Consiglio Nazionale delle Ricerche

I Documenti Elettronici nel Panorama Italiano

S. Bistarelli, S. Frassi, F. Santini

IIT B4-12/2005

Nota Interna

Dicembre 2005

Istituto di Informatica e Telematica

I Documenti Elettronici nel Panorama Italiano

I documenti elettronici di identificazione vigenti, emessi e circolanti sul territorio, che contengono uno o più elementi biometrici sono:

– Carta d'Identità Elettronica (CIE);
– Carta Multiservizi della Difesa (CMD).

In via di definizione e realizzazione:

– Permesso di Soggiorno Elettronico (PSE);
– Passaporto Elettronico (E-Passport).

Dal punto di vista dell'uso della biometria questo insieme di documenti si presenta in forma omogenea, in quanto l'identificatore biometrico comune utilizzato per tutti è costituito dall'impronta digitale, alla quale deve essere aggiunta, nel caso della CIE e del Passaporto Elettronico, anche la fotografia del volto del titolare in formato digitale.

Il formato di memorizzazione sui vari documenti elettronici dell'elemento biometrico è, nella fase attuale, in corso di standardizzazione. La tendenza consolidata a livello internazionale consiste nell'adozione delle indicazioni e degli standard di riferimento che pervengono dall'ICAO (*International Civil Aviation Organization*), organizzazione particolarmente accreditata su questo tema, Come rilevato in precedenza, l'acquisizione dell'impronta digitale e della fotografia, per tutti i quattro documenti elettronici CIE, PSE, CMD, E-Passport, avviene alla presenza di un funzionario accreditato appartenente all'Amministrazione Pubblica competente al rilascio (dell'anagrafe del comune emettitore nel caso della CIE, del Ministero della Difesa nel caso della CMD, della Polizia di Stato o del Ministero degli Affari Esteri per il passaporto elettronico, dell'UTG nel caso del PSE), ed è regolata (o dovrà esserlo prima dell'entrata in vigore).

Il Servizio Polizia Scientifica della Polizia di Stato ha storicamente maturato una significativa esperienza nel trattamento delle impronte digitali anche attraverso la gestione del sistema di riconoscimento AFIS (*Automated Fingerprint Identification System*) e la competenza tecnica acquisita è alla base della realizzazione e gestione dei documenti di identificazione biometrici a livello nazionale.

Il Ministero dell'Interno, soprattutto grazie alla competenza istituzionale in materia, ha definito, e sta definendo, le specifiche di realizzazione della CIE, del PSE e, di concerto con il Ministero degli Affari Esteri, del passaporto elettronico dello Stato Italiano, contribuendo all'allineamento del quadro normativo di riferimento e alla precisazione dei contesti organizzativo e tecnologico (come nel caso della CIE dove il Ministero dell'Interno detiene anche il controllo della fase di realizzazione del progetto).

Elemento fondamentale nella realizzazione e nella gestione dei diversi tipi di documenti elettronici è costituito dalla loro compatibilità in termini di trattamento dell'identificativo biometrico e delle infrastrutture necessarie alla gestione del ciclo di vita di ciascun documento.

CARTA D'IDENTITÀ ELETTRONICA

La CIE, nell'ambito degli aspetti biometrici, contiene il template e l'immagine dell'impronta digitale del legittimo titolare, compressa secondo l'algoritmo WSQ (*Wavelet Scalar Quantization*), che è un algoritmo ottimizzato per la compressione delle immagini delle impronte digitali, e garantisce un elevato livello di sicurezza in fase di identificazione del portatore che la esibisce.

Il cosiddetto il Sistema di Sicurezza del Circuito di Emissione, S.S.C.E., provvede a controllare ogni operazione prevista nell'intero processo del ciclo di vita del documento: rilascio dei certificati digitali agli Enti coinvolti, controlli in fase di inizializzazione dei supporti fisici, autenticazione del Comune emettitore, verifica dei dati anagrafici del cittadino, rilascio del documento.

Il template viene utilizzato ai fini di riconoscimento dell'impronta originale pur non consentendone una sua qualsivoglia ricostruzione, consentendo quindi la salvaguardia del diritto alla privacy. Si sottolinea come tale riconoscimento non presupponga la presenza di nessuna banca dati, avvenendo il confronto direttamente tra il template memorizzato sulla C.I.E. e quello generato durante la fase di lettura da parte del dispositivo di acquisizione utilizzato dalla postazione *client* che richiede il servizio.

Nessuna operazione di tracciamento è effettuata né dal *client*, nè dal server. Un simile confronto garantisce, per i servizi che lo richiedano, la presenza fisica del titolare della CIE.

Durante la fase di inizializzazione, l'impronta assunta tramite i lettori certificati dal sistema SSCE, Sistema di Sicurezza del Circuito di Emissione, è trasformata in template, secondo l'algoritmo fornito dal Ministero dell'Interno, e memorizzata nell'area dedicata assieme ad un progressivo (da zero a nove) per l'individuazione del dito utilizzato per l'assunzione dell'impronta (ciò consente di rilasciare la CIE anche a persone mancanti di alcune delle dita).

