

carta di identità elettronica -CIE-

Metodo di lavoro ed esperienze coinvolte

- ✧ Costituzione di un gruppo di lavoro Aipa, Assinform, Assintel, Anasin (delibera n.8 del 19 marzo 1999) per gli aspetti tecnico-operativi;
- ✧ coinvolgimento del Ministero dell'Interno, del Ministero della Sanità e dei comuni per l'analisi dei requisiti della carta;
- ✧ coinvolgimento dell'Istituto Poligrafico dello Stato per gli aspetti relativi alla produzione ed alla sicurezza del supporto fisico;
- ✧ supporto specialistico dei fornitori della banda laser.

La normativa di riferimento

- **La legge n.127 del 15 maggio 1997**

Recante misure per lo snellimento dell'attività amministrativa e dei procedimenti di decisione e di controllo

all' art. 2 comma 10

introduce la carta di identità elettronica con la duplice valenza di:

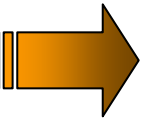
documento di
riconoscimento

documento per la semplificazione
amministrativa e l'erogazione dei servizi al
cittadino

- **Il D.P.C.M. 437 del 22 ottobre 1999**

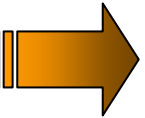
- **Il R.D. 18.6.31, n. 773 di approvazione del T.U.L.P.S.**

principi ispiratori



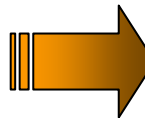
la sicurezza:

- del dispositivo fisico,
- del circuito di emissione, formazione e rilascio,
- del processo di riconoscimento del titolare "a vista" ed in



la ^{rete} carta servizi:

- possibilità di fruire i servizi a carattere nazionale (sanità, finanze, certificato elettorale...)
- possibilità di fruire dei servizi a livello locale (trasporti, musei, sportello unico, ...)



l'interoperabilità:

- su tutto il territorio nazionale (e non solo ...)
- indipendenza dai fornitori

tipologie di identificazione



**scelta
progettuale**

microprocessore

consente il riconoscimento in rete e la fruizione dei servizi

banda ottica a lettura laser - worm

consente la non contraffazione del documento per il riconoscimento a *vista* del titolare

La sicurezza dei componenti della CIE

il supporto plastico:

- in policarbonato; ottima resistenza passiva nel tempo (deve durare almeno 5 anni),
- evidenza dei danni ad esso arrecati,
- inalterabilità delle informazioni stampate e registrate (uso di inchiostri speciali ed embedded ologram);

la banda laser:

- resistenza agenti esterni (magnetismo, calore, ...)
- grande capacità di memoria,
- "stampa" di ologrammi in fase di masterizzazione,
- inalterabilità (è un supporto Worm),
- riscontro "a vista " tra i dati stampati e quelli registrati;

il microprocessore:

- utilizzo di coprocessore crittografico,
- strutturazione in directory accessibili tramite PIN/autorizzazione.

Fp = Fornitori di microprocessore

sono le aziende produttrici dei microprocessori

- durante la produzione memorizzano, in area non riscrivibile, un numero seriale = ID_fornitore + data produzione + lotto fornitura;
- consegnano a IPZS distinta cartacea ed elettronica contenente i dettagli dei numeri seriali.

Fb = Fornitori di banda laser

sono le aziende produttrici delle bande ottiche a lettura laser

- durante la produzione memorizzano, un numero seriale = ID_fornitore + data produzione + lotto fornitura;
- consegnano a IPZS distinta cartacea ed elettronica contenente i dettagli dei numeri seriali.

IPZS = Istituto Poligrafico dello Stato

**responsabile manifattura delle carte ed inizializzazioni
componenti informatiche**

- **effettua l'assemblaggio dei componenti elettronici sul supporto plastico;**
- **genera le strutture dati sui componenti elettronici;**
- **memorizza sui supporti informatici il numero univoco su scala nazionale (ID_Carta) fornitogli dal Ministero dell'Interno;**
- **stampa gli elementi grafici "costanti" (logo, sfondo, embedded ologram su banda ottica, ...);**
- **si tiene in costante allineamento con il Ministero dell'Interno per la gestione di ID_Carta.**

SSCE = Sistema di sicurezza del circuito di emissione - Ministero dell'Interno dipartimento Pubblica Sicurezza -

- a fini di sicurezza, realizza, gestisce e mantiene la struttura informatica a supporto del circuito di emissione;
- certifica ogni operazione e ne tiene traccia;
- consente alle questure di accedere ai documenti conservati in forma cifrata presso il Sistema.

