Schema per il circuito di emissione della Carta d'Identità Elettronica

Roma, 2 febbraio 2000

Indice

0. CHANGE LOG

Data	*Versione*	*Descrizione*	*Note*
3 settembre 1999	00	Prima emissione	--
22 ottobre 1999	01		--
15 novembre 1999	02		--
15 novembre 1999	03		--
15 dicembre 1999	04		--
16 dicembre 1999	05		--
20 dicembre 1999	06		--
20 dicembre 1999	07		--
22 dicembre 1999	08		--
23 dicembre 1999	09		--
5 gennaio 2000	10		--
14 gennaio 2000	11		
2 febbraio 2000	12		--

1. INTRODUZIONE

Il presente documento illustra la soluzione a livello tecnologico, applicativo ed organizzativo, che risponde, in termini concreti, alle esigenze ,ai requisiti ed ai vincoli architetturali ed organizzativi emersi durante le riunioni del gruppo di lavoro istituito nell'ambito del mandato della delibera n. 8 del 19 marzo 1999 dell' AIPA sulla carta d'identità elettronica.

1.1 Obiettivi

Gli obiettivi che il gruppo di lavoro si è imposto nella progettazione della carta di identità elettronica e del relativo circuito di lavorazione, sono stati essenzialmente tre.

Il primo risponde alla esigenza di produrre uno strumento sicuro sotto i diversi aspetti della produzione, rilascio nonché utilizzo da parte del titolare. La sicurezza non solo deve accompagnare tutti i flussi informatici necessari al circuito di emissione, 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.

Il secondo costituisce una novità importante rispetto alla versione attuale della carta di identità cartacea e consiste, nel rispetto della normativa vigente, nell'utilizzo del documento di identità come carta servizi. Per poter usufruire dei servizi in rete messi a disposizione dalle Pubbliche Amministrazioni Centrali è necessario garantire un processo che, attraverso l'utilizzo di tecniche di autenticazione opportunamente combinate alla specificazione di un codice personale di identificazione (PIN), assicuri il titolare da un lato, ed il fornitore del servizio dall'altro, del corretto utilizzo della carta.

Il terzo obiettivo è relativo alla necessità di fornire di un supporto in grado di funzionare allo stesso modo e su tutto il territorio nazionale nei confronti delle Pubbliche Amministrazioni Centrali. La richiesta di un servizio ad una Pubblica Amministrazione Centrale deve essere uguale da Milano a Palermo e le diverse modalità di richiesta, a parte i contenuti specifici del servizio coinvolto, devono conservare, ai fini dell'usabilità da parte dell'utente, le stesse caratteristiche di rappresentazione: soltanto in questo modo si riuscirà a costruire il modello mentale necessario a far decollare l'utilizzo della carta d'identità come carta servizi.

Il raggiungimento di simili obiettivi presuppone l'utilizzo di materiali e tecnologie standard, affidabili e nello stesso tempo in grado di garantire alti livelli di sicurezza.

Inoltre, per rispondere alle esigenza di sicurezza da parte del Min. dell’interno e delle forze dell’ordine, connesse alle specifiche finalita’ della Carta di identita’,

secondo quanto previsto dalle normative vigenti, è stato richiesto l'uso di una carta ibrida, basata su due approcci tecnologici distinti:

- uso di bande ottiche a lettura laser, per salvaguardare le esigenze di pubblica sicurezza, oltre a mettere a disposizione una elevata capacità di memoria (1,8 Mb),
- uso di microprocessori, per permettere l'identificazione in rete e, quindi, l'erogazione di servizi telematici.

Più specificatamente, le esigenze di sicurezza da parte delle forze dell'ordine sopra citate, richiedono un supporto con le caratteristiche di:

- ottima resistenza passiva del supporto che renda meno semplici attacchi diretti;
- capacità del supporto di rendere evidenti gli eventuali danni ad esso arrecati, volutamente o per cause accidentali;
- inalterabilità delle informazioni stampate e registrate sulla carta,

La banda laser permette di rispondere ai requisiti di:

- ottima resistenza agli agenti esterni (magnetismo, calore, sollecitazioni meccaniche, chimiche e virus informatici.);
- grande capacità di memoria;
- il rilevamento ad occhio nudo dei danneggiamenti eventualmente subiti;
- elevati livelli di sicurezza, attraverso il processo di masterizzazione che consente la riproduzione fotografica di immagini ad alta risoluzione durante la fase di produzione della banda laser;
- inalterabilità, garantita dalla tecnologica, "Write Once Read Many" (WORM), che non permette aggiornamenti o cancellazione di dati;
- confronto, ad occhio nudo, dei dati stampati in chiaro con quelli incisi sulla banda stessa in modo grafico, (enbedded ologram).
- utilizzo del nuovo file-system, che permette la creazione di partizioni indipendenti (fino a 16) ognuna delle quali può avere la dimensione desiderata fino alla massima capacità della carta. Dette partizioni possono essere sottoposte a chiavi di accesso.

D'altro canto, per le necessita' di erogare servizi da parte delle nuove Carte di Identita' elettroniche, secondo quanto previsto dal DPCM n° 437 del 22\10\1999 , le caratteristiche del supporto devono permettere:

- l'identificazione del titolare in modo certo anche per via telematica;
- l'erogazione di servizi diversificati, su scala nazionale e/o locale, eliminando tutte le possibili barriere all'accesso, pensando anche ad anziani, disabili e ragazzi.
- l'aggiunta di nuovi servizi, man mano che questi vengono ideati e predisposti dalle amministrazioni;

- l'uso di tali servizi, abbassando complessità e costo delle attrezzature necessarie per la loro fruizione.

Il microprocessore, permette tali funzionalita', garantendo, a livello logico, nelle transazioni telematiche in cui le parti non si "vedono", l'identità del possessore della carta, oltre a richiedere dei lettori di basso costo e sempre di più larga diffusione.

Gli algoritmi a chiave asimmetrica, sono ritenuti i più adatti a garantire la sicurezza logica del circuito e delle procedure di autenticazione, tanto per quanto riguarda i dati memorizzati sulla banda laser che per quelli riguardanti il microchip.

Infine, la disponibilità di due fonti di dati indipendenti introduce la possibilità di verifiche incrociate, che costituiscono una garanzia ulteriore per la sicurezza del documento d'identità.

Le associazioni di categoria Anasin, Assinform, Assintel, partecipanti al sopra citato Gruppo di lavoro, causa la non diretta conoscenza della banda laser, affermano la non possibilita', da parte loro, di certificare le informazioni relative a tale tecnologia.

Pertanto, al fine di integrare, nel presente documento anche informazioni relative a tale aspetto, sono stati inseriti alcuni paragrafi, relativi alla banda laser, redatti da altre fonti.

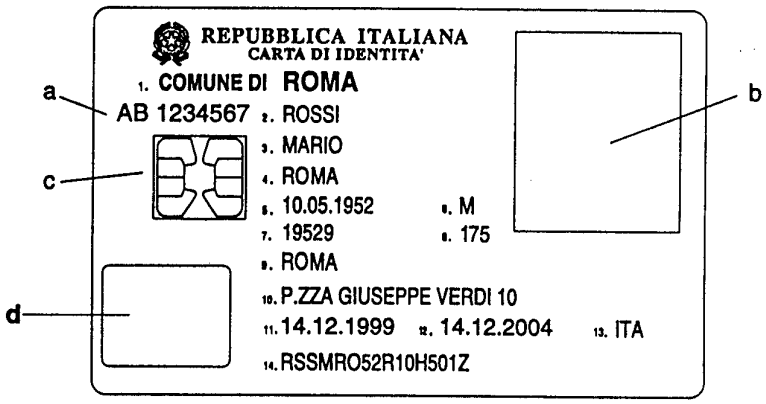
2. DISPOSIZIONE DEGLI ELEMENTI GRAFICI

Il layout della CIE deve tener conto degli standard internazionali ISO ed ICAO per la giusta disposizione dei componenti tecnologici e delle aree destinate alla foto, alla firma ed ai dati previsti, nonchè alla lettura automatica dei dati stessi riportati in caratteri OCR-B nella zona MRZ.

Il layout della CIE è pertanto definito secondo quanto appresso specificato nelle due alternative possibili :

2.1 Prima versione

2.1.1 4.1.1. Layout del fronte

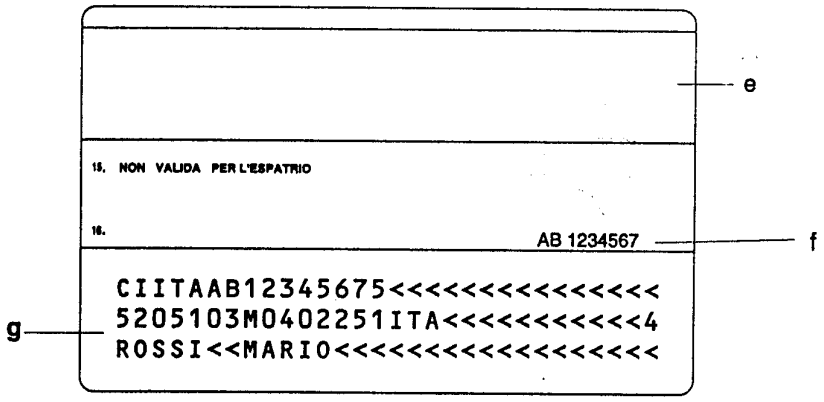


All. A - Dis. 1

Sul fronte della CIE vanno riportati i dati appresso specificati con la relativa lunghezza del campo di scrittura :

1.	Comune che emette il documento	n.posizioni	30
2.	Cognome	"	25
3.	Nome	"	15
4.	Comune di nascita	"	30
5.	data di nascita	"	10
6.	sesso	"	1
7.	estremi atto di nascita	"	5
8.	statura (cm)	"	3
9.	Comune di residenza	"	30
10.	indirizzo	"	30
11.	data emissione documento	"	10
12.	data scadenza documento	"	10
13.	cittadinanza	"	3
14.	codice fiscale	"	16
a.	numero assegnato al documento in bianco	"	9
b.	spazio di 23 x 28 mm riservato alla stampa della fotografia del titolare		
c.	ologramma di sicurezza		
d.	microprocessore		

2.1.2 4.1.2 Layout del retro



All. A - Dis. 2

Sul retro della CIE vengono riportati i dati e gli elementi appresso specificati

15. eventuale annotazione circa la non validità del documento per l'espatrio n.posizioni 25

16. firma del titolare

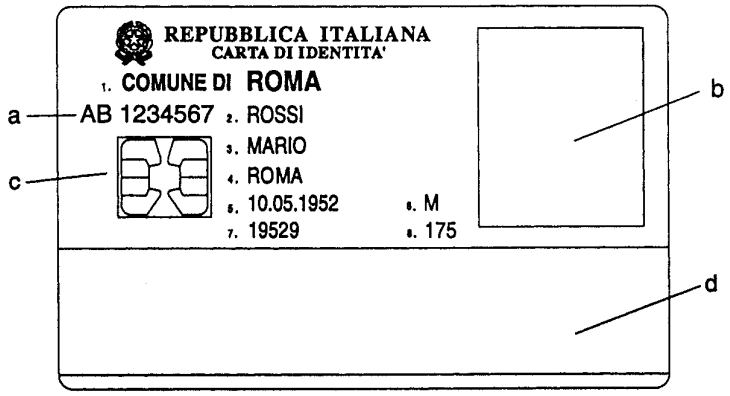
e. banda per memoria ottica

f. n. del documento in bianco ripetuto ad incisione laser " 9

g. zona MRZ riservata alla codifica dei dati con
caratteri OCR B secondo quanto previsto dalla normativa ICAO
per i documenti di tipo TD-1

2.2 Seconda versione

2.2.1 Layout del fronte



All. A - Dis. 3

Sul fronte della CIE vanno riportati i dati appresso specificati con la relativa lunghezza del campo di scrittura :

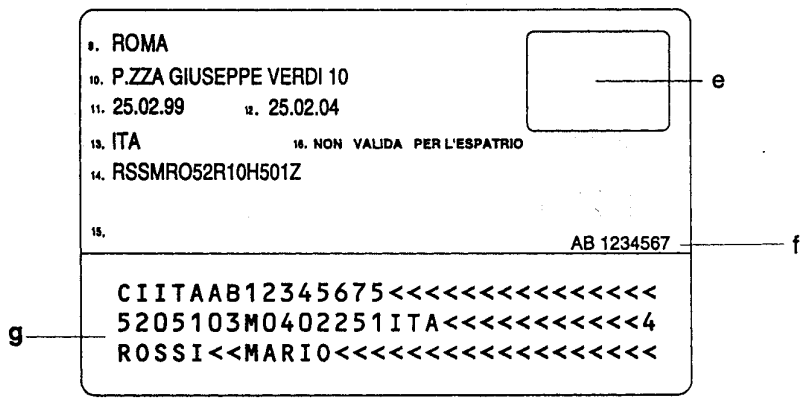
	1. Comune che emette il documento	n.posizioni	30	
	2. Cognome		"	25
	3. Nome		"	15
	4. Comune di nascita		"	30
	5. data di nascita	"	10	
	6. sesso		"	1
	7. estremi atto di nascita	"	5	
	8. statura (cm)		"	3
a.	numero assegnato al documento in bianco	"	9	

b. spazio di 23 x 28 mm riservato alla stampa della fotografia del titolare

c. microprocessore

d. banda per memoria ottica

2.2.2 Layout del retro



All. A - Dis. 4

Sul retro della CIE vengono riportati i dati e gli elementi appresso specificati

9. Comune di residenza	"	30	
10. indirizzo	"	30	
11. data emissione documento	"	10	
12. data scadenza documento	"	10	
13. cittadinanza		"	3
14. codice fiscale	"	16	
15. firma del titolare			
16. eventuale annotazione circa la non validità del documento per l'espatrio	n.posizioni	25	
e. ologramma di sicurezza			
f. numero del documento in bianco ripetuto ad incisione laser	"	9	
g. zona MRZ riservata alla codifica dei dati con caratteri OCR B secondo quanto previsto dalla normativa ICAO per i documenti di tipo TD-1			

3. STANDARD DEL DOCUMENTO

3.1 Dimensioni nominali

Le dimensioni nominali saranno di 53,98 x 85,6 mm come specificato nella norma ISO/IEC 7810 : 1995 per la carta di tipo ID-1.

