Reliable peer-to-peer access for Italian citizens to digital government services on the Internet *

Franco Arcieri[1], Fabio Fioravanti[1,2], Enrico Nardelli[1], and Maurizio Talamo[1]

[1] NESTOR - Multimedia services security and certification Laboratory, Univ. of Rome "Tor Vergata", Rome, Italy. nardelli@nestor.uniroma2.it
[2] Dept. of Informatics - Univ. of L'Aquila, L'Aquila, Italy.

Abstract. In the delivery of e-government services to citizens it should be clear that the viewpoint cannot simply be the standard one of client-supplier commonly used to provide services on the Internet. In a modern society it has rather to be the peer-to-peer approach which is typical of democracies, where institutions are equal to citizens in front of the law. But this is not yet a widely accepted standpoint in digital government efforts going on in many advanced countries in the world.

Italian government, in its ever increasing effort to provide citizens with easier access to online government services, has instead adopted and is pursuing this symmetric approach, which is going to represent a fundamental tool in the ongoing march towards e-democracy.

In this paper we describe the organizations involved in the process and the Information Technology (IT) infrastructure enabling the effective management of the whole process while ensuring the mandatory security functions in a democratic manner.

Organizational complexity lies in the distribution of responsibilities for the management of people's personal data among the more than 8000 Italian Municipalities and the need of keeping a centralized control on all processes dealing with identity of people.

Technical complexity stems from the need of efficiently supporting this distribution of responsibilities while ensuring, at the same time, interoperability of IT-based systems independent of technical choices of the organizations involved, and fulfillment of privacy constraints. The IT architecture defined for this purpose features a clear separation between security services, provided at an infrastructure level, and application services, exposed on the Internet as Web Services.

Keywords: Trust and security, e-service interoperability.

* This work has been partially supported by the Grant MIUR L.449/97, CNR Project "P1 - INTERNET networks: efficiency, integration and security", Research Action "Security Services" and by the Grant MIUR PNR 2001-2003, FIRB Project RBNE01KNFP "GRID.IT: Enabling Platforms for High-Performance Computational Grids Oriented to Scalable Virtual Organizations"

1 Introduction

The ubiquitous presence of the Internet has offered to Public Administrations the great opportunity of being able to bring their offer of public services directly in the home of citizens, improving the level of provided services while keeping under control the associated costs [8, 10].

But this opportunity opens also the way to possible abuses, identity theft is the most prominent example of. So the point is how to set-up mechanisms and systems to enable citizens and public administrations to reliably identify each other on the Internet, without compromising people's rights and organizations' responsibilities.

The whole area of authentication of individuals and transaction parties is the really critical issue to transform such an opportunity into a working reality delivering its promises. It is often said "On the Internet nobody knows you are a citizen" and it is plainly true that while anonymity may be desirable for certain kind of Internet services, certainty of parties identification is a necessary condition for giving full validity to many kinds of transaction on the Internet.

Our solution supports the use of two access mechanisms to services on the Internet: the Electronic Identity Card (CIE - Carta d'Identita' Elettronica) and the National Service Card (CNS - Carta Nazionale dei Servizi). While the former is an identity document with full legal validity allowing the citizen also to access to digital government services, the latter is not an identification document and was introduced with the purpose of enabling a quicker and easier deployment of local services from Regional Public Administrations, during the initial phase of rolling out CIE to citizen.

The infrastructure supporting this solution has been developed during a multi- year cooperation between the Italian Ministry of Interior and the NESTOR Laboratory of the University of Rome "Tor Vergata". Many organizations are currently involved in this project. The Head of Department of Internal and Territorial Affairs of the Italian Ministry of Interior is responsible for the project and the whole project is being developed as an institutional duty of the Central Directorate for Demographic Services of the Ministry of Interior, on its responsibility and with its support [15]. 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 CIEs. The security system of the CIEs architecture (Sistema di Sicurezza della CIE - SSCE), generates keys used for activating CIEs and is responsible for guaranteeing security during the formation of data and issue of CIEs. Municipalities contributed to the definition of end-user requirements and ANCI, the Association of Italian Municipalities, by means of ANCITEL, its IT subsidiary, is cooperating to the deployment of the system all over the Italian territory.

