E-GOVERNMENT SERVICES: CERTIFICATION AND SECURITY OVERLAY

Franco Arcieri, Roberto Giaccio
NESTOR Lab, University of Roma "Tor Vergata", Roma, Italia.*

Abstract E-government services are very difficult to implement because they present legislative, organizational and technical issues all together, each of them causing very strict design and implementation requirements.

In this paper we present the *Certification and security overlay* as an effective solution to design and implement e-government services; this solution has already been adopted in several existing Italian PA services like the Cadastral Municipalities Interchange System, the National Census Index, providing different e-government services to all Italian citizens.

Keywords: e-government services, service certification, security issues

1. INTRODUCTION

The design and implementation of E-government services is a very difficult task [12, 13, 14], because they present many legislative, organizational and technical issues posing very strict requirements on aspects like security, monitoring and system interoperability: normative aspects, and their possible evolution during time, have to be taken into account by explicitly defining in the service implementation all objects referenced in the exiting regulations and by monitoring all procedure invocations for errors; note that, even if a single procedure invocation can be correct in itself, a sequence of different correct procedure invocations is not guaranteed to be sound according to the existing legislation.

The organizational issues become complex when the service users or providers are different organizations [9, 11]: in this case, in order to identify errors in the workflow we have to explicitly monitor what is going on among organizations; this allows us to identify if the error has been originated inside an

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

organization, or it depends on communication mismatches between different organizations. Even if a service involves different organizations, possibly being split into subservices, there is always only one organization in charge of it, its *owner*.

In this case also the technical aspects are very challenging, since while in a single organization we can precisely define architectures, network protocols, security and accounting policies, when we have multiple organizations we have to coherently integrate different design choices, often without having the possibility to modify them at all. Furthermore, the organizational requirement to monitor inter-organizational processes requires to somehow correlate the different codes used in different organizations to refer to the same object.

We will focus on technical issues of e-government services, keeping in mind that any technical solution has also to comply and possibly simplify the legislative and organizational problems; we present the *Certification and security overlay* as an effective solution to the technical problems outlined above. This solution has already been adopted in the analysis and implementation of several existing Italian PA services: the Mountain Information System ("Sistema Informativo della Montagna", SIM), Cadastral Municipalities Interchange System ("Sistema di Interscambio Catasto-Comuni", SICC) and the National Census Index ("Indice Nazionale delle Anagrafi", INA).

The SIM [8] is a distributed network interconnecting more than 800 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 services for territory management, automation of authoritative procedures, distributed sharing and update of geographical data [7]. Moreover, it gives a homogeneous access to Central Public Administration Services; for instance, it provides other distributed access points to the SICC. The SIM reaches about 10.000.000 citizens and covers half of the Italian territory with 4.000 municipalities. The SIM is now part of the bigger National Agriculture Information System (Sistema Informativo Agricolo Nazionale, SIAN), which has adopted all the SIM solutions.

The SICC [1, 2, 15, 16] is the Italian distributed cadastral system, and provides 8.000.000 cadastral and mortgage transactions per year to citizens and Local Public Administrations by means of distributed access points over the national territory.

The INA [17] provides distributed updates of all Italian citizen's data from the municipalities to the central repository at the Home Office, notifying data changes to all registered Public Administration,

While designing and implementing these distributed systems for the Public Administrations we developed some original solutions sometimes to overcome existing technologies limitations; basically, we developed a hardware/software architecture supporting application cooperation with the capability to trace inter-organizational processes, but also by improving security and user authentication; the key innovation in such architecture is that it is added on top of existing applications, requiring few modifications to existing applications and, more important, organizations.

In the following, we define the entities involved in an e-government service, and introduce the Certification and security overlay; then we show how the Certification and security overlay has been implemented in the SIAN System, also handling the case of clients accessing services in charge of different organizations. Finally, we present some conclusions and discuss some future improvements to the existing implementations.

2. E-GOVERNMENT SERVICES

An e-government *service* is a set of procedures that must be accomplished in some order in compliance to given legislative rules; a *procedure* is a sequence of one or more transactions involving a single procedure *client* and a single procedure *provider*. As an example, consider that a citizen census modification in the central index (first procedure) must be transmitted to the community where the citizen lives (second procedure, the community provides a procedure for updating its census index); the two procedures build a census modification service.

