costantemente le linee-guida per le attività correlate:
 - a. alla produzione e alla formazione dei supporti fisici;
 - b. alla personalizzazione e al rilascio del documento presso le strutture preposte;
 - dare ausilio alle strutture del Ministero al fine di risolvere tutti i punti critici di ordine tecnico aperti dagli emettitori,
 - certificare le dotazioni delle stazioni di emissione allo scopo di consentire il buon esito dell'emissione del documento.
2. Le determinazioni tecniche assunte dal Comitato tecnico permanente sono pubblicate nel sito www.cartaidentita.it.
3. Il Comitato tecnico permanente è composto da rappresentanti del Ministero dell'interno - C.N.S.D. e S.S.C.E., dell'Associazione nazionale dei comuni d'Italia e dell'Istituto. Qualora necessitasse, il Comitato potrà avvalersi di risorse esterne per risolvere problematiche di propria competenza.
4. In via di prima attuazione del presente articolo, è confermata la costituzione del Comitato come determinata con il *decreto dirigenziale 20 marzo 2003*.

9. Inizializzazione e numerazione del documento.

1. L'Istituto, cui è riservata la produzione dei documenti a norma dell'art. 11 del presente decreto, provvede alla inizializzazione delle componenti fisiche ed informatiche del documento secondo le procedure di sicurezza descritte nell'allegato *B*. A seguito della inizializzazione il documento acquisisce la qualità di documento in bianco.
2. I supporti fisici prodotti nella prima fase di sperimentazione fino all'entrata in vigore del presente decreto recano la numerazione da AA0000001 a AA0155940.

I supporti fisici prodotti dall'entrata in vigore del presente decreto saranno numerati in progressione a partire da 0000001AA.

I numeri non attribuiti non possono essere riassegnati e verranno pubblicati con cadenza trimestrale nella Gazzetta Ufficiale con apposito decreto dirigenziale del Ministero dell'interno.

10. Configurazione hardware e software per la formazione del documento.

1. Ai fini della formazione dei documenti, i comuni utilizzano la configurazione *hardware* descritta nell'allegato *B*.
2. Ai fini della compilazione, rilascio, aggiornamento e rinnovo dei documenti i comuni utilizzano il *software* di sicurezza di cui all'art. 6, comma 1.

Capo III - Norme procedurali

11. Produzione del documento.

1. La produzione del documento è riservata all'Istituto che vi provvede ottemperando alle norme che disciplinano la produzione delle carte valori e dei documenti di sicurezza della Repubblica italiana e agli *standard* internazionali di sicurezza previsti per l'emissione di carte di pagamento.
2. Nella fase di produzione a regime dei documenti elettronici di cui al presente decreto, l'Istituto, nell'ambito di proprio stabilimento, costituisce uno speciale settore con accesso limitato ai dipendenti addetti alle specifiche lavorazioni e sorvegliato dalle Forze di polizia, dotato altresì delle sicurezze fisiche antieffrazione e dei sistemi di sorveglianza elettronica definiti di intesa con il Ministero dell'interno.

12. Trasmissione del documento in bianco in periferia e sua custodia da parte del comune.

1. La trasmissione alle prefetture dei documenti in bianco è effettuata dal Provveditorato generale dello Stato, d'intesa con l'Istituto, in condizioni di sicurezza, mediante affidamento dei plichi a vettori specializzati nel trasporto di valori.
2. Il comune adotta ogni idonea misura per la custodia dei documenti in bianco in condizioni di sicurezza.

13. Procedura di sicurezza per la formazione e rilascio del documento.

1. La formazione ed il rilascio del documento avvengono nel rispetto della seguente procedura di sicurezza:
 - a. il comune, utilizzando le funzionalità del *software* di sicurezza di cui all'art. 10, comma 2, genera un messaggio informatico cifrato, costituito dai dati del richiedente e dal codice cifrato necessario all'identificazione in rete del documento e lo invia telematicamente al S.S.C.E.;
 - b. i dati, ad eccezione del codice fiscale e del numero identificativo del documento, vengono registrati cifrati dal S.S.C.E.; l'accesso ai predetti dati in chiaro è consentito esclusivamente alla questura territorialmente competente;
 - c. il comune, ricevuta la necessaria abilitazione ad emettere il documento da parte di S.S.C.E., riporta i dati identificativi della persona sul microprocessore e sulla banda ottica secondo le modalità indicate nell'allegato *B* ed effettua la stampa di tali dati sul supporto fisico;
 - d. il comune genera il P.I.N., lo stampa su carta chimica retinata in grado di garantire la riservatezza dell'informazione e lo consegna, insieme al documento, al titolare.
2. In via transitoria, i comuni possono avvalersi dell'Istituto ai fini della formazione del documento, utilizzando una configurazione *hardware* conforme ad uno *standard* minimo corrispondente alle dotazioni descritte nell'allegato *B*. In tali casi il *software* di sicurezza provvede ad inoltrare all'Istituto il messaggio informatico di cui al comma 1, lettera *a*). L'Istituto non conserva traccia dei dati utilizzati per la formazione del documento.
3. L'Istituto assicura livelli di servizio che consentono la disponibilità presso le prefetture dei documenti formati entro il termine di venti giorni successivi alla ricezione del messaggio informatico di cui al comma 2.

Capo IV – Sperimentazione²

14. Avvio della fase di sperimentazione.

- [1. I comuni che intendono partecipare alla fase di sperimentazione prevista dall'art. 9 del D.P.C.M. presentano il relativo progetto al Ministero dell'interno.
2. I progetti di cui al comma 1 devono contenere:
 - a. l'indicazione della data di inizio e della durata della sperimentazione e del responsabile del progetto;
 - b. la descrizione delle modalità organizzative in rapporto alla dimensione territoriale della sperimentazione e alla stima del quantitativo, effettuata su base presuntiva, dei documenti da rilasciare nel periodo di sperimentazione;

² Il presente capo e gli artt. 14 e 15 in esso compresi sono stati soppressi ai sensi di quanto disposto dall'art. 1, *D.M. 6 novembre 2003*.

- c. la descrizione delle procedure di gestione e dei flussi di dati con specifico riferimento alle modalità di connessione di cui all'art. 3, la descrizione delle procedure di sicurezza, la descrizione delle procedure di controllo;
 - d. l'analisi dei rischi e la descrizione delle relative contromisure, con specifico riferimento a quelle destinate a prevenire la perdita accidentale delle informazioni trattate;
 - e. l'indicazione dei servizi da erogare relativamente alla carta-servizi.
3. La sperimentazione è autorizzata ai sensi dell'art. 9 del D.P.C.M. in relazione al numero di carte disponibili, tenendo conto dell'ordine cronologico di presentazione dei progetti di sperimentazione.
 4. Il Ministero dell'interno può chiedere che il progetto di sperimentazione venga modificato o integrato. In tal caso si applica la disposizione dell'art. 9, comma 3, secondo periodo, del D.P.C.M.]³.

15. Relazione sullo stato della sperimentazione.

- [1. Il responsabile del progetto trasmette, con cadenza bimestrale, al Ministero dell'interno relazioni sullo stato di avanzamento della sperimentazione.
2. Il Ministero dell'interno trasmette copia del progetto di sperimentazione e delle relazioni sullo stato di avanzamento della sperimentazione al Comitato di monitoraggio previsto dall'art. 10 del D.P.C.M.]⁴

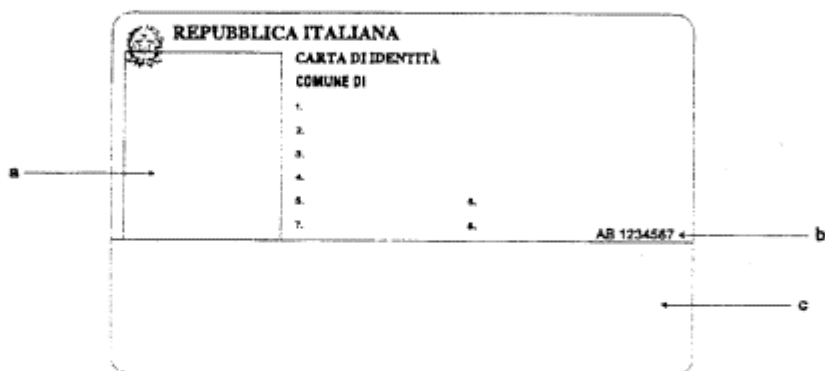
³ Ibidem.

⁴ Ibidem.

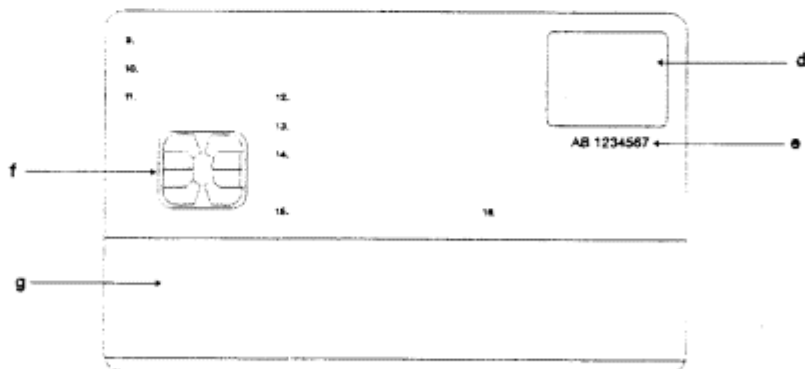
VERSIONE ITALIANO

LEGENDA:

- 1 = COMUNE CHE RILASCIAMO IL DOCUMENTO
- 2 = COGNOME DEL TITOLARE
- 3 = NOME DEL TITOLARE
- 4 = COMUNE DI NASCITA
- 5 = DATA DI NASCITA
- 6 = SESSO
- 7 = ESTREMI ATTO DI NASCITA
- 8 = STATURA (in cm)
- a = fotografia del titolare (dimensioni 23x28 mm)
- b = numero assegnato al documento in bianco
- c = spazio riservato alla codifica ICAO con caratteri OCRB



AII. A - FRONTE -



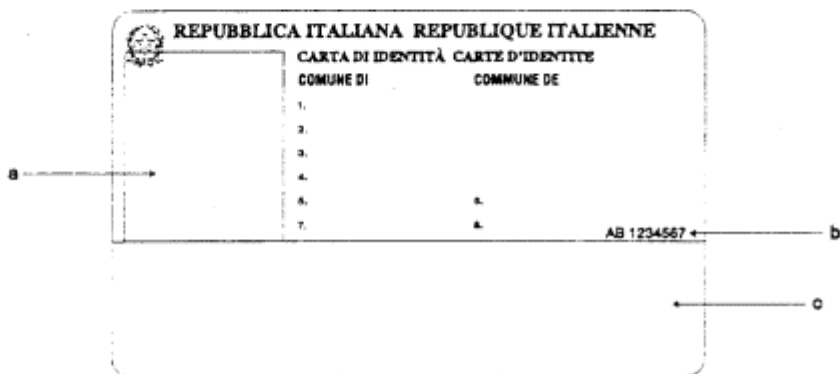
AII. A - RETRO -

- 9 = COMUNE DI RESIDENZA
- 10 = INDIRIZZO
- 11 = DATA EMISSIONE DOCUMENTO
- 12 = DATA SCADENZA DOCUMENTO
- 13 = CITTADINANZA
- 14 = CODICE FISCALE
- 15 = FIRMA
- 16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
- d = ologramma (dimensioni 18x14 mm)
- e = numero assegnato al documento in bianco
- f = modulo CHIP
- g = banda a memoria ottica

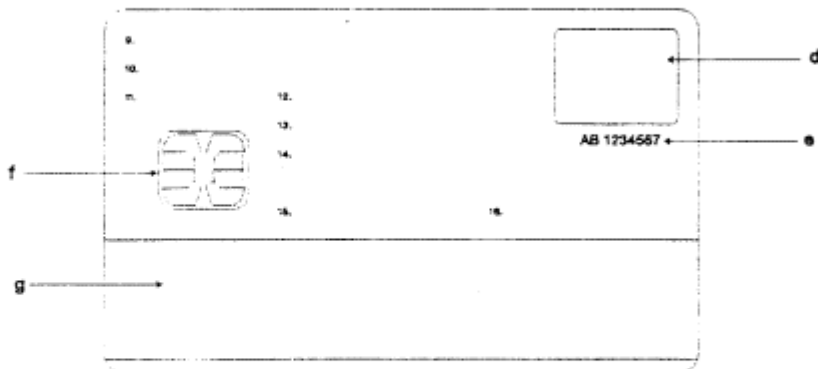
VERSIONE ITALIANO/FRANCESE

LEGENDA:

