The Italian Electronic Identity Card: a short introduction

Franco Arcieri[1] Mario Ciclosi[2] Fabio Fioravanti[1,3] Enrico Nardelli[1]
Maurizio Talamo[1]

1. NESTOR - Multimedia services security and certification Laboratory, Univ. of Rome "Tor Vergata", Rome, Italy. http://www.nestor.uniroma2.it
2. Central Directorate for Demographic Services - Italian Ministry of Interior, Rome, Italy. http://www.mininterno.it
3. Dept. of Informatics - Univ. of L'Aquila, L'Aquila, Italy.

The italian Electronic Identity Card (EIC, for short) is a polycarbonate smart card equipped with a microchip (supporting cryptographic functions) and a laser band (featuring an embedded hologram). It contains personal (e.g. name, surname, date of birth, ...) and biometric data (photo and fingerprint) of a citizen.

The EIC is an identity document which, according to Italian Laws, is fully equivalent to the paper based ID card and can serve two different purposes: (*i*) it can be used as a traditional paper based ID-card, and (*ii*) can be used as an authentication credential, allowing access to network enabled government services. For example, citizens could use their EIC for accessing a Municipality's web site allowing them to perform operations like generation of self-certified documents, online tax payment, access to administrative databases, online applications and many other. Any public administration or agency which wants to give access to online services to citizens using the EIC, must register at the Ministry of the Interior. In this way, it is possible to guard citizens' rights as well as those of the service provider, as needed in a digital government system.

The Head of Department of Internal and Territorial Affairs of the Italian Ministry of Interior is responsible for the whole project, which is being developed as an institutional duty of the Central Directorate for Demographic Services of the Ministry of Interior, under its leadership and with its support. The NESTOR Laboratory of the University of Rome "Tor Vergata" is the technical coordinator of the project. Prof. Talamo of the University of Rome "Tor Vergata" is the supervisor of the project. The Italian mint (Istituto Poligrafico e Zecca dello Stato - IPZS), manufactures and initializes EICs. The security system of the EICs architecture (Sistema di Sicurezza del Circuito di Emissione - SSCE), generates keys used for activating EICs and is responsible for guaranteeing security during the formation of data and issue of EICs.

1 The scenario

In Italy, Municipalities are responsible for maintaining an archive of personal data of people having established residence within the Municipality's territory (APR = Anagrafe della Popolazione Residente). A person is inserted into a Municipality's APR when is born or establishes the residence in its territory. A person is deleted from a Municipality's APR when dies or establishes the residence outside its territory.

Issuing of Identity Card is a fully distributed process, based on data stored in APRs. A citizen gets it from the Municipality where he or she has the residence. The Ministry of Interior has the overall responsibility for the correct maintenance of Personal Data Registries in all Italian Municipalities. Also, since it is responsible for the public security, its police functions require a strict control on correctness of identity cards issuing process. In order to understand the dimensions of the problem, it is important to note the variety in size and complexity of APRs, since about 6000 of the 8102 Italian Municipalities have less then 5000 citizens, but 8 of the 20 Region chief towns have more than one million inhabitants.

To complete the scenario, please note that databases containing people's personal data are subject in Italy to a severe privacy legislation, forbidding to any public or private organization to set-up and maintain - even temporarily - databases storing personal facts about people unless this is done to discharge a precise obligation settled by law. Hence any approach based on establishing and using a central repository for people's personal data was unlawful - notwithstanding its technical feasibility, and any approach based on changing current legislation to centralize responsibility was bound to failure, given the understandable desire of various organizations to keep their autonomy and their responsibilities.

In moving from a paper-based ID card to an electronic one it was therefore required to define IT-based mechanisms ensuring to the highest degree all IT security functions (confidentiality, integrity, source and destination authentication, authorization, non-repudiation) in the interaction between Municipalities and the Ministry of Interior, and supporting the auditing of interactions. Any technical solution, moreover, had to be implementable even by small Municipalities without disrupting their work organization and their IT systems and strategies. Indeed, the real obstacle for the true uptake of whichever IT solution one could devise is not the financial cost, but is the organizational impact, both in the short term and in the long run.