Allo scopo di aumentare la sicurezza dei dati contenuti nel documento, lo spazio dedicato alla memorizzazione del template, dopo la sua installazione, viene reso non riscrivibile: Anche fase di installazione dell'impronta non richiede la memorizzazione di dati sulle postazioni del comune (o centro servizi) emettitore.

La C.I.E., è una smart card 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 ai fini della salvaguardia delle esigenze di pubblica sicurezza, ivi inclusa la fotografia, la firma ed una impronta digitale del titolare. L'elevata capacità di memoria disponibile (circa 1 MB), utilizzata per la memorizzazione di immagini o di informazioni di grosso volume, associata alla capacità di elaborazione 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", per consentire l'identificazione in rete e, quindi, l'erogazione di servizi telematici di *E-government*.

I rischi di utilizzo fraudolento e falsificazione delle carte d'identità, dovuti anche ai furti di carte "in bianco", con l'adozione del documento elettronico, sono notevolmente ridotti, principalmente grazie alla natura del supporto e alle garanzie di inalterabilità delle informazioni riportate, tanto sul chip che sulla banda ottica.

La banda ottica rappresenta l'elemento centrale della sicurezza: 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 possono unicamente consistere in aggiunte.

Come per gli altri documenti elettronici, tutte le attività di trasmissione dati avvengono in modalità cifrata al fine di garantire l'integrità dei dati e certificare che le informazioni pervenute a destinazione siano identiche a quelle originariamente inviate.

Obiettivi della nuova carta di identità elettronica

- Aumento della sicurezza del documento di identità che consentirà, alle forze dell'ordine, una identificazione certa del possessore;
- Riconoscimento certo del titolare per consentire l'esercizio del diritto di voto elettronico;

- Possibilità di verifica dei dati biometrici per garantire la presenza fisica del titolare della CIE durante l'accesso ai servizi in rete.
- Integrazione tra i sistemi informativi e la cooperazione applicativa tra amministrazioni sono oggi un obiettivo fondamentale perseguito da questo Ministero.
- Funzioni di documento di viaggio equipollente al passaporto e, grazie al rispetto delle caratteristiche previste dalla vigente normative ICAO e ISO, abilitazione all'espatrio in 32 Paesi esteri.

Gli enti governativi responsabili del nuovo documento d'Identità sono:

– Ministero dell'Interno:

- Dipartimento per gli Affari Interni e Territoriali
- Direzione Centrale per i Servizi Demografici (compito di verifica dello stato anagrafico dei cittadini italiani)
- Dipartimento della Pubblica Sicurezza – Direzione Centrale della Polizia Criminale – Servizio Polizia Scientifica (tramite il Sistema di Sicurezza del Circuito di Emissione, SSCE, controllo di tutte le operazioni previste nell'intero processo dal rilascio dei certificati digitali agli Enti coinvolti, ai controlli durante l'inizializzazione dei supporti fisici alla autenticazione del Comune emettitore, verifica dei dati anagrafici del cittadino e rilascio del documento).

– Ministero dell'Economia e delle Finanze (vigilanza sulla produzione dei supporti e distribuzione presso gli Uffici Territoriali di Governo).

La prima fase di sperimentazione, con il coinvolgimento di 83 Comuni distribuiti sull'intero territorio nazionale, è stata completata ed è in attuazione la fase di consolidamento e razionalizzazione della sperimentazione che prevede l'emissione delle nuove carte d'identità elettroniche per l'intera popolazione, con età superiore ai 15 anni, nei 56 Comuni individuati dalla Direzione Centrale per i Servizi Demografici, con oltre un milione di C.I.E. distribuite ai sopra citati Comuni (giugno 2004).

Di seguito riportiamo la legislazione completa riguardante la C.I.E.:

Legge 15 maggio 1997, n. 127
Misure urgenti per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo

Legge 16 giugno 1998, n. 191
Modifiche ed integrazioni alle leggi 15 marzo 1997, n. 59, e 15 maggio 1997, n. 127

Decreto del Presidente del Consiglio dei Ministri 22 ottobre 1999, n. 437
Regolamento recante caratteristiche e modalità per il rilascio della carta di identità elettronica e del documento di identità elettronico

D.M. 19 luglio 2000
Regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici

D.P.R. 28 dicembre 2000, n. 445 (limitatamente art. 36)
Disposizioni legislative in materia di documentazione amministrativa . (Testo A)

D.M. 14 maggio 2003
Modifiche al decreto del Ministero dell'interno in data 19 luglio 2000 recante regole tecniche e di sicurezza relative alla carta di identita' e al documento di identità elettronici.

D.M. 6 novembre 2003
Rettifica al decreto 19 luglio 2000 recante regole tecniche e di sicurezza relative alla carta d'identità e al documento d'identità elettronici.