- 1 = COMUNE CHE RILASCI IL DOCUMENTO
- 2 = COGNOME DEL TITOLARE
- 3 = NOME DEL TITOLARE
- 4 = COMUNE DI NASCITA
- 5 = DATA DI NASCITA
- 6 = SESSO
- 7 = ESTREMI ATTO DI NASCITA
- 8 = STATURA (in cm)
- a = fotografia del titolare (dimensioni 23x28 mm)
- b = numero assegnato al documento in bianco
- c = spazio riservato alla codifica ICAO con caratteri OCRB



AII. A - FRONTE -



AII. A - RETRO -

- 9 = COMUNE DI RESIDENZA
- 10 = INDIRIZZO
- 11 = DATA EMISSIONE DOCUMENTO
- 12 = DATA SCADENZA DOCUMENTO
- 13 = CITTADINANZA
- 14 = CODICE FISCALE
- 15 = FIRMA
- 16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
- d = ologramma (dimensioni 18x14 mm)
- e = numero assegnato al documento in bianco
- f = modulo CHIP
- g = banda a memoria ottica

VERSIONE ITALIANO/FRANCESE

LEGENDA:

- 1 = COMUNE CHE RILASCIÀ IL DOCUMENTO
- 2 = COGNOME DEL TITOLARE
- 3 = NOME DEL TITOLARE
- 4 = COMUNE DI NASCITA
- 5 = DATA DI NASCITA
- 6 = SESSO
- 7 = ESTREMI ATTO DI NASCITA
- 8 = STATURA (in cm)
- a = fotografia del titolare (dimensioni 23x28 mm)
- b = numero assegnato al documento in bianco
- c = spazio riservato alla codifica ICAO con caratteri OCRB

AII. A - FRONTE -

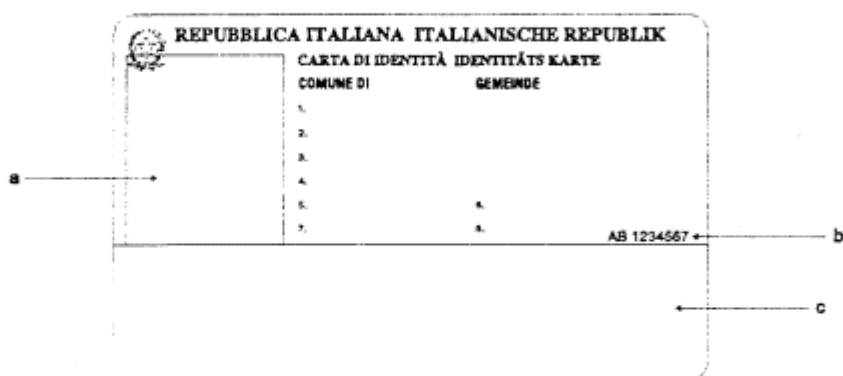
AII. A - RETRO -

- 9 = COMUNE DI RESIDENZA
- 10 = INDIRIZZO
- 11 = DATA EMISSIONE DOCUMENTO
- 12 = DATA SCADENZA DOCUMENTO
- 13 = CITTADINANZA
- 14 = CODICE FISCALE
- 15 = FIRMA
- 16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
- d = ologramma (dimensioni 18x14 mm)
- e = numero assegnato al documento in bianco
- f = modulo CHIP
- g = banda a memoria ottica

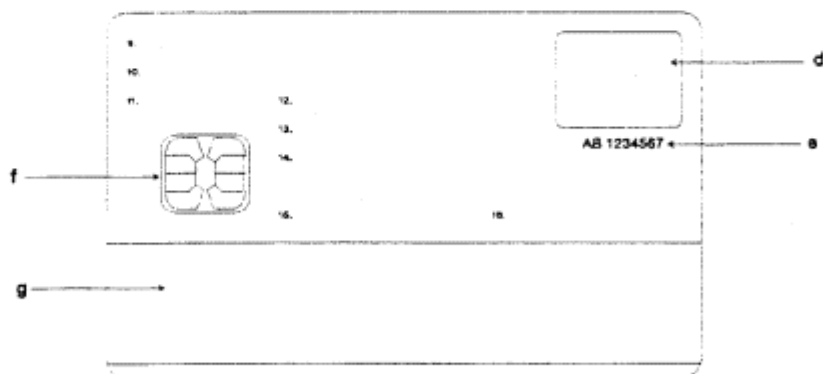
VERSIONE ITALIANO/TEDESCO

LEGENDA:

- 1 = COMUNE CHE RILASCI IL DOCUMENTO
- 2 = COGNOME DEL TITOLARE
- 3 = NOME DEL TITOLARE
- 4 = COMUNE DI NASCITA
- 5 = DATA DI NASCITA
- 6 = SESSO
- 7 = ESTREMI ATTO DI NASCITA
- 8 = STATURA (in cm)
- a = fotografia del titolare (dimensioni 23x28 mm)
- b = numero assegnato al documento in bianco
- c = spazio riservato alla codifica ICAO con caratteri OCRB



AII. A - FRONTE -



AII. A - RETRO -

- 9 = COMUNE DI RESIDENZA
- 10 = INDIRIZZO
- 11 = DATA EMISSIONE DOCUMENTO
- 12 = DATA SCADENZA DOCUMENTO
- 13 = CITTADINANZA
- 14 = CODICE FISCALE
- 15 = FIRMA
- 16 = INDICAZIONE DELLA VALIDITÀ PER L'ESPATRIO
- d = ologramma (dimensioni 18x14 mm)
- e = numero assegnato al documento in bianco
- f = modulo CHIP
- g = banda a memoria ottica

Allegato B

Indice dei contenuti

1. INTRODUZIONE

1.1 BIBLIOGRAFIA DI RIFERIMENTO E STANDARD UTILIZZATI

1.2 STRUTTURA DELLA CARTA

2. INFRASTRUTTURA ORGANIZZATIVA (FA RIFERIMENTO ALL'ART. 3 DEL D.M.)

3. INFRASTRUTTURE TECNICHE E DI RETE

3.0 SITO DELLA CARTA D'IDENTITÀ ELETTRONICA

3.1 DOTAZIONI DEL SSCE (FA RIFERIMENTO ALL'ART. 6 DEL D.M.)

3.1-BIS DOTAZIONI DEL CNSD

3.2 DOTAZIONI DEI COMUNI

3.2.1 Dotazioni hardware (fa riferimento all'art. 10 comma 1 del D.M.)

3.2.2 Dotazioni hardware minimale (fa riferimento all'art. 13 comma 2 del D.M.)

3.2.3 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)

3.2.3-bis Modalità di accesso ai servizi fruibili tramite il documento

3.2.3-ter Dotazioni per i cittadini

3.2.4 Modalità di connessione al Sistema di Sicurezza del Circuito di Emissione (SSCE)

3.2.4-bis Modalità di connessione al Centro Nazionale dei Servizi Demografici

4. MATERIALI E STANDARD DI RIFERIMENTO

4.0 USO DEL DOCUMENTO

4.1 SUPPORTO FISICO (FA RIFERIMENTO ALL'ART. 7, COMMA 1 DEL D.M.)

4.1.1 Dimensioni nominali e le componenti

4.2 CARTA A MEMORIA OTTICA (FA RIFERIMENTO ALL'ART. 8, COMMA 1 DEL D.M.)

4.3 MICROPROCESSORE (FA RIFERIMENTO ALL'ART. 8, COMMA 1 DEL D.M.)

4.4 DATI (FA RIFERIMENTO ALL'ART. 13, COMMA 1, LETTERA D DEL D.M.)

5. MISURE DI SICUREZZA (FA RIFERIMENTO ALL'ART. 4 DEL D.M.)

5.1 SICUREZZA DEL SUPPORTO FISICO

5.1.1 Elementi di sicurezza grafici e di stampa

5.1.2 Inchiostri

5.1.3 Numerazione di serie

5.1.4 Applicazione di elementi Optical Variable Device (OVD)

5.2 SICUREZZA DELLA FASE DI PERSONALIZZAZIONE

5.3 AFFIDABILITÀ DEI DATI

5.3.1 Laser su banda ottica

5.3.2 Microcircuito

5.4 SICUREZZA DEL CIRCUITO (FA RIFERIMENTO ALL'ART. 6, COMMA 1 DEL D.M.)

5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)

5.4.2 Sicurezza della carta

5.4.3 Furto della carta «attivata» o documento in bianco

5.4.4 Controlli a vista

5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6 comma 2 del D.M.)

5.4.6 Software di sicurezza distribuito ai comuni (fa riferimento all'art. 6 comma 1 del D.M.)

6. SERVIZI EROGABILI (FA RIFERIMENTO ALL'ART. 5 DEL D.M.)

6.1 LE LISTE DEI SERVIZI

6.1-BIS LA LISTA DELLE CARTE INTERDETTE (BLACK-LIST)

6.2 MODALITÀ DI EROGAZIONE DEI SERVIZI

6.2.1 Crypto Middleware ed API PKCS#11

6.2.2 Processo di Strong Authentication

6.2.3 Comandi di gestione utilizzati dalla Strong Authentication

6.3 CONSIDERAZIONI SULLA INTEROPERABILITÀ

6.3.1 Algoritmi

6.3.2 Formati

6.4 STRONG AUTHENTICATION LATO SERVER

6.4.1 Server Authentication Middleware

6.5 L'INSTALLAZIONE DEI SERVIZI

6.6 L'AGGIORNAMENTO DEI DATI RELATIVI ALLA FRUIZIONE DEI SERVIZI

6.7 AUTENTICAZIONE ESTERNA

6.8 SECURE MESSAGING

7. PROCESSO DI EMISSIONE

7.1 PRODUZIONE DI BANDA LASER E MICROPROCESSORE

7.2 PRODUZIONE ED INIZIALIZZAZIONE DELLA CARTA D'IDENTITÀ ELETTRONICA E DEL DOCUMENTO ELETTRONICO

7.2.1 Struttura delle informazioni sulla banda ottica

7.2.2 Struttura delle informazioni nel microprocessore

7.3 LE FASI PRELIMINARI

7.3.1 Generazione numeri identificativi per le carte d'identità ed i documenti elettronici.

7.3.2 *Produzione*

7.3.3 *Inizializzazione*

7.3.4 *Attivazione*

7.4 PERSONALIZZAZIONE ED EMISSIONE DELLE CARTE

7.4.1 *Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)*

7.4.1.1 Sottofase di compilazione

7.4.1.2 Sottofase di autorizzazione

7.4.1.3 Sottofase di formazione

7.4.1.4 Sottofase di rilascio

7.4.1.5 Sottofase di verifica e controllo

8. **VERIFICA DELLE CIE (FA RIFERIMENTO ALL'ART. 6, COMMA 1 DEL D.M.)**

8.1 CONSERVAZIONE DEL CARTELLINO ELETTRONICO (FA RIFERIMENTO ALL'ART. 6, COMMA 3 DEL D.M.)

8.2 INTERDIZIONE DELL'OPERATIVITÀ DELLA CIE (FA RIFERIMENTO ALL'ART. 6, COMMA 2 DEL D.M.)

8.3 CARTA SANITARIA

8.3.1 *Carta sanitaria - Pilota italiano Netlink*

8.4 FIRMA DIGITALE

8.4.1 *Certificati di firma digitale*

8.5 IMPRONTA DIGITALE

1. Introduzione

1.1 Bibliografia di riferimento e standard utilizzati

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;

Il Sistema INA - SAIA: architettura e note per l'attivazione. Maggioli editore - settembre 2002. ISBN 88.387.2121.1;

Progetto del Centro nazionale servizio demografici - Roma, dicembre 2002 - Ministero interno/Università di Roma Tor Vergata;

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;

ISO/IEC 11694-1-2-3-4 Annex A e Annex B per la parte relativa alla banda ottica;

ISO/IEC 7816-1-2-3-4-5-6-7-8-9 per la parte relativa alla smart card;

PKCS#1 per l'interfacciamento delle smart card;

Allegato tecnico al Protocollo d'Intesa in data 13 maggio 2003 Governo - Produttori di microcircuiti
(20).

1.2 Struttura della carta

La carta d'identità elettronica (CIE) è una carta ibrida, in grado di integrare nel supporto fisico sia una banda a memoria ottica che un microprocessore.