2 People Identification and Access to E-Services in Italy

The Electronic Identity Card (CIE, for short) is a polycarbonate smart card equipped with a microchip, a laser band and a hologram which contains personal

(e.g. name, surname, date of birth,. . .) and biometric (e.g. photo, fingerprint,. . .) data of a citizen.

The CIE is an identity document which, according to Italian Laws, is fully equivalent to the paper based ID card and it has two purposes: (*i*) in-presence identification of a person, like a traditional paper based ID-card, and (*ii*) remote authentication of a citizen, allowing access to digital government services. For example, citizens could use their CIE 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 CIE, 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. For a more detailed presentation of its characteristics and of the overall process involved see [1, 5].

The National Service Card (CNS, for short) is a polycarbonate smart card equipped with a microchip and containing personal data of a citizen.

CNS allows identification of a citizen in the Internet access to services provided by a Public Administration. CNS can be issued by any Public Administration but cannot have data for in-presence identification of people (e.g., photography) nor be used for this purpose. Also CNS can be issued or renovated to a citizen only if he or she has not already received his/her CIE [17]. CNS it is therefore a tool introduced to allow to Public Administrations to make them possible to provide e-services to citizens in their territory of interest during the initial transient phase of deployment of CIE. During this phase, CNS and CIE are fully interchangeable (i.e., plug-to-plug compatible) to access e-services of a public administration. Also a citizen holding a CNS has to be able to access (if he/she has the right to) also e-services provided by a Public Administration different from the one which has issued the CNS used for the access itself.

3 The Reference Scenario and CIE deployment

We only remember here the most important characteristic of the reference scenario for the management of personal data in Italy. For a more detailed view see [4].

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).

The Ministry of Interior has the overall responsibility for the correct maintenance of Personal Data Registries in all Italian Municipalities. In order to understand the dimensions of the problem, it is important to note the variety in size and complexity of these archives, since about 6000 of the 8192 Italian Municipalities have less then 5000 citizens, but 8 of the 20 Region chief towns have more than one million inhabitants.

In Italy we have defined an organizational and architectural solution featuring fully independence of involved organizations and a clear separation between security services, provided at an infrastructural level, and application services,

exposed on the Internet as Web Services. Our solution is therefore able to fully support the delivery of promises of better services to citizens by government through the use of IT.

The organizational component of our solution defined a single access index to the Municipality which is responsible for a citizen's personal data (INA = Indice Nazionale delle Anagrafi). This index, whose institution was established by a supplement [14] to the ordinary law regulating the Personal Data Registries kept in Municipalities [13], provides - for a given person - the reference to the Municipality responsible for his/her personal data. Uniqueness of reference to a person is ensured by using fiscal code as INA's access key.

Organizational competence for management of INA and of its services towards Municipalities and PAs was given to the National Center for Demographic Services (CNSD = Centro Nazionale Servizi Demografici), a newly established organizational unit of the Ministry of Interior [16]. CNSD is responsible for both the IT infrastructure supporting access to and management of INA and its services and for the end-user support in the utilization of its services. CNSD is also responsible for the management of telematics infrastructure ensuring secure and certified access to its services to all organizations. Technical solutions able to implement efficient and effective IT systems to support CNSD activities were devised and tuned by NESTOR Laboratory.

In the first phase of deployment of the CIE, 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 CIE architecture has already started. The target of this second phase is to provide the 56 Municipalities involved with 2.000.000 CIEs, and to issue them by the end of year 2004 thus satisfying the local demand for ID cards. 600.000 CIEs have already been produced until the first half of April.

4 The Security Backbone

Our solution to implement a secure distributed interoperability among Municipalities and PAs to provide secure digital government service in the field of Personal Data Registries is based on establishing a permanent infrastructure

layer (the Security Backbone) providing security services, placed between the base communication services layer and the application service layer.

The Security Backbone 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.

The various technical 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. For more details on the Security Backbone see [2, 3].

A large amount of technology is available dealing with many issues related to security for the Internet [6, 7, 9, 11, 12] and research activity is still very high with many conferences discussing more advanced security topics.

Also, advances in lower level protocols for communication (e.g. IPv6) or recently developed PKI-based approaches to inter-organizational security infrastructures (e.g. bridge CAs) will hopefully result in a widespread intrinsically secure communication infrastructure. For the time being, though, relying on the availability of such technologies to provide secure services does not constitute a solution that in general works.