Segue un estratto dell'Allegato B del precedente decreto

8.5 Impronta digitale.

Il titolare della CIE puo' richiedere, al momento dell'emissione, l'installazione del template della propria impronta digitale.
Il template e' una rappresentazione numerica di un elemento biometrico (in questo caso l'impronta del dito) e viene utilizzato ai fini di riconoscimento dell'impronta originale pur non consentendone una sua qualsivoglia ricostruzione. Va inoltre messo in evidenza che 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 possibilita' di manipolazione successiva, lo spazio dedicato alla memorizzazione del template, dopo la sua installazione, viene reso non riscrivibile. Piu' in dettaglio, durante la fase di installazione l'impronta assunta tramite lettori certificati da SSCE e' trasformata in template secondo lo specifico algoritmo fornito dal Ministero dell'interno e memorizzata nell'area dedicata assieme ad un progressivo che puo' variare da zero a nove in funzione del dito utilizzato per l'assunzione dell'impronta. Si sottolinea che anche la fase di installazione dell'impronta non richiede la memorizzazione di dati sulle postazioni del comune (o centro servizi) emettitore.

Il campo 4 del record dati contenuto nella banda ottica è la chiave biometria individuale.

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

Descrizione Campo	Tipo
Numero assegnato al documento in bianco	carattere
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 23x28mm – 200dpi – 16 Ml di colori(a 24 bit)	BMP JPG (fattore 5)
Impronta digitale (indice destro) 1"x1" – 500dpi – 256 liv. di grigio	BMP WSQ

D.P.R 2 marzo 2004, n. 117
Regolamento concernente la diffusione della carta nazionale dei servizi

CARTA MULTISERVIZI DIFESA

Nell'elaborazione del progetto della Carta Multiservizi Difesa (CMD) è stato deciso che essa dovesse avere una valenza giuridica sia "Esterna" all'amministrazione Difesa sia "Interna" ad essa. Quindi, utilizzabile a "vista" ed in forma elettronica in modo da:

– Contenere i certificati di "Firma Digitale" e "Strong Authentication" pienamente rispondenti alle attuali normative di legge;
– fungere da "Documento di Riconoscimento" (identità personale);
– contenere i dati sanitari relativi al dipendente e necessari ad assicurare le funzionalità di "emergency card";
– contenere i "template" delle impronte di 2 (due) dita delle due mani da memorizzare solo sulla smart-card;
– essere in grado di memorizzare altre evidenze biometriche (es. geometria della mano, impronta facciale, iride, ecc) nella zona "servizi" della carta;
– realizzare la piena e completa interoperabilità a livello:

- nazionale, con la Carta d'Identità Elettronica (CIE);
- internazionale, con la struttura dati sanitari "NetLink";
- interforze ed in ambito Ministero della Difesa;

– essere dotata di banda magnetica, idonea a salvaguardare gli investimenti pregressi.

Inoltre fu parimenti considerato requisito irrinunciabile, ai fini della sicurezza INFOSEC e DATASEC, la certificazione a livello ITSEC "e4-High", relativa al "Chip" ed al sistema operativo, che rappresenta la massima protezione attualmente in Europa.

Sviluppi attuali e futuri

La Carta Multiservizi Difesa vuole essere usata in particolare per le seguenti applicazioni:

- Gestione dati sanitari: le informazioni sanitarie sono inserite automaticamente, sotto la responsabilità di un medico militare, tramite le procedure informatiche sviluppate in ambito infermerie/ospedali militari.
- Posta sicura: scambio di e-mail firmate e/o cifrate con garanzia di autenticità del mittente integrità e sicurezza.
- Postazione di lavoro sicura: accesso in totale sicurezza alla postazione di lavoro (eventualmente congiunta all'uso dell'impronta digitale).
- Ingresso ad aree riservate: autenticazione forte tramite utilizzazione congiunta della CMD e delle impronte digitali in essa contenute.
- Accesso a servizi: rifornimento carburanti, prelievo materiale/vestiario, "passi" per ingresso in infrastrutture, acquisto beni presso strutture della Difesa (borsellino elettronico).

Il progetto per la CMD, nato nel 2001, è stato approvato in data 29 Luglio 2003, e la scelta è stata quella di garantire l'inteoperabilità con la C.I.E. e la C.N.S., adottando sistema operativo e set di comandi identici. La banda ottica è stata ritenuta però troppo costosa e sostituibile con altri accorgimenti di sicurezza (un ologramma pre-stampato).

Carta Multiservizi della Difesa
Reparto Telecomunicazioni Elettronica ed Informatica (TEI)
Forum P.A. 2004 Roma 10 –14 Maggio

PASSAPORTO BIOMETRICO

Il progetto del nuovo Passaporto Elettronico italiano, sotto la responsabilità del Ministero degli Affari Esteri e del Ministero dell'Interno, prevede l'introduzione di identificativi biometrici (immagine digitale del volto e impronte digitali di due dita, una per ciascuna mano) nel documento di viaggio, provvisto di un dispositivo elettronico microchip a Radio Frequenza, c.d. *contactless* (la comunicazione avviene per mezzo di onde a radiofrequenza, quindi, senza contatto) per la memorizzazione e la protezione dei dati del portatore.

Al fine di ampliare i requisiti di sicurezza dei documenti di viaggio, fino ad oggi costituiti essenzialmente da elementi di sicurezza fisica, come per i documenti di identità tradizionali, in ambito ICAO (International Civil Aviation Organization) sono in corso di elaborazione documenti tecnici per estendere le funzionalità dei documenti di viaggio leggibili in maniera automatica, i cosiddetti MRTD (Machine Readable Travel Document).

Le novità rispetto al modello ad oggi in uso sono sia tecnologiche che organizzative.