E = Emittitore = Comune

- reperisce i dati anagrafici del titolare;
- si mantiene in costante allineamento con SSCE;
- stampa e rilascia la CIE al titolare.

S = Centro servizi

- reperisce le richieste dei comuni;
- si mantiene in costante allineamento con SSCE;
- stampa la CIE;
- spedisce la CIE al Comune richiedente.

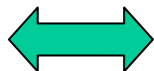
SAIA = Sistema di accesso ed interscambio anagrafico

Struttura dati della banda ottica a lettura laser

Le informazioni, ai fini della sicurezza e della tracciabilità, vengono registrate in modalità LOG sequenziale, quindi con l'evidenza del tipo di operazione avvenuta, di chi ha effettuato la richiesta e di chi ha autorizzato la stessa.

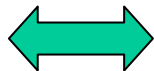
Record dati = informazioni del titolare della carta e dei servizi installati

record dati richiesta 1
segmento IPZS o E



...

record dati richiesta n



+ Record controllo = informazioni relative alle richieste di autorizzazione ed alle autorizzazioni (chi, dove, quando)

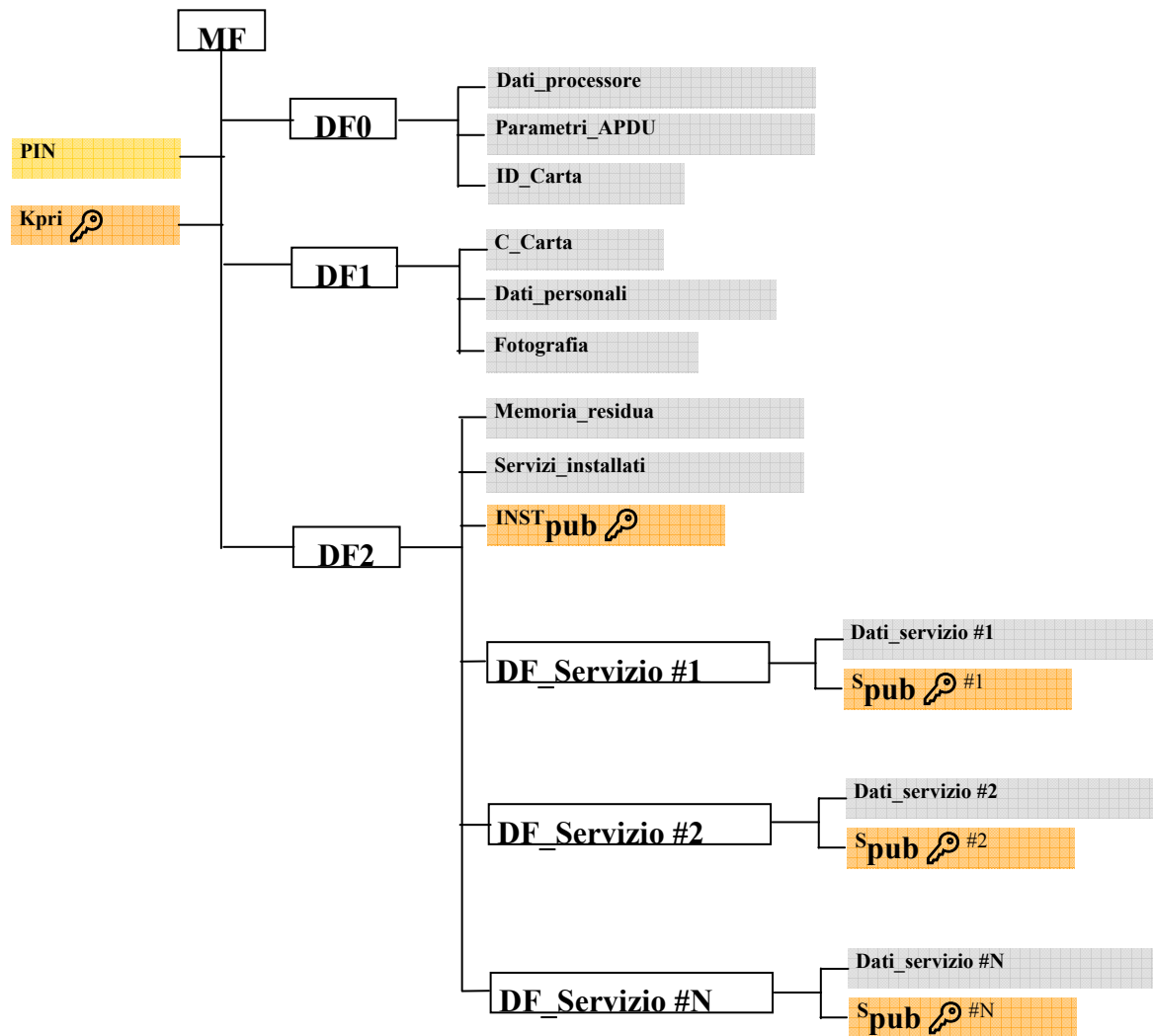
record di controllo richiesta 1	
segmento IPZS o E	segmento SSCE