On the other side, the architecture we have described in this paper can be implemented with commercially available components and does not require updates or change to existing end-user applications. We therefore think that it may contribute to spread the use of digital government services, where individual and collective security is a primary concern.

5 Conclusions

In this paper we have described the approach taken in Italy to ensure citizens access to digital government services while keeping the essence of a democratic society: the equality of all citizens and institutions in front of the law. We have presented the reference scenario and we have identified normative and organizational constraints on the activities to be performed when issuing CIEs and CNSs, the two access means in Italy to e-services made available on the Internet by Public Administrations.

Information security in the overall architecture is provided by adopting a solution to the provision of security services which can be deployed without relying on advanced security technologies and without needing any update or change to existing systems and applications.

The various functional subsystems used in our solution, called the Security Backbone, provide end-to-end security in the interaction among involved organizations and constitutes an addition, not a replacement, of security solutions deployed locally. Thus, we have shown that, by putting security services in an infrastructure layer of inter-organizational communication, to be placed between the communication service layer and the application service layer, it is possible to provide, at reasonable cost, efficiency of service provision and effectiveness

of security functions while preserving organizational and technical autonomy. Moreover, our approach is able to guaranteee equality of all parties in transactions related to e-services.

References

1. F.Arcieri, M.Ciclosi, F.Fioravanti, E.Nardelli, M.Talamo: The Italian Electronic Identity Card: a short introduction. *The National Conference on Digital Government Research (DG.O-04)*, Seattle, Wa., USA, May.04, 2004.
2. F.Arcieri, G.Melideo, E.Nardelli, M.Talamo: Experiences and issues in the realization of e-government services. *IEEE Int. Workshop on Research Issues in Data Engineering (RIDE'02)*, San Jose, Ca., USA, Feb.02, IEEE Computer Society Press, 2002.
3. F.Arcieri, G.Melideo, E.Nardelli, M.Talamo. A reference architecture for the certification of e-services in a digital government infrastructure. *Distributed and Parallel Databases*, 12:217–234, 2002.
4. F.Arcieri, F.Fioravanti, E.Nardelli, M.Talamo. A layered IT infrastructure for secure interoperability in Personal Data Registry digital government services. *IEEE Int. Workshop on Research Issues in Data Engineering (RIDE'04)*, Boston, USA, Mar.04, IEEE Computer Society Press, 2004.
5. The Italian Identity Card Experience: European Interoperability for Travel Identification and Citizen Authentication in Service Delivery. *International Conference*, Rome, Italy, Apr.04, `http://www.nestor.uniroma2.it/italianEIC`.
6. W.R.Cheswick, S.M.Bellovin, A.D.Rubin. Firewalls and Internet Security: Repelling the Wily Hacker, 2nd edition. Addison-Wesley, 2003.
7. S.Deering and R.Hinden. Internet Protocol version 6 specification. RFC 2460, Internet Engineering Taks Force. Dec.98. `http://www.rfc-editor.org/rfc/rfc2460.txt`.
8. A.K.Elmagarmid, W.J.McIver: The Ongoing March Toward Digital Government, Guest Editors' Introduction to the special section on Digital Government, *IEEE Computer*, 34(2):32–38, Feb.01.
9. R.Hinden and S.Deering. Internet Protocol version 6 addressing architecture. RFC 2373, Internet Engineering Taks Force. Jul.98. `http://www.rfc-editor.org/rfc/rfc2373.txt`.
10. J,Joshi, A.Ghafoor, W.G.Aref, E.H.Spafford: Digital Government Security Infrastructure Design Challenges. *IEEE Computer*, 34(2): 66-72, Feb.01.
11. S.Northcutt, L.Zeltser, S.Winters, K.K.Frederick, R.W.Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003.
12. W.T.Polk, N.E.Hastings, A.Malpani. Public Key Infrastructures that Satisfy Security Goals. *IEEE Internet Computing*, 7(4):60–67, Jul-Aug.03.
13. Law n.1228, 24/dec/1954.
14. Law n.26 28/feb/2001.
15. Ministerial Decree of 16/jan/2002 of the Ministry of Interior.
16. Ministerial Decree of 23/apr/2002 of the Ministry of Interior.
17. Article 2, Paragraph 3, Decree of the President of the Republic n.177 of 2/mar/2004.