Innovazioni tecnologiche

– Microprocessore di prossimità integrato anche all'interno di supporti cartacei, leggibile senza contatto elettrico diretto. Il chip "contactless" amplia le possibilità fino ad ora offerte dalla zona MRZ a lettura

ottica, Machine Readable Zone, che contiene informazioni utili per verificare la genuinità del documento stesso. Nel documento di nuova concezione la MRZ non viene soppressa, ma diviene il collegamento essenziale tra le informazioni stampate graficamente, e quelle in formato digitale contenute nel microprocessore. La struttura interna del microchip *contactless* dovrà essere predisposta secondo le indicazioni dell'ICAO.

- Identificativi biometrici - La risoluzione di New Orleans, elaborata dall'ICAO/*New Technology Working Group*, ha indicato nella fotografia digitale l'elemento di interoperabilità globale per la conferma dell'identità assistita da strumenti informatici. La stessa risoluzione e le successive indicazioni dell'ICAO hanno indicato nelle impronte digitali e nell'iride ulteriori due elementi biometrici da affiancare, in modo opzionale, al viso. Recenti indicazioni della Commissione Europea
- indicano le impronte digitali quale ulteriore identificativo biometrico, obbligatorio, per consentire anche identificazioni personali automatiche.
- Infrastruttura a Chiave Pubblica (PKI) – al fine di evitare possibili alterazioni dei dati memorizzati all'interno del microchip *contactless*, questi dovranno essere firmate con la chiave privata dell'Autorità di Certificazione del Paese che ha emesso il documento. La relativa chiave pubblica dovrà essere inviata a tutti i Paesi aderenti all'ICAO, al fine di consentire la lettura del passaporto elettronico e offrire le necessarie garanzie sull'autenticità del documento.

Innovazioni Organizzative

- Controllo sulla identità personale: l'introduzione di un microchip contactless e di due identificativi biometrici consente di modificare sensibilmente i controlli prima dell'emissione del documento e nel corso del suo utilizzo. Prima dell'emissione, al momento dell'assunzione degli elementi biometrici, è possibile verificare, anche su basi dati biometriche, se il richiedente possiede i requisiti necessari a ricevere un passaporto. I controlli successivi possono limitarsi alle verifiche, per accertare che l'identità del legittimo titolare del documento sia la stessa del portatore che lo esibisce. La presenza di due identificativi biometrici, viso e impronte digitali, migliora notevolmente la capacità di verifica eliminando completamente i rischi di false accettazioni o di falsi rigetti.
- Verifiche automatiche: grazie alla presenza di identificativi biometrici ed alla presenza di sistemi di cifratura asimmetrica, gran parte delle attività di controllo presso le frontiere possono essere rese automatiche, lasciando agli specialisti le eccezioni (falsi rifiuti, documento non funzionante, etc.).
- Metodologie di controllo uniformi: con il nuovo passaporto elettronico le attività precedenti l'emissione ed il rilascio dovranno subire dei processi di trasformazione che ne aumentino gli automatismi. All'atto della richiesta sarà necessaria la presenza fisica del richiedente per assumerne gli elementi biometrici (almeno per quanto riguarda le impronte digitali).

Da quanto si legge dal sito della Polizia di Stato italiana, dal 26 ottobre 2004 è scattato l'obbligo, per chi entra negli Stati Uniti nell'ambito del programma Visa Waiver Program (Programma viaggio senza visto, del quale fa parte anche l'Italia), di possedere un passaporto leggibile attraverso lo scanner (il cosidetto passaporto a lettura ottica), requisito questo che tutti i documenti emessi dal 15 aprile 1998 posseggono. Questo tipo di documento viene definito come un Machine Readble Passaport (MRP) e segue le specifiche dello standard "Doc 9303, Part 1 Machine Readable Passports" redatto dall'ICAO: in pratica, con questo standard vengono rese leggibili in modo automatizzato alcune informazioni attraverso uno scanner.

Dal 2006 entrerà in vigore il passaporto biometrico nel quale sarà presente anche un chip elettronico che conterrà le impronte facciali e digitali del proprietario del passaporto. Le caratteristiche del chip e la sua codificazione saranno conosciuti soltanto da chi ha prodotto il documento, così come la lettura dei dati riportati all'interno; tutto ciò renderà il passaporto molto più difficile da falsificare. Anche in questo caso, gli standard da seguire per questo tipo di documento saranno quelli dell'International Civil Aviation Organization.

L'iter che porterà al passaporto biometrico sarà graduale e per quanto riguarda l'Italia si inizierà dal 2006 con alcune città campione e si procederà poi per tappe; per entrare in territorio americano, comunque, a partire

dal 26 ottobre 2005 i cittadini stranieri dovranno essere dotati di un passaporto biometrico, anche se probabilmente questa data verrà posticipata dato che alcuni paesi europei (come l'Italia) ed il Giappone sono in ritardo: le stime prevedono un'adozione per Agosto 2006.