...

record di controllo richiesta n

- ☞ In accordo con gli standard internazionali (rif. ISO 7816) la "maschera" del chip è una struttura "a cipolla" costituita da un Master file (MF) con funzionalità di root directory, da Dedicated file (DF) con funzionalità di directory "specializzate" a contenere informazioni omogenee tra di loro e da Elementary file (EF) contenenti le informazioni vere e proprie.
- ☞ Il microprocessore è provvisto poi di un motore crittografico interno (cripto-engine) utilizzato per autogenerare all'interno della carta, la coppia di chiavi privata e pubblica della carta (Kpri e Kpub) da utilizzare per l'utilizzo della carta come carta servizi.
- ☞ Kpri è invisibile all'esterno e viene utilizzata per tutte le operazioni di autenticazione in rete.
- ☞ Kpub, insieme al numero univoco identificativo della carta ed insieme al "bollo elettronico" del SSCE del Ministero dell'Interno, costituisce il certificato della carta (C_Carta) che garantisce, per tutte le operazioni che lo richiedono, il legame tra il microprocessore della carta ed il supporto fisico.

Struttura dati del microprocessore ... 2/3



Legenda dei principali Elementary file

PIN = numero personale rilasciato dal comune al titolare. È richiesto per usare la chiave privata della carta (Kpri) per tutte le operazioni di identificazione in rete.

INSTpub = chiave pubblica del servizio di installazione delle strutture dati relative ai servizi telematici a carattere nazionale da installare. La responsabilità di installazione della carta servizi è del comune.

