A layered IT infrastructure for secure interoperability in Personal Data Registry digital government services

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

1. NESTOR - Laboratorio Sperimentale per la Sicurezza e la Certificazione di Servizi Telematici Multimediali - Univ. of Roma "Tor Vergata", Roma, Italia.
2. Dipartimento di Informatica, Univ. of L'Aquila, L'Aquila, Italia.
3. NESTOR, Univ. of Roma "Tor Vergata", Roma, Italia, & Istituto di Analisi dei Sistemi ed Informatica, C.N.R., Roma, Italia. nardelli@nestor.uniroma2.it. CONTACT AUTHOR.

Abstract

In this paper we describe the architectural solution defined and implemented to ensure secure interoperability among Information Technology (IT) systems managing Personal Data Registries in Italian Municipalities and Ministry of Interior. The architecture features a clear separation between security services, provided at an infrastructure level, and application services, exposed on the Internet as Web Services. This approach has allowed to easily design and implement secure interoperability, since - notwithstanding the huge variety of IT solutions deployed all over the Italian Municipalities to manage Personal Data Registries - existing application services have not required major changes to be able to interoperate.[1]

Keywords: digital government support, security of e-services, technologies and infrastructures for e-services, legacy application interoperability.

1 Introduction

Digital government services [18] is one of the most delicate areas in the whole field of Web Services. In fact, it seems to be "just another kind of e-service", but since it is dealing with critical issues of people identification and people rights, a peculiar set of requirements has to be satisfied.

In the recent IEEE Computer's special issue on Digital Government [18] the article on "Digital Government Security Infrastructure Challenges" [21] literally says: "Among all government functions, maintaining collective security remains the most crucial element, requiring that security concerns be addressed at each level of the government's information infrastructure". One of the key challenges there identified is "ensuring secure interoperability among systems from several agencies".

In particular, the phase of citizens' identification deserves special attention, since its correctness is the leverage point for a successful realization of all digital government services. Failure in properly running this phase may result, beyond the impossibility to provide the planned service, in a dispersion of highly sensitive identity data, thus making even easier one of the IT crimes with the highest rate of increase: the identity theft, which has become so spread that the Federal Trade Commission (FTC) has established a web site devoted to it [27].

It is therefore necessary that access to people's personal data is provided with the best possible security levels and with the highest quality in accuracy of information provided. When the service needs to be provided on a country-wide base, a further obstacle is posed by the fact that, generally, responsibility for citizen's personal data is given to local government authority.

With the increasing tendency - in more technologically advanced countries - towards federal forms of government, this kind of situation is becoming more and more common. The distribution of responsibility clearly makes the overall IT solution more difficult to identify, since it has to be not only technically good but also respectful of each institution's authority, competence, and organizational structure.

In this paper we describe the architectural solution we have identified and adopted in Italy to deal with and successfully manage this subject, developed during a multi-year cooperation between the Italian Ministry of Interior and the NESTOR Laboratory of the University of Rome "Tor Ver-

[1]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"

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

gata". The Central Directorate for Demographic Services of the Ministry of Interior started the whole initiative, as part of its institutional mission, and has the organizational leadership of activities. The NESTOR Laboratory is responsible for the definition of technological solutions and University of Rome "Tor Vergata" has the technical leadership of activities. Municipalities contributed to the definition of end-user requirements and ANCI, the Association of Italian Municipalities, by means of ANCITEL, its IT subsidiary, is contributing to the deployment of the system all over the italian territory.

The work here described is only a portion of what is currently under development in Italy in the field of digital government. The initial development of many of these initiatives has been sponsored and supported within the organizational mission of AIPA ("Autorità per l'Informatica nella Pubblica Amministrazione"), the Italian Authority for IT in Public Administration [22].

The paper is structured as follows. Firstly, in section 2, we present the reference scenario for the management of people's personal data in Italy. Then, section 3 discusses problem requirements and possible approaches to deal with them. Next, in section 4, we discuss the adopted solution from an organizational viewpoint, and in section 5 the IT architecture supporting it. Section 6 discusses our solution in comparison with related work and argues about the innovation character of our solution. Finally, section 7 concludes the paper.