Le tolleranze dimensionali sono quelle definite dalla stessa citata norma.

3.2 Spessore

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

3.3 Caratteristiche fisiche

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.

La CIE, per un uso normale durante il periodo di validità, deve rispondere alle specifiche definite 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.

La CIE ed i dati su di essa stampati non devono deteriorarsi per esposizione alla luce durante il normale impiego.

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, 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. MATERIALI E STANDARD PER LA CIE

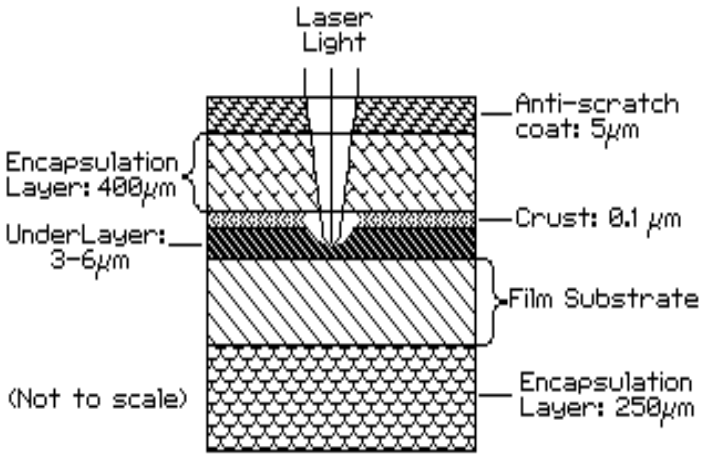
4.1 Materiali e standard per la banda ottica

4.1.1 Descrizione

La carta ottica è realizzata in policarbonato, un materiale plastico di provenienza aeronautica, 1.000 volte più resistente del PVC, lo stesso con cui è fatta una normale carta di credito e rispondente alle attuali esigenze internazionali sulla tutela del rispetto ambientale.

Il PC oltre a garantire un'ottima trasparenza per la scrittura su banda ottica, offre elevata resistenza 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 Figura sopra riportata rappresenta il Sandwich Drexler

Per ragioni fisiche, legate anche a caratteristiche di migliore trasparenza, il materiale di supporto indicato su cui viene stesa la banda ottica è il policarbonato (di seguito definito PC).

L'applicazione della banda ottica potrebbe essere realizzata su diversi supporti plastici ed anche utilizzando diversi materiali metallici, ma per garantire una migliore trasparenza e contemporaneamente rispondere a requisiti di tipo ecologico, la scelta effettuata è stata quella del policarbonato.

Nelle carte ottiche lo strato con capacità di memorizzazione è un'emulsione fotografica che diventa una superficie stabile e riflettente tramite un processo ottenuto mediante raggi-E (300.000 volts). Tale superficie risulta insensibile alla luce, ai campi magnetici ed ai campi elettrici, ma può essere intaccata da un raggio laser a bassa intensità.

Il raggio laser produce una modifica permanente nella capacità riflettente: questo principio è utilizzato per la memorizzazione dei bit che compongono l'informazione da registrare. La lettura viene effettuata tramite un laser di potenza ancora inferiore.

Per una migliore costruzione della stessa card, la laminazione dello strato trasparente di PC avviene su un altro strato di PC opaco e prestampato per quanto si riferisce alla grafica di sicurezza; la laminazione su PVC determinerebbe probabili difetti di planarità delle stesse card e quindi è da evitare. I problemi di stampa su PC, sono risolti dal posizionamento di un primer che rende la superficie identica a quella delle più comuni plastiche.

Un'altra tecnica di produzione prevede un sandwich di PC o, in alternativa, di PC per il lato dove compare la banda ottica e, per il lato opposto, altro materiale plastico (PET o PVC) che garantisce un'ottima resa delle procedure di stampa. In questo tipo di carte il materiale che costituisce la banda ottica è applicato sul PC con un processo di sublimazione *(spattering)* del tutto simile a quello utilizzato per la produzione dei dischi per computer.

4.1.2 Gli standard

Gli **standard** di formato esistenti per le carte ottiche sono il DELA ed il SIOC che rispondono all'ISO/IEC 11694. Il formato DELA (ISO/IEC 11694, Annex B), attualmente il più diffuso sul mercato, prevede un metodo di DMC (Data Modulation Code) chiamato PPM (Pit Position Modulation). Il PPM utilizza il centro dell'area di scrittura come posizione sensibile per la memorizzazione dei dati. Ciò significa che ogni settore destinato a contenere un bit è testato solo al suo centro, permettendo quindi una buona tolleranza al grado di imperfezione della dimensione/posizione del foro di scrittura. Il metodo d'identificazione e correzione dei dati utilizzato da questo formato è il B.E.S.T. (Burst and rundom Error correction System for Teletext).

Il formato SIOC (ISO/IEC 11694, Annex A) utilizza il metodo di codifica Pulse Width Modulation (PWM). Esso permette la dimensionabilità dei settori (2^n), l'accesso casuale (random) in scrittura ai settori stessi e la scrittura dei dati in modo bidirezionale (DRAW) con lettura immediata per verificarne la loro correttezza.

DRAW permette il raddoppio della velocità di scrittura e lettura.

Il metodo di identificazione e correzione dei dati è il Reed-Solomon, standard industriale utilizzato dalla maggioranza dei dispositivi di memorizzazione ottica (CD-Rom, CD-Worm, CD-Rewritable ecc.).

4.1.3 Capacità di memoria

La **capacità di memoria** di una carta ottica, a seconda dei modelli, va dai 4,1 MByte ai 6 MByte (ma tramite tecniche di compressione si può arrivare oltre i 20 MByte), che scendono a 2,86 MByte o a 4,89 Mbyte, a seconda dei modelli, in caso di pieno utilizzo della capacità d'identificazione e correzione degli errori (edac).

4.1.4 Carte ibride

Le **carte ibride** sono formate da una banda riflettente ridotta a 16 mm che permette la memorizzazione di circa 1,8 MByte (che si riducono a 1,2 MByte se si utilizza il **sistema edac**) e da un microchip di diversa capacità.

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

4.2 Materiali e standard per il microcircuito

4.2.1 Materiali

La struttura fisica d'una carta intelligente (*smart card*), specificata negli standard ISO 7810, 7816-1 e 7816-2, si compone di tre elementi: il supporto, che ha le dimensioni di una carta di credito ed è realizzato in materiale plastico; il circuito stampato, che esercita le funzioni di interfaccia verso l'esterno, ed il circuito integrato (*chip*), incastonati sulla scheda. La protezione fisica è assicurata dalla modalità costruttiva, che rende di fatto impraticabile l'accesso ai dati custoditi per mezzo di tecniche intrusive, anche se condotte con mezzi sofisticati. La capacità di memoria del microcircuito è, in larga parte, quella offerta dalla sua memoria riscrivibile e non volatile (EEPROM). Essa, seppure largamente inferiore a quella della banda ottica, è tuttavia in costante aumento (più o meno raddoppia ogni anno), ed attualmente varia da 2 a 64 Kb a seconda dell'uso cui il microcircuito è destinato. Per la carta d'identità elettronica è richiesta una memoria EEPROM di capacità non inferiore a 16 Kb.

Un'altra caratteristica del microcircuito, particolarmente utile quando *la smart card* è utilizzata per operazioni di cifratura/decifratura, è la presenza di un coprocessore crittografico, che permette, appunto, di rendere estremamente più veloci operazioni di questa natura. Per la carta d'identità elettronica è richiesta la presenza, nel microcircuito, di un motore crittografico in grado di eseguire nativamente *almeno* l'operazione di RSA *signature* con chiavi non inferiori a 1024 bit.

Il circuito stampato, che protegge il *chip* dallo sforzo meccanico e dall'elettricità statica, deve essere conforme alla norma ISO 7816-3 che fornisce cinque punti di collegamento per potenza e dati.

4.2.2 Standard

Gli standard di riferimento, per il microcircuito presente sulla carta d'identità elettronica e per i comandi del sistema operativo da esso ospitato, sono i seguenti:

ISO 7816-3

ISO 7816-4

ISO 7816-8

I comandi, nella forma di APDU, che devono obbligatoriamente rispettare gli standard citati, sono quelli utilizzati dal middleware crittografico di interfaccia con la carta, le cui specifiche sono discusse in altro documento.

Fa eccezione il comando per lo scambio delle chiavi di sessione, descritto nella sezione riguardante i servizi, che dovrà essere implementato secondo le specifiche colà riportate.

4.2.3 Capacità di processo

Il nome *smart card* (carta intelligente) deriva, appunto, dalla capacità di processo propria del microcircuito (*chip*), che lo distingue da qualunque altro supporto "passivo" come, ad esempio, la banda ottica precedentemente descritta. La presenza di un vero sistema operativo e di una memoria riscrivibile e non volatile (EEPROM), rende possibile "nascondere" i dati memorizzati ed eseguire istruzioni e programmi, in modo del tutto simile ad un vero computer. La caratteristica, propria del microcircuito, di poter nascondere informazioni all'*esterno* di esso, ed al contempo di poter eseguire istruzioni o programmi *interni*, rende possibile il **riconoscimento sicuro del possessore della carta per via telematica**, ossia senza che questi sia fisicamente presente presso il punto di erogazione del servizio, per cui l'identificazione si è resa necessaria. Questa circostanza, come è facile capire, apre la strada ad una radicale semplificazione del rapporto del cittadino con la pubblica amministrazione.

In particolare, la presenza del microcircuito sulla carta d'identità elettronica rende possibili queste tre funzionalità, necessarie per l'erogazione sicura di servizi per via telematica:

- identificazione sicura, anche per via telematica, della carta (e del suo titolare) da parte di un server remoto, sede di un servizio erogato (anche h24);
- identificazione, anche per via telematica, del servizio remoto da parte della carta (il titolare della carta deve essere sicuro che il servizio cui accede - senza poterlo "fisicamente" vedere - sia autentico, altrimenti potrebbe esporre i dati sensibili, memorizzati sulla carta, a lettura non autorizzata o addirittura a contraffazione non rilevata);
- cifratura dei dati sensibili, memorizzati nel microcircuito, nel loro transito dalla EEPROM**,** presente sul chip, al server erogatore del servizio. Il canale cifrato deve quindi "attraversare" l'applicazione client (ad es. il browser) utilizzata per accedere al servizio, al fine di evitare le classiche tecniche di "attacco nel mezzo", descritte nel capitolo relativo ai servizi.

5. PRODUZIONE CARTE D'IDENTITÀ ELETTRONICA

5.1 Sicurezza del Supporto Plastico

Con l'obiettivo di garantire alla carta d'identità elettronica un supporto plastico difficilmente riproducibile e falsificabile se non con tecnologie altamente sofisticate o costose, elenchiamo qui di seguito gli elementi che potrebbero essere utilizzati per ottenere tale scopo:

Per facilitare l'esame visivo del documento onde accertarne l'autenticità è incorporata nel supporto dello stesso una combinazione di accorgimenti di sicurezza di seguito specificati:

5.1.1 Grafica

La grafica stampata sul fronte e sul retro della CIE è realizzata con accorgimenti propri delle carte valori :

- motivi antiscanner ed antifotocopiatura a colori
- stampa con effetto rainbow
- motivi grafici multicolore richiedenti elevata qualità di registro di stampa
- microprint,
- processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico,
- security ROM,
- embedded hologram (incisione grafica su banda laser);

5.1.2 Inchiostri

Per la stampa è previsto l'impiego di inchiostri speciali, fluorescenti, interferenziali e/o OVI.

