"Smart Card Distribution for e-Government Digital Identity Promotion: Problems and Solutions"

Flavio Corradini, Eleonora Paganelli and Alberto Polzonetti
University of Camerino, Via Madonna delle Carceri 9, 62032 Camerino, Italy
{flavio.corradini,eleonora.paganelli,alberto.polzonetti}@unicam.it
Lucio Forastieri and Donatella Settimi
Regione Marche, Via Tiziano 44, 60125 Ancona, Italy
{lucio.forastieri,donatella.settimi}@regione.marche.it

Abstract. *The introduction of e-Government services and applications leads to significant changes in the structure and organization of Public Administrations. In this paper we analyze a new solution ideated by Regione Marche to access electronic services that is the national services card, called Raffaello. Furthermore we explain the difference between a Digital Identity and a Digital Citizenship in order to introduce a new framework for e-government authentication: the "e-government identity management framework" composed by shared and standardized services that support specific mechanisms of authentication. We explain the use of the presented framework together with smart cards technologies for the Digital Citizenship.*

Keywords. E-services, Digital Identity, smart card, e-government, Identity Management Framework.

1. Introduction

Nowadays Information and Communication Technologies (ICT) are widely used within Public Administrations (PA) and their governance. In this context, e-Government refers to the "use of ICT in Public Administrations combined with organisational changes and new skills in order to improve public services and democratic processes and strengthen support to public policies" [5]. These technologies can have a variety of different aims: better delivery of government services to citizens, improved interactions with the business and the industry world, citizen authorization through access to information, or more efficient government management. The resulting benefits can be less corruption, increased transparency, greater convenience, gain growth and cost reductions. The area of e-Government is one of rapid changes where services are improved and integrated. It is clear that such integration is not imposed from the outside or from above, but it is generated within the working contexts of service development planning and delivery.

The digital Identity deals with user identification and access rights. In particular, the phase of a citizen's identification deserves a special attention, since it is important for the successful realization of the digital government services.

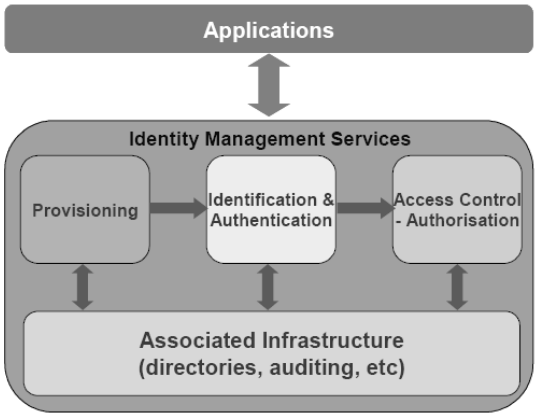
The digital identity promotion discussed in this paper relies on a smart cards distribution plan and on an authentication and authorization solution. The rest of the paper is organized as follows: the next section explains the concept of digital identity and how to manage it, whereas section three describes the main types of smart cards for e-government applications: the national services card (NSC) and the electronic identity card (EIC); section four shows problems connected to smart cards distribution, section five describes practical projects developed by Regione Marche, finally concluding remarks are given in section six.

2. The Digital identity and the e-government Identity Management Framework

We can define a digital identity as the electronic representation of the personal information of an individual or organization [1]. The term digital identity is usually used to refer to two (non-disjoint) concepts: nyms and partial identities. Nyms can be used to give a user a different identity under which operate at any interaction. A partial identity is any subset of the properties (e.g., name, age, credit-card, employment, etc.) associated with a user. Partial identities may or may not be named (i.e., may or may not be related to the human identity of the user).

At first sight the concept of digital citizenship can be related to the concept of digital identity but if we analyze them in detail we can observe that the digital citizenship

provide digital identity and credentials [6]. With the word "credentials" we mean the set of generic Identity Management Services and it is made up by three categories: provisioning, Identification and Authentication and finally Access Control and Authorisation (see Fig. 1).