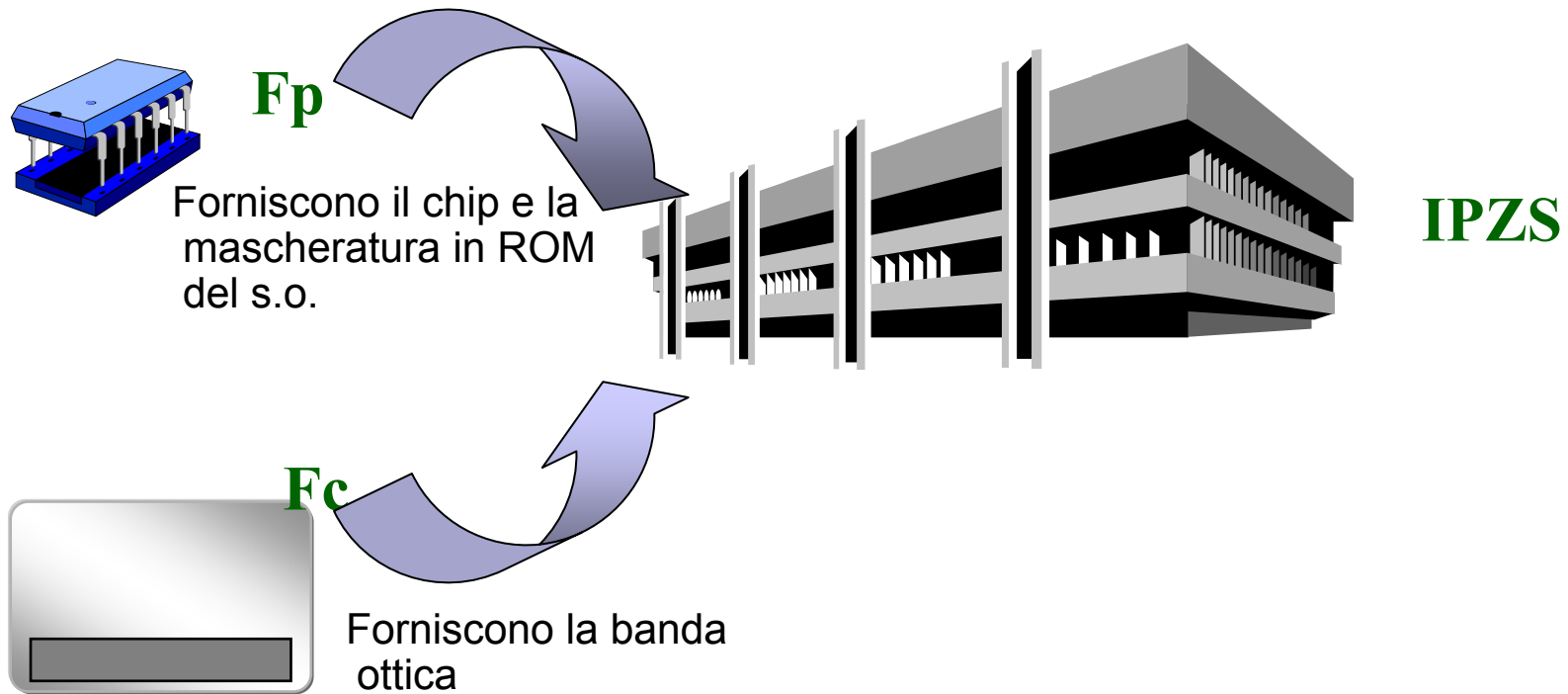
Parametri_APDU = riporta, ai fini dell'interoperabilità delle applicazioni, le caratteristiche dei comandi elementari (APDU) utilizzati dal s.o. del microprocessore.

ID_carta = numero progressivo, univoco a livello nazionale, che identifica la carta.

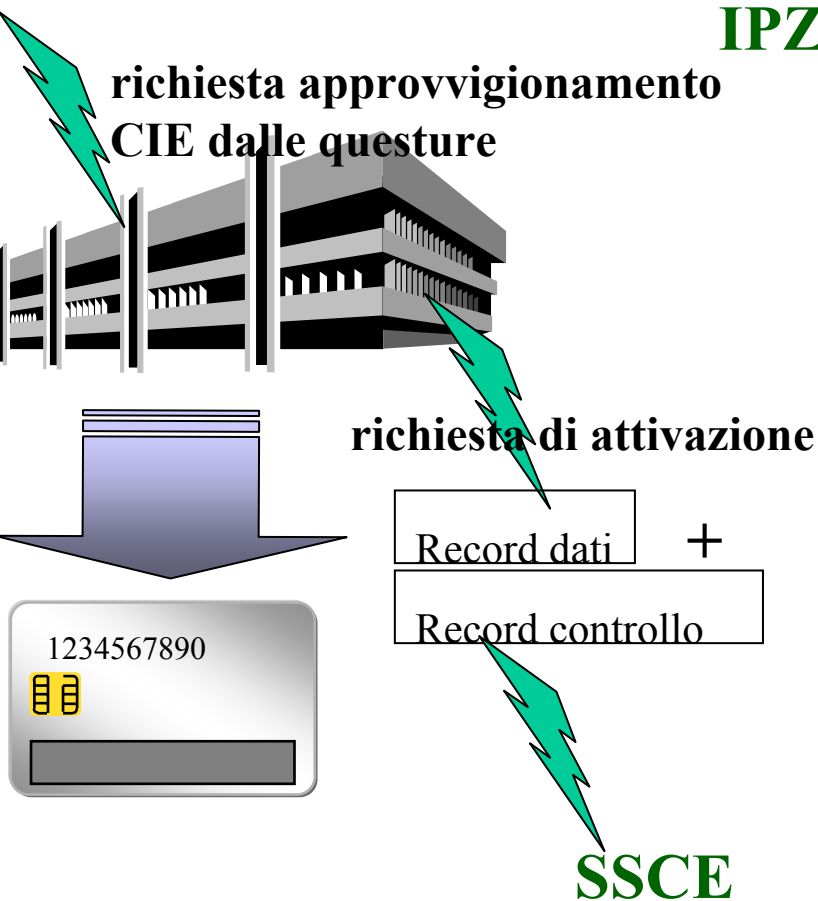
C_Carta = certificato rilasciato dal SSCE = ID_carta + Kpub + bollo elettronico di SSCE.

