Introduction

E-GOVERNMENT SERVICES: CERTIFICATION AND SECURITY

Maurizio Talamo

NESTOR Lab, University of Rome "Tor Vergata", Italy*

1. SCENARIO

Issues related to cooperation on the network among different organizations have been studied for a long time with great interest by the international community.

The new trend of government of providing to citizens unitary and integrated information of public administration service systems, also adds to the need to initiate, coordinate and manage complex inter-organizational workflows [4, 5, 6, 7, 14].

All e-government plans have the main goal to simplify interaction among citizens and the Public Administration by means of the development of inter-organizational network services where all involved Public Administrations cooperate to initiate, synchronize and monitor all processes needed for a given service, and to guarantee the global coherency of data related to a given service in several Public Administrations.

There is now a big general effort to define common standards and protocols to represent and communicate structured information and services (XML, UDDI, SOAP) that simplify the definition of integrated network services. It is important however to observe that the problem to define inter-organizational services is primarily an organizational one, that is, even a complete solution to the problem of accessing services and exchanging information would not help the deployment of inter-organizational services unless we also consider problems like how such services are currently handled by the organizations, how the responsibilities for the services are assigned, how the organizations keeps track of the status of the services.

For instance, the design of an inter-organizational networking service is simpler if there exist a single organization which has the capability to impose its technical solution to the other organizations, since in this case we basically

*Laboratorio Sperimentale per la Sicurezza e la Certificazione di Servizi Telematici Multimediali

The original version of this chapter was revised: The copyright line was incorrect. This has been corrected. The Erratum to this chapter is available at DOI: [10.1007/978-0-387-35696-9_19](https://doi.org/10.1007/978-0-387-35696-9_19)

E. Nardelli et al. (eds.), *Certification and Security in E-Services*

© IFIP International Federation for Information Processing 2003

have the same behaviour as a mono-organizational service; such assumption is reasonable where the organizations are hierarchically organized, and allows one to adopt a “technocratic” approach.

Much more difficult is the case where involved organizations are autonomous: in this case we cannot impose a common set of protocols for the technical part, and processes and responsibilities are spread among the organizations with possibly different requirements on issues like authentication and security.

As a proof of this difficulty, United States of America, which are in general biased toward the adoption of innovative technologies, and which often have a high standardization of organizational processes, are quite cautious in publishing complex and cooperative Public Administration network services, and tends to only offer simple informative services.

For instance, Rand Corporation [8] says:

- “We are not aware of government agencies in the United States that are using the Internet to transmit sensitive personal data, e.g., tax, social security, and health information.”
- “This limitation on the current use of the net stems from our current inability to guarantee privacy, integrity, and authenticity. Obstacles to achieving the necessary level of security are NOT technical, however. Rather, they are institutional and organisational.”
- “These problems are compounded when data are combined from different agencies.”
- “Concerning the problem of new services arising by increasing the efficiency in the back-office, the following 4 types of architecture are possible for exchanging information among different organisations:

- A free access in read/write to the database;
- B trusted third party who takes care of logging the information fluxes;
- C trusted third party who stores/forwards all information;
- D publish and subscribe.

Case A corresponds to a merging among different organisations and can be used only when such a merging has been decided at all organisational levels. Case C implies the building of a new form of bureaucracy which may not be needed in developing the services. Case D should be limited to non-critical information (i.e. no privacy constraints, no economic content). Finally, Case B is the most broadly suitable and easily implemented possibility.

Technological tools like CORBA, DCOM and others are considered to be too complex in order to design (in a robust way) new services. On the

other hand, XML standard is considered to be extremely important to follow and, with respect to government Agencies, it is considered to be a crucial point to develop a common dictionary to develop applications based on XML-structured messages.”

From the previous analysis, it is evident that the design of a system of inter-organizational services has to minimize impact over existing organizational and technical models, that is, the definition of such a system must be guided by relationships among organizations involved in the services.