5.1.3 Numerazione

La numerazione del documento in bianco, stampata sul fronte del documento, è ripetuta sul verso con sistema ad incisione laser.

5.1.4 Applicazione di elementi OVD (Optical Variable Device)

Sul fronte della CIE è applicato a caldo un ologramma di sicurezza.

È prevista l'applicazione di overlay olografico dopo la personalizzazione attraverso la stampa della foto e dei dati sul fronte del documento.

Ulteriore sicurezza si ottene attraverso:

- il processo di masterizzazione photomask con stampa ad alta risoluzione di immagini direttamente su film ottico,
- l'inserimento di elementi che collegano la tipologia della carta ai lettori/scrittori della stessa;
- l'apposizione di embedded hologram (incisione grafica su banda laser).

Questi elementi di sicurezza sono tipici del settore bancario e vengono applicati al supporto plastico in fase di produzione . La verifica dell'alterazione/presenza di questi elementi può essere facilmente eseguita sia visivamente che utilizzando strumenti presenti sul mercato a costi assolutamente irrisori.

La durata degli elementi sopraelencati è garantita per tutto il ciclo di vita della carta stessa.

Il supporto fisico deve essere conforme alle norme che regolamentano i Documenti di Identità International Standards Organization (ISO) 7810 –ID-1 (54mm x 86mm) e per la disposizione dei supporti informatici (chip e banda ottica), conforme alle norme ISO/IEC International Electrotechnical Committee (IEC) 11694 mentre per le caratteristiche del chip alle già citate norme ISO/IEC.

5.2 Sicurezza della Personalizzazione dei dati a vista

In seguito ad un processo di attenta valutazione ed analisi, si è deciso che la tecnica da utilizzare per la stampa della CIE è quella della termografia che risponde a requisiti di economicità e di diffusione di mercato. Si applica direttamente su strati in PVC, mentre occorre ricorrere ad opportune interfacce su carte in policarbonato (PC) nel caso di stampa a colori.

Le potenziali difficoltà di personalizzazione, foto a colori e dati personali da trasferire sulle due superfici del PC attraverso la stampa termica, sono tecnicamente superate da tempo, eseguendo un trattamento sulle stesse o con un primer, mediante stampa serigrafica, oppure con la stesura di un sottile film di PVC.

La vita media di una carta ottica realizzata su supporto in policarbonato è sicuramente superiore ai 5 anni di vita previsti dalla normativa per la validità della carta d'identità elettronica.

Successivamente alla stampa termica il lay-out produttivo provvede ad una protezione con "overlay" di 12 micron che ne garantisce la durata per oltre 5 anni oppure con "overlay" di 25 micron che supera abbondantemente i 10 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 sono ad oggi prodotti sia in USA che in Giappone e soddisfano l'attuale mercato mondiale.

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 elevati, infatti, per quanto attiene ai dati contenuti nella banda laser, è attivo un metodo di identificazione e correzione d'errore che quale garantisce la ricostruzione delle informazioni digitali eventualmente perse per ragioni eccezionali.

5.3.2 Microcircuito

Esistono due distinti livelli di protezione dei dati conservati nella carta: un livello fisico, ed un livello logico. La protezione a livello fisico è gestita dal produttore del *chip* che provvede a *mascherare* sulla carta, in maniera indelebile, il sistema operativo proteggendolo mediante una chiave segreta di cui egli solo è a conoscenza.

Il livello logico è invece gestito dall'entità che inizializza e personalizza la carta (entità emittente). I dati inseriti in questa fase sono protetti da lettura/scrittura mediante un PIN (Personal Identification Number) di cui solo l'utente è a conoscenza.

La carta consente l'accesso alle informazioni protette solo dopo aver ricevuto il PIN corretto. In particolare, se qualcuno tentasse di accedere alla carta inserendo ripetutamente PIN diversi nella speranza di individuare quello corretto, dopo un certo numero di tentativi falliti la carta reagirebbe all'attacco bloccando il PIN e negando di conseguenza l'accesso al suo contenuto fino ad un eventuale successivo sblocco.

Le carte dotate di coprocessore crittografico forniscono un metodo alternativo (o da usare in congiunzione) al PIN per ottenere i permessi di accesso alla carta, basato su un algoritmo di tipo *challenge-response*: la carta genera una stringa casuale di bit; l'applicazione che richiede i permessi firma la stringa con la propria chiave privata e la restituisce alla carta; infine quest'ultima, usando una copia della corrispondente chiave pubblica, precedentemente memorizzata sulla carta, verifica la firma e, in caso di successo, dà i permessi di accesso.

5.3.3 Sicurezza della tecnologia di produzione della carta ibrida

Nell'assembalggio della CIE occorrerà avere particolare accortezza nelle seguenti fasi produttive:

- Creazione della cavità (*milling*) su una struttura complessa formata da diversi strati di materiale.
- Inserimento del modulo (*embedding*) di un microcircuito in una struttura che abbia un layer trasparente rigido.
- Prestare attenzione alla profondità della cavità in modo da evitare che si raggiunga la protezione trasparente e quindi che si veda il microcircuito.
- Nella realizzazione delle carte ibride la cavità può raggiungere al massimo una profondità di 400µm e richiede quindi l'utilizzo di tecnologie specifiche quali ad esempio il *Potting* o il *Moulding*.

In alcuni casi occorre trattare la superficie della carta con appositi materiali prima di procedere con la fase dell'*embedding*.

6. COMPONENTI S/W E STANDARDS PER IL CHIP

6.1 I componenti S/W

La figura 6.1-A schematizza i componenti S/W che consentono ad una applicazione di operare con una Smart Card.

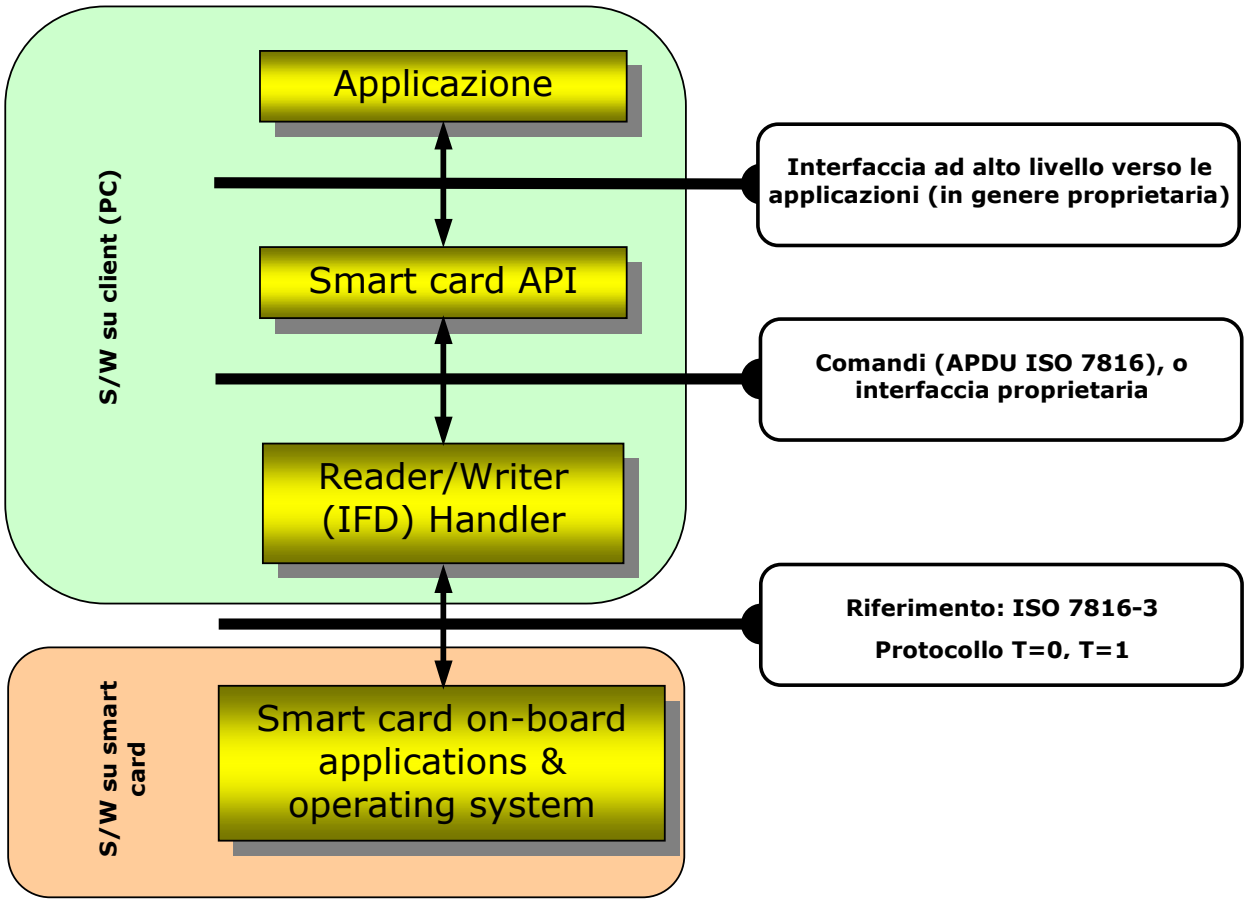


Fig. 6.1-A

I principali componenti di quest'architettura vengono di seguito descritti.

6.1.1 Smart Card API

E' il modulo software più vicino alla applicazione e fornisce servizi ad alto livello per la gestione della Smart Card.

Verso il *Reader/Writer handler* confeziona le strutture dati da e per le smart card, di norma secondo lo standard di riferimento ISO 7816-4 e nella forma di APDU.

Molto spesso questo modulo è proprietario sia per quanto concerne la interfaccia verso le applicazioni sia per la comunicazione con lo *handler*. In questo ultimo caso le *Smart Card API* non possono prescindere dal lettore.

6.1.2 Read/Writer handler

E' il modulo software che interfaccia il lettore/scrittore di smart card.

Verso la smart card esso gestisce:

- La sequenza di reset;
- La risposta della Smart card al reset (ATR)
- Il protocollo di trasporto dei dati (T=0 o T=1)

Verso gli strati più alti mette a disposizione una interfaccia che consente di veicolare i comandi di gestione della carta (APDU).

7. INFRASTRUTTURA ORGANIZZATIVA

Nel circuito di emissione intervengono gli enti descritti nella tabella [7-A]:

Codice	***Nome***	***Definizione***
F_p	Fornitori di chip	Sono le aziende produttrici dei microprocessori.
F_b	Fornitori di bande laser	Sono le aziende produttrici delle bande ottiche a lettura laser.
IPZS	Istituto Poligrafico e Zecca dello Stato	IPZS è responsabile della manifattura delle carte, della inizializzazione elettrica dei chip e della stampa degli elementi grafici costanti (il logo, lo sfondo, ecc.). Esso provvede anche a generare il numero seriale che identifica il lotto e la data di produzione.
MI	Ministero dell'Interno	E' l'ente di controllo (certificatore) che detiene la responsabilità dell'intero circuito di emissione. Esso ha la responsabilità di verificare ed accettare qualunque operazione che modifichi i contenuti e le strutture dati memorizzati sul microprocessore o sulla banda ottica relativi ai dati identificativi ed all'erogazione di servizi. L'ente verificatore genera per ogni carta un numero d'identificazione univoco, su scala nazionale, inscindibilmente legato ad essa attraverso un meccanismo di certificazione.
S	Centro servizi	E' l'ente cui vengono delegate le operazioni di formazione e stampa della carta nel caso di comuni che in esso, appunto, tendono a consorziarsi. Le attività del centro servizi potrebbero essere comunque assolte dallo stesso IPZS; esse tuttavia, per chiarezza logica (e come ipotesi possibile), sono state riportate separatamente nello schema del circuito di emissione.
E	Emettitore	E' l'ente responsabile della formazione e del rilascio della carta d'identità al cittadino, normalmente il comune.