S_pub = eventuale chiave pubblica del servizio a carattere nazionale da installare sulla carta.

1 - Produzione di banda laser e microprocessore

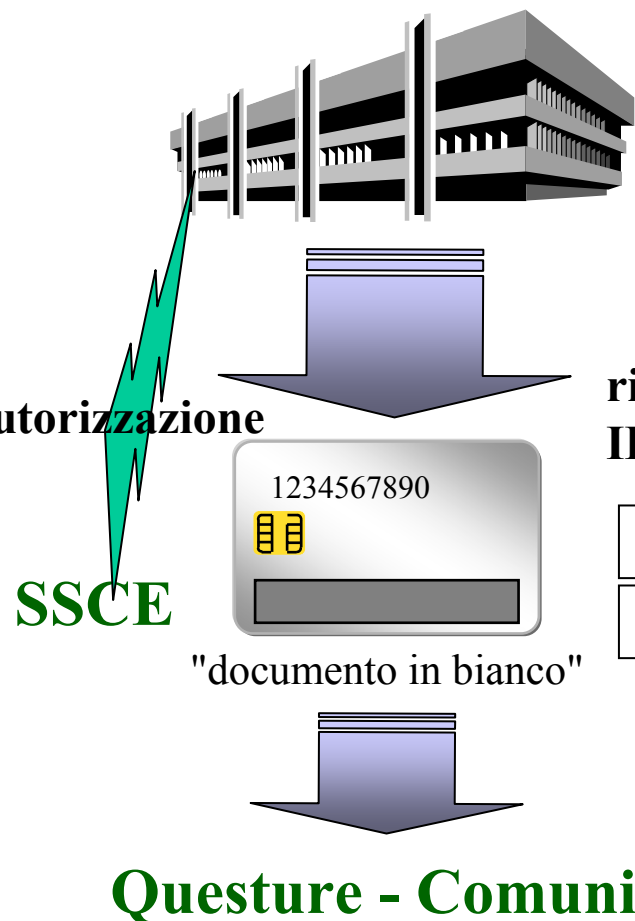


2 - Produzione della CIE e sua inizializzazione



- Embedding del chip sul supporto che contiene la banda ottica;
- generazione della struttura dati interna del microprocessore e della banda ottica (MF, DF0, ...);
- scrittura degli Elementary file "ID_carta", "Dati_processore" e "Parametri APDU" del microprocessore e "Dati_banda_optica" della banda ottica;
- impostazione delle condizioni di accesso a tali file;
- scrittura ed invio del Record dati e del Record di controllo a SSCE del Ministero;
- stampa dello sfondo, del logo, di ID_Carta e degli elementi costanti sul supporto fisico;
- embedding ologram sulla banda ottica;
- stoccaggio della CIE.

