THE ITALIAN ELECTRONIC IDENTITY CARD: OVERALL ARCHITECTURE AND IT INFRASTRUCTURE

Franco Arcieri[1], Mario Ciclosi[2], Andrea Dimitri[1], Fabio Fioravanti[1,3], Enrico Nardelli[1] and 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]*Direzione Centrale per i Servizi Demografici - Ministero dell'Interno, Roma, Italia.*

[3]*Dipartimento di Informatica, Univ. of L'Aquila, L'Aquila, Italia.*

Abstract

In this paper we describe the overall process of deployment of the Italian Electronic Identity Card: the way it is issued, services it is used for, 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. Organizational complexity lies in the distribution of responsibilities for the management of Personal Data Registries (on which identity of people is based) which is an institutional duty of the more than 8000 Italian municipalities, and the need of keeping a centralized control on all processes dealing with identity of people as prescribed by laws and for national security and police purposes. 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 fulfilment 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. 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.

Keywords: IT-Enabled Government Operations

1. Introduction

One of the greatest challenges of digital government research, consists in allowing citizens to access digital government services, while ensuring the best possible security levels both to service providers and to citizens. Guaranteeing security during provision of digital government services is of the outmost importance [ElMI01, JGA$^+$01] as it deals with people identity and rights, and is essential for maintaining collective security.

The success of all digital government services strongly depends on how citizens' identification is performed. Indeed, in case of failure of the mechanisms used for identification of citizens, not only it may become impossible to provide a given service, but there could be a leak of highly sensitive identity data, thus making it easier to steal someone else's identity. This crime, known as identity theft, is becoming more and more common on the network.

The solution which is being followed in Italy for identifying citizens accessing digital government services is based on the Electronic Identity Card.

The Electronic Identity Card (EIC, for short) is a polycarbonate smart card equipped with a microchip (supporting cryptographic functions), and a laser band (featuring an embedded hologram). It contains personal (e.g. name, surname, date of birth,. . .) and biometric data (photo and fingerprint) of a citizen.

The EIC can serve two different purposes: (i) it can be used as a replacement of the paper based ID-card, and (ii) can be used as an authentication credential, allowing access to network enabled government services. For example, citizens could use their EIC for accessing a municipality's web site allowing them the following operations: 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 EIC, 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.

In this paper we describe the architectural solution we have identified and adopted in Italy to manage the process by which Electronic Identity Cards are issued to citizens. Many organizations are involved in this project: the Italian Ministry of Interior has the ownership and management of the overall project, University of Rome "Tor Vergata" is the technical coordinator of the project, the Italian mint, Istituto Poligrafico e Zecca dello Stato (IPZS), manufactures and initializes EICs, the Central Directorate for Demographic Services of the Ministry of Interior (CNSD) is responsible for validating personal data to be written on EICs, and the security system of the EICs architecture, Sistema di Sicurezza della CIE (SSCE), generates keys used for activating EICs and is responsible for guaranteeing security during the formation of data and issue of EICs.

The problem of guaranteeing security in complex services, gets harder when independent agencies play different roles in service provision, as it happens with EIC. In these cases, the responsibility for correctness of service provision is distributed among all organization involved in the process. At the same time, it extremely important to be able to identify culprits of failure in service provision, as often there is a legal and economic value associated to a service. As already pointed out, in the EIC specific case, any information leak can compromise individual as well as collective security.

Any technical solution which is to be used for ensuring secure interoperability among systems from independent organizations, should feature low invasiveness with respect to locally deployed technological solutions and organizational policies.

The paper is structured as follows. In Section 2, we present the reference scenario and requirements for issuing Electronic Identity Cards in Italy. Then, in Section 3, we discuss the adopted solution from an organizational viewpoint. Next, in Section 4 we describe the deployment of the architecture for the Italian Electronic Identity Card, and in Section 5 we describe our approach to security services provision.

2. Management of Personal Data in Italy

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) 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 the overall responsibility for the correct maintenance of Personal Data Registries (APR and AIRE) 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 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. 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.

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 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.

In moving from a paper-based ID card to an electronic one it was therefore required to define IT-based mechanisms ensuring to the highest degree all IT security functions (confidentiality, integrity, source and destination authentication, authorization, non-repudiation) in the interaction between Municipalities and the Ministry of Interior, and supporting the auditing of interactions. These IT-based mechanisms have to enable the distribution of updates to people's personal data between Municipalities and other PAs, and to ensure certainty of the source authority for exchanged data and security of communication.

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.

Any technical solution, moreover, had to be implementable even by small Municipalities without disrupting their work organization and their IT systems and strategies. Indeed, the real obstacle for the true uptake of whichever IT solution one could devise is not the financial cost, but is the organizational impact both in the short term and in the long run.

3. INA and CNSD

Our approach has been conceptually based on an architectural solution, the so-called Access Keys Warehouse [ACM$^+$01, ACN$^+$99b, ACN$^+$02, AMN$^+$01] (AKW, for short) which was devised while working on similar issues in the context of the interaction of PAs. The AKW approach allows to define and implement IT systems able to keep aligned data referring to the same reality of interest but stored and managed in different and independent PAs, without violating their organizational and technical autonomy [ACN$^+$99a, ACN$^+$01a, ACN$^+$01b, ACN$^+$01c].

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 [Law26] to the ordinary law regulating the Personal Data Registries kept in Municipalities [Law1228], 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 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.