La banda ottica a lettura laser è utilizzata per la memorizzazione dei «dati» identificativi (D.M. Art. 1, comma 1, lettera f)) ai fini della salvaguardia delle esigenze di pubblica sicurezza. L'elevata capacità di memoria disponibile, utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità elaborativa del *microchip*, può consentirne un utilizzo anche per la fruizione di servizi locali o nazionali.

Il microprocessore è utilizzato per assolvere le funzioni di «carta servizi» (D.M. Art. 1, comma 1, lettera g)), per consentire l'identificazione in rete e, quindi, l'erogazione di servizi telematici.

Le caratteristiche grafiche della CIE (D.M. art. 7 comma 3), unitamente al dettaglio delle informazioni presenti, sono riportate nell'allegato A.

2. Infrastruttura organizzativa (fa riferimento all'art. 3 del D.M.)

Nel circuito di emissione intervengono gli enti nel seguito descritti:

Fornitori di microprocessori: *Aziende produttrici dei microprocessori.*

Provvedono alla fornitura dei microprocessori, durante la produzione memorizzano, in area non riscrivibile, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di chip, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di microprocessori consegnati ed i relativi numeri seriali impressi al loro interno. Acronimo **Fp**;

Fornitori di bande laser: *Aziende produttrici della banda ottica a lettura laser.*

Provvedono alla fornitura delle bande ottiche a lettura laser, durante il processo di produzione imprimono, tramite scrittura laser, un codice seriale composto di un numero progressivo, dal lotto e dalla data di produzione. Il numero deve essere univoco. Ogni consegna di lotti di bande ottiche, deve essere accompagnata da distinta cartacea ed elettronica dalla quale si evinca il numero di bande ottiche consegnate ed i numeri seriali impressi al loro interno. Acronimo **Fb**;

Istituto Poligrafico e Zecca dello Stato: *Ente a cui è riservata la produzione del documento.*

Provvede alla manifattura delle carte, all'inserimento (*embedding*) della banda ottica e del microprocessore nel supporto fisico, nonché alla inizializzazione elettrica di quest'ultimo.

Memorizza nel chip, ai fini della garanzia di autenticità, nella banda ottica tramite laser e nella banda ottica in modalità «*Embedded hologram*» il numero d'identificazione univoco su scala nazionale, fornitogli dal Sistema di sicurezza del circuito di emissione, ed inscindibilmente legato ad essa.

Imprime lo stesso numero in maniera grafica sul supporto fisico e stampa gli elementi grafici costanti (logo, sfondo, etc.).

Contabilizza i numeri seriali che identificano il lotto e la data di produzione del chip e della banda ottica.

Trasmette le informazioni risultanti dalle procedure di inizializzazione al Sistema di sicurezza. Acronimo **IPZS**;

Ministero dell'interno - Sistema di sicurezza del circuito di emissione: *Ente che fornisce le infrastrutture tecnologiche e garantisce la sicurezza dell'intero circuito di emissione.*

In attuazione dell'art. 8, comma 4, del *decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437*, il Ministero dell'interno - Dipartimento della pubblica sicurezza mette a disposizione l'infrastruttura organizzativa, informatica e di rete del Centro elaborazioni dati della Polizia scientifica, per la realizzazione, la gestione e manutenzione del Sistema di sicurezza del circuito d'emissione.

Al fine di garantire la sicurezza dell'intero circuito di emissione ha la responsabilità di verificare e certificare qualunque operazione che comporti l'inserimento, la modifica o la cancellazione delle informazioni (in particolare i dati identificativi) memorizzate sul microprocessore o sulla banda ottica, eccezion fatta per i dati relativi alla predisposizione ed erogazione dei servizi.

Ai fini della garanzia di autenticità, genera per ogni carta un numero di identificazione univoco, su scala nazionale, che trasmette all'IPZS.

Tramite collegamenti telematici consente alle singole questure di accedere ai documenti, conservati in forma cifrata presso il sistema.

Tramite collegamento telematico invia al CNSD la copia dei cartellini elettronici (copia elettronica), cifrati con chiave pubblica del comune, identificati mediante numero di carta, codice fiscale e codice ISTAT del comune.

Tramite collegamento telematico richiede al CNSD la convalida dei dati anagrafici dei cittadini durante la fase di emissione della CIE.

Ciascuna questura, e solo essa, può decifrare i documenti di sua competenza, ovvero quelli rilasciati dai comuni della stessa provincia. Acronimo **SSCE**.

Ministero dell'interno - INA: *Indice nazionale delle anagrafi.*

In attuazione della *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 durante la fase di emissione delle carte. La convalida dell'informazione anagrafica durante l'accesso ai servizi tramite carta può essere acquisita accedendo all'anagrafe comunale o accedendo ai servizi dell'INA tramite backbone INA/SAIA.

I comuni, ai fini del rilascio e dell'uso del documento, devono preventivamente provvedere all'aggiornamento dell'INA, tramite la porta applicativa per l'accesso, su backbone INA/SAIA, ai servizi del CNSD. Acronimo **INA**.

Ministero dell'interno - CNSD: *Centro nazionale dei servizi demografici.*

Il Ministero dell'interno, con decreto ministeriale 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 dell'anagrafe comunale, requisito essenziale ad una corretta gestione dei circuiti di emissione ed uso del documento. I comuni si collegano su rete Internet o Rete unitaria al CNSD attraverso la porta applicativa. Presso il CNSD è costituito l'archivio crittografato CIE-COMUNI contenente l'elenco delle CIE emesse da ciascun comune. Ciascun comune e solo esso può decrittare i documenti di sua competenza. Tramite collegamento telematico riceve dal SSCE la copia dei cartellini elettronici (copia elettronica), cifrati con chiave pubblica del comune, identificati mediante numero di carta, codice fiscale e codice ISTAT del comune. Con queste informazioni costituisce l'archivio crittografato CIE-COMUNI. Acronimo: **CNSD**.

Centri servizi: *Centri servizi.*

Le funzioni di pertinenza dei comuni, per i procedimenti connessi all'emissione della CIE, possono essere esercitate anche in forma associata da unioni di comuni o da comunità montane. Ai fini della formazione, secondo modalità asincrone, del documento CIE, i comuni possono avvalersi di centri servizi appositamente costituiti. La funzione di attivazione e di rilascio della CIE al cittadino resta di pertinenza di ciascun comune emittente. Acronimo: **CS**.

Emittitore: *Ente responsabile della formazione e del rilascio.*

È il comune al quale il cittadino si rivolge per richiedere la CIE. Acronimo **E**.

3. Infrastrutture tecniche e di rete

3.0 Sito della carta d'identità elettronica

Il sito Internet del documento è raggiungibile all'indirizzo www.cartaidentita.it

Tale sito è curato dal Ministero dell'interno ed è il riferimento ufficiale per le specifiche tecniche di dettaglio del documento.

3.1 Dotazioni del SSCE (fa riferimento all'art. 6 del D.M.)

Ai fini dell'emissione della CIE, il sistema di sicurezza del circuito d'emissione (SSCE) si compone di:

- connessione alle reti di accesso;
- funzioni di «security service provider» per consentire l'accesso, con modalità di sicurezza, dei comuni tramite Internet;
- rete digitale delle Questure (già presente) per consentire la visualizzazione e la stampa dei cartellini elettronici alle Questure competenti;
- connessione diretta con l'IPZS per l'interscambio d'informazioni nella fase d'inizializzazione;

- connessione alla rete del CNSD per l'accesso ai servizi di convalida anagrafica dell'INA e per l'invio delle copie dei cartellini elettronici (copia elettronica), cifrati con chiave pubblica del comune, identificati mediante numero di carta, codice fiscale e codice ISTAT del comune;
- software di sicurezza versione server per le funzionalità connesse alle diverse fasi di formazione della CIE.

3.1-bis - Dotazioni del CNSD

Ai fini dell'emissione e dell'uso del documento, il Centro Nazionale per i Servizi Demografici (CNSD) si compone di:

- connessione alle reti Internet ed alla Rete unitaria;
- servizi di porta applicativa per l'accesso, su backbone INA/SAIA, ai servizi del CNSD per consentire l'accesso, sicuro e certificato, ai comuni tramite rete Internet, Rete Unitaria o reti regionali, provinciali e civiche;

connessione alla rete di SSCE, per consentirgli:

- a. l'accesso ai servizi INA di convalida dei dati anagrafici delle CIE in fase di emissione;
- b. l'invio delle copie dei cartellini elettronici (copia elettronica), cifrati con chiave pubblica del comune, identificati mediante numero di carta, codice fiscale e codice ISTAT del comune.

3.2 Dotazioni dei Comuni

3.2.1 Dotazioni hardware (fa riferimento all'art. 10, comma 1 del D.M.)

La configurazione degli apparati hardware e dei prodotti software necessari per la formazione della CIE è riportata presso il sito della Carta d'identità elettronica.

Presso tale sito il Ministero dell'interno renderà disponibile l'elenco delle apparecchiature certificate come idonee per il rilascio della Carta d'identità elettronica.

3.2.2 Dotazioni hardware minimale (fa riferimento all'art. 13, comma 2 del D.M.)

[Nel seguito è riportata la configurazione minima degli apparati *hardware* necessari per la formazione della CIE in caso il comune si avvalga, in via transitoria, dell'IPZS. Le apparecchiature proposte possono subire variazioni in funzione dell'architettura del sistema informativo dei singoli comuni.

1. *Personal Computer* di fascia alta;
2. *Scanner* per la digitalizzazione della firma e, eventualmente, della fotografia del titolare;
3. Videocamera per la produzione digitalizzata della fotografia del titolare;

4. *Scanner* per l'assunzione delle impronte digitali. Lo *scanner* deve acquisire ad una risoluzione di 500 dpi].⁵

3.2.3 Dotazioni software applicativo (fa riferimento all'art. 6, comma 1 del D.M.)

I comuni, per le attività inerenti la formazione ed il rilascio delle CIE, saranno dotati di specifico software applicativo di sicurezza, sviluppato dal Ministero dell'interno e distribuito da SSCE.

Tale software avrà la possibilità di interoperare con i sistemi informativi dei comuni.

Il Ministero dell'interno rende disponibile, secondo le modalità descritte sul sito, sia il software specifico della porta applicativa per l'accesso su backbone INA/SAIA ai servizi del CNSD, sia il software di supporto all'uso del documento da parte dei cittadini e delle Amministrazioni (librerie dei metacomandi. CSP e PKCS11).

Il Ministero dell'interno, su motivata richiesta dei soggetti interessati, che devono garantire i livelli di sicurezza dallo stesso richiesti, fornisce le specifiche del file system del documento.

3.2.3-bis - Modalità di accesso ai servizi fruibili tramite il documento

Presso il sito della carta d'identità elettronica sono descritte le modalità per accedere ai servizi che richiedono l'utilizzo del documento.

3.2.3-ter - Dotazioni per i cittadini

Presso il sito della Carta d'identità elettronica sono descritte le configurazioni necessarie per accedere ai servizi di e-government mediante la Carta d'identità elettronica da postazioni private.

Presso tale sito è inoltre possibile reperire e scaricare il software di integrazione necessario per utilizzare le funzioni della Carta d'identità elettronica con i più diffusi ambienti software per personal computer.

3.2.4 Modalità di connessione al Sistema di Sicurezza del Circuito di Emissione (SSCE)

L'interconnessione a SSCE avverrà secondo le seguenti modalità di trasporto:

- tramite rete unitaria della Pubblica Amministrazione (RUPA);
- tramite altre reti a cui sono connesse le amministrazioni locali;
- tramite internet.

In tutti i casi è necessario l'utilizzo del *software* di sicurezza versione *client*.

Il *software* consente di eseguire le funzioni necessarie per l'acquisizione dei dati del titolare, utili alla formazione del documento, e quelle per operare, con modalità di sicurezza, le connessioni a SSCE.

3.2.4-bis - Modalità di connessione al Centro Nazionale dei Servizi Demografici

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

⁵ Punto soppresso dall'art. 2, D.M. 6 novembre 2003.

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

In tutti i casi, è necessario l'utilizzo della porta applicativa.

I servizi forniti dal CNSD consentono di ottenere la convalida anagrafica dei dati del titolare del documento nella sua fase di uso, inviare gli aggiornamenti anagrafici all'INA, accedere in modo esclusivo da parte del comune che li ha emessi alla copia dei cartellini elettronici dei documenti sull'archivio CIE-comuni.

4. Materiali e standard di riferimento

4.0 Uso del documento

In considerazione della natura del certificato CIE che non contiene informazioni anagrafiche, è necessario prevedere la definizione di meccanismi standard per garantire l'accesso ai servizi ai cittadini.