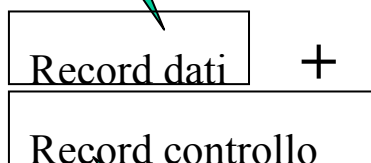
3 - Attivazione della CIE



IPZS

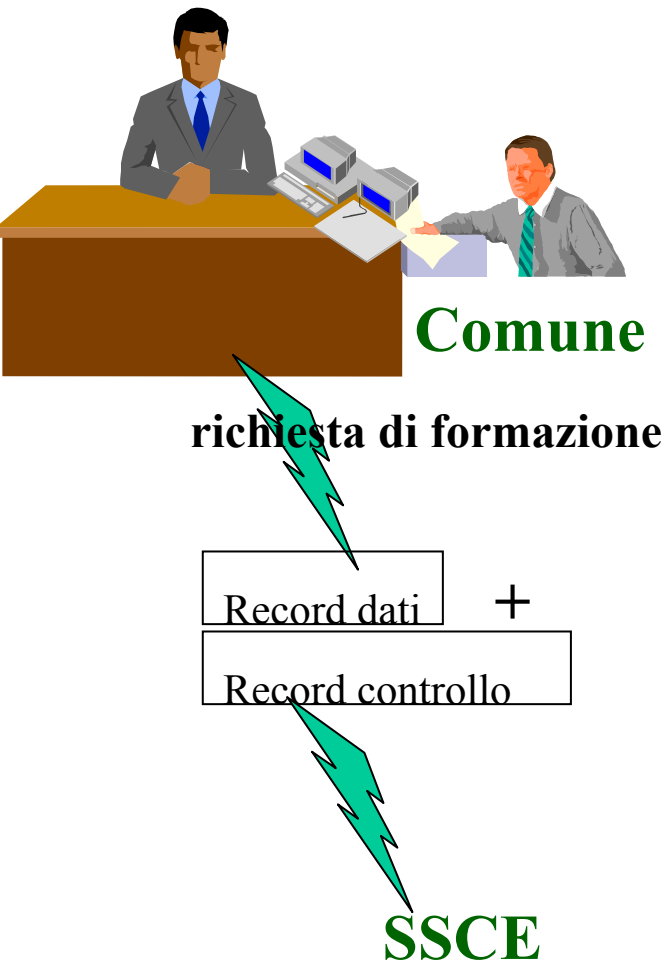
- Ricezione dell'autorizzazione;
- registrazione dell'autorizzazione;
- associazione CIE / Comune richiedente;
- trasmissione a SSCE della associazione ID_Carta / Comune di assegnazione;
- invio della CIE alle Questure (Comuni) richiedenti.

richiesta di abbinamento
ID_Carta / Questura



SSCE

4 - Formazione della CIE: raccolta dati anagrafici



- Raccoglie i dati personali del titolare;
- genera la coppia K_{rpi} e K_{pub} ed il PIN della CIE;
- genera una richiesta di bollo elettronico PKCS#10 ($ID_Carta + K_{pub} CIE + hash$ dei dati personali);
- genera Record dati e Record controllo relativi alla richiesta di certificato;
- invio richiesta a SSCE;
- attesa risposta da SSCE.

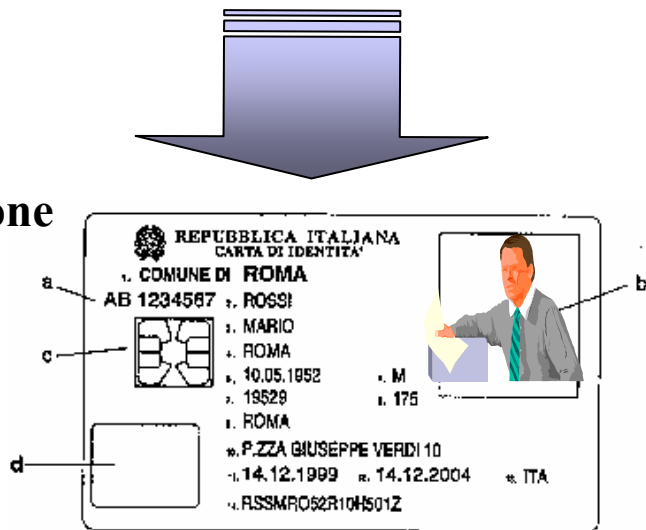
5 - Formazione della CIE: consegna carta al titolare