2. E-GOVERNMENT: ORGANISATIONAL ISSUES

What mentioned above gives rise to a set of organizational issues to be faced, analysed and solved. When different organisations cooperate to design and implement e-government services sharing data and resources, then:

- Each organisation must carry out, in an effective and efficient way, the assigned institutional activities: the information resources sharing with other organisations must be, therefore, mediated taking into account these chief needs.
- Each organisation has its own decision and management independence: the information resources to be shared with other organisations should not jeopardize such independence; i.e. considering in their operational plans activities that other organisations could carry out on internal computing systems and data.
- Each organisation has its own information dissemination policies: a flat data and information resources sharing should never be put in place. It's not true that everybody can use everything, but it's true that new generation network technologies allow to define horizontal sharing models (not for data and applications). As for its structure the organisational sharing is based on a graph model: each organisation can decide on each individual data, on each individual information resource and on which organisation have the access/use right. Put plainly: new generation network technologies guarantee that each node can be reached by any other node, by essentially defining a complete connectivity graph. Each organisation, on the ground of specific agreements, decide to share each individual computational resource. Therefore, we see application virtual connectivity, that is to say communities. In that environment we can speak of complete resources sharing made available by each partner of the community itself.

- Each organisation has its own security policies: it's well known that University security policies are completely different from those of an important physics laboratory that works in close co-operation with government and the army. In order to guarantee a real resources sharing among different kinds of organisations, it's necessary to ensure the maximum level of flexibility in the management of the above mentioned issues, without introducing technological stiffness that could prevent the real involvement of organisations with completely different security policies.

3. INTER-ADMINISTRATIVE SERVICE: A MODEL CASE

In the followings we are going to introduce a very widespread type of e-government service: inter-administrative service. Issues related to this type of service give us the chance to introduce all issues mentioned before and to define project guidelines of security and certification services that an e-government office should provide.

An inter-administrative service is a set of administrative procedures. A procedure is a set of actions (processes) necessary to provide a complete answer to a service requested by a citizen/user. This type of service (inter-administrative service) has the following characteristics:

For the service request the citizen has to submit a folder composed by the following components:

- One or more forms of the e-government service provider in charge for the the inter-administrative service;
- A set of official documents, provided by different e-government service providers, that authenticate some specific information declared in the form or certify some information to be updated in the same e-government office or in different ones.

3.1. EXAMPLE: BUILDING AUTHORISATION REQUEST PROVIDED BY A MUNICIPALITY

The citizen has to fill a set of forms with, for example, the following certified information:

- land ownership certificate (provided by the Public Record of Housing)
- number of the cadastral registration request (provided by the Cadastral Registry)

The result of the service must be:

- In the positive case: certifications of the e-government service provider declaring
 - 1 that all the provided information and documents are correct and complete
 - 2 the guarantee that the service request has been successfully accepted
- In the negative case: certifications of the e-government service provider declaring
 - 1 that the provided information or documents are incomplete or incorrect
 - 2 the necessary processes to be initiated for the successful service providing

An e-government service provider, using the nowadays available technologies, must provide at its own front-office a single unified access point that has to coordinate:

- access to different and independent PKIs
- access to services in charge by different public administrations, respecting their different security requirements.

Providing an inter-administrative service is not the simple collection of certificates provided by different administrations, as it is nowadays meant, but something that needs a complex coordination.

It's the coordination of all the components (procedures) that guarantees:

- 1 the technical control of the service successfully or unsuccessfully provided;
- 2 the possibility of the e-government service provider to certify, under its own responsibility, that the service requested has been successfully or unsuccessfully accepted and, if unsuccessfully, why.

The e-government service provider, being the citizen interface, must be the unique responsible for the provided service.

To be the unique responsible means that it has to guarantee:

- certification of procedures either for the citizen, or for the public administrations involved in the service providing;
- security that each procedure has respected security requirements of all involved parties. For example, to avoid that a citizen/user could use the service system as a back-door for violating other e-government service providers.

4. CONCLUSIONS

Introducing a new PKI we must know that it's not a technological solution, but we are imposing an organizational solution in which the PKI manager has a leadership role towards everybody who will use its services.