In particolare, per garantire l'accesso ai servizi verranno definite modalità operative che permettono l'estrazione dei dati anagrafici da inviare al web server che eroga i servizi, per implementare l'accesso basato su CIE, dai client verso i web server. A tal fine verranno forniti da parte del Ministero dell'interno, in logica open source, gli opportuni codici software.

In alternativa, per motivi di opportunità o di incompatibilità tecnologica del client del cittadino richiedente con le modalità operative adottate, al termine della fase di challenge tra il client ed il web server nella quale viene scambiato esclusivamente il certificato della CIE, i web server possono richiedere, attraverso i servizi di convalida del backbone INA-SAIA, il codice fiscale corrispondente all'ID carta del cittadino direttamente all'INA o alle anagrafi comunali.

Ai fini della possibilità da parte dei comuni e delle Amministrazioni interessate di attivare sulla CIE i servizi qualificati, il Ministero dell'interno, su motivata richiesta dell'Amministrazione o dell'Ente interessato che deve garantire i livelli di sicurezza richiesti dal Ministero dell'interno, fornisce le specifiche del file system della CIE.

4.1 Supporto fisico (fa riferimento all'art. 7, comma 1 del D.M.)

4.1.1 Dimensioni nominali e le componenti

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identità *International Standards Organization* (ISO)/IEC 7816-1, 7816-2.

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-I. La tolleranza, nelle dimensioni, è quella definita dalla norma stessa.

Lo spessore della CIE, compresi i film di protezione, dovrà essere conforme alla norma ISO/IEC 7810: 1995.

La CIE, sarà costituita da materiali plastici compatibili con gli strumenti tecnologici in essa contenuti, nonché con i sistemi di personalizzazione utilizzati per la sua compilazione.

La CIE, per un uso normale nel periodo di validità, dovrà rispondere alle specifiche definite:

- nella norma ISO/IEC 7810: 1995 relativamente a: deformazioni, tossicità, resistenza ad agenti chimici, stabilità dimensionale ed inarcamento con temperatura e umidità, inarcamento con l'uso, infiammabilità e durata.
- nella norma ISO/IEC 11693 per la contaminazione, per la trasmissione della luce attraverso lo spessore della carta e per la resistenza agli agenti atmosferici ed ai test di compatibilità con l'ambiente.

Per quanto attiene alla presenza del *microchip* la CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite nella norma ISO/IEC 7816 - 1.

L'area a memoria ottica della CIE, per un normale uso durante il periodo di validità, deve rispondere alle specifiche definite dalle norme ISO/IEC 11693, 11694-1, 11694-2, 11694-3, 11694-4.

4.2 Carta a memoria ottica (fa riferimento all'art. 8, comma 1 del D.M.)

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, 1.000 volte più resistente del PVC, che garantisce un'ottima trasparenza per la scrittura su banda ottica, una elevata resistenza, una maggiore durata nel tempo ed un intervallo termico di utilizzo molto ampio (-40° + 100°).

Il film è composto da diversi strati di materiale ed il supporto ottico registrabile è incapsulato tra due livelli di materiale protettivo trasparente che (sulla faccia esterna) è rinforzato da un ulteriore strato «antigraffio».

La capacità di memoria della carta ottica utilizzata, nella dimensione adottata, è di circa 1,8 MByte.

Ogni carta ottica permette la creazione di settori variabili basati su tracce, consentendo così l'archiviazione di informazioni multiple ed indipendenti.

Le carte ottiche, rispondono allo *standard* ISO/IEC 11694.

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

È 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, è 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.

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

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

DESCRIZIONE CAMPO	TIPO
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 Ml 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) è 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.

5. Misure di sicurezza (fa riferimento all'art. 4 del D.M.)

Questo paragrafo descrive le misure adottate, durante tutte le fasi della produzione e dell'utilizzo della CIE, per ottenere i corretti livelli di sicurezza e di interoperabilità della carta.

5.1 Sicurezza del supporto fisico

Nel seguito sono elencati gli elementi utilizzabili per la sicurezza del supporto e per accertarne l'autenticità, anche attraverso il semplice esame visivo.

5.1.1. Elementi di sicurezza grafici e di stampa

È previsto l'uso dei seguenti elementi di sicurezza tipici delle carte valori:

- motivi grafici ad elementi variabili;
- elementi grafici diffrattivi;
- microprint;
- processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico;
- Embedded hologram (incisione grafica su banda laser).

5.1.2. Inchiostri

Per la stampa è previsto l'impiego di inchiostri dotati di speciali caratteristiche, come quelli fluorescenti (visibili all'ultravioletto) e otticamente variabili (OVI - Optical variable ink).

5.1.3 Numerazione di serie

La numerazione del documento in bianco, realizzata con sistema ad incisione *laser* sul fronte del documento, è ripetuta visibilmente sulla banda ottica con il sistema dell'«*embedded Hologram*», memorizzata al suo interno ed inserita come dato all'interno del microprocessore.

5.1.4 Applicazione di elementi Optical Variable Device (OVD)

Sul retro del documento, nella fase di produzione, è applicato a caldo un ologramma di sicurezza.

5.2 Sicurezza della fase di personalizzazione

Al fine di consentire la stampa della CIE presso i Comuni o i Centri Servizi ad un costo contenuto, la tecnica da utilizzare è quella della termografia a colori su polycarbonato (eventualmente apponendo uno strato neutro intermedio).

Anche la compilazione grafica sarà uniforme per tutto il territorio nazionale tramite l'utilizzo di caratteri, provenienti da un unico «*font*» appositamente realizzato per la CIE che verrà distribuito unitamente al *software* di sicurezza, dal SSCE.

Inoltre, l'apposizione di *embedded hologram* (incisione grafica su banda *laser*) consente di replicare, su banda ottica, i dati identificativi del titolare del documento, al fine di rendere più sicura l'identificazione a vista.

Infine, come accennato, al termine della stampa termica, il processo prevede l'applicazione sul fronte di un «*overlay*» di protezione di 12 micron al fine di offrire ulteriori sicurezze e garantire la durata oltre i cinque anni.

5.3 Affidabilità dei dati

5.3.1 Laser su banda ottica

I dati vengono memorizzati permanentemente sulla banda *laser* (sistema WORM) in formato digitale e letti/scritti con appositi apparati, detti lettori/scrittori.

Ferma restando l'auspicabile corretta conservazione da parte del titolare della carta, per meglio garantire la leggibilità e la coerenza dei dati nel tempo, la superficie della tessera dovrebbe presentarsi pulita e uniforme (es. possibilmente senza graffi o abrasioni). Comunque i supporti informatici utilizzati offrono garanzie di conservazione dei dati molto elevate; infatti, per quanto attiene ai dati contenuti nella banda *laser*, è attivo un metodo di identificazione e correzione d'errore che garantisce la ricostruzione delle informazioni digitali eventualmente perse per cause accidentali.

5.3.2 Microcircuito

Le informazioni memorizzate sul microprocessore sono:

- le informazioni specifiche dell'hw e del sw;

- le informazioni anagrafiche del titolare;
- dati individuali aggiuntivi;
- dati relativi ai singoli servizi.

L'accesso a queste ultime due tipologie di dati è possibile solo dopo il consenso del titolare espresso ordinariamente tramite digitazione di PIN.

I dati individuali aggiuntivi sono informazioni relative al titolare che sono registrate sulla carta, ad integrazione delle informazioni anagrafiche, e che possono essere utilizzate ai fini dell'erogazione dei servizi. Queste informazioni estendono l'identità del titolare, non sono specifiche di un servizio e non sono modificabili a seguito dell'erogazione dei servizi. Vengono registrate o modificate sulla carta esclusivamente dal comune su esplicita richiesta del titolare e, in pratica, abilitano la carta all'accesso a quei servizi delle amministrazioni locali e centrali la cui erogazione necessita di tali dati.

L'elenco dei dati individuali aggiuntivi è definito ed aggiornato dal Dipartimento della funzione pubblica, d'intesa con il Ministero dell'interno e con l'Associazione nazionale dei comuni d'Italia.

I dati relativi ai singoli servizi sono informazioni registrate sulla carta, eventualmente modificabili durante l'erogazione del servizio, e relative ad attributi del titolare della carta che sono funzionali esclusivamente all'amministrazione erogante il servizio.

5.4 Sicurezza del circuito (fa riferimento all'art. 6, comma 1 del D.M.)

La migliore garanzia contro tentativi di falsificazioni e utilizzo di carte rubate si trova nella centralizzazione virtuale prevista dall'architettura del circuito d'emissione della CIE.

In tale logica, il sistema di sicurezza dei documenti traccia tutte le operazioni al fine di garantire il rispetto della normativa vigente sulla riservatezza delle informazioni e dei dati personali, per impedire l'emissione di documenti falsi e per individuare facilmente l'utilizzo fraudolento di documenti rubati e la contraffazione di documenti autentici.

Nel capitolo 7 verranno descritte dettagliatamente tutte le fasi del processo di emissione.

5.4.1 Sicurezza degli accessi ai dati (fa riferimento all'art. 6 del D.M.)

In base al Regolamento di esecuzione del Testo Unico delle Leggi di P.S., oltre al titolare possono accedere alle informazioni contenute nei documenti esclusivamente i Comuni, che emettono le carte d'identità, e le Questure competenti territorialmente. Infatti, sia gli uni che gli altri sono tenuti a conservare copia dei documenti emessi.

Passando da un documento cartaceo ad uno di formato elettronico, anche la copia conservata da Comune e Questura (cartellino cartaceo) diviene di tipo digitale (cartellino elettronico).

Pertanto, a fini di sicurezza e nel rispetto delle norme di legge, la «base dati» comune consente l'accesso e la visualizzazione dei cartellini elettronici al solo Comune di residenza ed alla Questura territorialmente competente.

A tal fine il Sistema di Sicurezza (SSCE) garantisce la tracciabilità di tutte le attività, relative ai dati identificativi, per ogni singolo documento, consentendo di risalire, in qualsiasi momento, alle informazioni di «chi ha fatto cosa e quando», nel rispetto delle attuale normativa, durante tutte le fasi di formazione, compilazione, rilascio, rinnovo ed aggiornamento dei documenti.

Il Sistema di Sicurezza, grazie ad un meccanismo di cifratura basata su algoritmo a chiave asimmetrica, non è in grado esso stesso di accedere ad alcuna informazione di carattere personale che può essere visualizzata, tramite la propria chiave privata, esclusivamente dalla Questura o dal Comune competente.

Da un punto di vista tecnico, i dati sono prima cifrati per mezzo di un algoritmo simmetrico di provata robustezza (ad es. 3DES) con una chiave di lunghezza non inferiore a 128 bit (generata in modalità casuale); quest'ultima, prima di essere distrutta, viene a sua volta cifrata sia con la chiave pubblica della Questura che con quella del Comune e memorizzata assieme all'informazione.

5.4.2 Sicurezza della carta

I rischi di utilizzo fraudolento e falsificazione delle carte d'identità, anche a causa di furti di carte «in bianco», con l'adozione del modello elettronico, sono notevolmente ridotti, principalmente in virtù della natura del supporto e delle garanzie di inalterabilità delle informazioni riportate, tanto sul chip che sulla banda ottica.

La banda ottica rappresenta l'elemento centrale della sicurezza per i motivi di seguito riportati.

La caratteristica di base della scrittura WORM (Write Once Read Many) non permette alterazioni, realizzate mediante la cancellazione di dati e la loro sostituzione con altri. Infatti, le informazioni memorizzate non sono cancellabili e riscrivibili. Eventuali aggiornamenti consistono esclusivamente in aggiunte, proprio come avviene per un normale CD-ROM.

In ogni caso esistono le protezioni inserite nell'hardware di scrittura, in dotazione esclusivamente a E ed IPZS, e di ogni operazione effettuata dal funzionario autorizzato con modalità gestite elettronicamente, si tiene traccia presso SSCE.

Il controllo a vista della carta, inoltre, è garantito dalla presenza dell'Embedded Hologram che permette di effettuare un'azione di costante validazione dei dati stampati in chiaro e di evidenziarne immediatamente il tentativo di manomissione.

Relativamente al microchip, questi non permette - grazie alla sicurezza del suo stesso sistema operativo - di modificare o scrivere informazioni se non in presenza di determinate autorizzazioni.

Inoltre tutte le informazioni sensibili, tanto sul chip che sulla banda ottica, sono garantite contro l'alterazione, perché «firmate» digitalmente ⁽³⁷⁾.

5.4.3 Furto della carta «attivata» o documento in bianco

La carta è in tale stato quando viene spedita da IPZS ai comuni, prima di essere formata e rilasciata.