For each service there exists a service *owner*, which is the organization that, according to the legislative and organizational issues presented above, has to monitor the service transaction in order to detect errors or workflow inconsistencies; the owner of a procedure is the owner of the service it belongs to. Note that in general the owner can be neither the client nor the provider: in the case of the census modification, the owner of the second procedure is the National Census Index, the provider is a community and the client can be a different organization.

As exposed before, when we have multiple organizations concurring to a service, the procedure owner must know all the details of all procedure invocations to guarantee that the procedure has been correctly provided; this requires that either the client or the provider send the useful details to the owner with some suitable protocol; hence some device is needed at least on one connection side to extract the relevant information and send them to the service owner. The service owner must provide some facility to store incoming information and to correlate them to test for global coherency.

In general, we can list the main tasks involved in implementing an e-government service as follows:

1 define a set procedures that correctly represents the legislative and organizational aspects of the service;

2 make sure that the clients and the servers recognize each others (parties certification);

3 given the sensitivity of the information involved in e-government transactions, guarantee that nobody can intercept service information but the clients, providers and service owner (security);

4 make sure that the service correctness is monitored (possibly both on the clients and providers sides) by some entity trusted by clients, servers and owner (service certification).

Of course all these problems can be solved with appropriate technologies, like using crypto-routers for the communication channel, adding remote logging facilities to applications, etc.; however, even with few different organizations involved, it becomes practically impossible to follow all these different technologies.

Hence, a different approach has been used: the main idea is to separate providers' *management* from owner's *control* of the service: we define an infrastructure, the *Certification and security overlay* that takes care of points 2, 3 and 4, all related to the control of the service: this allows the procedure implementers to focus on the service functionalities (the management) without worrying about additional problems.

3. CERTIFICATION AND SECURITY OVERLAY

The Certification and Security overlay is mainly based on three subsystems:

- the *Documentation subsystem*: it analyzes the procedure information flow on both client and provider side, extracts information to be logged and archives them in a centralized repository;
- the *Control subsystem*: it authenticates client and provider to each other, checks that the service access is compliant with the policies of the service owner and opens a secure channel for data communication. In order to provide these features we need specific hardware or software devices between the client and communication link, and between the communication link and the provider;
- the *Owner policy subsystem*: it provides the Documentation and Control subsystems with different configuration files depending on the proce-

dure/service owner. This allows us to specify different documentation and control policies for services with different owners; these documentation and control policies are implemented in configuration files which are switched on the fly by clients as they access services belonging to different owners.

We now present how the Certification and security overlay has been implemented in the SIAN System; the other e-government systems using it present minor modifications. The owner of all the SIAN services is the Italian Ministry of Agriculture and Forestry.

The SIAN System groups the documentation and control functions in the *DCT* module; the DCT module is made of several hardware and software devices: the central ones are all localized at the SIAN Service Centre in a server cluster, with the exception of the hardware probes and the documentation server, described below.

All the network devices of the Certification and security overlay can be programmed via configuration files to implement different service documentation and control policies and to handle different communication protocols; in the case of SIAN, we mainly have http with html or XML data but the architecture remains the same with different protocols and data.

3.1. THE DOCUMENTATION SUBSYSTEM

The documentation subsystem is mainly based on three devices:

- a *Documentation server* that archives all documentation data from centralized and peripheral systems in the SIAN Service Centre; The Documentation server is also responsible for correlating data from different organizations through a local minimal set of keys from all the organizations: the solution implemented is an Access Key Warehouse [3, 4, 5, 10];
- a software probe for the analysis of information flows on the client (SS Client), installed on all clients, that sends relevant data to the Documentation server;
- hardware probes for the analysis of information flows on the server (SS Probe) in the SIAN Service Centre, tracing all information from and to the data center; also the hardware probes send documentation data to the Documentation server

Figure 1 shows a transaction between a client and the SIAN portal; simple lines are information flows, and arrows are documentation data.