Biometrics deployment of machine readable travel documents
ICAO TAG MRTD/NTWG (Technical Report – Version 2.0), 21 May 2004

Il passaporto elettronico prevede tre diverse tecnologie biometriche al suo interno: volto, impronta digitale e iride. Qualsiasi tecnologia venga adottata (anche più di una), lo standard specifica di inserire obbligatoriamente l'immagine della caratteristica e, solo opzionalmente, un template associato. Tale scelta è stata effettuata per mantenere il più possibile la compatibilità tra fornitori differenti di tecnologie biometriche: è possibile infatti che due paesi confinanti utilizzino formati di dati e algoritmi di riconoscimento diversi; per esempio, per quanto riguarda le impronte digitali, esistono degli standard per la memorizzazione delle minuzie, ma è possibile che alcuni paesi utilizzino altre informazioni, come i pori della pelle o la frequenza delle creste. Per mantenere l'interoperabilità, all'interno di MRTD viene spiegato in quali formati devono essere memorizzati i dati.

Per il formato dei dati biometrici all'interno del passaporto, MRTD fa riferimento ai seguenti standard internazionali ISO:

- Fingerprint Pattern Format for Interoperable Data Interchange (Annex H): ISO/IEC 19794-3 Finger Pattern Data
- Fingerprint Minutiae Format for Interoperable Data Interchange (Annex G): ISO/IEC 19794-2 Finger Minutiae Data
- Fingerprint Image Format for Interoperable Data Interchange (Annex F): ISO/IEC 19794-4 Finger Image Data
- Iris Image Format for Interoperable Data Interchange (Annex E): ISO/IEC 19794-6 Iris Image Data
- Facial Image Format for Interoperable Data Interchange (Annex D): ISO/IEC 19794-5 Face Image Data

Per garantire l'interoperabilità nella lettura dei dati l'identità, è stato introdotto il "Logical Data Structure" (LDS), che ne standardizza il formato. Il LDS è stato creato per essere letto elettronicamente e per risultare espandibile e adattabile alle necessità dei diversi stati.

Nello standard viene anche affrontato anche il problema di quale tecnologia deve essere utilizzata per memorizzare i dati biometrici (il risultato migliore è un chip contactless): codici a barre 2D, banda magnetica, Contact Integrated Circuit Chip, Contactless Integrated Circuit Chip, Dual Interface Integrated Circuit Chip (allo stesso tempo sia Contact che Contactless), memoria ottica. È necessario stabilire uno standard di memorizzazione dei dati per garantire la possibilità di lettura alla frontiera; la tecnologia coinvolta deve essere "aperta", flessibile e assicurare l'integrità dei dati e la loro sicurezza durante il trasporto. Altre caratteristiche devono essere l'usabilità, la capacità in termini di spazio e di raggiungere alte velocità di trasferimento; in base a queste tre proprietà che il dispositivo deve avere, nello standard dell'ICAO vengono scelti i Contacless IC Chip, dato che le raggruppano tutte.

Per quanto riguarda la capacità di memoria minima del dispositivo, essa dipende chiaramente dal numero di caratteristiche biometriche utilizzate. La sezione dello standard *"Enabling Global Interoperability – Image or Template"* identifica la dimensione di ogni immagine compressa relativa ad una caratteristica biometrica; per la faccia ~12-20K, impronta digitale ~10K e ~30K per l'iride.

Per quanto riguarda invece il posizionamento del chip contactless all'interno del libretto del passaporto possono essere adottate più soluzioni, come, per esempio, essere nel centro del libretto o tra l'ultima pagina e la copertina. Il posizionamento viene comunque lasciato a discrezione dello stato che lo rilascia.

Development of a logical data structure (LDS) for optional capacity expansion technologies (Technical Report – Revision 1.7) 18 May 2004

Nel documento vengono presentate alcune definizioni che fanno comprendere meglio diversi aspetti del LDS . In figura 1 vengono inoltre mostrati tutti i campi obbligatori e opzionali del LDS:

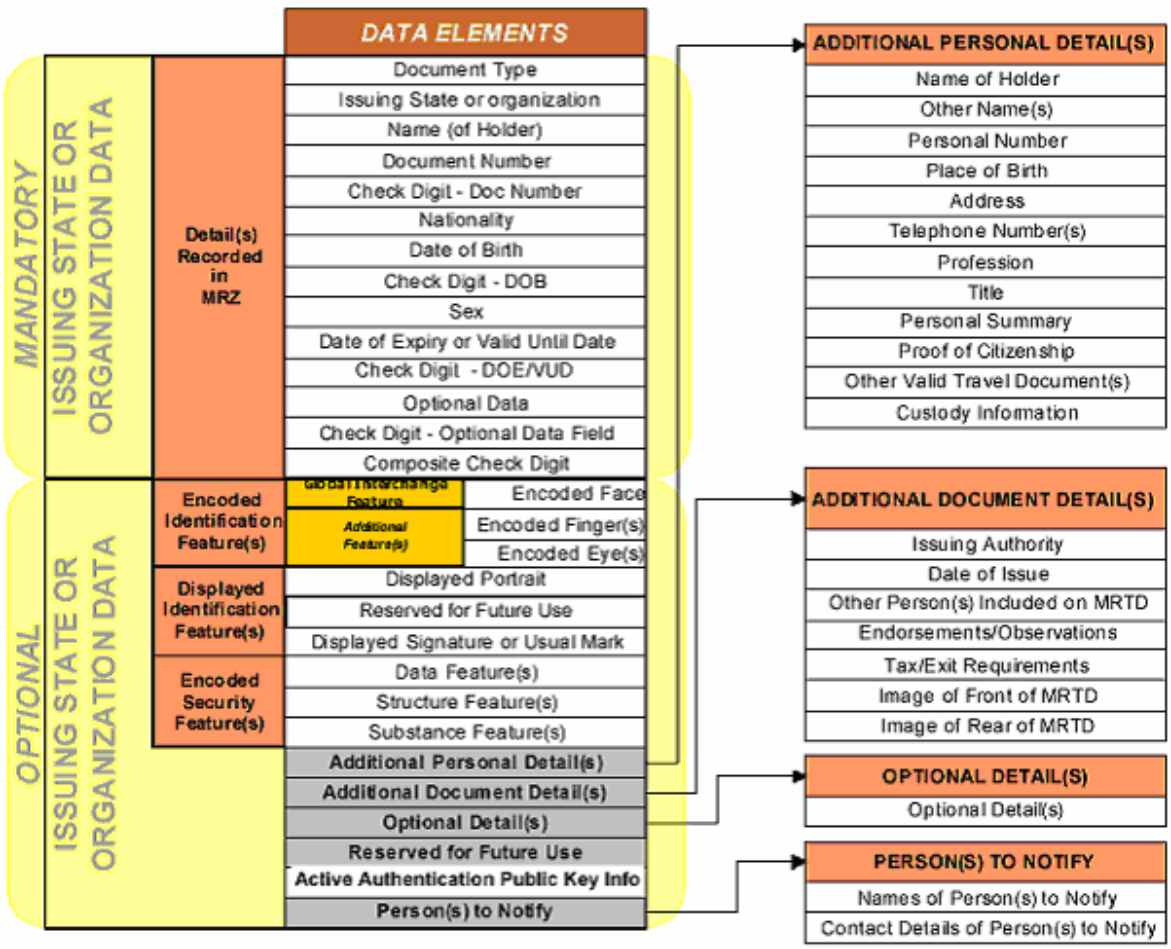

Fig 1: Elementi obbligatori o opzionali definiti per il LDS.

All'inteno del LDS, i dati correlati tra loro vengono raggruppati in Data Group; i gruppi riguardanti le caratteristiche biometriche sono riportati in figura 2: quello obbligatorio, il Data Group 2, memorizza il volto, mentre il DG3 e DG4 servono rispettivamente per le impronte digitali e le iridi. Lo standard utilizzato per il formato dei dati biometrici è il Common Biometric Exchange File Format (CBEFF), specificato nel NISTR 6529a.

Data Group	Data Element	Mandatory / Optional	Data Item
DG2		**M**	**GLOBAL INTERCHANGE IDENTIFICATION FEATURE – FACE** *[see 14.2.1]*
	01	M *(If encoded face feature recorded)*	Number of Face Biometric Encodings Recorded
	02[6]	M *(If encoded face feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded face feature recorded)*	Face Biometric Data Encoding(s) *[see A.13.3]*
ADDITIONAL IDENTIFICATION FEATURE(s) *[see 13.2.2]*			
DG3		**O**	**ADDITIONAL IDENTIFICATION FEATURE – FINGER(S)** *[see 14.2.2]*
	01	M *(If encoded finger(s) feature recorded)*	Number of Finger(s) Biometric Encodings Recorded
	02[6]	M *(If encoded finger(s) feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded finger(s) feature recorded)*	Finger Biometric Data Encoding(s) *[see A.13.3]*
DG4		**O**	**ADDITIONAL IDENTIFICATION FEATURE – IRIS(S)** *[see 14.2.2]*
	01	M *(If encoded eye(s) feature recorded)*	Number of Iris(s) Biometric Encodings Recorded
	02[6]	M *(If encoded eye(s) feature recorded)*	Header *[see A.13.3]*
	03[6]	M *(If encoded eye(s) feature recorded)*	Iris Biometric Data Encoding(s) *[see A.13.3]*

Fig 2 : Biometric Data Groups

PERMESSO DI SOGGIORNO

Il progetto del nuovo permesso di soggiorno apporta modifiche sostanziali alla struttura del documento e prevede che tutte le informazioni in esso presenti vengano memorizzate in una banca dati.

Tre sono stati i principali motivi ispiratori che hanno guidato la definizione dell'architettura del nuovo permesso di soggiorno:

- rispondere alla esigenza di produrre uno strumento sicuro sotto i diversi aspetti della produzione, rilascio e utilizzo da parte del titolare. La sicurezza non solo deve accompagnare tutti i flussi informatici, ma deve anche essere presente sul supporto fisico, al fine di scoraggiare facili contraffazioni, nonché di consentire una identificazione certa da parte delle istituzioni competenti;
- fornire un supporto standard, perfettamente in linea con le indicazioni dell'Unione Europea;
- consentire un migliore monitoraggio dei confini del Paese, grazie all'utilizzo del sistema informativo a cui sono delegati i controlli dattiloscopici degli immigrati illegali e dei chiedenti asilo politico in ambito UE.

