Italian Electronic Identity Card
- principle and architecture -

Mario Gentili

Autorità per l'informatica nella Pubblica Amministrazione
via Isonzo, 21/b
Rome
Italy
mario.gentili@aipa.it

Abstract

The plan for "e-Government", and the need to facilitate interactions between citizen and Public Administration, make find in the electronic identity card - **EIC** - one of the most important means to access network services in a secure way. There are five inspiring principles:

- *security* for the complete lifecycle of the card from production of the physical support to initialisation, emission and its use as a service card. Security must be addressed the point of view of both police and citizen;
- *network service access* to bring Public Administration (at both central and local level) nearer to the citizen;
- *interoperability* ie compatibility of national network services by use of the same card standard open technological architecture international standard compliance and vendor independence nationwide;
- *virtual centralisation* for authorisation and logging operations during production and emission processes;
- *full independence* of local authorities (which release the EIC) to install their local services.

1 Layout and environment

The EIC is a~~n~~ *hybrid* smart card with two different technologies aboard: a 16K microchip and a laser band. Due to the restricted printable area of the card, all data are written without labels. This approach allows a multilingual solution where needed, for example, in the frontier regions such as the Italian/French, Italian/Slovenian and Italian/German borders. On the first side are the name of the authority releasing the card, ~~the~~ personal data of the cardholder (surname, name, place and date of birth, photo and sex), a unique card ID number and the ICAO band. On the other side are the cardholder's address and fiscal code, the card's validity period and the two electronic devices: the chip and the laser band. On the laser band are replicated, in embedded hologram, personal data and images of the citizen's fingerprint (not mandatory) and holograph signature.

figure 1

1.1 Why two technologies ?

The use of two different technologies is necessary because the EIC acts in two different ways in the same physical support. The first is as the real identity card, with its security constraints and associated / other problems. The laser band impedes counterfeiting in three ways:

- use of a sophisticated writing technique to represent personal data, signature and fingerprint,
- logging of the whole emission process so that the card is validated only when the last step is authorised and written upon it~~,~~
- the possibility of using *stamps*.

The second way in which the card is used is as a service~~s~~ card. The microchip, with a cryptographic engine on

Proceedings of the 27th VLDB Conference,
Roma, Italy, 2001

board, ensures the right security in terms of network identification and authentication based on symmetric and asymmetric cryptography.

1.2 Regulatory framework

The EIC was described by Italian Law 127/1997 and implemented by Labour Decree 437/1999. The technical rules were published in the summer of 2000.

1.3 Requirement

The legal framework and its constraints, depending on police regulation, are at the base of EIC logical architecture and hence affects the choice of the implementation method. Among these constraints are:

- the need to have a unique central index for the Italian Population Registration Centre (Indice Nazionale Anagrafico - INA);
- the alignment of the fiscal code with the Ministry of Finance, which is the only administration releasing the fiscal code used for the citizen's financial interactions;
- the existence of 8104 independent local authorities, each with its own local services to include on the microchip and with the need to release the EIC on demand;
- the framework of the e-Government plan;
- a sophisticated physical layout to increase the security level of the actual paper model.

The following figure gives a logical representation of the different bodies and framework involved in the process:

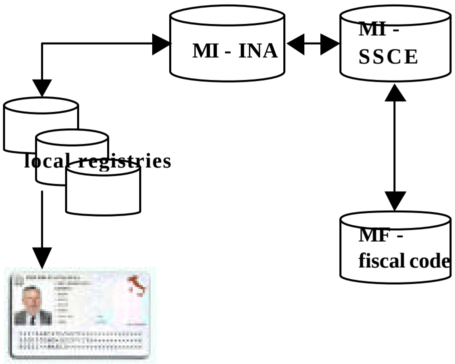

figure 2

2 Interoperability considerations

All EIC components are based on ISO standards.

The physical support is an ISO 7816-1, ISO 7816-2 and ISO/ID-001 compliant plastic card.

For the network authentication process an asymmetrical RSA algorithm is used: the format of the data is PKCS#1 compliant. The used certificate is X509 v3 compliant and the data envelope is PKCS#7 signed.

The APDU for microchip interactions are ISO 7816-3, 7816-4 and 7816-8 compliant. The APDU library is dynamically compiled in different environments.

The laser band formatting rules and data representation are ISO 11964 annex B compliant.