In questo caso, dal momento che la personalizzazione richiede, per poter aver luogo, l'autenticazione del funzionario nei confronti del sistema e la firma dei dati da parte di appositi apparati contenenti la chiave privata dell'ente, tale eventualità rientra nella tipologia del «rilascio fraudolento» realizzabile solo attraverso l'infedeltà del funzionario stesso le cui attività però, con la citata tracciatura, restano registrate nel Data Base delle approvazioni presso SSCE.

5.4.4 Controlli a vista

L'intero circuito di sicurezza attraverso l'adozione dell'architettura a centralizzazione virtuale consente di innalzare il livello di qualità dei controlli, c.d. a vista, effettuati dalle Forze di Polizia per verificare l'identità delle persone sottoposte ai controlli stessi.

Disporre di un documento particolarmente attendibile consente di eseguire tutte le normali procedure in tempi molto ridotti con indubbio vantaggio per le persone coinvolte.

Le sicurezze adottate durante la fase di inizializzazione del documento, la presenza sulla banda ottica, sotto forma di ologramma, delle stesse informazioni grafiche, lo rendono molto più affidabile del modello cartaceo.

Laddove si volessero approfondire le verifiche, due sono le possibili soluzioni:

- Controllo dei dati autenticati e memorizzati nella banda ottica. Tramite apposito lettore opportunamente inizializzato, in grado di rilevare con certezza l'autenticità del documento
- Controllo delle informazioni presso il SSCE. Le Questure di competenza possono, collegandosi al SSCE, verificare immediatamente, grazie al possesso di opportune chiavi crittografiche, se le informazioni in esso contenute corrispondono con quelle riportate nel documento.

5.4.5 Lista dei documenti interdetti (fa riferimento all'art. 6, comma 2 del D.M.)

In attuazione dell'art. 6, comma 1, del *D.P.C.M. 22 ottobre 1999, n. 437*, presso il SSCE è presente un elenco dei documenti interdetti (*black-list*). Tale elenco è indispensabile per impedire l'operatività della CIE in caso di smarrimento o furto della stessa.

Le procedure da seguire per l'interdizione della carta vengono dettagliatamente descritte nei successivi paragrafi.

5.4.6 Software di sicurezza distribuito ai comuni (fa riferimento all'art. 6, comma 1 del D.M.)

Per procedere alla formazione ed all'emissione dei documenti, i Comuni devono collegarsi al SSCE. In assenza di tale collegamento qualsiasi documento prodotto verrebbe facilmente individuato come falso.

I requisiti per collegarsi al circuito di emissione sono un collegamento telematico, secondo i criteri stabiliti al paragrafo 3.2 del presente documento, e l'adozione di uno speciale *software* di sicurezza rilasciato dal Sistema di Sicurezza stesso.

Il SSCE curerà l'analisi, lo sviluppo, la distribuzione e la manutenzione del *software*, per motivi di riservatezza, di interoperabilità e di economicità.

Il *software*, unitamente alla chiave privata del comune, la prima volta dovrà essere ritirato presso il Ministero dell'Interno. Le *release* successive, invece, grazie alla disponibilità della chiave privata potranno essere prelevato direttamente via Web.

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 è 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 è 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*.

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 è affidata alla responsabilità del comune.

La predisposizione e la gestione della lista dei servizi nazionali è 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 modalità di installazione ovvero aggiornamento (nel caso si tratti di un servizio già esistente) e, in caso di parere favorevole, presentare al SSCE un documento in cui si evidenzia:

- la descrizione del servizio da erogare;
- le modalità tecniche attraverso le quali sarà garantito il servizio;
- l'organizzazione a supporto del sistema di erogazione del servizio.

Ai fini delle verifiche di validità 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) è 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.

6.2 - Modalità di riconoscimento in rete.

In considerazione dell'architettura definita per la carta d'identità 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 è scelta è 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, è resa disponibile dal CNSD attraverso servizi distribuiti di validazione dei certificati delle CIE (OCSP distribuito), mentre la convalida anagrafica dei dati è resa disponibile attraverso i servizi di convalida anagrafica del CNSD.

6.2.1 Crypto Middleware ed API PKCS#11.

Il Cripto Middleware è 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 PKCS#11, 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 è trattata con queste API.

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 è 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 è 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 è autenticata. A questo proposito è necessario che l'algoritmo di verifica, residente sul server, sia compatibile con quello usato dalla carta per cifrare il challenge.

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 è pubblicato sul sito del CNSD, insieme alle librerie di gestione di tali APDU.

6.3 Considerazioni sulla interoperabilità

[Al momento della scrittura di questo documento, non esistono *standard* di riferimento che garantiscono l'interoperabilità dei sistemi di crittografia, per cui SSCE, per raggiungere questo obiettivo, ha ritenuto opportuno definire sia l'algoritmo crittografico di autenticazione, sia il formato del messaggio autenticato.

La scelta effettuata è quella di utilizzare RSA come algoritmo di autenticazione e PKCS#1 come formato; di seguito sono esposti i razionali che hanno condotto a questa tipo di soluzione].⁶

6.3.1 Algoritmi

[Gli algoritmi asimmetrici comunemente impiegati dalle *Smart Card* ed idonei per realizzare la autenticazione sono l'algoritmo RSA e l'algoritmo DSA.

Questi algoritmi sono onerosi dal punto di vista computazionale e quindi sono realizzati utilizzando un coprocessore aritmetico. La lunghezza della chiave dipende dalla capacità del coprocessore di effettuare moltiplicazioni in modulo. Questo comporta una lunghezza massima di chiave pari al massimo modulo supportato dal coprocessore per l'algoritmo DSA ed una lunghezza massima pari al doppio del modulo per l'algoritmo RSA grazie alla possibilità di utilizzare il *Chinese Remainder Theorem*.

In virtù delle considerazioni precedenti la scelta effettuata è stata quella dell'algoritmo RSA in quanto consente di:

- poter scegliere tra una vasta gamma di fornitori;

⁶ Punto soppresso dall'art. 2, D.M. 6 novembre 2003.

- estendere, in futuro, la lunghezza della chiave].⁷

6.3.2 Formati

[I formati generalmente utilizzati dalla crittografia asimmetrica sono:

- il formato ISO 9796 parte 2;
- il formato PKCS#1.

Il formato ISO 9796-2 è adottato dallo *standard* EMV per l'autenticazione statica e dinamica.

In applicazioni non EMV questo formato è consigliabile quando l'intero processo di autenticazione comporta l'utilizzo di due *Smart Card* (Mutua autenticazione interna ed esterna).

Il formato PKCS#1 è consigliabile in quanto può essere considerato «*standard de facto*» ed i messaggi di autenticazione (*Response*) costruiti secondo questo formato possono essere verificati dalle applicazioni che utilizzano gli strumenti tipici delle *Public Key Infrastructure*].⁸

6.4 Strong Authentication lato Server.

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

La figura [4] illustra i componenti che intervengono nel processo di autenticazione.⁹

QuickTime™ and a
TIFF (LZW) compressor
are needed to see this

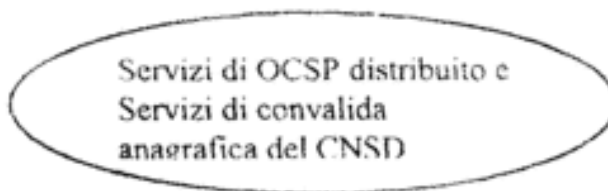


FIGURA 4

6.4.1 Server Authentication Middleware

[Il *Server Authentication Middleware* è lo strato *software* che fornisce i servizi crittografici alla Applicazione.

Le funzioni che questo strato rende disponibili sono:

- Generazione di quantità *random*;
- Funzioni di *Hash*;
- Gestione di Certificati digitali in formato X509v3;

⁷ Ibidem.

⁸ Ibidem.

⁹ Punto così sostituito dall'art. 2, D.M. 2 agosto 2005.

- *Verify Certificate* (per validare il certificato della CIE)
- *Verify Signature* (per validare il messaggio di Autenticazione)
- Caricamento della *Certificate Revocation List*
- Gestione della *Revocation List*.

Quelle descritte sono solamente un *subset* delle funzionalità del *Server Authentication Middleware* in una Infrastruttura a Chiave Pubblica ma sono comunque sufficienti per considerare la possibilità di utilizzo di *software* di mercato.

I requisiti di questa componente *software* sono:

- servizi crittografici come descritto nei punti precedenti;
- interoperabilità con i *Client*;
- indipendenza degli strumenti di produzione dei certificati.

Il primo requisito è una funzionalità tipica dei *Middleware* crittografici, il secondo requisito è soddisfatto dalla scelta fatta per Algoritmo e Formato che rende univoca la struttura del messaggio di Autenticazione mentre il terzo requisito è garantito dal circuito di emissione della Carta di Identità Elettronica essendo la produzione dei certificati di competenza di SSCE].¹⁰

6.5 Installazione dei servizi

L'installazione dei servizi avviene durante la fase di formazione e rilascio da parte dei comuni descritta in maniera analitica nel successivo capitolo 7.

6.6 Aggiornamento dei dati relativi alla fruizione dei servizi

[Nei paragrafi precedenti è stato approfondito il tema della autenticazione della CIE verso un Ente in grado di erogare servizi, in questo paragrafo viene completato il processo di autenticazione specificando le procedure che permettono alla CIE di verificare l'autenticità del servizio remoto con cui sta interagendo. Questo processo è chiamato: Autenticazione Esterna

Un altro tema trattato in questo paragrafo è il caricamento remoto sicuro di dati nella CIE da parte dell'Ente che eroga il servizio, questo processo è chiamato *Secure Messaging*.

I processi di Autenticazione e di *Secure Messaging* garantiscono l'interazione diretta tra Ente e Carta di Identità Elettronica e prevengono dai tentativi di intrusione che possono essere condotti sulla rete.

Il processo di autenticazione esterna utilizza metodologie di crittografia asimmetrica tramite la chiave pubblica del servizio (S_{pub}) mentre il processo di *secure messaging* utilizza crittografia simmetrica.

Per quanto concerne la gestione delle chiavi simmetriche sono stati oggetto di valutazione i seguenti due metodi:

- quello basato sullo utilizzo di «*diversified key*» (K_s) derivate da «*master key*» (K_m) e caricate nella CIE durante la fase di Installazione dei servizi;
- quello basato sullo scambio di una chiave di sessione (K_s) generata in modo casuale dalla CIE e crittografata ed autenticata dalla CIE stessa.

¹⁰ Punto soppresso dall'art. 2, D.M. 6 novembre 2003.

Il primo metodo è consolidato e comunemente impiegato nelle applicazioni *Smart Card Based* ma richiede particolare attenzione nella custodia e distribuzione delle chiavi.

Il secondo metodo, in fase di valutazione, richiede la scrittura di un comando *ad hoc* che consente la generazione, la crittografia e la autenticazione della chiave di sessione all'interno della CIE al fine di garantire alla Applicazione *Server* che quella chiave può essere decrittografata solo da lei e generata solamente dalla CIE].¹¹

6.7 Autenticazione esterna

[Il processo di autenticazione esterna è attivato dall'applicazione remota che deve poter accedere ai *file* della Carta di Identità Elettronica per aggiornarne i dati.

Questo processo utilizza la chiave pubblica del servizio (S_{pub}) che è stata caricata nella carta durante la fase di installazione del servizio.

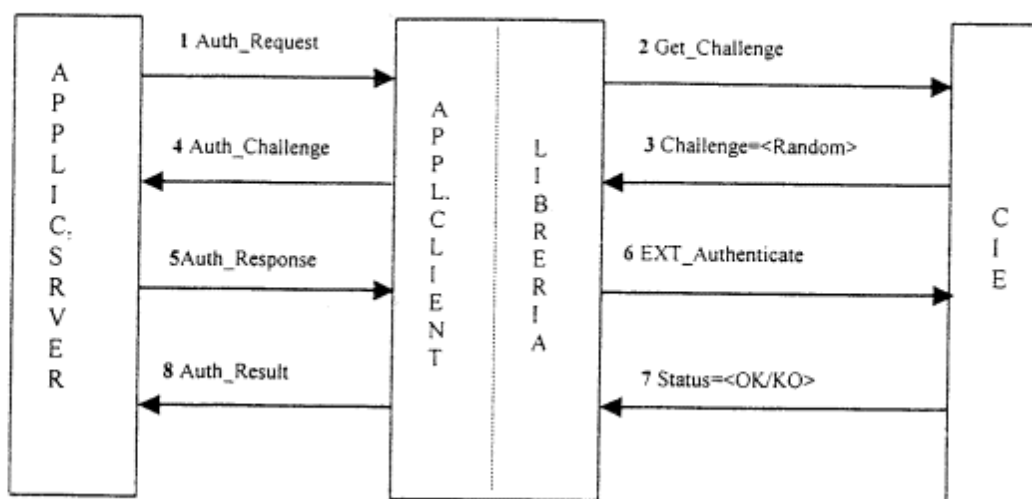
L'Autenticazione Esterna coinvolge i seguenti moduli:

- applicazione *Server*
- applicazione *Client*
- libreria di interfaccia e CIE.