"Figure 1. Identity Management Framework"

With the term provisioning we mean the authority that releases the digital citizenship and it is composed by several services:

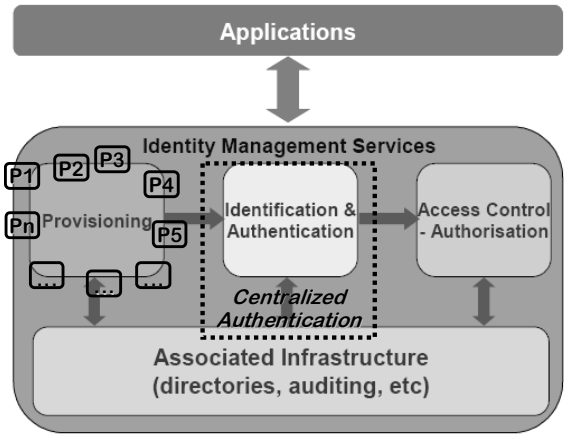
- Identity creation service; e.g. Registration Authorities able to verify and validate identity information in order to issue new digital identities. There may well be different registration 'levels'. The creation of an identity will normally involve the subsequent issuing of credential(s) to the requesting entity, for future authentication. These services may allow for pseudonymity:
- Identity Attribute input service; providing a level of verification for applications providing identity data;
- Enrolment service; providing entities with the authorisation levels needed to use particular e-Government services;
- Dissemination service; enabling the automated dissemination of new or changed identity data to all legitimate holders of such data.

The second category includes all the authorities that operate as authenticators and it provides the following services [7]:

- Authentication service; e.g. password authentication service, PKI based services, various biometric authentication services. Many authentication mechanisms are developed such as Identification – (or Knowledge based authentication) involving knowledge of one or more identity attributes, not necessarily secret; Credential Based Authentication – (or Shared Secret), typically involving username/password or certificate/PIN pairs, or shared secrets; Token Based Authentication – a special case involving a hardware token (smart card or SecureID) containing any of the above identity data.
- Single Sign On; that is, the services required to enable a principal, having authenticated in one system/application to use another system/application, without having to re-authenticate.
- Identity Attribute provision services; that is the services required to enable applications to retrieve identity attributes about a principal, once authenticated or identified.

The Access Control category is that which provides Authorisation services that is, Commonly Role Based Access Control within applications, it is a subset of the set of total accessible services.

Within a e-government's domain it is possible enforce the Identity Management framework in a more specific way. The three category previously seen can be translated in the following manner (see Fig. 2):



"Figure 2. E-government Identity Management framework"

The provisioning category becomes a set of provisioning authority because the digital citizenship is distributed by several local entities whereas the Identification and Authentication authority should be unique, a Centralized Authentication. Only a point of identification that authorises all the people holding a digital citizenship; in this way all the public administrations connect themselves on a central server in order to promote an applicative cooperation between the PA. The

Centralized Authentication provides the same authentication mechanism of the previous identity management framework in order to guarantee several Assurance levels [2]. It is common practice, in Government Interoperability Frameworks, to specify different levels of assurance of authentication required in relation to different e-Government application contexts and we defines them as:

- Level 1: Minimal assurance (e.g. National Identity Number, passport number, etc.);
- Level 2: Low Assurance (e.g. username/password, certificate/PIN pairs, etc.);
- Level 3: Substantial Assurance (e.g. biometric identification);
- Level 4: High Assurance (e.g. smart card or SecureID).

The third category of the e-government Identity Management Framework, that is the Access Control, keeps unchanged because it is realized by the application itself.

In the next section we will examine hardware tokens that realize the Token Based Authentication, typical of an e-government infrastructure, that is the smart card.

3. Different smart card typology in e-government

The smart cards for accessing to network services can be of various typology and they have share the following peculiarity:

- they are emitted by a public institution that validates sensible and social information included in the card;
- they have security requirement that allow the use of this information on the network with the highest security guaranty and tutelage of personal rights.

With these support tools we can pass the traditional interaction model that imposes to the users to provide a series of data over the network and specially to manage high number (around 40) of PIN or Password for the access to services distributed on-line by different public administrations.

Smart cards for services access are amenable to two typologies:

- the Electronic Identity Card (EIC), released by the municipalities in substitution of the traditional Identity Card;
- others smart cards for network service access (sanitary and tributary cards, regional service card, etc.), that must be accordant to a unique standard called National Services Card (NSC).

Now we described the two smart cards typologies in detail.

The EIC is a smart card allowing the holder to be identified "on sight" and it is designed to permit transparent and easy exploitation of e-government services supplied by the Italian public administrations. The EIC achieves two important security goals: it makes electronic transactions very secure, because it adopts sophisticated authentication techniques (challenge/response and asymmetric cryptography) and also saves the user from having to remember a huge number of user-IDs, passwords and PINs.

The EIC is built on a laser card optical memory card platform, which includes a one megabyte optical stripe, to which a contact IC chip is added in Italy [6]. The optical memory provides visual and automatic card authentication; a non-alterable audit trail of events (each digitally signed) in the card manufacturing, registration, activation, distribution, and issuance processes; a portable data "vault" containing each citizen's demographics, colour photograph, digitize signature and other biometrics; with back up should the chip fail.