3 Organisations involved

The EIC organisational infrastructure is very complex; however, a straightforward synergy between the private and public sectors (both local and central institutions) is foreseen. Among these:

- **microchip** manufacturers who supply microchips to the Italian mint (IPZS). During the production phase (see below the microchip is given a serial code consisting of a progressive number, a progressive stock number and the production date. The code is unique for each microchip and a list giving the match between each microchip and its assigned code follows each shipment;
- **laser band** manufacturers who supply IPZS with laser bands. As with microchips, each laser band is given a unique code which is later supplied to the customer;
- **IPZS,** which assembles the different technologies upon the plastic card and encodes, in both the chip and the laser band, the unique national ID number supplied by Ministry of the Interior;
- **Ministry of the Interior - Emission Circuit Security System - SSCE**. This is the security core of the project. SSCE is the Public Key Infrastructure for the EIC certificate. It receives card requests from local authorities and provides authorisation after normal checks such as: valid means of identification, duplicate request of the same citizen in different regions, access to CRL. All data are encrypted with the private key of the cardholder, who has exclusive access. From the storage point of view, SSCE resembles a bank safe: the security key is the private key of the owner of the data;
- **Ministry of the Interior - Access System for Population Registration Centre - SAIA** is the information system of the local authorities for ~~the~~ logging and inter-database integration of each addition and update of personal data;
- **Local authorities -** are responsible for issuing EIC cards.

4 Emission process

4.1 Production

The production phase involves three groups: the microchip and laser band manufacturers and IPZS. The manufacturers supply their products to the Italian mint, which embeds the chip and laser band into the plastic support and then stores the card until needed.

4.2 Initialisation

On receipt of request from the local authority for a shipment of smart cards, IPZS:

- formats the microchip (according ~~with~~ to the chip mask scheme) and laser band,
- installs microchip security accesses and privileges,
- writes the card ID (previously received from SSCE) on the chip, laser band and physical support, and prints standardised (Italian logo, etc) and security elements,
- submits an authorisation request to SSCE and waits for the final "ready to go".

4.3 Activation

When SSCE provides authorisation, IPZS activates the cards and adds the ministerial authorisations to its database, writes the authorisation on the laser band, assigns a stock of the cards (from ID number … to ID number …) to the local authorities, and sends these associations to SSCE, which uses them for formal checking of the ID card and the authority to which it is assigned.

The card is now called the *white document*. This cannot be manipulated, as the information contained in the microchip is the same as that written upon the laser band and all data are validated by SSCE digital signature.

4.4 Emission

The emission phase is realised by the local authorities. When an authority has insufficient resources for this process, it may delegate the operative functions to a Service Centre.

The authority obtains personal data by using a camera or scanner for the photo, a scanner for the signature, a special scanner for the fingerprint and the software provisioned by SSCE for generation of the EIC keys and transmission of a PKCS#10 certificate request to SSCE.

After the formal checks, SSCE issues the certificate, signs it with its private key and sends authorisation to the local authority.

At this point the authority can complete the process and:

- prints personal data and the photo upon the physical support,
- writes the authorisation upon the laser band,
- memorises the EIC certificate upon both microchip and laser band,
- generates the PIN/PUK and prints them in a special sheet contained in a closed envelope,
- enables the national services in the microchip nationally dedicated directories,
- adds and enables local services in the microchip locally dedicated directories,
- issues, in real time, the EIC to the citizen.

When provided by a Service Centre , the process is asynchronous and the requester must return to the local authority about a week later to receive the EIC.

5 EIC architecture

5.1 Microchip

The microchip's physical structure is a typical file system with a Master File, three Dedicated Files and three Elementary Files.

The Master File, that is the root directory of the file system, is generated and written by IPZS and the access mode is *read only*. The three Dedicated Files are under the initial control of IPZS but subsequent updates are performed by the local authorities. DF0 contains the initialisation data as the SSCE-assigned EIC ID number and microprocessor identification data. DF1 contains the X509 certificate released by SSCE and the personnel data of the citizen. The final Dedicated File - DF2 - contains information about the installed services (at national or local level) and the public keys of the institution providing the service. The crypto-engine is used to generate the two keys used for the network strong authentication of the card based on asymmetrical cryptography.