In a context where there are n PKIs and each one has its own users, it's a difficult problem from the technological point of view, but well defined. In this case, It has to be defined some mechanisms to guarantee an interoperability among different PKIs, so that a user of a PKI could interact, in a secure and certified way, with a user of a different PKI.

In a context where more PKIs have to cooperate in order to authenticate a workflow-based service towards an end-user, as we discussed above for inter-administrative services, it's necessary to introduce a more complex concept of interoperability. This case is particularly important for e-government services.

Each PKI authenticate only one step, that of its own responsibility and (as we see in the example above) one of the PKIs involved in the service providing must be able to authenticate the cooperation process in all its steps, as a whole. Therefore, in this model it's necessary to introduce in the architectures of the inter-administration services manager an *overlay*, that's to say a layer over the already available service layers. This overlay has to be able to guarantee the possibility of separating the *management* of the single services from the *control* (monitor, supervision and action in case of emergency) on synchronisation processes done to set all procedures in an inter-administrative service, as described above.

In particular this model mirrors the case B described by Rand Corporation (see above) [8] where the overlay plays the role of "trusted third party who takes care of logging the information fluxes".

The separation of control and management is essential. The control synchronisation processes among different services must be guaranteed, each time to each different administrative service provider, while initiating those procedures. The inter-administrative service is the set of procedures inside a process of inter-administrative service providing.

Control means to guarantee the coordination process, as above described, in particular in its two essential aspects:

- 1 certification of synchronisation process among different procedures
- 2 security of service providing process as a whole (step by step)

We think that the above described concepts have to be developed by research and technology in the reference models for e-government services, leaving a technology-driven logic and going to an organizational-driven one.

The issues discussed in this paper comes from the author's experience as designer and supervisor of the following projects:

Project "SICC" (finance ministry, municipalities) [1, 2, 9, 10]: is the Italian distributed cadastral system. Provide more than 12.000.000 cadastral and mortgage transactions per year (15.000.000) to citizens and Local Public Administrations by means of distributed (internet/intranet) access points over the national territory.

Project "SIM" (agricultural ministry, mountain communities, regions) [6, 13]: is a distributed ICT system interconnecting nowadays more than 1300 sites of heterogeneous Local (regions, forestry corps, mountain municipalities, mountain communities, national and regional parks) and Central (Agricultural and Forestry Ministry, Finance Ministry, Environment Ministry, National Statistical Institute, National Social Security Institute and others) Public Administrations. It provides a broad range of inter-administrational network civil services for territory management [5], automation of authoritative procedures, distributed sharing and update of geographical data [6]. Moreover, it gives a homogeneous access and sharing [10, 11, 12] with Central Public Administration Services; for instance, it provides other distributed bidirectional access points to the SICC. The SIM reaches about 10.000.000 citizens and covers 50

Project "SIAN" (agricultural ministry): is the distributed (internet/intranet, central administrations/regions/provinces/mountain community /municipalities/associations of farmers/farmers), ICT system for agricultural services in Italy. 2 million farmers involved for more than 5.000.000.000,00 given yearly to them as E.U. support.

Project INA (interior ministry) [7]: provides distributed updates of all Italian citizens census data from the municipalities to the central repository at the Home Office, notifying data changes to all registered Public Administration and which certify the emission and the usage of the Italian Electronic Identity Card. (The project started on may 2001 and nowadays we certify, on line, census data for more than 9.000.000 citizens).

Project SID (transport ministry): is the Italian distributed information system on the maritime cadastral. All the Italian coast municipalities, regions and ports/maritime authorities are involved.