The NSC, National Service Card represents a standard to access services provided by the public administration. It is a microprocessor card, with almost the same features as the EIC, but with different security elements (e.g. holder picture, holograms produced by the government to verify its authenticity). This simplification enables the use of easier and more flexible systems for distributing such cards, possibly delegating their production to a third-party, thus making the market more open and competitive. The NSC is an instrument to be identified on the network and through the introduction of electronic signature will enable the holder to submit official documents and the government and the government to provide certificates. This two elements will be completely interoperable and the ownership of one will allow the user to access the services available through the other (with the necessary authentication alignment). Therefore the National services Card represents the principal instrument that, like the EIC, enables the

citizen to the access of e-government services and to the request and statement forward.

4. Smart card distribution architecture

Citizens Smart card distribution is the first step towards sensitization and promotion of a digital citizenship. The NSC distribution phase involves several public actors:

- a central authority, that in e-government domain could be a Central Public Administration (CPA), who will manage all the identification services by a Centralized Authentication;
- Others external PA dislocated in periphery, also called associator institution or Local Public Administration (LPA), who will distribute additional credentials in order to receive digital citizenship.

But what an architecture planned in this way can imply? Every LPA has endowed itself with a technical infrastructure that allows to respect quality and trustworthiness characteristics ensuring the whole security circuit. A smart card distribution architecture completely reflects the e-government identity management framework, since the citizen identity is centralized only in the CPA. It is used to authenticate unambiguously the citizen, as the registration authorities who will verify, can validate and distribute the credentials which will be dislocated in several LPA [3].

5. Case Study

In this section we present a practical experience of the Regione Marche that has distributed over 30.000 smart cards to a pattern of resident citizens in Regione Marche in order to increase digital access to services.

5.1 Raffaello's Card

Regione Marche has started the distribution of a regional services card called Raffaello, in honour of the famous painter born in this Region, according to the NSC standard with the aim of promoting Digital citizenship diffusion.

The Raffaello's card allows the citizen to be identified unambiguously on the network and it permits the access to the PAs and companies services. Every digital citizen holds a series of qualified factors and tools such as:

- *Citizen's Digital Identity* by means of EIC or NSC for secure accessing to services given by PA's web sites through a strong authentication. It is based on an authoritative hierarchic structure (LDAP tree) and on an access registry;
- *Access right* to services provided by public web sites according to valid methods to be followed by all citizens-users, as stated in the services catalogue;
- *Digital Signature* of documents produced on-line and to be sent to PAs;
- *Electronic Certified Mail* and documental flow system for official communication between citizens and PAs;
- *Network personal data infrastructure* implemented by a shared repository containing citizens private data that acts as an integration instrument and as an harmonizer of different services provided to the citizen himself.

Regione Marche is the smart cards issuing institution. From a technical point of view the Raffaello's Card is a microprocessor card according to NSC standard. The major difference between them is that the IEC contains indispensable security elements for owner identification at sight, while the NSC Raffaello cannot guarantee any external elements necessary for the Identificative Card.

The Raffaello's card has two main functionalities:

- It is a network identificative instrument because it is furnished with an authentication certificate issued by an accredited authorizer;
- It holds the qualified digital signature, providing the holder with the possibility of subscribing electronic documents.

The NSC Raffaello respects all the constraints imposed by the international standard about smart card paying attention to the standard that rules the identity documents [8].

The Raffaello's Card layout is represented in Fig. 3.

"Figure 3. Raffaello's Card Layout"

5.2 Implantation and emission Phases

In this section we will summarize how the Regione Marche has managed the distribution and emission phases of the Raffaello's card.

The distribution phase has occurred in two different stages. The first phase is called Implantation phase and it has involved Regione Marche, Comunità Montane and Ministry of Economics and Finances (MEF). During this stage they have established which citizens could benefit by smart cards according to several criteria (e.g. age, job, social position, etc...). When the Comunità Montane have collected the citizen private data, information has been sent to the Regione Marche that finally has transmitted them to the MEF. The Ministry has controlled data consistence and has sent processing result to the Regione Marche that has filled the Regional Index of Welfare Users (RIWU).

Before proceeding with the second phase of the distribution it is better to clarify the actors' role involved in Raffaello's card emission:

- the producer, that is the company who provides microprocessor cards with a compatible NSC chip, it leaves clean the space dedicated to the digital signature;
- the authorizer, that is the subject qualified for releasing digital certificates;
- the Local Registration Authorities (LRA), that is the local public institute that is involved in the smart cards issuing;
- The Service Center (SC), that is a third part that works in collaboration with the LRA in order to personalize the smart card. The Service Center's tasks may be developed by the LRA too.