2 The Italian scenario for management of citizens' personal data

Italian laws give the responsibility for keeping records of, managing, and certifying citizens' personal data to Municipalities. They maintain an archive of people having established residence within the Municipality's territory (APR = Anagrafe della Popolazione Residente) and an archive of former resident people having now established residence outside Italy (AIRE = Anagrafe degli Italiani Residenti all'Estero).

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: in the case the residence is established outside Italy, a record is inserted into Municipality's AIRE.

The Ministry of Interior has - among its institutional duties - the overall responsibility for the correct maintenance of Personal Data Registries (APR and AIRE) in all Italian Municipalities. It is important to note the huge variety in size and complexity of these archives (whose vast majority is now IT-managed), 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. The Italian National Institute of Statistics (ISTAT) has also a control responsibility on these archives for statistical purposes and on their alignment with the outcome of national census.

In many administrative processes regarding citizens managed by a Public Administration (PA) there is the need, for the organization managing the process, to obtain a certified declaration relative to citizen's personal data[2]. Clearly, for facts regarding birth place and date, residence and civil state, this is responsibility of the Municipality where a person has established the residence. In a recent survey conducted during the preliminary study phase of the work reported in this paper, more than 25 distinct administrative processes have been identified, involving more than 15 Italian PAs, where there was the need, for the PA managing the process, to obtain or verify citizens' personal data.

To complete the reference scenario, and to stress its complexity, note that, by law [29], in Italy all communications relative to persons happening between PAs or between private institutions and PAs have to use the so-called "fiscal-code" for citizen's identification. The responsibility for assigning a unique fiscal code to each person is given by law to the Ministry of Finance. The fiscal code is generated on the basis of a known algorithm, and this has greatly supported its use as access key for people's personal data in Municipality DBMSs, independently from its actual production by the Ministry of Finance. But since the algorithm may produce the same fiscal code for different individuals and the resolution of collisions is responsibility of the Ministry of Finance, it is clear the this organization is the only one enabled to certify the correct value of a citizen's fiscal code.

3 Requirements

It is apparent from the scenario described in previous section that there is in Italy a large distribution of responsibilities among many organizations of widely different sizes for the management of citizens' personal data. Hence, technological solutions have to take into account this peculiar aspect.

Moreover, databases containing people's personal data are subject to a severe privacy legislation, forbidding to any public or private organization to set-up and maintain - even

[2] Note that, even if recent laws have offered the possibility to citizens to self-certify data regarding their person - thus relieving people from the need of obtaining in advance official certification from the administration in charge - still there is the need of checking citizens' self-certification

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

temporarily - databases storing personal facts about people unless this is done to discharge a precise obligation settled by law. Also, any maintenance and processing operation on databases storing people's personal data has to be traced both in terms of the operating machine executing it and of the user controlling it.

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.

The path followed in Italy was therefore one to require mechanisms enabling the distribution of updates to people's personal data between Municipalities and other PAs. These mechanisms needed obviously to be implemented by means of IT systems. Clearly, given the above recalled prescriptions of the Italian privacy law, certainty of the source authority for exchanged data and security of communication are requirements of paramount importance.

From the IT point of view, the issue is therefore how to ensure, in the above described framework of many geographically dispersed organizations with various level of responsibilities and many different kinds of IT systems, a secure distribution of updates to people's personal data towards all the interested institutions and how to provide, at the same time, reliability regarding the source of data.

Required security functions are the standard basic ones:

- confidentiality: none on the network beyond the communicating parties has to receive data they have exchanged;
- integrity: the destination has to receive exactly the data the source intended to send it;
- source authentication: the destination has to be sure that who is sending the data is the intended source;
- destination authentication: the source has to be sure that who is receiving the data is the intended destination;
- users and machines at the sites of both the communicating parties have to have the prescribed authorization;
- all exchanges of relevant data have to be traced for documentation and certification purposes, to be able to identify, in case of any failure, who was able to properly discharge his/her obligations.