Tab. 7-A - gli attori del circuito di emissione

La fig. [7-A] illustra graficamente lo schema del circuito di emissione:

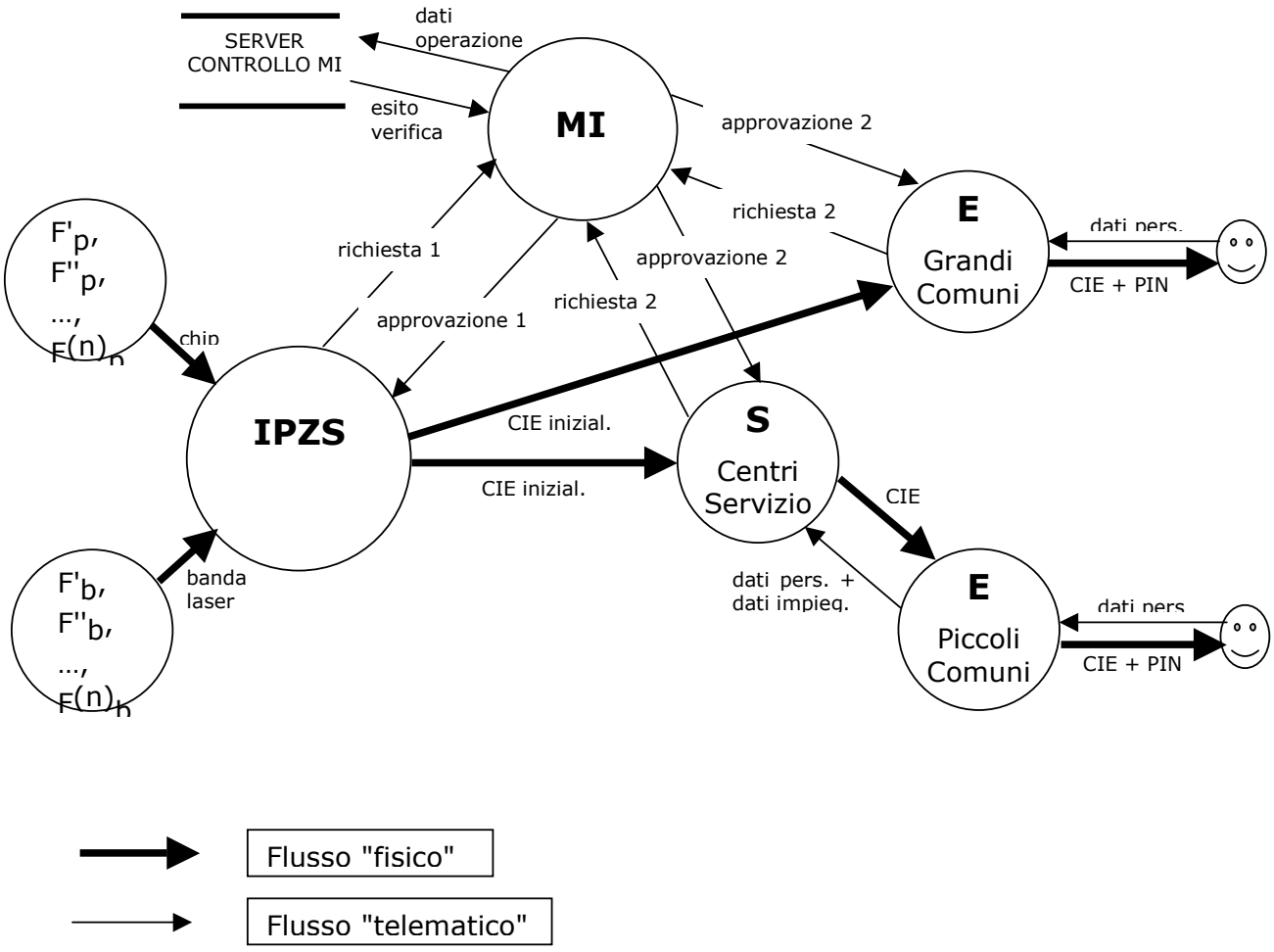


Fig. 7-A

Come già osservato, l'esistenza reale dei centri di servizio (S) è puramente un'ipotesi. Nel diagramma, tuttavia, la "bolla" corrispondente a (S) è utile per identificare logicamente un ben determinato insieme di attività.

Nel successivo cap. [8] vengono descritte in dettaglio le fasi del processo di emissione delle carte d'identità elettroniche.

7.1 Struttura delle informazioni sulla banda ottica

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[1], e consente di stabilire con certezza *chi*, *dove* e *quando* ha effettuato ed autorizzato ogni operazione. La certezza viene stabilita dall'uso incrociato delle firme digitali:

- dell'Istituto Poligrafico dello Stato, incaricato della manifattura fisica e dell'inizializzazione elettrica delle carte;
- degli enti incaricati dell'emissione delle carte (i comuni **E** o - per mandato di questi ultimi - i centri di servizio **S**);
- dell'ente incaricato delle operazioni di verifica e controllo, cioè il ministero degli interni **MI**.

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

I record R_d dell'area dati sono formati da **IPZS** o da **E** (S). I record R_c dell'area di controllo sono composti da due parti: una formata da **IPZS** o da **E** (S), l'altra formata da **MI**.

[1] Occorre definire degli appositi "tipi record" per descrivere le varie operazioni possibili sulla carta (inizializzazione, emissione, estensione di validità, revoca di validità, cambio di domicilio, …). In particolare, le uniche operazioni essenziali per la prima attivazione sono:

- Inizializzazione della carta
- Emissione della carta (durante questa fase viene apposto anche un "embedded hologram" a vista sulla banda ottica)
-

La fig. [7.1-A] mostra l'organizzazione in record corrispondenti dell'area dati (File_dati) e dell'area di controllo (File_controllo):

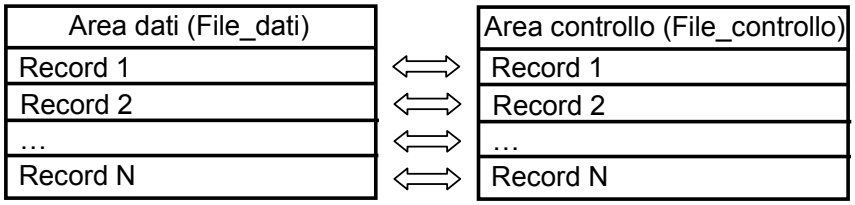


Fig. 7.1-A

La fig. [7.1-B] mostra, per ciascun record corrispondente dell'area dati e di quella di controllo, la suddivisione in campi:

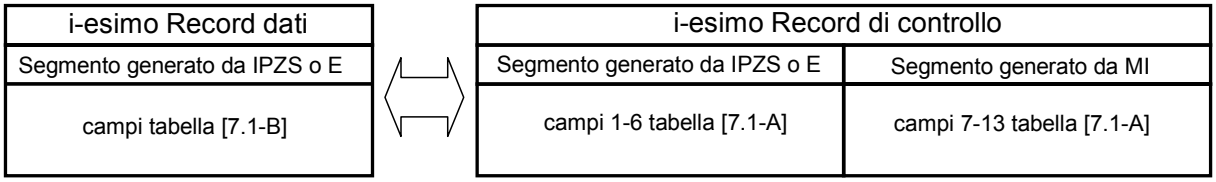


Fig. 7.1-B

Questi record contengono dunque richieste (di IPZS o E) ed approvazioni (di MI), e permettono di far avanzare la carta da uno stato 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:

Campo	***Generato da***	***Descrizione***	***Note***
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 (F_C), E (S)	Bollo elettronico dell'ente che ha creato il record.	Coincide con la firma del record dati (R_d) e dei campi [1-5] del corrispondente record di controllo (R_C), 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	MI	Numero progressivo dell'autorizzazione concessa (generato secondo un protocollo interno di MI)	Questa informazione è sempre presente.
8	MI	Data ed ora dell'autorizzazione	Questa informazione è sempre presente.
9	MI	Numero identificativo della carta	è il numero (ID_Carta) assegnato al documento d'identità dal Ministero degli Interni e stampato anche sul supporto plastico.
10	MI	Certificato del MI	Questa informazione è sempre presente.
11	MI	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	MI	Certificato anti-contraffazione della carta	E' il certificato (C_Carta) che lega il numero identificativo della carta (ID_Carta) ed una chiave pubblica (K_{pub}), corrispondente ad un'unica chiave privata (Kpri), generata all'interno del microcircuito e non esportabile all'esterno di esso. Esso è rilasciato da MI 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	MI	Bollo elettronico dell'ente di controllo e verifica.	Coincide con la firma del record dati (R_d) e dei campi [1-12] del corrispondente record di controllo (R_C), 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.

Tab 7.1-A

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

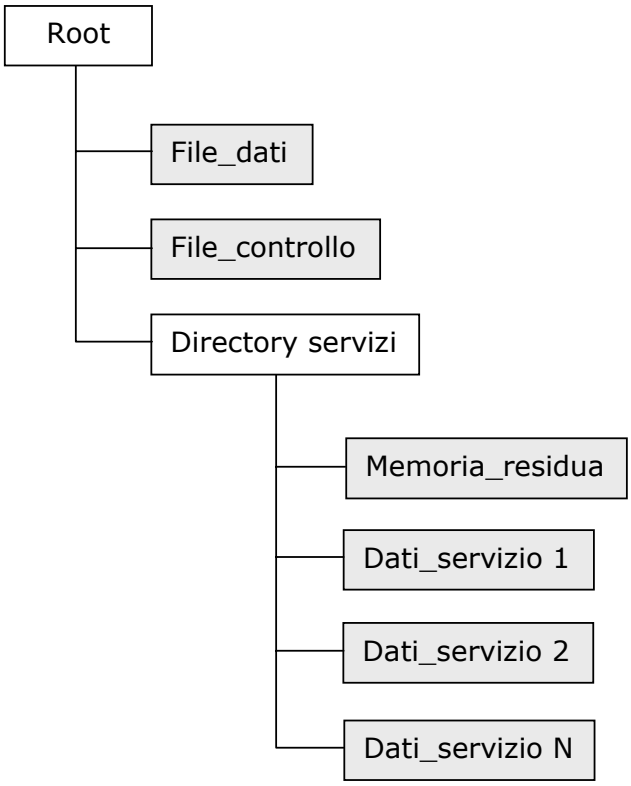
Campo	***Generato da***	***Descrizione***	***Note***
1	IPZS, E (S)	Numero progressivo del record nell'ambito dell'area dati (File_dati). Il numero progressivo di ogni record dell'area dati deve corrispondere a quello del record dell'area di controllo che descrive l'operazione eseguita	Questa informazione è sempre presente

		per generarlo e contiene le relative approvazioni (firme)	
2	E (S)	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	Chiave pubblica del servizio di installazione delle strutture dati relative a nuovi servizi ($INST_{pub}$). La responsabilità operativa del processo di installazione dei servizi è delegata ai comuni.	Non nullo solo nel record relativo all'inizializzazione, eseguita da IPZS
4	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
5	E (S)	Chiave biometrica individuale.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
6	E (S)	Dati personali dell'individuo, con l'eccezione della fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.
7	E (S)	Fotografia.	Non nullo solo nel record relativo all'emissione, eseguita dal comune.

Tab 7.1-B

La figura [7.1-C] descrive la struttura di memorizzazione della banda ottica. Le due aree di memorizzazione denominate File_dati e File_controllo sono state già descritte in precedenza. Una directory servizi è predisposta ad accogliere le strutture di memorizzazione relative ad eventuali servizi (Dati_servizo 1, 2,..., N), che avessero necessità di appoggiarsi a grosse aree di memorizzazione off-line, disponibili sulla banda ottica. Il file Memoria_residua mantiene lo stato

attuale della memoria, che decresce sempre, essendo la banda ottica un supporto non riscrivibile.



7.2 Fig. 7.1-CStruttura delle informazioni nel microprocessore

La tabella [7.2-A] definisce la struttura dei dati registrati nella memoria riscrivibile (EEPROM) del microcircuito. Le tre colonne indicate con *Fornito da*, *Predisposto da*, *Scritto da*, hanno lo scopo, pur in presenza di inevitabili approssimazioni, di dettagliare meglio il tipo di operazione eseguita:

- 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		E' 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 (S)	E (S)	E (S)	E' il PIN utente richiesto per usare la chiave privata K_{pri} per le operazioni di autenticazione. Questo codice deve essere consegnato dal comune di rilascio, con garanzia di segretezza, al titolare della CIE.
6	K_{pri}		E (S)		Chiave autogenerata internamente alla carta, congiuntamente a K_{pub}. Essa è invisibile all'esterno, ma utilizzabile per le operazioni di cifra richieste durante l'operazione di strong authentication. Il microcircuito deve essere provvisto di un motore crittografico interno (crypto-engine), al fine di rendere più rapide tali operazioni.
7	$INST_{pub}$	E (S)	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.
8	Dati_processore	IPZS	IPZS	IPZS	E' un file elementare (EF) che riporta alcuni dati identificativi univoci del processore (n. serie, lotto di produzione, fabbricante, ecc.)