La Figura [5] schematizza un esempio di flusso di informazioni scambiate tra i vari moduli che concorrono al processo di autenticazione esterna.

Il processo di Autenticazione Esterna è attivato dalla applicazione *Server* dopo che è stata riconosciuta (autenticata) la Carta ed il titolare.

Figura [5]



Orientativamente, il processo di Autenticazione si svolge secondo i seguenti passi procedurali:

1. L'Applicazione *Server* richiede alla Applicazione *Client* di essere autenticata dalla CIE (ad es. tramite il comando «**Aut_Request**»);

¹¹ Punto soppresso dall'art. 2, D.M. 6 novembre 2003.

2. L'applicazione *Client*, servendosi della LIBRERIA, invia una «*challenge*» alla CIE (ad es. con il comando «**Get_Challenge**»);
3. La risposta della CIE è un numero *random* (il *Challenge*);
4. L'Applicazione *Client* invia alla Applicazione *Server* il numero *random* generato dalla CIE (ad es. con il comando «**Aut_Challenge**»);
5. L'Applicazione *Server* firma il *Challenge* con la chiave privata del servizio (S_{pri}), e lo invia alla Applicazione *Client* (ad es. con il comando «**Auth_Response**»);
6. La applicazione *Client*, servendosi della libreria, richiede alla CIE un'operazione di «autenticazione esterna»;
7. La CIE utilizza la chiave pubblica del servizio (S_{pub}), relativa alla *directory* a cui si vuole accedere, per verificare la autenticità del *Response*; se la verifica è positiva viene inviato un messaggio di consenso alla Applicazione *Client* tramite la libreria e viene reso disponibile l'accesso ai *file* appartenenti a quella *directory*;
8. L'Applicazione *Client* comunica alla Applicazione *Server* l'esito del processo (ad es. tramite il messaggio «*Auth_Result*»);

Nella descrizione del processo di Autenticazione Esterna si sono trascurati dettagli procedurali quali la gestione delle eventuali anomalie e le «*Retry*» tipiche di questi processi in quanto non incidono sulle funzionalità della CIE].¹²

6.8 Secure Messaging

[Il processo di *Secure Messaging* è attivato dopo i processi di autenticazione e consente lo scambio dati crittografato tra CIE ed Applicazione *Server*.

Esso utilizza una chiave di sessione diversificata K_D che è:

- derivata da K_S attraverso la generazione di una quantità *Random*, qualora venga scelto di distribuire le chiavi secondo metodi convenzionali durante la fase di emissione;
- coincidente con la chiave K_S autogenerata in modalità casuale, qualora venga scelta la distribuzione delle chiavi di sessione dalla CIE alle Applicazioni *Server* con un apposito comando basato sull'utilizzo di crittografia asimmetrica.

Il comando di *Secure Messaging* dovrà essere implementato secondo la norma ISO 7816-4 nella modalità «*Secure Messaging for Confidentiality*»].¹³

7. Processo di Emissione

Nel presente capitolo sono descritte in dettaglio le fasi operative previste dal circuito d'emissione.

Per una migliore comprensione del processo d'emissione si riporta un glossario di riferimento.

Fb	Fornitori Bande Ottiche
Fp	Fornitori microprocessori

¹² Punto soppresso dall'art. 2, D.M. 6 novembre 2003.

¹³ Ibidem.

IPZS	Istituto Poligrafico Zecca dello Stato
SSCE	Sistema di sicurezza del circuito di emissione (Ministero dell'Interno)
E	Ente emittitore della CIE, Tipicamente un comune.
ID_Carta	Numero identificativo della carta Numero assegnato al documento d'identità e generato dal sistema di sicurezza.
C_Carta	Certificato anticontraffazione della carta Certificato che lega il numero identificativo del documento, del titolare e <ul style="list-style-type: none"> - una chiave pubblica (Kpub), corrispondente ad una privata (Kpri), generata all'interno del microprocessore e non esportabile all'esterno. - rilasciato dal SSCE e viene riportato nella banda ottica e nel microprocessore. - Unisce in maniera inscindibile i due supporti informatici.
Dati_processore	È un file elementare che riporta alcuni dati univoci del processore Le informazioni che contiene sono: Fp, numero seriale e data fabbricazione.
Dati_banda_ottica	È un file elementare che riporta alcuni dati identificativi univoci della banda ottica Le informazioni che contiene sono: Fb, numero seriale e data fabbricazione
Rd	Record dati. È un'area della banda ottica che contiene i dati necessari
PIN P1	Cifrato con la chiave pubblica del comune di destinazione. Serve per abilitare l'accesso in scrittura ai file elementari. Rende ulteriormente sicura la fase di compilazione.
PIN utente	È il PIN necessario al titolare per utilizzare la chiave privata Kpri per le operazioni di autenticazione in rete. Viene consegnato dal comune di rilascio con meccanismi di sicurezza (es. busta in carta chimica protetta).
PUK utente	È il PUK (Personal Unblocking Key) necessario al titolare per sbloccare la carta e reimpostare il PIN utente. Viene consegnato dal comune di rilascio con meccanismi di sicurezza (es. busta in carta chimica protetta).
PIN SO	È il PIN di Security Officer necessario per l'installazione della firma digitale sulla carta. Viene consegnato al titolare dal comune di rilascio con meccanismi di sicurezza (es. busta in carta chimica protetta).

7.1 Produzione di banda laser e microprocessore

I Fornitori di microprocessori (Fp) ed i Fornitori di bande ottiche (Fb) provvedono alla fabbricazione dei supporti informatici.

I Fornitori di microprocessori provvedono anche alla mascheratura in ROM del Sistema Operativo.

Entrambi i fornitori applicano, in fase di produzione, un numero seriale progressivo univoco, sui supporti informatici da loro forniti e predispongono una distinta, cartacea ed elettronica, che riporta le seguenti indicazioni: ID fornitore, numero seriale, numero del lotto di produzione, data di produzione.

I fornitori, successivamente inviano i loro prodotti, accompagnati dalle distinte, direttamente all'Istituto Poligrafico dello Stato (IPZS).

7.2 Produzione ed inizializzazione della carta d'identità elettronica e del documento elettronico

Per meglio comprendere le diverse fasi del circuito di emissione, è bene fare dei brevi cenni sull'organizzazione e sulla normalizzazione delle informazioni sui supporti informatici della CIE.

7.2.1 Struttura delle informazioni sulla banda ottica ⁽⁵⁴⁾

Sulla banda ottica vi sono due aree di memorizzazione differenti ma sincrone:

- Una area dati che contiene, codificati in record di formato opportuno (R_d), i necessari dati della carta, del titolare e i servizi installati.
- Una area di controllo che contiene, codificate in formato opportuno (R_c), le informazioni di controllo e verifica dei corrispondenti R_d .

L'area controllo è assimilabile ad un registro incrementale delle operazioni avvenute sulla carta, e consente di stabilire con certezza *chi, dove e quando* ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato dei «sigilli» apposti da:

- Istituto Poligrafico dello Stato;
- comuni;
- SSCE.

A ciascun record R_d dell'area dati corrisponde un record R_c dell'area di controllo. 1 record dati possono avere formati multipli secondo necessità.

I record R_d dell'area dati sono formati da IPZS e da E. I record R_c dell'area di controllo sono composti da due parti: una formata da IPZS e da E, l'altra formata da SSCE.

La successiva figura mostra l'organizzazione in record corrispondenti dell'area dati (File_dati) e dell'area di controllo (File_controllo):

Area dati (File_dati)
Record 1
Record 2
...
Record N

Area controllo (File_controllo)
Record 1
Record 2
...
Record N

La successiva figura mostra, invece, per ciascun record corrispondente dell'area dati e di quella di controllo, la suddivisione in campi:

i-esimo Record dati
Segmento generato da IPZS o E
campi tabella [7.1 - B]

i-esimo Record di controllo	
Segmento generato da IPZS o E	Segmento generato da MI
campi 1-6 tabella [7.1 - A]	campi 7-13 tabella [7.1 - A]

Questi record contengono dunque richieste (di IPZS o E) ed approvazioni (di SSCE), e permettono di far avanzare la carta da uno stato di lavorazione all'altro, lungo il "percorso" che la porta dalla manifattura fino al momento del rilascio al titolare.

Questo flusso di richiesta ed approvazione è lo stesso utilizzato anche per il microcircuito, per cui nel record di controllo sono presenti elementi che andranno poi memorizzati nel chip (come il certificato C_Carta), e che consentono in tal modo anche un utile corrispondenza dei dati tra chip e banda ottica.

La tabella seguente definisce la struttura (campi) del record di controllo:

<i>Campo</i>	<i>Generato da</i>	<i>Descrizione</i>	<i>Note</i>
1	IPZS, E (S)	Numero progressivo del record nell'ambito della carta	Questa informazione è sempre presente
2	IPZS, E (S)	Tipo del record (ossia dell'operazione)	Inizializzazione o Emissione
3	IPZS, E (S)	Data e ora della creazione del record	Questa informazione è sempre presente
4	IPZS, E (S)	Certificato dell'ente che ha creato il record	Questa informazione è sempre presente. Il certificato è emesso da MI
5	IPZS, E (S)	Identificativo dell'operatore che ha creato il record	Questa informazione ordinariamente è sempre presente, salvo casi eccezionali in cui non sia previsto l'intervento manuale di un operatore nella generazione del record.
6	IPZS (Fc),E (S)	Bollo elettronico dell'ente che ha creato il record.	Coincide con la firma del record dati (Rd) e dei campi [1-5] del corrispondente record di controllo (Rc), utilizzando la chiave relativa al certificato (4). Il bollo elettronico certifica i dati generati dall'ente che li ha generati ed immessi nel circuito.
7	SSCE	Numero progressivo dell'autorizzazione concessa (generato secondo un protocollo interno di SSCE)	Questa informazione è sempre presente.
8	SSCE	Data ed ora dell'autorizzazione	Questa informazione è sempre presente,

9	SSCE	Numero identificativo della carta	il numero (ID_Carta) assegnato al documento d'identità da SSCE e stampato anche sul supporto plastico.
10	SSCE	Certificato del SSCE	Questa informazione è sempre presente.
11	SSCE	Identificativo dell'operatore che ha creato il record	Questa informazione ordinariamente è assente, salvo casi eccezionali in cui sia previsto l'intervento manuale di un operatore nella generazione del record (ad es. se durante i controlli automatici emergono condizioni per cui è necessaria un'indagine più approfondita su un determinato individuo, ecc.).
12	SSCE	Certificato anti-contraffazione della carta	È il certificato (C_Carta) che lega il numero identificativo della carta (ID - Carta) ed una chiave pubblica (Kpub), corrispondente ad un'unica chiave privata (Kpri), generata all'interno del microcircuito e non esportabile all'esterno di esso. Esso è rilasciato da SSCE per essere memorizzato oltre che sulla banda ottica, anche nel microcircuito. Questa informazione permette di legare in modo biunivoco il microcircuito e la banda ottica presenti sulla stessa carta.
13	SSCE	Bollo elettronico dell'ente di controllo e verifica.	Coincide con la firma del record dati (Rd) e dei campi [1-12] del corrispondente record di controllo (Rc), utilizzando la chiave relativa al certificato (10). Il bollo elettronico certifica l'approvazione, da parte dell'ente di controllo e verifica, dei dati di inizializzazione e/o personalizzazione della carta.

La seguente tabella definisce la struttura (campi) del record dati.