- Ricezione da SSCE del bollo elettronico della CIE (C_Carta);
- memorizzazione di C_Carta e della fotografia del titolare su microprocessore e banda ottica;
- impostazione dei servizi a carattere nazionale;
- impostazione dei servizi a carattere locale;
- stampa dei dati anagrafici sulla CIE;
- stampa del PIN da consegnare al titolare.

autorizzazione

SSCE



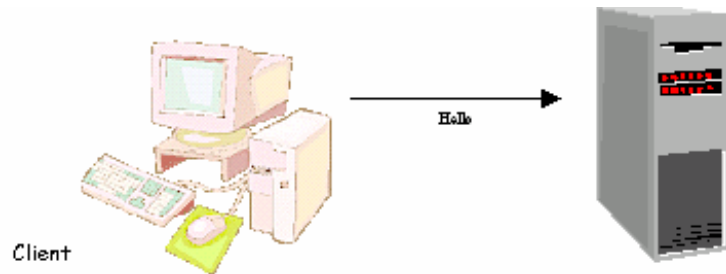
I servizi previsti sono di due tipi:

- **standard: che richiedono la sola identificazione in rete della carta e del suo titolare;**
- **qualificati: che richiedono un aggiornamento dei dati memorizzati nel microprocessore**

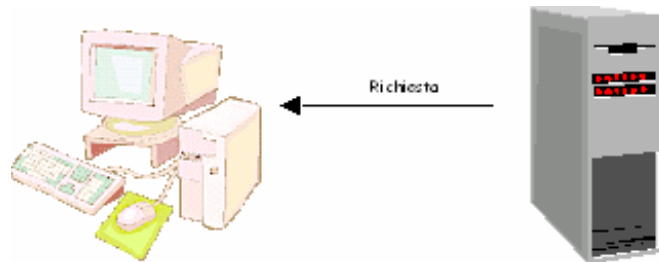
La differenza risiede nella necessità, nel caso dei servizi qualificati, di stabilire un canale di comunicazione sicuro dal server erogatore del servizio e il microcircuito e non dal server all'applicazione client, perché quest'ultima potrebbe essere sfruttata per operare un attacco.

Il mezzo utilizzato per cifrare il canale prende il nome di *secure messaging* e le chiavi che consentono l'aggiornamento della EPROM del microprocessore devono essere inserite nella struttura dati in fase di installazione del servizio da parte del Comune.

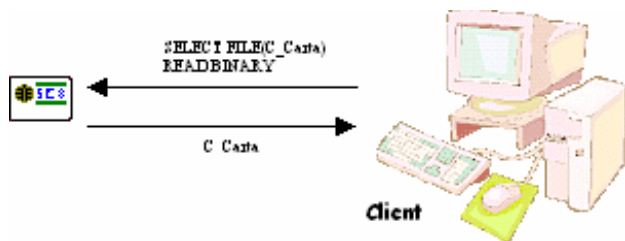
L'autenticazione in rete



Il client richiede la connessione con il server del servizio



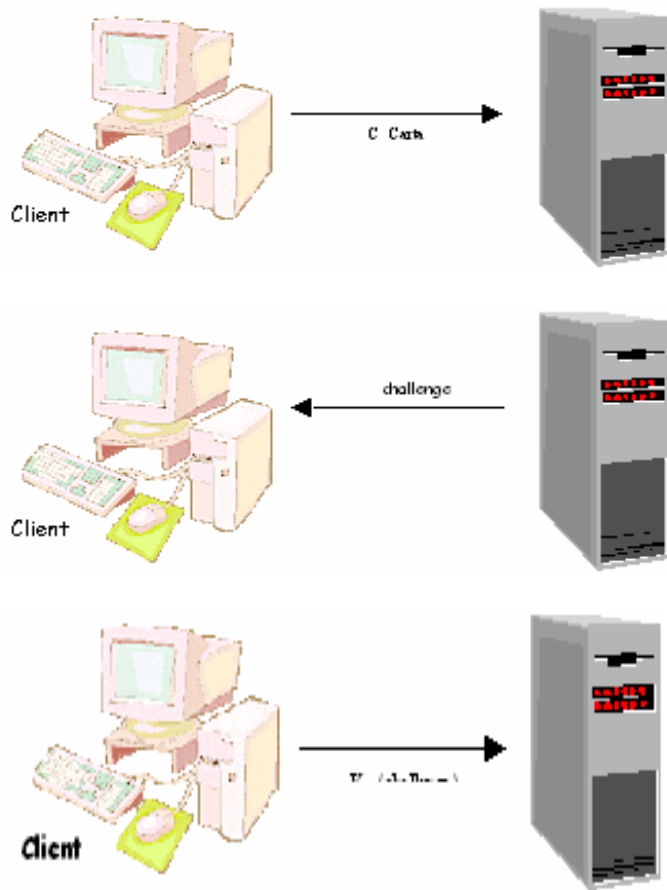
Il server chiede al client il certificato della carta (C_Carta)