Note that a critical point regarding the above functions is that there is the need of clearly distinguishing data relevant for security functions from data needed for a correct execution of the administrative processes. Too often, in fact, applications dealing with office procedures have to improperly manage also some of the security functions (e.g., authentication and authorization): the result is a bad mix-up between data serving different purposes, making maintenance of these applications more complex and exposing them to higher risks of introducing security flaws.

An example is an application for on-line tax payment, where IT system identification information (that might be provided by the user through a smart-card) should be managed at a different level from fiscal system identification information (that might be keyed in by the user and might even be referring to a different physical subject).

Any technical solution, moreover, had to be implementable even by small Municipalities without disrupting their work organization and their IT systems and strategies. More than the pure financial cost of whichever IT solution one could devise, in fact, the real obstacle in our case for its true uptake is its organizational impact in the long run. One-time money for some extraordinary financing could often be found, but the real problem is that after the initial phase each institution has to be able to stand up on its own resources.

4 INA and CNSD: the Organizational Component of our solution

The approach taken in our case has been conceptually based on an architectural solution the NESTOR Laboratory of the University of Rome "Tor Vergata" had devised while working on similar issues in the context of the interaction of PAs: the so-called Access Keys Warehouse [2, 3, 4, 11] (AKW, for short). By following the AKW approach we could define and implement IT systems able to keep aligned data referring to the same reality of interest but stored and managed in different and independent PAs, without violating their organizational and technical autonomy [1, 5, 6, 7].

Hence, for this case dealing with people's personal data, the organizational component of our solution defined a single access index to the Municipality responsible for one's personal data (INA = Indice Nazionale delle Anagrafi). This index, whose institution was established by a supplement [31] to the ordinary law regulating the Personal Data Registries kept in Municipalities [30], 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.

Therefore, INA is not a central database of the Italian population but simply a provider of the reference to the place where information about a specific person can be

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

found and a means of ensuring overall coherence of the distributed system.

All Municipalities are obliged to communicate to INA any change of established residence for any person in its own territory, and INA keeps under control the overall coherence of Personal Data Registries by rising exceptions whenever an incoherence is detected (e.g.: an Italian citizen, not previously known, establishes her residence in a Municipality, or a person establishes a new residence in a Municipality but is current established residence is not deleted).

All PAs needing to know or to validate personal data about a given person can first access INA to know which is the responsible Municipality and then obtain directly by such a Municipality required data. In such a way an organization can keep its internal databases up-to-date with respect to changes happening in the real-life (e.g., the agency providing social security services can always send pension checks to the correct address and stop sending them when the pension check receiver dies) without violation to the privacy legislation.

Clearly, since INA is the "leverage point" for the coherence maintenance of the overall distributed system, it is then absolutely necessary to guarantee accuracy of its stored data. Therefore, before the insertion in INA of any piece of information about a person by a Municipality, all elementary components of personal data about such a person have to be verified.

This is easy for what regards the personal data components (e.g., name, birthdate, ...), since this is competence of the Municipality itself, but for the fiscal code component, this requires an interaction with the Ministry of Finance to verify the current value of fiscal code stored in a Municipality's database and eventually obtain the correct one.

This "data cleaning" activity of information contained in a Municipality's database is a very critical step, like it often happens when operating a reconciliation on data coming from different sources [28]. In our case, the about 10-20% of data referring to the same subject in the reality of interest but differently recorded in different organizations, have been cleaned by means of direct human checking, executed by Municipalities. Since our system is based on the AKW approach [2, 3, 4, 11], there is the guarantee that in the future data elements will keep their alignment, hence this is a one-time cost.

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 [32]. 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.

The presence of CNSD means that the logical topology of communication is star-shaped, in the sense that there is not a physical exchange of messages directly between two Municipalities (e.g. when a person moves her established residence from a Municipality to a different one), or between a PA and a Municipality (e.g. when the Ministry of Health wishes to check a person's established residence), but CNSD is the control center ensuring official character to these requests.

5 INA Backbone: the Technological Component of our solution

On the Information Technology level, our approach is rather different from the standard ones in the same application field: in a layered description of our architecture we place security services in a layer, called *INA Backbone*, clearly distinguished both from the communication and the application ones.