Il controllo dell'intero ciclo di vita del nuovo documento fino alla sua naturale scadenza e la possibilità di verificare per via telematica la copia elettronica del permesso di soggiorno, consente di rilevare con immediatezza eventuali tentativi di falsificazione o contraffazione e di procedere all'identificazione a vista del titolare con margini di sicurezza maggiori.

Il raggiungimento degli obiettivi di sicurezza presuppone l'utilizzo di materiali e tecnologie standard, affidabili e nello stesso tempo in grado di garantire alti livelli di sicurezza. Il solo utilizzo di un supporto plastico, per quanto sofisticato, non sarebbe sufficiente a soddisfare tutte le esigenze sopra esposte. Per questo la scelta e' stata quella di una carta in grado di ospitare anche un duplice supporto elettronico, costituito da un microprocessore e da una banda a memoria ottica, al pari della C.I.E., al fine ulteriore della più completa interoperabilità tra i due documenti elettronici.

Il supporto elettronico consente di memorizzare sia i dati presenti sul documento in forma grafica, ottenendo una duplicazione di sicurezza, sia ulteriori informazioni che altrimenti non potrebbero essere riportate sul documento stesso.

La capacità di elaborazione propria del microcircuito chip permette di annoverare il P.S.E. tra le smart card.

All'interno del supporto sarà pertanto inserito sia il template che l'immagine di una impronta digitale, utile per confermare l'identità del titolare nei controlli successivi, ed i dati (Nome, data di nascita, etc.) relativi ai figli.

Come per gli altri documenti elettronici,

– tutte le attività di trasmissione dati avvengono in modalità cifrata al fine di garantire l'integrità dei dati e certificare che le informazioni pervenute a destinazione sono identiche a quelle originariamente inviate;

– la presenza di una memoria non riscrivibile e non volatile, rende possibile una maggior protezione dei dati memorizzati.

La caratteristica, propria del microcircuito, di poter nascondere informazioni al suo esterno, al contempo, di poter eseguire istruzioni programmate al suo interno, rende possibile il riconoscimento sicuro della carta per via telematica e la conseguente ed immediata erogabilità dei servizi. La caratteristica propria della banda di memoria ottica è l'assoluta inalterabilità accidentale o fraudolenta dei dati identificativi e biometrica in essa contenuti, ai fini di garantire l'identità del titolare, per l'accesso a servizi e per eventuali controlli operati dalle forze di P.S, al pari della C.I.E.

Decreto del Ministero degli Interni del 3 Agosto 2004
Regole tecniche e di sicurezza relative al permesso ed alla carta di soggiorno
(GU n. 235 del 6-10-2004)

Estratto dal decreto precedente

per «chiave biometrica»: la trasformazione in sequenza numerica dell'immagine dell'impronta digitale o altro dato biometrico;

Art. 6. Produzione, inizializzazione e formazione del documento

4. Nella fase di formazione dei documenti di soggiorno, l'Istituto, ricevuta la necessaria abilitazione ad emettere i documenti di soggiorno da parte di SSCE-PSE, utilizzando le chiavi di sicurezza di cui all'art. 7, comma 1, lettera c), memorizza, secondo le modalita' indicate nell'allegato B, i dati identificativi della persona e quelli relativi ai figli minorenni nella banda ottica e nel microprocessore, in quest'ultimo memorizza anche la chiave biometrica. L'Istituto, garantendo l'allineamento con i dati memorizzati nel microprocessore, effettua la personalizzazione grafica del documento di soggiorno riportando i dati identificativi della persona e quelli relativi ai figli minorenni.

Nel PSE saranno contenute due impronte digitali in formato immagine (1x1 – 500 dpi – 256 livelli di grigio) ed in formato numerico (template).

FIRMA DIGITALE E BIOMETRIA

La firma digitale è un particolare tipo di firma elettronica qualificata basata su un sistema di chiavi asimmetriche a coppia, una pubblica e una privata, che consente al titolare tramite la chiave privata e al destinatario tramite la chiave pubblica, rispettivamente, di rendere manifesta e di verificare la provenienza e l'integrità di un documento informatico o di un insieme di documenti informatici.

La normativa italiana sulla firma digitale prevede, nel caso specifico, che "il dispositivo sicuro di firma deve poter essere attivato esclusivamente dal titolare prima di procedere alla generazione della firma".

Per il rispetto di questa norma sono possibili due modalità funzionali: verifica di una cosa che il sottoscrittore conosce e verifica di una caratteristica biometrica del sottoscrittore.

Il primo metodo è quello classico della digitazione di un PIN; il secondo richiede la presentazione di dati inerenti alla fisiologia del sottoscrittore stesso.

Relativamente a questa seconda possibilità verrà illustrato nel seguito il possibile utilizzo di una smart card con controllo di accesso biometrico.

L'identificatore biometrico come PIN

L'uso dell'identificatore biometrico come PIN prevede:

- la procedura di memorizzazione dei dati, avendo preventivamente definito quali dati devono essere salvati e le modalità di memorizzazione all'interno della smart card;
- la disponibilità del sensore di rilevamento dei dati biometrici che rilevi questi in fase di sottoscrizione e li invii alla smart card per il confronto.

In quanto alla procedura al punto 1 è indispensabile definire alcuni standard al fine di garantire l'interoperabilità tra i vari ambienti.