9	Parametri_APDU	F_p	IPZS	IPZS	E' un file elementare che riporta le particolarità dei comandi elementari (APDU) del sistema operativo della carta, al fine di rendere interoperabili le applicazioni.
10	ID_Carta	MI	IPZS	IPZS	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	MI	IPZS	E (S)	E' il certificato, rilasciato dal Ministero dell'Interno, che garantisce la validità del legame tra la componente pubblica, K_{pub}, 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 (S)	IPZS	E (S)	E' un file elementare che contiene i dati personali dell'individuo, con l'eccezione della fotografia.
13	Fotografia	E (S)	IPZS	E (S)	Date le sue dimensioni, non è conveniente inserire la fotografia direttamente nel file Dati_personali. Per questo, essa è riportata in un file a parte, detto appunto "Fotografia".
14	Memoria_residua	E (S)	IPZS	E (S)	E' l'ammontare dello spazio totale previsto per i servizi, decurtato dello spazio utilizzato da quelli già installati.
15	Servizi_installati	E (S)	IPZS	E (S)	E' un file elementare che riporta l'elenco dei servizi già installati sulla carta.
16	DF_Servizio #1, DF_Servizio #2, … DF_Servizio #N	E (S)	E (S)	E (S)	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 (S_{pub}).

Tab. 7.2-A

La figura [7.2-A] descrive graficamente la struttura di memorizzazione interna al microprocessore:

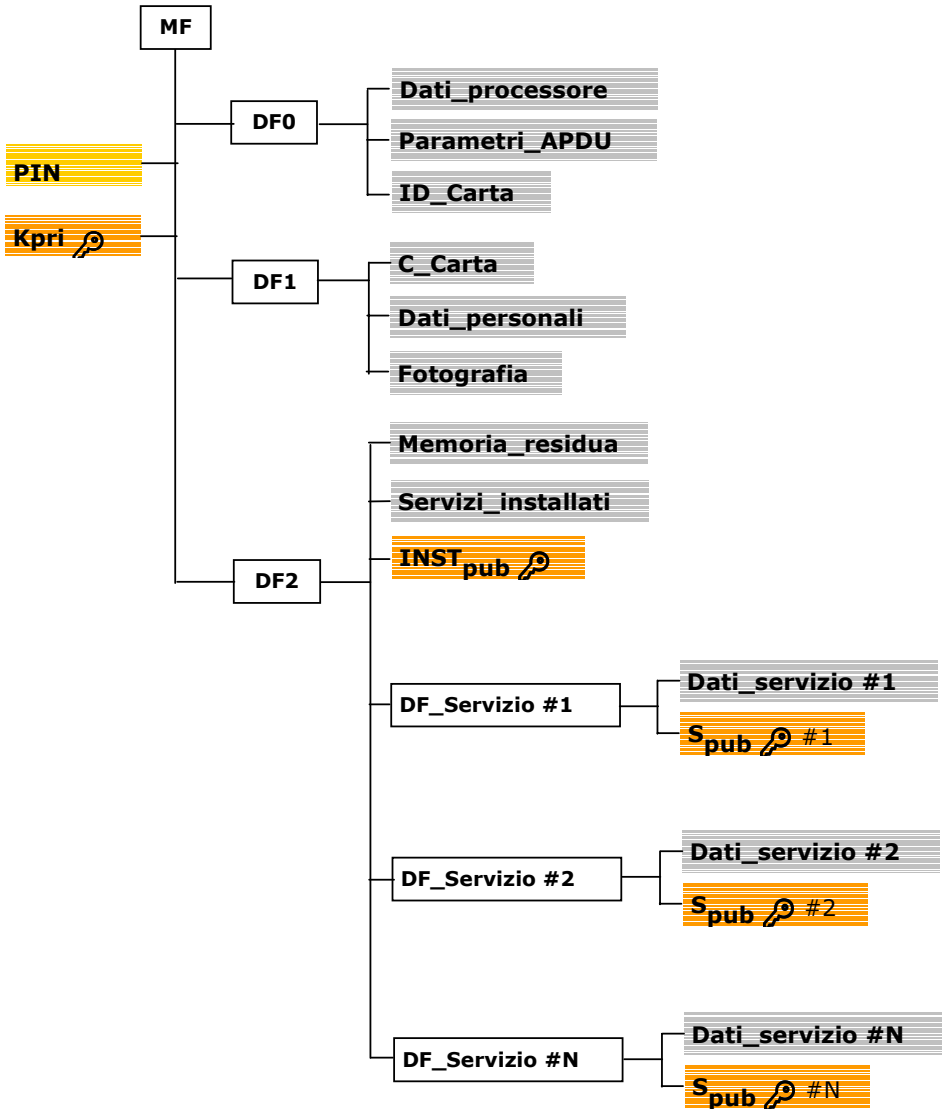


Fig. 7.2-A

7.2.1 Il certificato "C_Carta"

Sebbene altre forme siano possibili, il mezzo standard ed universalmente noto per legare una chiave pubblica al suo titolare è il "certificato". Si è ritenuto pertanto opportuno utilizzare questa forma anche per la CIE. Il formato proposto è quello descritto nella specifica X509v3, che prevede le cosiddette "estensioni".

Al Ministero dell'Interno viene assegnata la responsabilità di ente certificatore, mentre titolare del certificato è la "carta", attraverso il suo numero di matricola. Ciò che viene certificato, dunque, è il legame tra la chiave pubblica e il numero identificativo (univoco) della carta, ID_Carta.

Tuttavia ogni carta è assegnata ad uno ed un solo cittadino, e questo legame deve risultare garantito per la sicurezza del circuito e, in ogni caso, durante la fase di autenticazione. A questo scopo l' "impronta", o *hash,* dei dati raccolti durante la formazione della carta va a far parte di un'estensione del certificato, *non obbligatoria*, appositamente creata. L'algoritmo designato per la funzione di hash è lo SHA-1.

Come noto, non è possibile risalire dall'impronta alla sequenza di *bytes* originaria. Ciò esclude la possibilità della presenza, presso MI, di un'anagrafe unica dei titolari della carta, in quanto l'unico dato fruibile, a partire dal certificato, è il numero di matricola (ID_Carta) assegnato alla CIE.

Il *DSN* della CIE è formato da due sole informazioni: "*Country Name*" (valore = IT), *e "Carta d'Identità Italiana*" (valore = ID_Carta). La definizione del tipo "Carta d'Identità Italiana" va registrata presso gli organismi internazionali a ciò deputati. Questi due valori sono sufficienti ad identificare in modo univoco la carta e soddisfano, di conseguenza, il requisito previsto dall'X.509.

Il fatto che l'estensione sia contrassegnata come "*non obbligatoria*", comporta che il certificato è ritenuto valido anche da eventuali applicazioni che non ne conoscono a priori il particolare formato. Naturalmente l'estensione deve comunque contenere l' *hash* dei dati raccolti durante la personalizzazione, se si vuole che nel processo di autenticazione possa con certezza essere identificato, oltre la carta, anche il soggetto richiedente.

I dati personali, a partire dai quali viene calcolata l'impronta che va a far parte dell'estensione, sono i seguenti:

Nome	Stringa
Cognome	Stringa
Sesso	Stringa
Statura	Numerico
Data di nascita	Data
Luogo di nascita	Data
Estremi dell'atto	Stringa
Cittadinanza	Stringa
Codice Fiscale	Stringa
Indirizzo	Stringa
Comune di residenza	Stringa
Provincia di residenza	Stringa
Data di emissione del documento	Data
Data di scadenza del documento	Data

Tab. 7.2.1-A

Sono, questi, i dati presenti nel file elementare (EF) "Dati_personali", riportato in fig. [7.2-A] e descritto nella tabella [7.2-A].

Come può notarsi, tra i dati elencati è assente la fotografia. Ciò è fatto di proposito, al fine di migliorare le *performances* della procedura di autenticazione. Infatti, quando la fotografia non sia esplicitamente richiesta, basta estrarre dalla carta il file Dati_personali, calcolarne l'hash, e confrontarlo con quello presente nel certificato. Se l'impronta, presente nel certificato, fosse stata calcolata considerando anche la fotografia, ciò avrebbe comportato la necessità di dover comunque estrarre anch'essa dalla carta, per includerla nel calcolo di verifica dell'hash, ogniqualvolta si desiderasse identificare il titolare. E poiché le dimensioni della fotografia (nonostante la compressione) sono circa 20 volte superiori a quelle del file Dati_personali, ne sarebbe risultato un proporzionale rallentamento dell'operazione.

Tuttavia, possono esserci casi in cui la verifica della fotografia sia richiesta. Per questo è inclusa nel certificato una ulteriore estensione, che riporta l'impronta, o hash, del contenuto del file "Fotografia", presente nella directory DF1 (vedi tabella [7.2-A]).

E' possibile che, oltre a queste due estensioni, ne vengano aggiunte delle altre, come ad esempio la "KeyUsage" per l'ambito di utilizzo delle chiavi o "PrivateKeyUsagePeriod" per il periodo di utilizzo della chiave privata, tuttavia nella tabella seguente, che descrive in sintesi le informazioni presenti nel certificato, si fa riferimento ai soli dati ritenuti essenziali ai fini dell'identificazione sicura:

Elemento	Tipo	Descrizione
Country_name ID_Carta	DSN	E' il distinguished name X500 del titolare del certificato che, per quanto detto, è la "carta d'identità italiana numero ID_Carta".
Impronta del file estensione "Dati_personali"		E' una sequenza di 160 bit (20 bytes), calcolata a partire dal contenuto del file Dati_personali, attraverso l'algoritmo di hash SHA-1.
Impronta del file estensione "Fotografia"		E' una sequenza di 160 bit (20 bytes), calcolata a partire dal contenuto del file Fotografia attraverso l'algoritmo di hash SHA-1.

Tab. 7.2.1-B

8. L'ARCHITETTURA DEI SERVIZI

Il presente capitolo descrive come la carta sia predisposta all'installazione ed erogazione dei servizi, che le conferiscono la capacità di semplificare il rapporto dei cittadini con le amministrazioni pubbliche.

8.1 Servizi "standard" e servizi "qualificati"

La possibilità, propria del microcircuito, di garantire l'identificazione sicura, e a distanza (telematica), del titolare della CIE, permette di ipotizzare una serie quasi inesauribile di servizi, che enti pubblici e privati potranno offrire, in modo semplice, al cittadino. Sono tuttavia due le tipologie di servizi, erogabili attraverso la CIE. Al primo tipo possono essere ricondotti tutti quei servizi per la cui erogazione è sufficiente l'identificazione sicura del richiedente, ad esempio la richiesta di un certificato, effettuata on-line, la prenotazione di una visita, una visura catastale, ecc.Sebbene i servizi, in gran maggioranza, ricadano nella prima categoria, esistono tuttavia alcuni servizi per i quali appare indispensabile prevedere la memorizzazione di informazioni sulla CIE. Ad es., un ipotetico servizio di emergenza sanitaria potrebbe richiedere la memorizzazione sulla CIE del gruppo sanguigno. Questi servizi richiedono, come vedremo, un'attenzione ulteriore alle problematiche di sicurezza. Anche in questo caso, comunque, la capacità di processo del microcircuito permette di garantire che i dati residenti sulla CIE siano aggiornati solo dagli enti abilitati, in presenza del titolare o per via remota.

In sintesi, valgono le seguenti definizioni:

- sono definiti servizi "standard" quelli che, per poter essere erogati, richiedono la sola identificazione della carta e del suo titolare.
- sono definiti servizi qualificati quelli che, per poter essere erogati, richiedono la presenza di una struttura dati sulla CIE e possono aggiornare le informazioni ivi memorizzate.

8.2 Condizioni di accesso e relativi test

Al fine di meglio comprendere il modello proposto, vale la pena spendere qualche parola sui processi di test che proteggono le operazioni di creazione e riempimento delle strutture presenti sulla carta ed illustrate nella Fig. [7.2-A].

La creazione delle strutture dati (DF ed EF) viene eseguita attraverso il comando ISO 7816-4 "CREATE FILE". Una volta creata una struttura, essa può essere "popolata" attraverso altri comandi (es. WRITE BINARY). I comandi richiedono, per poter essere eseguiti, il superamento di un test (condizione logica), che nel caso più semplice corrisponde alla conoscenza di un PIN. I test sono

normalmente memorizzati in oggetti appositi, detti *Test Objects*. Questi test objects possono racchiudere un numero di cui è necessario dimostrare la conoscenza, ad es. un PIN, ma possono anche, in alternativa, riferire la chiave pubblica (o quella segreta, in caso di crittografia simmetrica) di un'entità esterna alla carta[2]. In quest'ultimo caso, il superamento del test avviene non perché si conosce il PIN, ma perché la carta riconosce l'entità esterna in possesso della chiave privata corrispondente a quella pubblica memorizzata nell'oggetto riferito dal test (oppure, in caso di crittografia simmetrica, perché le due chiavi coincidono). Questo approccio viene usato quando non è direttamente l'utente a dover approvare un'operazione (ad es. l'uso della chiave privata per firmare un documento), ma è piuttosto un'applicazione esterna che deve risultare ben nota alla carta perché questa le permetta di operare.