That is, we do not deal with security functions within application, but consider them as infrastructure services, much in the same way communication services are nowadays considered: from the application viewpoint, in fact, details regarding how messages are transported along the communication network up to their destination are completely transparent. In the same way, applications in our architecture do not take care of the management of security functions described in section 3, which are instead provided by an independent layer 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 [15, 20], DNSsec [17]) 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.

Also, due to the critical nature of functions provided by security services, these cannot be set-up in a completely dynamic way, but have to be established only after some kind of agreement among involved organizations is formally in place. This aspect was a further motivation for our choice

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

of putting security services in a layer fully independent from the application one.

The INA Backbone therefore contains the following functional subsystems:

- confidentiality and integrity services
- authorization service
- authentication service
- documentation subsystem
- access policy management
- quality of service monitoring

We now give some detail on the functions executed by the subsystems in the INA Backbone and how they have been realized.

Confidentiality and integrity services Protection of exchanged messages against eavesdropping and guarantee of their integrity are provided through a mechanism resembling the behaviour of SSL/TSL. TCP packets are encrypted before transmission using symmetric cryptography based on session keys. These are generated anew for each session and exchanged between communicating parties using asymmetric cryptography.

A part of a Municipality's private key is distributed by CNSD to the Municipality itself by means of the internal registered mail of the Ministry of the Interior. Once this part of a Municipality's private key is arrived at the destination site, the confidentiality and integrity subsystem at the site has to be activated. This is discussed in the paragraph below on authorization service. After the activation the local and remote modules of the confidentiality and integrity subsystem are fully operational.

Authorization service This subsystem takes care of the initial set-up of functions in the security layer. On the basis of the part of the private key distributed by CNSD an exchange of encrypted messages between the local subsystem and a central control server happens, aiming at registering the local subsystem at the central control server. Hardware identifiers of the communicating machines are exchanged during this phase, so that it is possible to uniquely identify physical sites having the right to access the communication network. After the successful completion of this registration procedure the site is activated and is thus authorized to exchange messages using its private key that is now complete and bound to registered end-user(s) and registered machine(s).

Authentication service Guarantee of the identification of source and of destination of messages is implemented by having local and remote modules of the authentication subsystem exchange messages in a "tunneled" way. That is, an end-to-end communication tunnel is established having as its endpoints the local and the remote modules of the authentication subsystems: tunnel is implemented by encrypting TCP packets and placing them as the payload of IP packets addressed to the other endpoint of the tunnel. Once again, encryption is executed using symmetric cryptography based on session keys, securely exchanged using private keys. In such a way, whenever IP packets arrive at the destination endpoint, only the ones coming from the other authenticated endpoint are accepted, while all the remaining ones are discarded.

Documentation subsystem A dedicated subsystem of the INA Backbone has the task of recording all application-level messages exchanged between authorized access points of the communication network, so that documentation can be produced, if needed, on which data was actually exchanged. In fact, since communications related to personal data are often executed to discharge legal obligations, it is important the overall system is able to document, when a problem is later found, if and when communications where sent and received.

The documentation subsystem is based on an architecture using network probes at the access points to communication network to record actual application-level messages exchanged. This solution has been extensively described elsewhere [7, 12, 13]. Here we only recall that it is able to work without needing any change to existing applications, it is based on picking-up and filtering selected IP packets from the networks and reconstructing application-level flow of exchanged messages, and it is based on highly efficient algorithmic solutions [23], hence scalable and with a very low overhead.

Access policy management At CNSD site it is possible to define and enforce the desired policy for access management. In fact, both authorization and documentation services are fully parameterized, hence it is possible, from the central control point to implement various control policies for accesses to the system.

Remote end-users can be given read-only rights to INA, query rights towards Municipalities, publication rights toward other selected end-users, write rights to INA (this always under the ultimate responsibility of CNSD). After the initial set-up and registration phase of the access point (see above paragraph on authorization service), in fact, end-users' actual rights can be dynamically established by means of a communication between the local and the central modules of the access policy management subsystem.