2 The Architecture for the Italian Electronic Identity Card

In the first phase of deployment of the EIC, which was carried out in Italy during 2001, 100.000 ID cards manufactured and initialized by the italian mint (IPZS), were assigned to 83 Municipalities, in proportion to their respective population. Municipalities also received hardware and software tools needed for issuing ID cards to citizens, and have been given the opportunity of obtaining support by different means, including on site assistance, through a call center, and by accessing a dedicated Internet site. The feedback received from the organizations involved in the experimental phase represents an invaluable contribution to the success of the project, as no previous experience was available with projects having similar characteristics in terms of geographic distribution, inter-organizational issues and sensitivity of data, even in other countries. The experience gained during this experimental phase, helped in identifying the activities which must be carried out by the organizations involved, as well as technical and organizational requirements needed for guaranteeing correct operation of the overall architecture. The second phase of deployment of the Italian EIC architecture has already started. The target of this second phase is to provide the 56 Municipalities involved with 1.500.000 EICs, and to issue them by the end of year 2004 thus satisfying the local demand for ID cards.

We recall that, by Italian laws, Municipalities are the only organizations which are responsible for issuing EICs to citizens. In particular, they collect and prepare the personal and biometric data to be written on the EIC (manufactured and initialized by IPZS) and subsequently activate the EIC itself.

Currently, there exist two procedures which can be used for issuing an EIC: (i) the "on-line" procedure, and (ii) the "off-line" procedure. When following the "on-line" procedure, all activities required for issuing the EIC, except initialization, are performed "on line", while the citizen is waiting at the desk of the Personal Data Registry office of the Municipality. During the "off-line" procedure, some of the activities required for issuing EICs are performed by a third party, the Service Center (SC), which is typically an organization constituted by neighbor federated Municipalities providing services in various fields to people living in the same region. A typical example of this is that of Mountain Communities, federations of Municipalities in mountain territory which is explicitly envisaged by Italian laws for providing services to small Municipalities in the same mountain area.

3 The Security Backbone

Our IT solution to implement secure distributed interoperability among Municipalities and Ministry of Interior is based on a radical departure from current approaches. We do not deal with security functions within applications, but consider them as infrastructure services, much in the same way communication services are nowadays considered. Therefore, applications in our architecture do not take care of the management of security functions, which are instead provided by an independent layer, called *Security Backbone*, put on top of the layer providing communication services.

In fact, notwithstanding the work already done and still under development for a full deployment of secure functions within the lower communication layers (e.g. IPv6, DNSsec) the existing communication infrastructure of the Internet is largely lacking for what regards basic security functions. The wide availability of commercial products dealing with IT security, on the other side, is not enough to recover from this situation, since they either requires a deep knowledge of a complex technology (e.g. firewall configuration) or put the burden of dealing with security functions in the applications' modules.

Our solution to implement a secure distributed interoperability among Municipalities and PAs is based on establishing a permanent infrastructure layer (the Security Backbone) providing all security services, and dynamically reconfigurable in terms of access policies. It contains the following functional subsystems: (i) confidentiality and integrity services, (ii) authorization service, (iii) authentication service, (iv) documentation subsystem, (v) access policy management, and (vi) quality of service monitoring. Note also that our architectural solution can be used independently from and simultaneously with local provisions in organizations to deal with security (e.g. perimeter firewalls, physical access control, personal identification, ...).

The single functional components we have used to build the Security Backbone are not, just by themselves, an intrinsic innovation, since each of them is already known in the literature. But their combination in setting up a permanent infrastructure layer providing security services is surely an innovation in the area of distributed digital government services based on the interoperability of legacy systems.

Note, in fact, that when dealing with security in interaction between institutions (as opposed to interaction among people) it is not generally accepted by organizations that any inside person can unilaterally establish trust to the outside. The reality of institutional cooperation shows that inter-institutional trust is always based on bilateral agreement at the organizational level. The electronic counterpart of this point is that, at the IT level, there must be an infrastructure layer providing security functions. It is our convintion that this approach, by allowing - at reasonable costs - efficiency of service provision and effectiveness of security functions, while preserving organizational and technical autonomy, may contribute to spread the use of digital government services, where individual and collective security is a primary concern.