<i>Campo</i>	<i>Generato da</i>	<i>Descrizione</i>	<i>Note</i>
1	IPZS, E	Numero progressivo del record nell'ambito dell'area dati (File_dati). Il numero progressivo di ogni record dell'area dati deve corrispondere a quello del record dell'area di controllo che descrive l'operazione eseguita per generarlo e contiene le relative approvazioni (firme)	Questa informazione è sempre presente
2	E	Embedded Hologram	Viene «Impresso» anche in evidenza visiva sulla banda ottica al momento dell'emissione. Solo il record che descrive questa fase è non nullo.
3	IPZS	Dati identificativi univoci della banda ottica (n. serie, lotto di produzione, fabbricante, ecc.)	Non nullo solo nel record relativo all'inizializzazione, eseguita da IPZS. Questi dati vengono comunicati dai fornitori della banda ottica
4	E	Chiave biometrica individuale.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
5	E	Dati personali dell'individuo, con l'eccezione della fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
6	E	Fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.

7.2.2 Struttura delle informazioni nel microprocessore

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

Fornito da: indica l'operazione in ragione della quale viene messo a disposizione un contenuto informativo, consistente in una sequenza di *bytes*. Ad esempio, il risultato della raccolta dei dati personali del titolare, effettuata dall'ente emettitore (il comune).

Predisposto da: indica l'operazione di creazione di una nuova struttura dati (DF o EF), ossia di un «contenitore» vuoto, pronto ad essere riempito con le informazioni che risultano da un'operazione del tipo precedente.

Scritto da: è l'operazione con la quale un contenitore vuoto (EF) viene riempito con le informazioni che risultano da una precedente operazione di generazione.

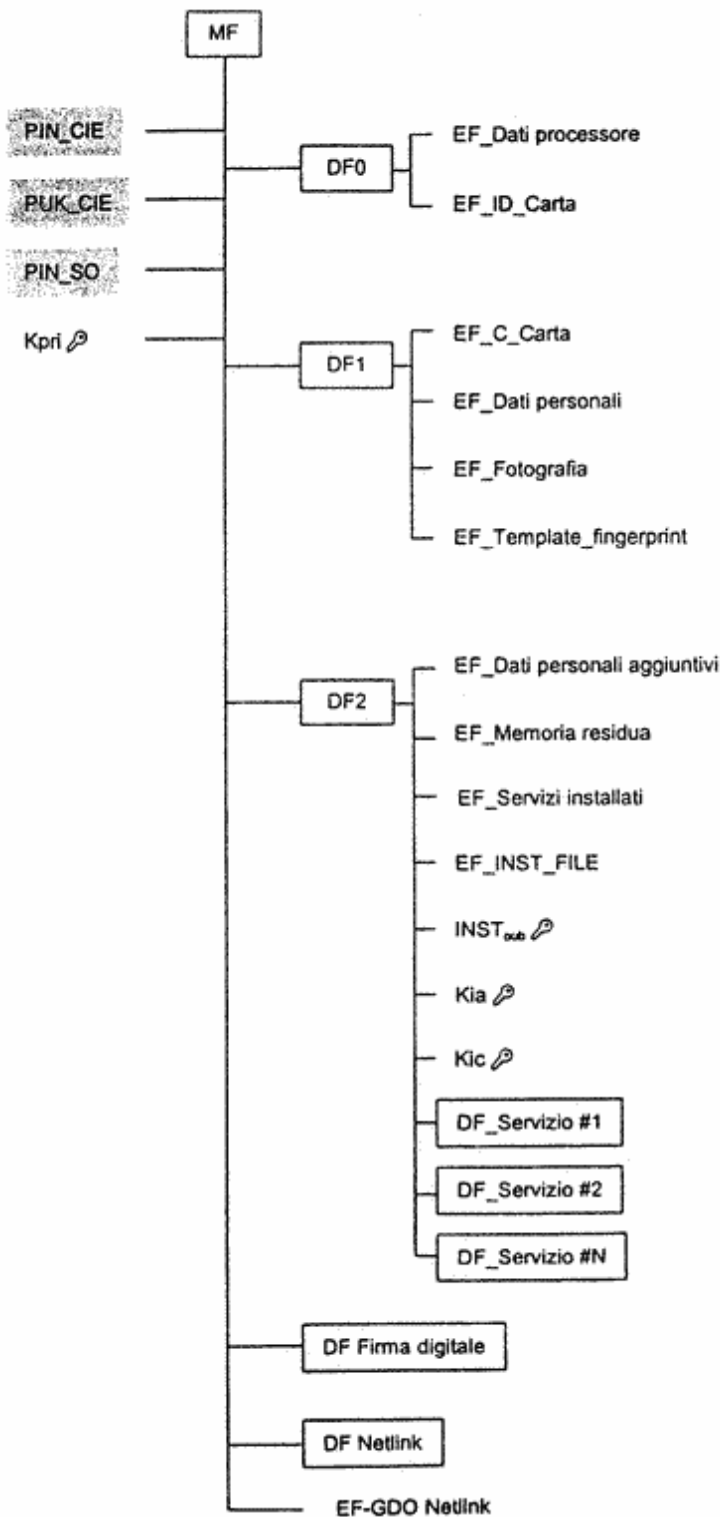
#	Elemento	Fornito da	Predisposto da	Scritto da	Descrizione
1	MF		IPZS		È il «Master File» della struttura di memorizzazione. Corrisponde più o meno alla directory radice di un ordinario sistema operativo.
2	DF0		IPZS		Dedicated file (directory) dove vengono memorizzate le informazioni prodotte durante la fase di inizializzazione della carta.
3	DF1		IPZS		Dedicated file (directory) dove vengono memorizzate le informazioni raccolte durante la fase di personalizzazione della carta.
4	DF2		IPZS		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.
5	PIN	E	E	E	È il PIN utente richiesto per usare la chiave privata Kpri per le operazioni di autenticazione. Questo codice deve essere consegnato dal comune di rilascio, con garanzia di segretezza, al titolare della CIE.
	PUK	E	E	E	È il PUK utente richiesto per sbloccare la carta nel caso non si disponga del PIN. Questo codice deve essere consegnato dal comune di

	PIN_SO		IPZS		rilascio, con garanzia di segretezza, al titolare della CIE. È il PIN di Security Officer necessario per l'installazione della firma digitale. Questo codice deve essere consegnato dal comune di rilascio, con garanzia di segretezza, al titolare della CIE.
6	Kpri		E		Chiave autogenerata internamente alla carta, congiuntamente a Kpub. 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.
7	INSTpub	E	IPZS	IPZS	Chiave pubblica del servizio di installazione delle strutture dati relative ai servizi. La responsabilità operativa del processo di installazione del servizio è delegata ai comuni.
	EF_INST_FILE	E	IPZS	IPZS	È un file elementare che contiene le chiavi per l'installazione dei servizi qualificati. È cifrato con la chiave INSTpub
8	Dati_processore	IPZS	IPZS	IPZS	È un file elementare (EF) che riporta alcuni dati identificativi univoci del processore (n. serie, lotto di produzione, fabbricante,

10	ID_Carta	SSCE	IPZS	IPZS	ecc.) Numero identificativo (matricola) della carta d'identità, generato dal Ministero dell'Interno e corrispondente al numero stampato da IPZS sul supporto plastico.
11	C_Carta	SSCE	IPZS	E	È il certificato rilasciato da SSCE, che garantisce la validità del legame tra la componente pubblica, Kpub, della coppia di chiavi generata internamente al microcircuito, e ID_Carta; esso contiene, come estensione, il risultato dell'esecuzione di una funzione di hash sui dati identificativi raccolti all'atto della formazione della carta (e riportati anche sul supporto plastico).
12	Dati_personali	E	IPZS	E	È un file elementare che contiene i dati personali dell'individuo, con l'eccezione della fotografia.
13	Dati_personali aggiuntivi	E	IPZS	E	È un file elementare che contiene dati, relativi alla persona, che integrano le informazioni anagrafiche, che possono essere necessarie ai fini dell'erogazione di alcuni servizi.
14	Memoria_residua	E	IPZS	E	È l'ammontare dello spazio totale previsto per i servizi, decurtato dello spazio utilizzato da quelli già installati.

15	Servizi_installati	E	IPZS	E	È un file elementare che riporta l'elenco dei servizi già installati sulla carta. Sono le strutture dati relative ai servizi installati sulla carta. Esse comprendono, quando il servizio richiede particolari garanzie di sicurezza, la chiave pubblica del servizio per l'autenticazione in rete di quest'ultimo da parte della carta (Spub).
16	DF_Servizio #1, DF_Servizio #2, ... DF-Servizio #N	E	E	E	

La successiva figura descrive graficamente la struttura di memorizzazione interna al microprocessore:



7.3 Le fasi preliminari

L'Istituto Poligrafico, responsabile della manifattura della CIE, riceve dalle Prefetture, in via telematica, le richieste di fornitura di «documenti in bianco», distinte per Comune, e dai fornitori i microprocessori e le bande ottiche.

La consegna, alle Prefetture, dei «documenti in bianco» avviene al termine delle seguenti sottofasi di generazione numeri identificativi, produzione, inizializzazione ed incisione grafica degli elementi costanti.

7.3.1 Generazione numeri identificativi per le carte d'identità ed i documenti elettronici

L'IPZS richiede al SSCE i numeri identificativi (ID-Carta) necessari;

SSCE genera i nuovi ID-Carta ed inserisce un equivalente numero di *record* «in attesa» di divenire CEE nel suo database centrale;

L'IPZS riceve via telematica i lotti di numeri identificativi da assegnare alle nuove carte in corso di produzione.

7.3.2 Produzione

L'IPZS, attiva le procedure necessarie ai fini della:

- predisposizione del supporto fisico;
- inserimento nel supporto fisico della pellicola di banda ottica e del microprocessore;
- stampa del logo e degli elementi grafici costanti e di sicurezza;
- inizializzazione elettrica del microprocessore.

7.3.3 Inizializzazione

La sottofase di inizializzazione, una delle più delicate dell'intero processo di emissione, consente di trasformare i tre supporti previsti, in un unico elemento inscindibile.

Dopo la fase di integrazione fisica del supporto plastico, con la banda ottica ed il microprocessore, l'inizializzazione provvede alla integrazione logica tramite l'apposizione di codici univoci.

Mentre risulta di immediata applicazione il codice apposto graficamente sul supporto fisico, l'inizializzazione di quelli informatici ha quale prerequisito la loro «formattazione» che, di fatto, consiste nella loro strutturazione in «*directory*» e l'impostazione delle condizioni di test necessarie a definire i diritti di accesso alle *directory*.

Le *directory*, definite in dettaglio nei precedenti paragrafi, servono per tracciare tutte le fasi di inizializzazione e personalizzazione della Carta, per consentire l'installazione dei servizi qualificati e per normalizzare i dati identificativi del titolare, le informazioni alfanumeriche nonché le immagini.

In particolare, IPZS provvede alla:

- generazione della struttura dati interna della banda ottica;
- generazione della struttura dati interna del microprocessore;
- scrittura dei *files* elementari che riportano i dati specifici del microprocessore («Dati-processore»), della banda ottica («Dati banda ottica») e del sistema operativo («Parametri-APDU»);
- scrittura ID-Carta;

- impostazione delle condizioni di accesso a tali *file*;
- - scrittura del *record* dati (Rd) e di alcuni campi (1-6) di quello di controllo (Rc) relativi all'operazione di inizializzazione. Il *record* di controllo deve contenere almeno:
 - ID Carta;
 - Dati Processore/Dati Banda Ottica;
 - Data di fabbricazione;
 - PIN P1 (per abilitare l'accesso in scrittura dei *files* elementari che devono essere riempiti dal Comune al momento della formazione della carta) cifrato con la chiave pubblica del comune).
 - Indicazione della Provincia e del comune cui la carta è destinata.
- inserimento del *record* dati e di quello di controllo in coda ad un *file* di richieste di autorizzazione da inviare a SSCE;
- stampa dello sfondo, del Logo, del numero di carta (ID Carta, quello generato da SSCE) e degli altri elementi costanti;
- incisione grafica sulla banda ottica (*Embedded Hologram*) degli elementi costanti e dell'ID-Carta;
- stoccaggio della carta.

7.3.4 Attivazione

Al termine della presente sottofase la carta d'identità risulta «attivata», e diventa «documento in bianco», ossia pronto alla fase successiva di formazione e rilascio, ad opera dei Comuni.

Durante la presente sottofase l'IPZS esegue le seguenti attività:

- riceve da SSCE il *file* di approvazione per attivare il lotto di carte in lavorazione;
- inserisce le carte, che fanno parte del lotto autorizzato, nello/negli apparati per la lettura del *chip* e della banda ottica e legge l'ID-Carta contenuto nei due supporti (la lettura in entrambi i supporti costituisce un ulteriore controllo sui dati inseriti);
- trasmette a SSCE le associazioni ID-Carta/Provincia richiedente;
- invia le carte in bianco attivate alle Prefetture. Queste ultime sono, a loro volta, incaricate della distribuzione nella provincia di loro competenza agli enti autorizzati alle procedure di emissione (Comuni E).