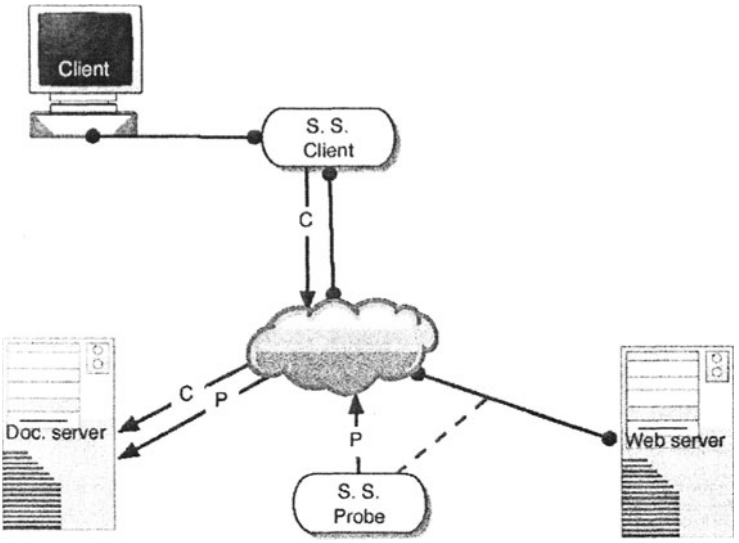

Figure 1 The documentation subsystem

3.2. THE CONTROL SUBSYSTEM

The control subsystem uses two main devices:

- on the client, the software module SS Client perform parties authentication and communication through a secure channel;
- on the server the software module SS Server is used for the same purposes; this module is installed as the first Apache or Microsoft IIS filter and intercepts and controls all service requests, and it has its own database for storing authentication data.

  As an alternative, it is possible to use tne hardware/software module SS Server Proxy before the web server to give control functionalities independently from the specific web server.

Figure 2 shows a transaction between a client and the SIAN portal; dark arrows represent information flows seen by the client and web server, whereas light ones are control flows on the secure channel; note that the control subsystem is transparent to both client and server.

3.3. OWNER POLICY SUBSYSTEM

The owner policy subsystem uses a policy server module (RCSS) for each owner; the server provides configuration files for the documentation and con-

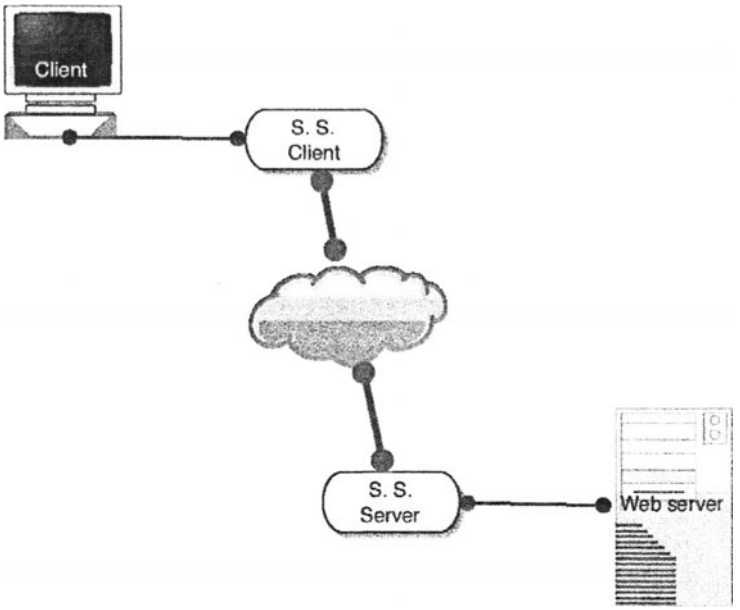

Figure 2 The control subsystem

trol devices SS Client, SS Server and SS Probe; this allows different service owners to define their own documentation and control policies, for instance defining different set of fields to be traced, or allowing encrypted communication only for specific services.

Figure 3 shows the usual transaction between a client and the SIAN portal; simple lines are information flows, and arrows are configuration files that are dynamically loaded to set the documentation and control policies featured by the documentation and security subsystems of the invoked procedure.

4. CONCLUSION AND FUTURE WORK

We have presented the main technical issues in designing and implementing e-government services, and shown that they can be partitioned into the categories of management and control; By grouping the technologies needed for the service control into an appropriate layer, the Cooperation overlay, which is independent of the possibly different technologies involved, the designer is free concentrate its efforts on the peculiarities of the service being designed. The idea has been extended to the case of systems integrating different service owners, each with its own control policies. This approach has been proved