Infine va osservato come un test possa risultare dalla combinazione logica di più test elementari (ad es. T = T1 AND T2). Ciò è particolarmente utile, ad esempio, se l'esecuzione di un comando richiede non solo l'autenticazione dell'applicazione "esterna" che lo esegue, ma anche l'assenso esplicito del possessore (ad es. mediante la digitazione del PIN).

8.3 Predisposizione, installazione ed erogazione di servizi qualificati

Nel modello architetturale proposto per i servizi qualificati, individuiamo tre momenti distinti, descritti nei punti seguenti:

Predisposizione

Viene definita "predisposizione" di un servizio la procedura informatica attraverso la quale viene creata, all'interno del *file system* del microcircuito , una nuova struttura dati, *vuota* ed atta a contenere informazioni relative al servizio *da erogare*. La responsabilità della predisposizione di nuovi servizi compete esclusivamente al comune (o a chi ne fa le veci[3]).

Installazione

Viene definita "installazione" di un servizio la procedura informatica attraverso la quale viene inizialmente popolata una struttura dati, già presente nel file system del microcircuito, con le informazioni necessarie all'erogazione del servizio istallato. La responsabilità dell'installazione di un nuovo servizio compete esclusivamente all'ente incaricato della sua erogazione. Lo schema architetturale, adottato per i servizi, previene la possibilità che terzi possano variare i dati istallati dall'ente erogante.

Erogazione

---

[2]In pratica il test in questo caso fa riferimento ad un cosiddetto "Key Object".

[3] Centri servizio ovvero IPZS.

Viene definita "erogazione" di un servizio l'insieme delle operazioni eseguite da una applicazione, istallata su un server remoto, successive all'identificazione del titolare della carta, e conseguenti ad una sua precisa volontà. Qualora il servizio erogato preveda l'aggiornamento di informazioni memorizzate nel file system del microcircuito, l'ente che eroga il servizio deve coincidere con quello che lo ha istallato, e le uniche variazioni possibili sono quelle effettuate nella struttura dati di competenza.

8.4 Il modello per i servizi qualificati

Se è possibile ipotizzare che il cittadino, che desideri predisporre sulla propria carta d'identità l'istanza di un nuovo servizio qualificato, si rechi presso un apposito ufficio messo a disposizione dal comune di appartenenza, ciò appare troppo limitante per l'installazione e l'erogazione del servizio stesso, che deve - almeno in alcuni casi - poter avvenire da postazione remota ed attraverso il mezzo insicuro (Internet).

Ciò pone ovviamente alcuni problemi di sicurezza, che vengono brevemente analizzati in questo paragrafo. Come già ricordato, i servizi erogabili sono divisi in due categorie:

- servizi che richiedono un aggiornamento dei dati memorizzati nel microcircuito, "detti qualificati";
- servizi che richiedono la sola identificazione della carta e del suo titolare, definiti "standard" o "non qualificati".

Va detto subito che la seconda categoria, con ogni probabilità, comprende la larga maggioranza dei servizi che verranno erogati per mezzo della CIE. Per questo genere di servizi, il problema di sicurezza può con sufficiente tranquillità essere ristretto a quello della riservatezza del canale di trasmissione, tra l'applicazione *client* (ad es. il *browser*) ed il *server* che espone il servizio. Infatti, anche nel caso che le funzionalità che eseguono l'accesso alla carta fossero sostituite con un'*applet* pirata, questa non avrebbe alcun modo di eseguire comandi diversi da quelli previsti per l'autenticazione (es. INTERNAL AUTHENTICATE o PSO).

Diverso è il caso in cui il servizio erogato richieda l'aggiornamento di una struttura dati sulla carta. In questo caso è necessario creare un canale "sicuro" dal server al microcircuito, e non dal *server* all'applicazione *client*, perché altrimenti quest'ultima potrebbe essere sfruttata per operare un attacco "nel mezzo", con conseguente effrazione della sicurezza.

Il mezzo utilizzato per cifrare il canale tra server e microcircuito prende il nome *di secure messaging*. Esso viene usato solo per i comandi di aggiornamento dei dati nella memoria EEPROM del microcircuito, che consistono in poche APDU. Le chiavi per il secure messaging (K_{SM}) devono essere inserite nella struttura dati del microcircuito, per ciascun servizio, all'atto della predisposizione dello stesso. Non è esclusa a priori, tuttavia, la possibilità di generare dinamicamente tali chiavi all'interno del microcircuito, e scambiarle col server in modo sicuro,

sfruttando le possibilità della crittografia asimmetrica e scrivendo un'opportuna estensione (applet o procedura) del sistema operativo del microcircuito. In quest'ultimo caso, la sola chiave pubblica del server che eroga il servizio verrebbe inserita nel microcircuito, a cura del comune, all'atto della generazione della struttura dati del servizio.

Definiamo pertanto servizi qualificati quei servizi che soddisfano ad entrambe le seguenti condizioni:

- devono poter essere erogati attraverso il mezzo insicuro (es. Internet)
- devono poter aggiornare dati residenti sulla carta

La lunghezza della chiave di secure messaging deve essere non inferiore a 128 bit. La lunghezza della chiave S_{pub}, come per le altri chiavi asimmetriche utilizzate, deve essere non inferiore a 1024 bit. L'operazione di autenticazione del servizio deve far uso del comando ISO 7816-4 EXTERNAL AUTHENTICATE, e l'algoritmo di cifratura-decifratura, associato alla chiave, deve essere conforme allo standard PKCS#1 RSA Encryption Standard.

8.5 Sequenza tipo

Uno dei problemi principali nella progettazione dell'architettura dei servizi è quello della generazione e distribuzione delle chiavi di cifratura. Queste devono essere usate, in vario modo, per permettere tre operazioni indispensabili, riassunte sinteticamente di seguito:

- permettere al SERVER di autenticare la CARTA;
- permettere alla CARTA di autenticare il SERVER;
- custodire la riservatezza del canale, che transita attraverso l'APPLET, tra CARTA e SERVER,

dove:

- SERVER è il server che ospita ed eroga il servizio; ad esso è assegnata una coppia di chiavi, di cui una pubblica (S_{pub}) ed una privata (S_{pri}).
- CARTA è la carta d'identità, inscindibilmente legata al suo titolare mediante il PIN, che solo lui conosce e può inserire quando necessario. Alla CARTA è assegnata una coppia di chiavi, di cui una pubblica (K_{pub}) ed una privata (K_{pri}). La chiave pubblica K_{pub} è inserita nel certificato C_CARTA, memorizzato nella directory DF0 del microcircuito.
- APPLET è l'applicazione *client* che "parla" da un lato con la CARTA, e dall'altro col SERVER. Essa trasmette alla CARTA i comandi e le informazioni provenienti dal SERVER, ed invia a quest'ultimo le "risposte" che questi si attende.

- APPLET PIRATA è l'applicazione client che si sostituisce in tutto o in parte, con il consenso del titolare o a sua insaputa, all'APPLET autentica inviata on-line dal SERVER, od ottenuta per altra via.

I pericoli che è necessario scongiurare sono i seguenti:

- evitare che il SERVER "pensi" di parlare con la CARTA, mentre invece sta parlando con un'APPLET PIRATA, ossia evitare che quest'ultima simuli di essere la CARTA;
- evitare che la CARTA "pensi" di parlare con il SERVER, mentre invece sta parlando con un'APPLET PIRATA;
- evitare che le informazioni in transito possano essere interpretate, o addirittura modificate.

Queste problematiche non sono certamente nuove. Esse sono state affrontate e risolte utilizzando tecniche di cifratura e la capacità di processo del microcircuito. Alcuni comandi, previsti dallo standard ISO 7816, servono proprio ad assolvere i compiti precedentemente elencati. Tuttavia, se si fa affidamento a questi soli comandi, è necessario prevedere la diffusione di chiavi simmetriche di cifratura, che fungano da "*master key*" per il colloquio e la mutua autenticazione tra CARTA e SERVER. Ben note tecniche di *key derivation* possono essere infine utilizzate per derivare dalla *master key* una chiave valida per una sola sessione. Ciò al fine di evitare che un comando, cifrato con la *master key*, possa essere ripetuto cosi com'è in un altro contesto: in mancanza di *key derivation*, esso risulterebbe valido ed accettato dalla CARTA.

Come detto, facendo riferimento a questa metodologia standard, il problema della mutua autenticazione e della riservatezza è risolto, ma l'architettura dei servizi (almeno di quelli qualificati) paga qualcosa quanto ad "agilità": è infatti necessario distribuire con sicurezza delle chiavi simmetriche.

Una possibile soluzione al problema, basata unicamente su tecniche di crittografia asimmetrica, richiederebbe la scrittura di un'estensione del sistema operativo della carta (o lo sviluppo di un'applet, procedura, ecc.), non standard, ed è tuttora in fase di valutazione. Il comando avrebbe lo scopo di generare dinamicamente e scambiare in modo sicuro la chiave di sessione, liberando dalla necessità della sua distribuzione e gestione, e snellendo pertanto l'architettura dei servizi.

Una sequenza di lavoro tipica per l'erogazione di un servizio è indicata nella tabella seguente. La prima parte, che descrive la sola identificazione del titolare, è sufficiente per i servizi standard (che non richiedono la modifica delle informazioni presenti sulla carta). In questo caso (che è di gran lunga il più frequente), come già ricordato in precedenza, non è necessario il secure messaging. La seconda parte descrive invece i passi necessari per accedere ad un servizio qualificato, che può aggiornare informazioni presenti sul microcircuito.

#	SERVER	APPLET	CARTA	FASE
1		Richiesta di connessione a SERVER		AUTENTICAZIONE DELLA CARTA (E DEL TITOLARE)
	Richiede ad APPLET C_Carta			
		SELECT FILE(C_Carta) READ BYNARY		
			C_Carta viene selezionato e letto; C_Carta è un file a lettura libera.	
		Invia C_Carta a SERVER		
	Verifica la validita' del certificato mediante MI_{pub} ed estrae da esso ID_Carta e K_{pub}			
	Genera challenge (RANDOM) e la invia all'APPLET			
		Seleziona Kpri per mezzo del comando MSE (manage security environment)		
			Kpri è selezionata	
		Esegue la cifratura del challenge (RANDOM) per mezzo del comando PSO (Perform security operation)		
			Restituisce ad APPLET Kpri(RANDOM)	
		Invia a SERVER Kpri(RANDOM)		
	Esegue Kpub(Kpri(RANDOM)) e verifica RANDOM per vedere se è uguale a quello inviato			
CARTA AUTENTICATA (per i servizi non qualificati questo è il punto di uscita) **INIZIO EROGAZIONE SERVIZIO STANDARD** **PROSEGUE SE IL SERVIZIO RICHIESTO E' QUALIFICATO**				
CHIAVE DI SESSIONE Ks GIA' INSTALLATA, **OPPURE** **CHIAVE DI SESSIONE Ks GENERATA E SCAMBIATA (richiede scrittura comando ad hoc)**				
	Invia ad APPLET il comando GET CHALLENGE			AUTENTICAZIONE DEL SERVER DA PARTE DELLA CARTA (SOLO SERVIZI QUALIFICATI)
		Invia alla CARTA il comando GET CHALLENGE		

			In risposta al comando GET CHALLENGE, restituisce all'APPLET una challenge (RANDOM)	QUALIFICATI)
		Invia RANDOM al SERVER		
	Cifra il challenge con Ks e lo restituisce all'APPPLET: Ks(RANDOM)			
		Invia alla CARTA Ks(CHALLENGE)		
			Verifica Ks(CHALLENGE), eseguendo Ks(Ks(CHALLENGE)), ed in caso di successo autentica il SERVER	
SERVER AUTENTICATO, SECURE MESSAGING INSTAURATO **INIZIO EROGAZIONE SERVIZIO QUALIFICATO**				
	Cifra/decifra comunicazioni con Ks	Inoltra/riceve comandi cifrati con Ks	Cifra/decifra comunicazioni con Ks	SECURE MESSAGING

8.6 Il modello architetturale

Il modello adottato per la generazione delle strutture dati e l'installazione dei servizi qualificati è di seguito descritto.