Al completamento di questa fase il data base di SSCE conterrà tanti *record* quante sono le carte in bianco in attesa di formazione. Tali *record* contengono già informazioni come il numero identificativo della carta (ID-Carta), la Provincia ed il Comune di destinazione.

Durante la fase di personalizzazione i campi di tali *record* verranno ulteriormente popolati con i codici fiscali (scritti in chiaro) dei titolari e con i dati identificativi (scritti in forma cifrata) degli stessi.

La cifratura avverrà, tramite un sistema automatico, utilizzando la chiave pubblica della Questura, territorialmente competente, e quella del comune che ha rilasciato la Carta d'Identità Elettronica.

7.4 Personalizzazione ed emissione delle carte

La formazione delle carte ed il loro rilascio è condotta direttamente dai Comuni. Nei paragrafi successivi le chiavi asimmetriche saranno indicate con la seguente notazione:

- $K_{\text{pri-aut}}$, chiave privata di autenticazione;
- $K_{\text{pub-aut}}$, chiave pubblica di autenticazione;
- $K_{\text{pub-enc}}$, chiave privata di crittografia;
- $K_{\text{pub-enc}}$, chiave pubblica di crittografia.

7.4.1 Ricezione dei documenti in bianco (fa riferimento all'art. 12 del D.M.)

Il comune per il tramite delle Prefetture della propria provincia, riceve i documenti in bianco;

I documenti devono essere conservati dai comuni in appositi armadi di sicurezza, possibilmente in locali ad accesso riservato.

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 K_{pub} e K_{pri} (della carta) necessarie per garantire l'autenticazione in rete della carta e generazione del PIN utente per la protezione dei dati personali. È ammissibile per la CIE un ulteriore PIN per abilitare le operazioni di crittografia asimmetrica che utilizzano la K_{pri} 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 è indispensabile per proteggere i dati durante la trasmissione al SSCE utilizzando la $K_{\text{pub-enc}}$ 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 $K_{\text{pri-aut}}$ (Comune). L'apposizione di tale bollo garantisce il mittente al SSCE;

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

7.4.1.2 Sottofase di autorizzazione

La sottofase di autorizzazione viene effettuata dal SSCE quando, da un qualsiasi comune, riceve una richiesta di rilascio di una nuova CIE. Vengono eseguite le seguenti attività:

1. SSCE riceve i dati raccolti dal comune;
2. SSCE estrae, tramite la propria $K_{\text{pri-enc}}$, il *record* dati;
3. SSCE mantiene in chiaro codice fiscale, provincia e comune richiedente e cifra tutte le altre informazioni con due chiavi: la $K_{\text{pub-aut}}$, del comune richiedente e la $K_{\text{pub-aut}}$ della Questura territorialmente competente;
4. SSCE esegue il controllo automatico di «non esistenza» sulla propria base dati, tramite i dati in chiaro e la K_{pub} della CIE;
 - a. Controllo positivo (es. CIE già rilasciata per quel codice fiscale, richiesta avanzata da un comune diverso da quello previsto e soprattutto che la K_{pub} della CIE non sia identica ad una già certificata, etc.) viene rigettata la richiesta non vengono seguite ulteriori attività e all'ente emittitore viene ritornato un opportuno codice di errore.
 - b. Controllo negativo (la richiesta può essere soddisfatta).
5. SSCE trasmette l'esito dell'operazione di autorizzazione. I dati vengono inviati cifrati utilizzando la $K_{\text{pub-enc}}$ del Comune ed una chiave di trasporto a 128 bit generata sessione per sessione e certificati con il bollo elettronico del SSCE ($K_{\text{pri-aut}}$ di SSCE).

7.4.1.3 Sottofase di formazione

Sottofase di competenza dell'Ente emittitore che riporta i dati su tutti i supporti: microprocessore, banda ottica e grafici sul supporto fisico. La criticità maggiore sta nel fatto che, qualsiasi inconveniente possa verificarsi non deve mettere a rischio l'integrità dei dati (per es. scrivendo informazioni diverse sui vari supporti). Allo scopo si suggerisce di garantire agli strumenti informatici continuità elettrica.

1. **E** riceve il *record* dati validato da SSCE;
2. memorizza i dati nel microprocessore;
3. memorizza i dati nella banda ottica. Al fine di garantire l'allineamento delle informazioni il lettore/scrittore di banda ottica dovrebbe avere la possibilità di leggere anche il microprocessore. Al fine di consentire una identificazione sicura, e dare certezza sulla originalità della CIE, i dati memorizzati nella banda ottica devono essere quelli firmati con il bollo elettronico del SSCE.
4. stampa grafica dei dati sul supporto fisico. Anche in questo caso sarebbe opportuno che la stampante sia in grado di leggere il microprocessore.
5. stampa del PIN utente su speciale carta chimica retinata, tale da garantire la riservatezza dell'informazione contenuta e di evidenziare eventuali tentativi di apertura.

7.4.1.4 Sottofase di rilascio

Anche questa sottofase è di esclusiva competenza dei comuni che:

1. rilasciano la CIE al cittadino che ne ha fatto richiesta;
2. consegnano la busta conte.
3. comunicano a SSCE l'avvenuto rilascio tramite comunicazione telematica diretta.

7.4.1.5 Sottofase di verifica e controllo

La verifica ed il controllo sono le uniche attività sempre presenti in tutte le sottofasi di lavorazione della CIE, dal momento della produzione fino al loro rilascio e vengono condotte da SSCE. Per questo motivo tutti gli enti coinvolti nei vari momenti del processo devono disporre di una connessione telematica con il Sistema.

Ovviamente la verifica ed il controllo citato nel processo di formazione, non è riferito a quello che verrà dettagliato nel capitolo successivo che, invece, si riferisce ai controlli effettuabili dalla Polizia come previsto dal Testo Unico delle Leggi di P.S.

8. Verifica delle carte di identità elettroniche (fa riferimento all'art. 6, comma 1 del D.M.)

Nel presente capitolo sono descritti in dettaglio i casi in cui è consentito l'accesso alle CIE ed alle informazioni in esse contenute. Vengono, altresì, indicati gli organi competenti e le modalità di accesso.

8.1 Conservazione del cartellino elettronico (fa riferimento all'art. 6, comma 3 del D.M.)

Il processo di ammodernamento della CIE deve necessariamente portare ad una differente interpretazione di alcune delle norme precedenti, soprattutto di quelle destinate alla gestione del modello cartaceo, ormai superato.

È pressoché intuitivo come non trovino ragione di essere le prescrizioni relative alla conservazione e consultazione della copia del cartellino presente in ciascuna Questura. L'obbligo previsto per i Comuni di trasmettere copia del cartellino per ogni carta di identità rilasciata, viene sostituito dalla seguente procedura prevista per il nuovo cartellino elettronico:

- i Comuni eseguono le attività di formazione e rilascio delle CIE;
- SSCE riceve comunicazione che è stata rilasciata la CIE e memorizza la copia elettronica, della stessa, nell'archivio della Questura territorialmente competente. La copia elettronica, viene cifrata con la chiave pubblica della Questura stessa. Tale modalità consente di attendere al Testo Unico delle Leggi di P.S. che indica nelle Questure l'ufficio a cui è demandata la conservazione della copia delle CIE;
- i controlli sulle CEE, una volta memorizzate, possono essere effettuati secondo le seguenti modalità:
- da qualsiasi operatore delle Forze di Polizia tramite controlli a vista, apparecchiature *stand-alone* (lettori di banda ottica) o transazioni a SSCE. In quest'ultimo caso, se la richiesta arriva da una Questura di una Provincia diversa da quella dove è stata rilasciata la CIE, l'operatore può, tramite il codice fiscale del titolare o il numero della CEE verificarne l'esistenza, il comune e la provincia in cui è stata rilasciata, non può vedere nel dettaglio le informazioni della CIE;
- da un operatore della Questura nella cui Provincia è stata rilasciata la CIE. In questo caso l'operatore può, tramite il codice fiscale del titolare o il numero di CIE, verificarne l'esistenza e, tramite l'inserimento della propria chiave privata, verificarne anche il contenuto nel dettaglio.

- le Questure territorialmente competenti tramite SSCE conservano e consultano la copia elettronica della CIE. Possono eseguire anche stampe e tutte le attività già possibili con la passata gestione.

8.2 Interdizione dell'operatività della CIE (fa riferimento all'art. 6, comma 2 del D.M.)

Le caratteristiche principali della nuova CIE, che la differenziano dal vecchio modello cartaceo, sono rappresentate dalla presenza dei supporti informatici e dalla gestione centralizzata del flusso di emissione. Entrambi gli elementi da un lato aumentano il livello di sicurezza del nuovo documento e dall'altro offrono la possibilità di accesso a servizi telematici sia nazionali che locali.

Proprio questa nuova possibilità di accedere a servizi implica la necessità di dover interdire, più che in passato, l'utilizzo della CIE che potrebbe essere impiegata, in caso di furto o smarrimento, da persone diverse dal titolare.

Nel seguito vengono descritte le modalità a cui è necessario attenersi in caso di furto o smarrimento di una CIE.

- il titolare telefona al numero verde e comunica l'avvenuto smarrimento/furto della CIE;
- per motivi di sicurezza, l'interdizione temporanea della CIE avviene dopo che è stata svolta una successiva verifica telefonica;
- a seguito di tale comunicazione nel *record* relativo alla CIE viene apposto un «flag» e, per un periodo di 7 (sette) gg, la CIE non è in grado di accedere a servizi;
- successivamente alla comunicazione telefonica, il titolare della CIE deve presentare regolare denuncia ad un ufficio di Polizia;
- la denuncia viene trasmessa alla Questura della Provincia dove è stata rilasciata la CIE;
- la Questura inibisce, definitivamente, l'utilizzo in rete della CIE ed il titolare può richiedere un duplicato, recandosi al comune;
- se durante i sette gg. di interdizione momentanea non viene applicata l'interdizione definitiva, la CIE torna ad essere, nuovamente, «NON interdetta».

8.3 Carta sanitaria

L'installazione della componente sanitaria (Netlink) sulla CIE avviene in due fasi distinte che sono di seguito brevemente descritte:

- inizializzazione della CIE a cura di IPZS;
- formazione della CIE e caricamento dei dati sanitari.

Nella prima fase IPZS predispone le strutture dei dati sanitari (secondo le specifiche Netlink), compila i file elementari che non contengono dati specifici del cittadino e carica le quantità di sicurezza derivate dalle chiavi di gruppo fornite dal Ministero della salute.

Per la gestione della seconda fase (formazione 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 dai comuni:

- si utilizza un centro servizi regionale, delegato dal comune (e quindi omologato dal Ministero dell'interno) il quale, per i comuni che intendono fruire di questa soluzione, effettua la fase di formazione della CIE e l'installazione dei dati sanitari;
- i comuni gestiscono autonomamente la formazione della CIE oppure si avvalgono di un centro servizi omologato dal Ministero dell'interno ma diverso da quello regionale; in questo caso durante la fase di formazione sono installati i dati sanitari tramite collegamento con le ASL con cui i comuni hanno stabilito una opportuna convenzione;
- i comuni gestiscono autonomamente la formazione della CIE oppure si avvalgono di un centro servizi omologato dal Ministero dell'interno ma 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;
- i Comuni gestiscono autonomamente la formazione della CIE e la rilasciano senza i dati sanitari; in questo caso i cittadini si recano presso l'ASL di competenza per l'installazione dei dati sanitari; le ASL devono essere dotate delle infrastrutture hardware e software necessarie a gestire la CIE e a interfacciare le basi dati contenenti le informazioni sanitarie.

8.3.1 Carta sanitaria - Pilota italiano Netlink

Le specifiche PDC (Patient data card) per la carta sanitaria sono disponibili nei documenti di riferimento «NETLINK-Pilota italiano, Specifiche PDC - Inizializzazione» del 30 novembre 2000, «Dati PDC (pilota italiano)» del 21 settembre 2000 e «NETLINK-Pilota italiano, Specifiche PDC - pre-personalizzazione» del 30 novembre 2000.

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.

8.4.1 Certificati di firma digitale

In accordo con quanto previsto dalla normativa vigente e successive modificazioni, il certificato di firma digitale per un utilizzo della CIE come strumento di sottoscrizione dei documenti, deve essere conforme alla normativa vigente anche in materia di interoperabilità.

8.5 Impronte digitali.

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

Il template è 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.