5.2 Cryptographic elements

The cryptographic components are used for the network strong authentication, the signature operations of the card, and the authentication and secure messaging process during the installation phase of the qualified national services. The private key length is 1024, and the algorithm used for service installation is 3-DES.

The EIC X509 v3 certificate is released by SSCE, which acts as both Registration and Certification Authority. The certificate, called C_Carta, is generated during the emission phase after request from a local authority and installed in an Elementary File with read-only access.

C_Carta structure is as follows:

Version ::= X509v3;
Serial number ::= Certificate serial number;
Issuer ::= Sub CA Distinguished Name;
Start Date ::= Date of emission;
End Date ::= Date of emission + 5 years;
Subject ::= CIE Distinguished Name
Public Key ::= 1024 bit RSA public key.

The extensions are:

Key Usage ::= Non repudiation;
Extended Key Usage ::= Client Authentication;
CRL Distribution Point ::= CRL LDAP URL;
Personal ID ::= CIE Public Key Hash;
CA ID ::= CA Public Key Hash.

It should be noted that the Distinguished Name has the following additional structure:

Country ::= IT;
Organisation Unit ::= Ministry of ~~Internal~~ the Interior;
Common Name ::= ID_Carta + hash (personal data);

which shows that the digital certificate does not identify the EIC cardholder (the citizen), but the EIC itself. In this case the authentication process is not able to identify the user, but the EIC can be used as a valid document.

5.3 Laser Band

The laser band has two cross-referencing areas,: the **data area** containing the data needed for an authorisation request to SSCE and the **control area** containing the response to the request with the necessary *stamps*. The control area is an incremental registry in which is written *who, where, when* and *why* has released an authorisation. Only when the last stamp is written on the laser band, is the EIC ~~is~~ a valid document (this allows immediate recognition of a false EID).

6 EIC as a service card

EIC allows access to several services which can be classified on the basis of interaction type and issuer administration. We can identify **standard, qualified**, **national** and **local** services.

Standard services do not modify or update ~~the EIC~~ information held on the EIC. These services use the EIC certificate, its private key and the citizen's personal data for the strong network authentication process. The **qualified** services are used for the update and insertion of data on the EIC. The qualified services' manager is the local authority, which uses the symmetric algorithm 3-DES for authentication of the installation services server and for secure messaging for the creation of the service data structure. In this case, the symmetric keys are stored or in a free access Elementary File (after encryption by the public key of the installation service server) or in Key Files used for network authentication and secure messaging. Each installation service server is able to access EIC, read Key Files and decode the EIC with its private key. Depending on qualified service topics, the installation service server can install symmetric or asymmetric keys for use during network authentication processes. **National services** are those provided by Public Administration. For each national service it is necessary to define the structure of its file system dedicated directory, its dimension in bytes, its security requirements, and the implementation method for secure messaging.

All this information is stored in the SSCE data base and is provided to the local authorities for service activation. No information ~~are~~ is needed for standard services using the EIC as a *cryptographic token*. **Local** services are provided by the local authorities. No constraints are imposed on the local administration: only in the case of qualified services must the local authority define the correct structure of the file system dedicated directory.

7 Authentication process

The EIC authentication process is provided with both SSLv3 protocol and challenge/response mechanism.

7.1 SSLv3 protocol

The use of SSLv3 protocol allows a secure connection with the web server providing the service and EIC and service server authenticity. The web service provides software functions for extracting the EIC certificate and, from this, the citizen's personal data to be checked against the application Access Control List. The transmission of personal data between card and service server is implemented by an SSL session. The EIC cardholder's data are extracted from the Elementary File *personal data* of the microchip file system (see ? 5), and the application calculates the hash function and matches the result with the Common Name certificate information.

The SSL protocol has the advantage of using the EIC with a browser without the need to install any other software client component, but, on the other hand, reduces server performance (due to the lack of connection of the open session).

7.2 Challenge/Response authentication

This authentication is based on the signature (response) of a random string (challenge) generated by the server and sent to the client. The server verifies the response using the EIC public key contained in the digital certificate and matches the result with the original challenge. This simple mechanism has the disadvantage of having no memory, hence for connectionless communication, it must be repeated each time the cardholder identity is necessary. The software used for the challenge/response implementation can be provided as a Plug-in applet or ActiveX. To allow an open market solution for the server component of the challenge/response mechanism, using PKI middleware, the format of the response must be PKCS#7 signed.

Mario Gentili April 27th, 2001