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

Quality of service monitoring Since in the digital government service framework very often a legal value is attached to information exchanged, it is not possible to use, for quality of service measuring and monitoring, estimation based approaches, where sophisticate techniques have been proposed for accounting and billing [16, 19]. The same motivation prevents the use of flow statistics like those being provided by Cisco NetFlow [26]. Hence, from the network traffic monitoring viewpoint, a new kind of application level measurement techniques is required.

For our purposes, in fact, we need to measure and to certify actual performance of service flows which spread in the network in consequence of an end-user's request. To obtain precise measurements, it is then needed to record the actual behaviour in the network of IP packets corresponding to service flows. To the best of our knowledge no solution for the problem of actual performance measurement of distributed e-services is known in the literature beyond ours: our solution is based on the same technique used to provide documentation services (see paragraph above) and is described in more detail in [8, 9].

6 Discussion and Related Work

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

The single functional components we have used to build the INA 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 e-services based on the interoperability of legacy systems.

In our vision, security functions in e-services have to be based on a permanent infrastructure layer, since this is the only approach able to guarantee, at a reasonable cost, efficiency of e-service provision and effectiveness of security in an open and intrinsically insecure environment like the Internet.

It is important to stress that in the real world of non-electronic services and whenever some kind of contractual responsibility is involved, security functions are always based, to various degree, on some form of permanent infrastructure. For example, public utilities like power supply, water, and sewage are provided by Municipalities to houses on the basis of the house ownership or renting. People interacts with banks in buildings and offices clearly and permanently identifiable as bank settings (even ATMs are usually placed in trustable environments). Also the currently most widespread e-service among the ones where trust is a fundamental aspect, that is e-banking, is based on an initial set-up phase where a security infrastructure is established: the person goes physically to branch offices to sign the contract and to receive codes and other eventual instructions to access the service on the Internet.

A further important point regarding security in interaction between institutions (as opposed to interaction among people) is that 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.

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, ...).

A large amount of technology is available dealing with many issues related to security for the Internet (just see [14, 24] for two very recent treatments of the subject) and research activity is still very high with many conferences discussing more advanced security topics. The most noteworthy technological components are the many kinds of firewalls (under their various form of packet, circuit, and application firewalls - and the more advanced versions with stateful and dynamic filtering), the solutions to set-up Virtual Private Networks, the various kind of systems for Intrusion Detection and the Infrastructures for Public Key based security functions.

Also, advances in lower level protocols for communication (e.g. IPv6 [15, 20]) will hopefully result in a widespread intrinsically secure communication infrastructure. For the time being, though, relying on the availability of IPv6 compliant systems and applications to provide secure e-services does not constitute a solution that in general works.

Analogously, it may well be that PKI-based approaches to interorganizational security infrastructures, like the "bridge certification authority" [25], will ultimately lead to efficient and cost-effective solutions for secure interoperability. But concerning solutions that can be implemented and used right now, we can quote conclusions from [25] itself: "In practice, our ability to construct these complex PKIs has surpassed the functionality provided in COTS desktop applications, especially in the areas of path discovery and validation". Thus it seems that these approaches, while promising, are not yet fully mature.

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 IEEE

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 thinks it may contribute to spread further the use of e-services for those areas where security is a primary concern.

A further advantage of our architecture is that our approach to build the private key as the combination of one part bound to the machine and one part bound to the end-user allows to build for a same organization different private keys for accessing different services from the same machine. It suffices to change the part of private key which is bound to the end-user. In such a way an organization will have different authorizations for accessing different services, at it has to be.

The infrastructure thus allows to the same end-user to use the same machine to access all and only the services for which the corresponding part of the private key has been received, using for each service a different private key. In this way a great flexibility is obtained since the infrastructure can support the provision of new distinct services without requiring any change.

In Italy, this architecture is currently being used to provide basic security functions in the deployment of Electronic Identity Card (CIE = Carta d'Identita' Elettronica). CIE project is in the first stage of releasing 1,5 million cards by the end of 2004. A second project (CNS = Carta Nazionale dei Servizi) aiming at deploying a personal electronic card to provide e-services to citizens also provides for connection to CNSD to verify and validate people's personal data.

7 Conclusions

In this paper we have described our architectural solution to provide security functions in the deployment of a distributed e-service dealing with legacy system managing Personal Data Registry in Italian Municipalities and Public Administrations.