Il client chiede alla CIE C_Carta attraverso i comandi standard:

- select binary
- read binary

L'autenticazione in rete



Il client fornisce al server C_Carta

Il server verifica la validità di C_Carta mediante K_{pub_SSCE} , estrae K_{pub_CIE} e genera un challenge che invia al client

Il client seleziona K_{pri_CIE} ed esegue la cifratura del challenge: $K_{pri_CIE}(challenge)$ inviandolo al server.

Il server esegue $K_{pub_CIE}(K_{pri_CIE}(challenge))$ e confronta il challenge decrittato con quello inviato. Se l'esito è OK la carta è valida.

La fase di sperimentazione

Obiettivi:

- verificare le soluzioni tecnico organizzative individuate,
- patrimonializzare le esperienze "di campo",
- migliorare e/o ottimizzare l'architettura.

Le modalità di partecipazione

Alla fase di sperimentazione potranno partecipare tutti i comuni che presenteranno un progetto al Ministero dell'Interno secondo le modalità ed i termini stabiliti dalle regole tecniche del 21 luglio 2000

Il Ministero dell'interno trasmette copia del progetto di sperimentazione al Comitato di monitoraggio previsto dall' art. 10 del DPCM 437.

Alcuni numeri:

- 100.000 CIE per la fine dell'anno,
- 10 milioni /anno a regime

La fase di sperimentazione

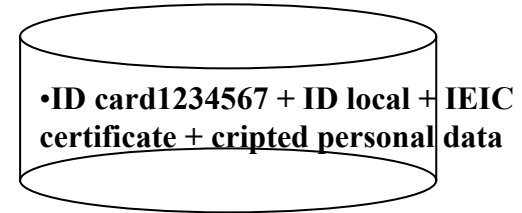
La dotazione minima dei comuni:

- ◆ PC, con il sw distribuito da SSCE,
- ◆ collegamento a RUPA o via Internet,
- ◆ scanner, telecamera e lettore impronta digitale,
- ◆ stampante a trasferimento termico,
- ◆ laminatrice per l'applicazione a caldo di foglio trasparente protettivo,
- ◆ programmatore di microcircuito
- ◆ programmatore di banda ottica.

Alcune considerazioni

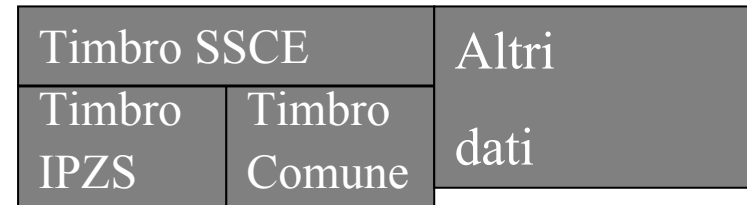
SSCE

- Non è il "Grande Fratello",
- è simile al caveau di una banca dove ognuno in funzione della sua competenza (chiave privata) può accedere alle informazioni di pertinenza,
- nessuno può accedere a tutte le informazioni registrate.



Laser card

- Permette di avere una carta valida solo quando l'ultimo "timbro del comune è presente



Microchip

- Permette di accedere ai dati della carta in funzione dei profili di autorizzazione