Tali standard sono definiti nella serie ISO 7816 e in particolare nel documento numero 4 "Interindustry commands for interchange" e nel documento numero 8 "Security related interindustry commands". Nel documento ISO 7816-11 "Personal verification through biometric methods" sono state inserite delle estensioni che consentono di supportare la verifica delle chiavi biometriche e una serie di funzioni indispensabili per l'interazione con l'utente.

Le strutture da utilizzare sono definite in ISO 7816-11 in conformità al Common Biometric Exchange File Format.

Per le esigenze di interoperabilità, bisogna anche standardizzare l'interfacciamento dei dati biometrici di verifica. In particolare devono essere standardizzati la codifica e la struttura di tali dati. Sia il NIST che l'ANSI hanno emesso documenti in tal senso.

Trattandosi di dispositivi sicuri per la creazione della firma, ovviamente saranno necessarie anche valutazioni e certificazioni di sicurezza conformi all'ITSEC o ai Common Criteria. Per quest'ultima operazione dovranno essere definiti uno o più "Protection Profile".

Applicate tutte queste regole è possibile, procedere alla acquisizione dell'identificatore biometrico da inviare per la verifica alla smart card. Questa tecnica viene definita "match-on-card" e garantisce un elevato grado di sicurezza e di protezione dei dati personali in quanto non esistono memorizzazioni dell'identificatore biometrico al di fuori della smart card o, in generale, del dispositivo sicuro.

Se la verifica è positiva sono possibili tutte le operazioni successive allo sblocco della carta, come l'autenticazione forte tramite TLS/SSL o la firma digitale.

I processi per standardizzare le funzionalità al fine di garantire l'interoperabilità non sono brevi, né semplici. In Italia la biometria dell'impronta viene utilizzata per l'abilitazione all'utilizzo della smart card per la firma digitale e per il voto elettronico (Progetto e-poll).

Ciò significa che esistono apparati funzionanti e affidabili e, ogni volta che il problema dell'interoperabilità non è critico, come non lo è stato per il voto elettronico, si può procedere utilizzando l'offerta di mercato. Nel caso del "match-on-card" vengono utilizzati ancora dei template e algoritmi proprietari, ma si auspica che in tempi ragionevoli si potrà disporre di algoritmi conformi a quanto stabilito in ISO/IEC 7816-11.

In conclusione, deve essere considerato il fatto che il "match-on-card" è ancora in fase di assestamento tecnologico e può risentire della scarsa potenza di calcolo di alcune tipologie di dispositivi.

Sarà quindi in base alle esigenze di sicurezza scaturite dall'analisi del rischio che si dovranno valutare quali siano le soluzioni più opportune tra quelle ibride disponibili sul marcato. Il paragrafo seguente delinea uno scenario generale sull'argomento.

Decreto del Presidente della Repubblica 28 dicembre 2000, n. 445

Direttiva europea 1999/93/CE sulle firme elettroniche

Decreto legislativo 23 gennaio 2002, n. 10

Decreto del Presidente della Repubblica 7 aprile 2003, n. 137

Decreto del Presidente del Consiglio dei Ministri 13 gennaio 2004

CONCLUSIONI

In conclusione, la legislazione italiana chiarisce poco gli standard relativi alle varie carte di identità o servizi previste nel prossimo futuro (C.I.E., P.S.E., etc..), anche se comunque i pochi riferimenti indicano la famiglia dell'ISO 7816, ed inoltre sono totalmente assenti le indicazioni per quanto riguarda gli standard usati per la memorizzazione del template (se presente) ed il riconoscimento biometrico ottenuto grazie ai dati contenuti nella carta: ad oggi si prefigura che la tecnologia usata sarà quella di "Template On Card" e quindi la carta si presterà solo come contenitore di dati sensibili.

Per quanto riguarda però le indicazioni fornite dall'Unione Europea sulla carta di identità nazionale e l'identità elettronica (eID), un documento del CEN/ISSS (Towards an electronic ID for the European Citizen) orienta più decisamente e particolarmente le scelte verso gli standard ISO 7816 e in particolare la parte 11 (Personal verification through biometric methods), 19785-1 (CBEFF), 19794-2 (Finger Minutiae Data) e 19784 (BioAPI). Anche i vari technical report dell'ICAO per quanto riguarda le specifiche del passaporto elettronico, il

cui progetto di standardizzazione avviene in sede internazionale, delineano scelte rivolte anch'esse ai sopra citati standard ISO.

Risulta quindi molto probabile che le scelte adottate in Italia saranno pienamente conformi a quelle europee e dell'ICAO.

Le informazioni più dettagliate sul file system della carta necessarie per lo sviluppo di software di interfacciamento alla C.I.E. non sono pubbliche, ma vengono rese disponibili solo su richiesta esplicita al Ministero dell'Interno.

Towards an electronic ID for the European Citizen: a strategic vision
CEN/ISSS WS/eAuthentication Vision Document
CEN/ISSS Workshop eAuthentication, Brussels 3/10/2004

Riferimenti:

Alcune parti del presente testo sono state estratte o rielaborate a partire dal documento "*I Quaderni*", numero 9, anno I - Novembre 2004. Centro Nazionale per l'Informatica nella Pubblica Amministrazione (CNIPA).