References

- [1] F. Arcieri, C. Cammino, E. Nardelli, M. Talamo, and A. Venza. The Italian Cadastral Information System: a Real-Life Spatio-Temporal DBMS. *Workshop on Spatio-Temporal Database Management (STDBM'99)*, Ed-

- inburgh, Scotland, U.K., Sep.99, Lecture Notes in Computer Science vol.1678, 79–99, Springer-Verlag.
- [2] F. Arcieri, C. Cammino, E. Nardelli, M. Talamo, and A. VENZA. Italian Cadastral Data Exchange System. *GIM International*, Dec.99, 13(12): 6–9.
 - [3] F. Arcieri, E. Cappadozzi, P. Naggar, E. Nardelli, and M. Talamo. Access Key Warehouse: a New Approach to the Development of Cooperative Information Systems. *4th Int. Conf. on Cooperative Information Systems (CoopIS'99)*, Edinburgh, Scotland, U.K., 46–56, Sep.99.
 - [4] F. Arcieri, E. Cappadozzi, P. Naggar, E. Nardelli, and M. Talamo. Coherence Maintenance in Cooperative Information Systems: the Access Key Warehouse Approach. *International Journal of Cooperative Information Systems*, to be published on Sep.01.
 - [5] F. Arcieri, E. Cappadozzi, E. Nardelli, and M. Talamo. Geographical Information Systems Interoperability through Distributed Data Exchange. *1st International Workshop on Databases, Documents, and Information Fusion (DBFusion'01)*, Magdeburg, Germany, May 01, Preprint n.8/2001, Fakultät fuer Informatik, Universität Magdeburg.
 - [6] F. Arcieri, E. Cappadozzi, E. Nardelli, and M. Talamo. Distributed Territorial Data Management and Exchange for Public Organizations. *3rd International Workshop on Advanced Issues of E-Commerce and Web-Based Information Systems (WECWIS'01)*, San Jose, Ca., USA, Jun.01, IEEE Computer Society Press, 2001.
 - [7] F. Arcieri, E. Cappadozzi, E. Nardelli, and M. Talamo. SIM: a Working Example of an E-Government Service Infrastructure for Mountain Communities. *Workshop On the way to Electronic Government (DEXA-eGov'01)*, associated to the 2001 Conference on Databases and Expert System Applications (DEXA'01), Sep.2001, Munich, Germany, IEEE Computer Society Press.
 - [8] Rand Corporation, AIPA Meeting. The internet and Public Administration in Italy. Summary report available at [http://www.aipa.it/english\[4\]/internet\[4\]/index.asp](http://www.aipa.it/english[4]/internet[4]/index.asp)
 - [9] M. Talamo, F. Arcieri, G. Conia, and E. Nardelli. SICC: An Exchange System for Cadastral Information. *6th Int. Symp. on Large Spatial Databases (SSD'99)*, Hong Kong, China, July 99, Lecture Notes in Computer Science vol.1651, 360–364, Springer-Verlag.
 - [10] F. Arcieri, G. Melideo, E. Nardelli, and M. Talamo. Experiences and Issues in the Realization of E-government Services. *12th International Workshop on Research Issues on Data Engineering: Engineering E-Commerce/E-Business Systems (RIDE-2EC'2002)*.

- [11] F. Arcieri, G. Melideo, E. Nardelli, and M. Talamo. Keeping Coherence among Web Sources. *ACM CIKM'01 3rd Workshop on Web Information and Data Management (WIDM'01)* (held in conjunction of ACM CIKM 2001, November 2001).
- [12] F. Arcieri, E. Cappadozzi, G. Melideo, P. Naggari, E. Nardelli, and M. Talamo. A Formal Model for Data Consistency Maintenance. *Foundations Of Models For Information Integration*, September 2001 (FMII-2001).
- [13] F. Arcieri, R. Giaccio, E. Nardelli, and M. Talamo. A Framework for Inter-Organizational Public Administration Network Services. *Proc. of International Conference Advances in Infrastructure for Electronic Business, Science, and Education on the Internet (SSGRR 2001)*, L'Aquila, August 2001.
- [14] C. Batini, E. Cappadozzi, M. Mecella, and M. Talamo. Cooperative Architectures. *Advances in Digital Government*, edited by William J. Mever, Jr. Ahmed K. Elmagarmid: Kluwer Academic Publishers - 2002.