Our solution can be deployed without relying on advanced security technologies like IPv6 and without needing any update or change to existing systems and applications.

The various functional subsystems used in our solution, called the INA Backbone, provide end-to-end security in the interaction among distributed access points and constitutes an addition, not a replacement, of security solutions deployed locally.

The baseline of our approach is that security services have to be part of an infrastructure layer of inter-organizational communication, to be placed between the (lower) communication service layer and the (higher) application service layer. Only in this way is possible to provide at reasonable cost efficiency of service provision and effectiveness of security functions.

References

[1] F.Arcieri, C.Cammino, E.Nardelli, M.Talamo, 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, E.Cappadozzi, G.Melideo, E.Nardelli, P.Naggar, 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.

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

[5] F.Arcieri, E.Cappadozzi, E.Nardelli, 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.

[6] F.Arcieri, E.Cappadozzi, E.Nardelli, 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, 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.

[8] F.Arcieri, F.Fioravanti, R. Giaccio, E.Nardelli, M.Talamo: Certifying performance of cooperative services in a digital government framework. *Int. Symposium on Applications and the Internet (SAINT-03)*, Orlando, Fl., USA, Jan.03, IEEE Computer Society Press, 2003.

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 **IEEE**

[9] F.Arcieri, F.Fioravanti, E.Nardelli, M.Talamo: Inter-organizational E-Services Accounting Management. *3rd IFIP conference on e-Commerce, e-Business, and e-Government (I3E-03)*, Sao Paolo, Brasil, Sep.03, Kluwer Academic Publishers, 2003.

[10] F.Arcieri, R.Giaccio, E.Nardelli, 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.

[11] F.Arcieri, G.Melideo, E.Nardelli, 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.

[12] F.Arcieri, G.Melideo, E.Nardelli, 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.

[13] 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.

[14] W.R.Cheswick, S.M.Bellovin, A.D.Rubin. Firewalls and Internet Security: Repelling the Wily Hacker, 2nd edition. Addison-Wesley, 2003.

[15] 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`.

[16] N.Duffield, C.Lund, M.Thorup. Charging from sampled network usage. ACM-SIGCOMM Internet Measurement Workshop (IMW'01), San Francisco, Ca., USA, Nov.01.

[17] D.Eastlake. Domain Name System Security Extensions. RFC 2535. Internet Engineering Taks Force. Mar.99. `http://www.rfc-editor.org/rfc/rfc2535.txt`.

[18] 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.

[19] C.Estan, G.Varghese. New directions in traffic measurement and accounting. ACM-SIGCOMM Internet Measurement Workshop (IMW'01), San Francisco, Ca., USA, Nov.01.

[20] 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`.

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

[22] M.Mecella, C.Batini. Enabling Italian E-government through a cooperative architecture. *IEEE Computer*, 34(2):40–45, Feb.01.

[23] E.Nardelli, M.Talamo, and P.Vocca. Efficient searching for multidimensional data made simple. *7th Annual European Symposium on Algorithms (ESA'99)*, Prague, Czech Republic, Jul.99, Lecture Notes in Computer Science vol.1643, pp. 339–353, Springer-Verlag.

[24] S.Northcutt, L.Zeltser, S.Winters, K.K.Frederick, R.W.Ritchey. Inside Network Perimeter Security. New Riders Publishing, 2003.

[25] 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.

[26] Cisco NetFlow, `http://www.cisco.com/warp/public/732/Tech/nmp/netflow/`

[27] `http://www.ftc.gov/idtheft`

[28] IEEE TCDE Bulletin, Special Issue on Data Cleaning, 23(4), Dec.2000.

[29] Law n.63, 17/mar/1993.

[30] Law n.1228, 24/dec/1954.

[31] Law n.26 28/feb/2001.

[32] Ministerial Decree of 23/apr/2002 of the Ministry of Interior.

Proceedings of the 14th International Workshop on Research Issues on Data Engineering: Web Services for E-Commerce and E-Government Applications (RIDE'04)
0-7695-2095-2/04 $20.00 © 2004 **IEEE**