Now we analyze in detail the steps that the citizen has to fulfil to obtain the Raffaello's Card:

A. The citizen goes to LRA office with an identificative document;
B. LRA using a regional web application searches the citizen into RIWU database;
C. The software displays the citizen private data and his/her fiscal code;
D. LRA operator inserts user data (document ID, telephone number, email, address, etc.) in the application;
E. The Web application generates PIN and PUK codes to be printed on an envelope by a laser printer;
F. The LRA operator delivers the envelope to the citizen who has come back to the office after seven days for obtaining the NSC. The system immediately provides to the Service Center request with the NSC generation request and;
G. When the Service Center downloads the generation request:
   - It inserts personal data into the NSC chip,
   - It writes the first two traces of the magnetic band,
   - It prints the NSC by a thermographic printer,
   - It inserts into the NSC authentication and signature certificates,
   - It changes the default PIN,
   - It perforates the first three letters of the fiscal code in Braille alphabet on the front side card,
   - It registers the citizen into the Cohesion regional framework,
   - It assigns to the citizen a certified mail box user@postaraffaello.it
H. The Service Center delivers to the LRA the cards' batch;
I. The system automatically sends to the MEF the identification numbers, the NSC issuing and expiring date;
J. In the last step of the emission phase the citizen goes to the LRA and picks up the Raffaello's card.

5.3 Raffaello's Card Management Informative system (RCMIS)

Regione Marche, in order to support the whole distribution phase, has created a Raffaello's Card Management Informative System (RCMIS) supported by a Call Center at the Regional Service Center. The Call Center provides citizens with assistance, it manages Cards' malfunctions and renews the expired cards.

The RCMIS has the aim of supporting the whole emission circuit and providing the necessary integrations with the regional informative systems in order to furnish a digital citizenship to every Regione Marche's inhabitants. From an architectural point of view, RCMIS is a web procedure with a secure and authenticated access based on regional services framework. It allows a centralized authentication on a regional server farm called Cohesion. In details Cohesion is a framework used to implement infrastructural services. It permits to deploy applicative cooperation actions, secure front-office access, authorization and accounting function through the single sign-on, directory system like LDAP, content management services, work-flow and collaboration services. Cohesion generates a new record, with the user's identification data, whenever a new user receives the Raffaello's card in order to allow him the access to e-government e-services. In this way the citizen will be automatically qualified to use the authentication services in every PAs web sites that uses Cohesion as authentication server.

6. Conclusions

In this paper has been presented an architectural solution to provide a digital citizenship through a central solution of authentication using smart cards technology. In particular it has been defined a logical framework for e-government digital identity management. The framework Cohesion represents the centralized authentication described in e-government identity management framework and it is used for public service provision enhancing cooperation, coordination and integration of services. In this setting, of course, the human and technological resources available are optimised and have been improved by the distribution of e-Services information for citizens and firms of the Regione Marche [4].

Digital Identity covers a fundamental role and solves the authentication and authorization problems. The case study of the Raffaello's card represents a good starting point for involving the citizens in innovation processes and the smart cards technology support this process accomplishing the e-ID concept.

Further refinement of this system can extend its usage for increasing on-line transaction.

The future objective of the Regione Marche is to make Cohesion the only authentication point to access e-services with aiming at increasing knowledge and reducing costs and time.

7. References

[1] Camp L.J., 2004. Digital Identity. IEEE Technology & Society, Vol. 23, No. 3, pp 34-41.

[2] Claub S. et al, 2001. Identity Management and Its Support of Multilateral Security. Computer Networks, Vol. 37, pp 205-219.

[3] Damiani E., De Capitani di Vimercati S. and Samarati P.: Managing multiple dependable identities. IEEE Internet Computing.

[4] Rust R. et al, 2001. E-Service and the Consumer. International Journal of Electronic Commerce, Vol. 5, No. 3, pp 85-102.

[5] Corradini F. et al: A case study of participatory design in e-government systems: e-services and e-id. Proceedings of the IADIS International Conference www/2005; 2005 Oct 19-22, Lisbon, Portugal.

[6] Gentili M.: Italian Electronic Identity Card: principle and architecture. Proceedings of the 27th VLDB Conference, Roma, Italy, 2001.

[7] Woerndl W.: Authorization of User Profile Access in identity Management. Proceedings of IADIS International Conference 2004, Lisbon, Portugal.

[8] ISO/IEC 7816-1/2 standard http://www.ttfn.net/techno/smartcards/iso7816123.html