8.6.1 Gli attori

Gli enti interessati nel modello architetturale dei servizi sono:

- Il Ministero dell'Interno
- I Comuni
- Gli enti interessati ad erogare un servizio (che richiede l'installazione di una nuova struttura dati sulla carta)
- Il titolare della carta

8.6.2 L'elenco dei servizi

L'elenco ufficiale dei servizi è mantenuto e dislocato presso il Ministero dell'Interno. Le informazioni contenute, per ogni servizio, sono:

- Formato della struttura dati da creare sulla carta
- Spazio richiesto in EEPROM ed, eventualmente, sulla banda ottica
- Chiave di accesso (certificato dell'ente erogatore, contenente S_{pub})
- Informazioni descrittive del servizio

L'accesso all'elenco è libero, ed i comuni possono detenere copie di esso, salvo verificarne periodicamente gli aggiornamenti.

8.6.3 I ruoli

Nell'ambito dell'architettura proposta, il Ministero dell'Interno:

- mantiene l'elenco ufficiale dei servizi che è possibile predisporre sulla CIE,
- vaglia ed accetta le richieste di inserimento nell'elenco, effettuate tanto da enti pubblici che, eventualmente, da privati,
- permette l'accesso all'elenco agli enti incaricati della predisposizione dei servizi (Comuni, Centri di servizio o IPZS stesso).

I comuni, invece:

- sono responsabili dell'effettiva installazione sulla carta di un nuovo servizio,
- gestiscono l'applicazione in grado di installare (o disinstallare) le nuove strutture dati,
- verificano la presenza del servizio nell'elenco pubblicato dal Ministero dell'Interno,
- verificano in modo automatico, per mezzo dell'applicazione in carico della predisposizione delle strutture dati, lo spazio residuo nella memoria riscrivibile (EEPROM) del microcircuito e, se previsto, nella banda ottica.

Gli enti interessati all'erogazione di servizi qualificati[4]:

- sono le istituzioni (pubbliche o private) autorizzate ad erogare servizi che prevedono la modifica di informazioni presenti nel microcircuito.
- devono fare richiesta al Ministero dell'Interno, per inserire nell'elenco pubblico le informazioni relative al proprio servizio (necessarie per la sua predisposizione).

Infine il titolare della carta:

- s'informa dei servizi disponibili presso il Comune di appartenenza (anche per via telematica, es. pagina web),
- richiede al Comune la predisposizione (o la cancellazione) di un servizio di suo interesse,
- al momento dell'installazione, conferma la sua volontà attraverso la digitazione del PIN utente e/o l'utilizzo della chiave biometrica.

[4] *Gli enti che intendono erogare servizi per i quali è sufficiente l'identificazione del titolare (servizi standard, o non qualificati), non hanno alcun bisogno di far inserire informazioni nell'elenco pubblico, perché non richiedono alcuna predisposizione di strutture dati sulla carta.*

9. FASI DEL PROCESSO DI EMISSIONE

Nel presente capitolo vengono descritte in dettaglio le fasi operative previste dal circuito di emissione.

9.1 Produzione di banda laser e microprocessore

Le bande laser ed i microprocessori vengono fabbricati rispettivamente dagli enti F_b ed F_p in grado di eseguire tale operazione. Gli F_p provvedono anche alla mascheratura in ROM del sistema operativo. Tali enti successivamente inviano i loro prodotti direttamente all'Istituto Poligrafico dello Stato (IPZS). Nella figura 9.1-A sono rese evidenti tali attività.

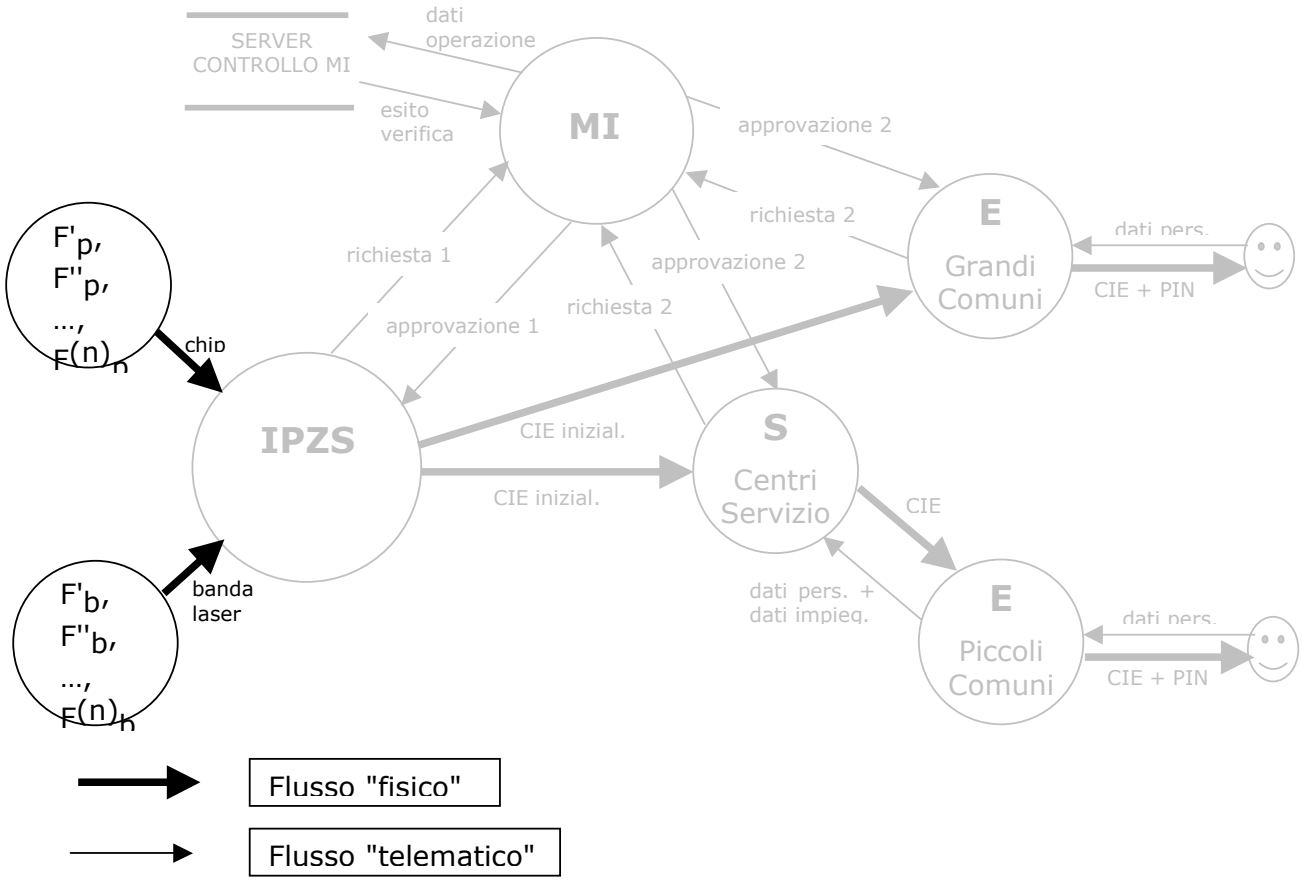


Fig 9.1-A

9.2 Produzione della CIE e sua inizializzazione

I chip e le bande laser, prodotte da F_p e F_b, vengono inseriti nel supporto in policarbonato direttamente da IPZS.

IPZS è responsabile della manifattura delle carte, della inizializzazione elettrica, del chip, della banda ottica e della stampa degli elementi grafici costanti (il logo, lo sfondo, ecc.). Inoltre provvede anche a stampare il numero seriale che identifica il lotto e la data di produzione (fornito da MI).

Sebbene da un punto di vista teorico non sia strettamente necessario, appare oltremodo conveniente[5] separare il processo di produzione-inizializzazione in due sottofasi. Nella prima sottofase, detta di *produzione*, avviene la manifattura fisica delle carte, l'inizializzazione elettrica del chip e la stampa del logo e degli elementi grafici "costanti".

Le due sottofasi sono dettagliate nei seguenti due paragrafi.

Il Ministero dell'Interno, da parte sua, genera periodicamente interi lotti di nuovi ID_Carta. Tali lotti, raccolti in files, vengono poi inviati a IPZS, che è così in grado di sapere quali numeri assegnare alle nuove carte in corso di produzione. IPZS a inizializzazione completata, comunica al Ministero dell'Interno l'associazione ID_Carta / Comune richiedente. L'invio di queste informazioni avviene per via telematica, e la modalità è "off-line".

9.2.1 Sottofase di produzione

In questa fase viene portata a termine l'inizializzazione elettrica del microcircuito e della banda ottica. La separazione permette anche una semplificazione della tipologia dei macchinari utilizzati, a favore del contenimento dei costi.

[5] *Come apparirà nel seguito, la convenienza è dettata anzitutto dalla necessità di eseguire una sequenza di richiesta-approvazione col Ministero dell'Interno per ogni carta prodotta. L'invio per via telematica di tale richiesta, e l'attesa della corrispondente approvazione, si tradurrebbero in un vincolo pesante per il processo produttivo. Separando il processo in due sottofasi è possibile invece svincolarlo dai tempi di risposta del collegamento telematico. Un secondo vantaggio è dovuto alla possibilità di svincolare la fase di scrittura sulla banda laser da quella di inizializzazione del chip, il che dovrebbe consentire di fare a meno di macchinari speciali.*

Vediamo nel dettaglio le operazioni eseguite da IPZS:

#	*Operazione*	*Note*
1	Produzione della carta con la banda ottica.	
2	Embedding del chip sulla carta contenente la banda ottica.	
3	Generazione della struttura dati interna del processore e della banda ottica (MF, DF0, DF1, DF2, DF3, ecc.) e definizione dei test che è necessario superare per poter operare (in lettura, scrittura, ecc.) su ciascuna di esse. In questa fase vengono create tutte le strutture dati la cui presenza e dimensione è già nota (es. ID_Carta, Dati_processore, Dati_banda ottica, DatiParametri_APDU, C_Carta, ecc.). Ovviamente per la maggior parte di esse si tratterà di "contenitori" vuoti.	I test individuati sono 2, di cui uno è sotto forma di PIN (P1), per l'accesso in scrittura dei files della directory DF1 (C_Carta e Fotografia), e l'altro sotto forma di chiave pubblica ($INST_{pub}$) per l'autenticazione delle applicazioni utilizzate dai comuni (o da IPZS o dai centri servizio) per la predisposizione dei servizi sulla carta.
4	Riempimento (scrittura) dei files elementari che riportano i dati specifici del microcircuito ("Dati_processore"), del sistema operativo ("Parametri_APDU") e della banda ottica ("Dati_banda_ottica"). Scrittura del file ID_Carta col dato relativo (numero della CIE). Impostazione delle condizioni di accesso a tali files in modo da renderli inalterabili a chiunque in futuro.	Il file Dati_processore permette di individuare univocamente il microcircuito (riporta il numero di serie, il lotto di produzione, ecc.); il file Parametri_APDU elenca i parametri dei comandi elementari APDU, relativamente al sistema operativo, al fine di garantire l'interoperabilità delle applicazioni. Il file Dati_banda_ottica identifica univocamente la banda ottica.
5	Scrittura del record dati (Rd) e dei campi [1-6] del record di controllo (Rc) relativi all'operazione di inizializzazione. Il Record di controllo (Rc) deve contenere almeno le seguenti informazioni: • ID_Carta • Dati_processore / Dati_banda_ottica • Data di fabbricazione della carta • PIN P1 (per abilitare l'accesso in scrittura dei files elementari C_Carta e Fotografia presenti nella directory	La data di fabbricazione qui impostata è quella che fa testo per il calcolo della durata della carta. IPZS produce lotti di carte su richiesta dei comuni. E' quindi in grado di indicare a MI, a questo livello, a quale comune è indirizzata la carta. Non è necessario scrivere subito i dati anche sulla banda ottica; questa operazione può essere lasciata tutta alla seconda sotto-

	DF1 che devono essere riempiti dal comune di destinazione) cifrato con la chiave pubblica del comune di destinazione. • Indicazione del comune cui la carta è destinata.	fase, consentendo così una semplificazione dei macchinari utilizzati.
6	Inserimento del record dati e di quello di controllo in coda ad un file di richieste di autorizzazione da inviare a MI.	
7	Stampa dello sfondo, del logo, del numero di carta (ID_Carta) e degli altri elementi costanti.	
8	Incisione grafica sulla banda ottica degli elementi costanti (logo, ID_Carta ecc.).	
9	Stoccaggio della carta.	

Tab. 9.2.1-A

9.2.2 Sottofase di attivazione

Al termine di questa sottofase la carta d'identità risulta "attivata", e diventa pertanto "documento in bianco", ossia pronto alla successiva fase di formazione e rilascio, da condurre in loco (il comune od il centro servizi).

L'apparato necessario può constare semplicemente di un lettore-scrittore di banda ottica e di un lettore di chip, necessari a leggere l'informazione relativa al numero della carta.