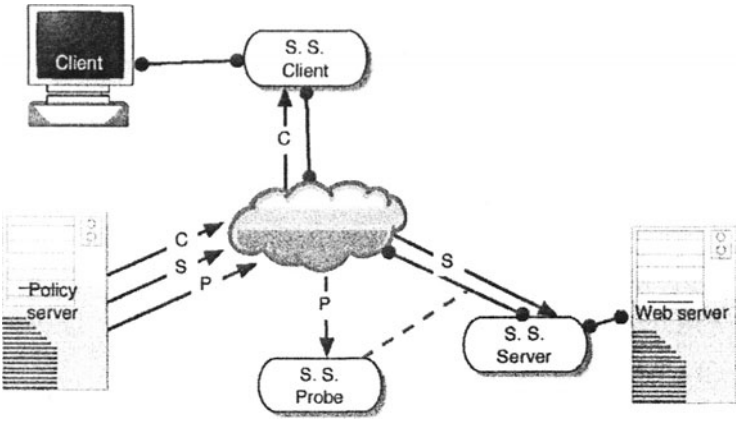

Figure 3 The owner policy subsystem

correct having been used with success for the deployment of several big Italian e-government systems since 1997.

A useful improvement to the proposed techniques would apply to the case of XML transactions, where a standardized e-government header with meta-information would greatly simplify the implementation of service documentation policies. We are currently working to define such a standard, starting with the XML procedures in the SIAN system.

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)*, Edinburgh, 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, G. Melideo, P. Naggar, E. Nardelli, and M. Talamo. A Formal Model for Data Coherence Maintenance. *Int. Workshop on Foundations of Models for Information Integration (FMII'01)*, 10th

Workshop in the series Foundation of Models and Languages for Data and Objects (FMLDO), Viterbo, Italy, Sep.01. Lecture Notes in Computer Science Vol., Springer-Verlag, 2001.

[5] F. Arcieri, E. Cappadozzi, P. Naggar, E. Nardelli, and M. Talamo. Coherence Maintainance in Cooperative Information Systems: the Access Key Warehouse Approach. Accepted for publication in the *Int. J. of Cooperative Information Systems*, 11(1-2):175–200, 2002.

[6] 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 für Informatik, Universität Magdeburg.

[7] 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.

[8] F. Arcieri, E. Cappadozzi, E. Nardelli, and M. Talamo. SIM: a Working Example of an E-Government Service Infrastructure for Mountain Communities. *Workshop on Electronic Government (DEXA-eGov'01)*, Conf. on Databases and Expert System Applications (DEXA'01), Sep.01, Munich, Germany, IEEE Computer Society Press, 2001.

[9] F. Arcieri, R. Giaccio, E. Nardelli, and M. Talamo. A Framework for Inter-Organizational Public Administration Network Services. *Int. Conf. on Advances in Infrastructure for Electronic Business, Science, and Education on the Internet (SSGRR'01)*, L'Aquila, Italy, Aug.01. IEEE Computer Society Press, 2001.

[10] F. Arcieri, G. Melideo, E. Nardelli, and M. Talamo. On the Dynamics of an Infrastructural Approach Supporting Coherence Maintenance for Inter-Organizational Collaboration. *Int. Symp. on Business Strategy Based Software Engineering (SoftwareTrends'01)*, Sept.01, Gersau, Switzerland, NetAcademy Press.

[11] F. Arcieri, G. Melideo, E. Nardelli, and M. Talamo. Experiences and Issues in the Realization of E-Government Services. *Int. Workshop on Research Issues in Data Engineering (RIDE'02)*, San Jose, Ca., USA, Feb.02, IEEE Computer Society Press, 2002.

[12] A. Bouguettaya, M. Ouzzani, B. Medjahed, and J. Cameron. Managing Government Databases. *Computer*, 34(2):56–64, Feb.01.

[13] A.K. Elmagarmid, and 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.

[14] J. Joshi, A. Ghafoor, W.G. Aref, and E.H. Spafford. Digital Government Security Infrastructure Design Challenges. *Computer*, 34(2):66–72, Feb.01.

[15] M. Talamo, F. Arcieri, G. Conia. Il Sistema di Interscambio Catasto-Comuni (parte I). *GEO Media*, vol.2, Jul-Aug 1998, (parte II), *GEO Media*, vol.2, Sep-Oct 1998, Maggioli Editore, Roma (in italian).

[16] 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, Jul.99, Lecture Notes in Computer Science vol.1651, 360–364, Springer-Verlag.

[17] How to connect municipalities to the applicative backbone of the National Census Index.
`http://cedweb.mininterno.it:8092/autonomie/saia/ina29102001.html`