Le fasi sono circostanziate nella tabella seguente:

#	***Operazione***	***Note***
1	Ricezione del file delle approvazioni da parte di MI.	
2	Messa in macchina del lotto di carte relativo alle approvazioni ricevute.	
3	Per ciascuna carta, lettura di ID_Carta dal chip e dalla banda ottica.	Ridondanza per motivi di sicurezza.
4	Estrazione dal file delle approvazioni di Rd ed Rc corrispondenti all'ID_Carta precedentemente letto.	
5	Trasmissione a MI delle associazioni ID_Carta /Comune richiedente.	
6	Invio della carta in bianco (attivata) agli enti incaricati delle procedure di emissione (comuni (E) o centri servizio (S)).	

Tab. 9.2.2-A

La fig. 9.2.2-A illustra graficamente le attività di questa fase.

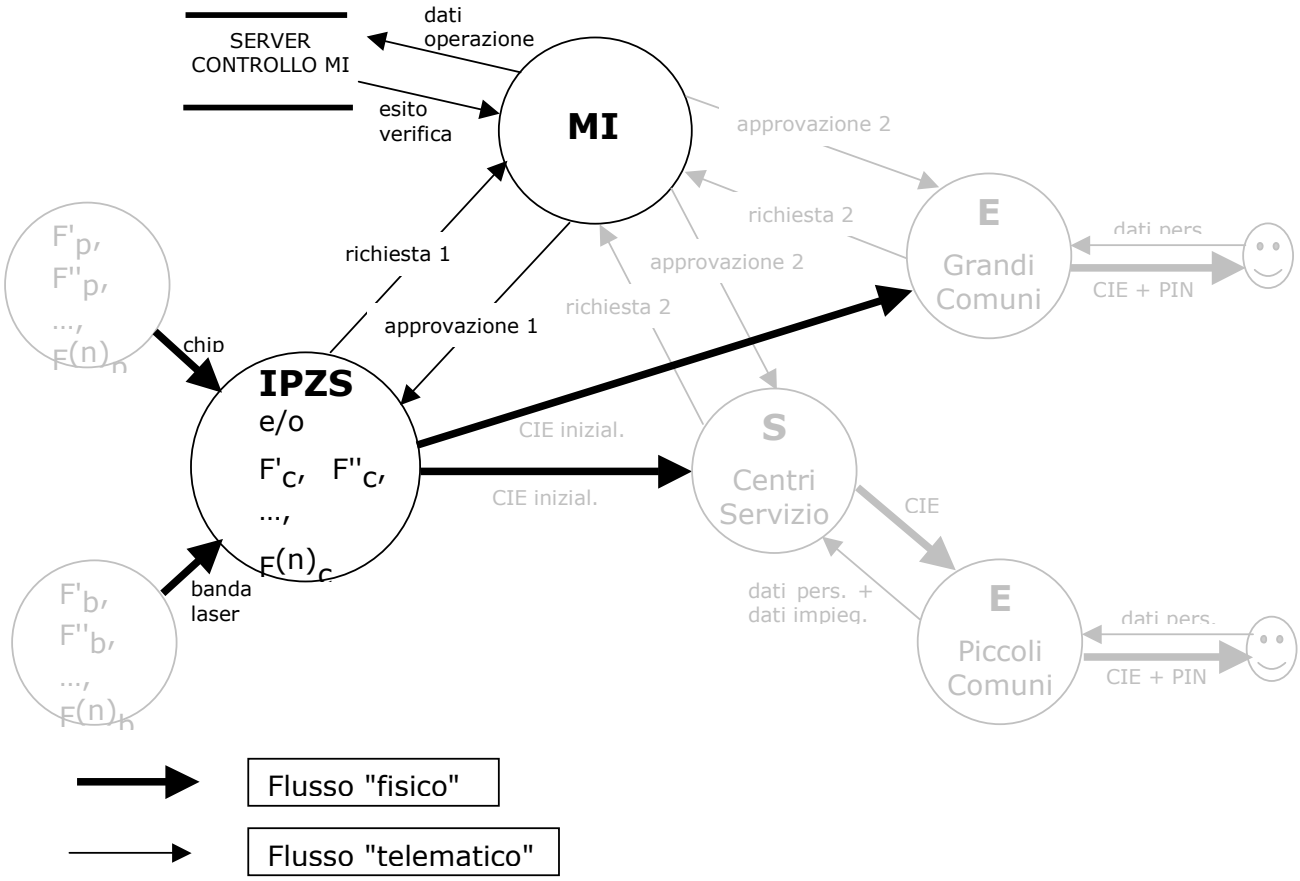


Fig. 9.2.2-A

L'associazione ID_Carta/Comune è contenuta nel flusso di richiesta (in figura "richiesta 1") che IPZS invia a MI. Tanto la richiesta, che la relativa approvazione di MI (in figura "approvazione 1") sono controfirmate dall'ente originatore dei dati (IPZS o MI), determinandone la responsabilità. Si veda anche il paragrafo [3.2].

9.3 Personalizzazione ed emissione delle carte

La formazione e rilascio delle carte è condotta direttamente dai comuni o indirettamente attraverso centri di servizio. Nel seguito faremo riferimento ai soli comuni (E), non essendo sostanzialmente differente la procedura per quanto riguarda i centri di servizio.

Vediamo nel dettaglio le operazioni eseguite:

#	Operazione	Note
1	Ricezione dei documenti in bianco, nel numero richiesto a IPZS.	
2	Raccolta dei dati personali del titolare, da effettuarsi direttamente allo sportello (anche per mezzo di videocamera digitale).	
3	Generazione della coppia di chiavi K_{pri} e K_{pub} necessarie per garantire l'autenticazione in rete della carta e generazione del relativo PIN utente.	La generazione della coppia di chiavi deve avvenire internamente al microcircuito.
4	Creazione di una richiesta di certificato in formato standard PKCS#10, contenente ID_Carta e la chiave pubblica K_{pub} della carta. Tutti i dati raccolti durante la personalizzazione della carta vanno a far parte di un'estensione del certificato (sotto forma di hash), non obbligatoria, appositamente generata. La richiesta ingloba la "firma" del proprio contenuto eseguita con la chiave privata K_{pri} della carta.	
5	Creazione del record dati e del record di controllo relativi all'operazione di emissione. Il record dati contiene essenzialmente la richiesta di certificato che deve essere elaborata dal server certificatore di MI, ID_Carta ed i dati identificativi del microcircuito (Dati_processore) e/o della banda ottica (Dati_banda_ottica) necessari per i confronti.	MI, dopo aver estratto dalla richiesta di certificato Kpub, esegue un controllo sulla sua base dati al fine di verificare che questa non sia identica ad una chiave pubblica già certificata. Ciò permette di prevenire possibili "collisioni". L'utilizzo di Dati_banda_ottica riduce esponenzialmente il rischio di collisioni. In caso sia rilevata una collisione,

		MI non concede l'approvazione, ritornando all'ente emettitore un opportuno codice di errore. Il procedimento viene quindi rieseguito a partire dal passo 3 (ossia viene generata una nuova coppia di chiavi).
6	Invio della richiesta (Rd + Rc) a MI per via telematica.	
7	Ricezione di Rc completato con i dati di MI. Il record di controllo contiene anche C_Carta.	In caso di collisione, C_Carta viene sostituito dall'indicazione del problema che non ha consentito l'approvazione dell'operazione.
8	Ricezione del PIN P1, cifrato nella fase precedente con la chiave pubblica del comune che ha effettuato la richiesta. L'algoritmo di cifratura utilizzato deve essere conforme allo standard PKCS#1 RSA Encryption Standard.	P1 era stato precedentemente cifrato con la chiave pubblica del comune di destinazione, al fine di assicurare la riservatezza durante la trasmissione.
9	Decifratura del PIN P1 per mezzo della chiave privata dell'ente E. L'algoritmo di decifratura utilizzato deve essere conforme allo standard PKCS#1 RSA Encryption Standard	
10	Memorizzazione di C_Carta e della fotografia del titolare nella directory DF2, blocco della directory e distruzione del PIN P1.	La directory ed i dati personali ivi memorizzati vengono resi non modificabili.
11	Impostazione delle strutture dati relative ai servizi qualificati.	Il comune usa per questa operazione un server a ciò abilitato, che può "firmare" la richiesta di autenticazione attraverso la conoscenza di $INST_{pri.}$ L'algoritmo di cifratura utilizzato deve essere conforme allo standard PKCS#1 RSA Encryption Standard
12	Stampa del PIN del titolare su busta protetta.	
13	Stampa dei dati personali sul supporto.	La stampante usata può eventualmente essere in grado di leggere il microprocessore e/o la banda ottica prima di stampare i dati al fine di verificarne la

		congruenza con quelli impostati per la stampa.
14	Consegna - in tempo reale - della CIE e del PIN all'interessato.	

La fig. 9.3-A illustra graficamente le attività di questa fase.

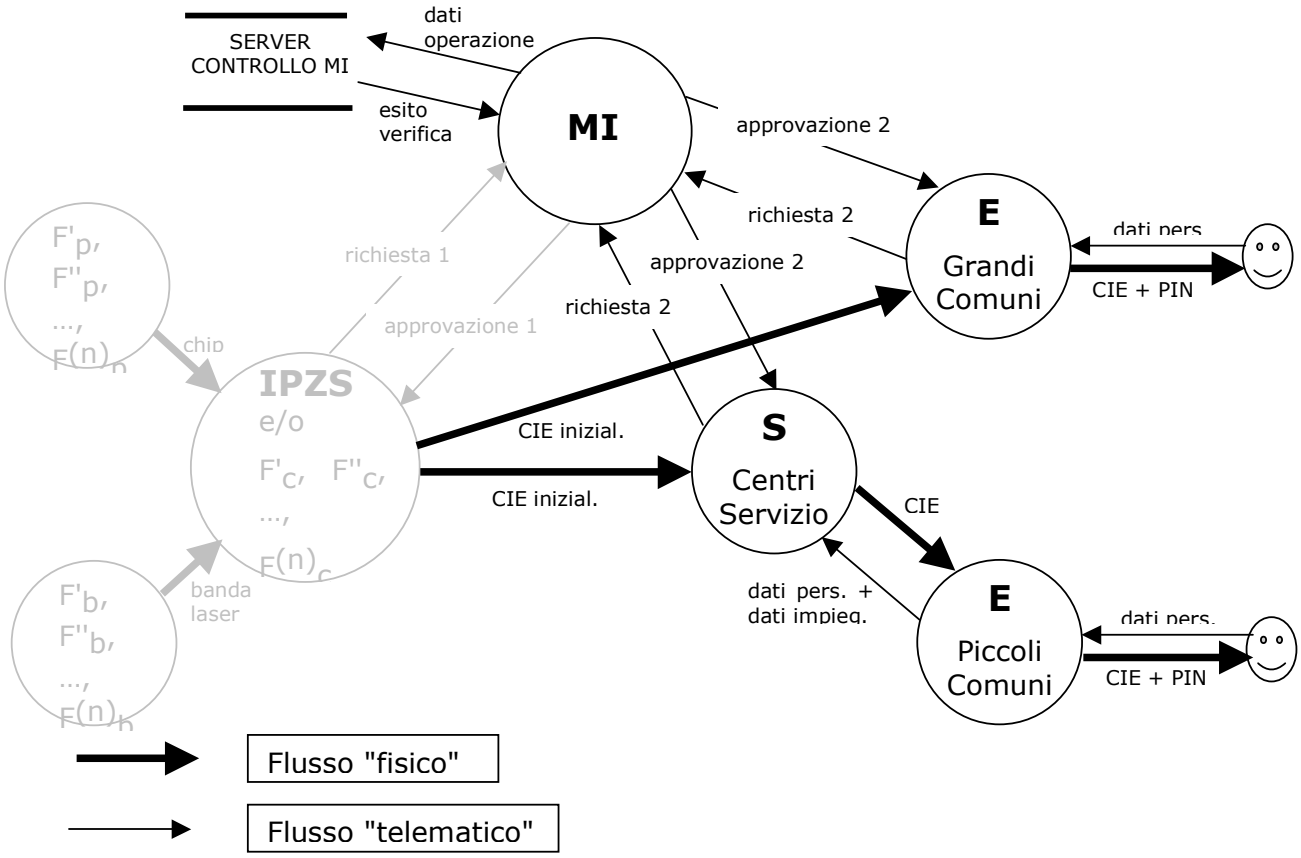


Fig. 9.3-A

9.4 Verifica e controllo

Il controllo e la verifica di tutte le fasi della produzione e dell'emissione è condotto presso MI, che mantiene ed aggiorna un database delle carte dove è sempre sotto controllo lo stato attuale delle carte (da produrre, inizializzate, rilasciate, scadute, rifiutate, interdette). Tutti gli enti coinvolti nelle varie fasi del processo devono disporre di una connessione telematica con MI, al fine di trasmettere le richieste di autorizzazione e ricevere la relativa autorizzazione da parte di MI.