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 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 [TCDE00]. 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 [ACM$^+$01, ACN$^+$99b, ACN$^+$02, AMN$^+$01], 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 [MD02]. 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.

4. The Architecture for the Italian Electronic Identity Card

In the first phase of deployment of the EIC, 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 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 EIC architecture has already started. The target of this second phase is to provide the 56 municipalities involved with 1.500.000 EICs, and to issue them by the end of year 2004 thus satisfying the local demand for ID cards. 400.000 EICs have been issued to citizens by the end of October 2004.

The overall financial effort sustained by the italian government for all the various design, testing and experimentation phases has been, up to the end of 2004, about 70 millions Euros.

We recall that, by Italian laws, municipalities are the only organizations which are responsible for issuing EICs to citizens. In particular, they form personal and biometric data to be written on the EIC and subsequently activate the EIC itself. However, in order to complete the process of issuing an EIC, several activities must be performed by other institutional organizations, possibly by interacting with municipalities.

The main activities performed during the deployment of the EIC architecture and during the issue of the EIC are described below.

Fiscal code coherence. This activity is performed in order to establish coherence between data held by Personal Data Registries at municipalities, which contain essential data needed for issuing identity cards, and data owned by the Ministry of Finance, which is the unique responsible for releasing fiscal codes to citizens. Ensuring validity of a citizen's fiscal code is especially important as, by law [Law63], it must be used in all communications with PAs for univocally identifying a fiscal subject.

INA setup and operation. This activity involves the creation and the management of a central archive, located at the Ministry of Interior, containing synthetic information about the relationship between citizens' personal data and the municipalities which are responsible for managing citizens' data. The INA archive is consulted by various organizations during the emission of an EIC for certifying the correctness and the validity of personal data to be written on it. The INA architecture is described in detail in Section 3.

Manufacturing and initialization of EIC. The Italian mint, IPZS, manufactures EICs by assembling its components and initializes them by setting up the microchip and the laser band. Moreover, IPZS initializes each card by writing on it a nation-wide unique code, provided by the Ministry of Interior. Municipalities perform requests to IPZS for lots of "blank" EICs. IPZS, upon receiving such formal offline request, contacts the SSCE for an authorization decision. Only after successful approval of the request by SSCE, IPZS delivers EICs to the requesting municipality.

Appliances setup at municipalities. During this activity, municipalities are equipped with special purpose hardware and software appliances which are needed for issuing EICs to citizens and for ensuring security in communication with interacting parties.

Personal and biometric data acquisition. Municipalities can acquire citizens' personal data either by using a web-based application or by standard offline procedures performed at the municipalities' offices. In both cases, information supplied by the requesting citizen is checked for validity against INA's data.

In case of acquisition of personal data via a web-based application, the municipality's system verifies coherence with personal data present in its database. If all validity checks are successful, the system makes a date with the citizen for completing the request at the municipality's offices. Otherwise, an error message is returned to the requesting subject.

Instead, biometric data, like photos and fingerprints, can only be acquired at the municipalities' offices.

Data formation and exchange. This activity involves secure data exchange between a municipality and SSCE, as well as formation of data to be written on the different parts of EICs (microchip, laser band and polycarbonate support) which are essential for enabling access to e-government services.

In particular, by using a special-purpose cryptographic software, municipalities generate for each EIC a certificate request in the PKCS#10 format containing personal and biometric data of the requesting citizen. Then the certificate request is sent to SSCE, which performs validity checks on the information provided, possibly by contacting other services, like INA for example. If all checks are successful, SSCE returns a certificate to the requesting municipality, signed with its private key. Of course, for reasons of efficiency, certificate requests can be sent in lots.

EIC release. Upon receipt of the certificate, the municipality is ready to release the EIC to the requesting citizen, along with a closed envelope containing a special sheet with the EIC keys printed on it, which are necessary for using the EIC for accessing digital government services and for revoking the EIC in case of theft.

Currently, there exist two procedures which can be used for issuing an EIC: (i) the "on-line" procedure, and (ii) the "off-line" procedure.

When following the "on-line" procedure, all activities required for issuing the EIC, except initialization, are performed "on line", while the citizen is waiting at the desk of the Personal Data Registry office of the municipality, as described above.

During the "off-line" procedure, some of the activities required for issuing EICs are performed by a third party, the Service Center (SC), which is typically an organization constituted by neighbor federated municipalities providing services in various fields to people living in the same region.

The Service Center is thus a new actor taking part in the issue of the EIC, as described below, with specific liabilities towards Municipalities and SSCE.

The SC receives from municipalities, personal and biometric data of citizens which requested the EIC, in univocally identified lots. Then, it performs a first validity check of personal data against INA. If this check is successful, the SC uses data provided by the municipality to generate a certificate request, performing the data formation and secure exchange activity described above. However, differently from what happens during the on-line procedure, SSCE returns a certificate whose status is "suspended". When the citizen goes back to the municipality's office for obtaining the EIC, the operator verifies that personal and biometric data on the EIC correspond to those of the requesting subject and, again, that it is coherent with INA's data. Then, if information on the card is valid, the operator changes the state of the certificate from "suspended" to "active"; at the same time the status of that EIC is set to "active" on the SSCE's database. Finally, the EIC is released to the citizen.

5. The Security Backbone

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 *Security 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, 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, DNSsec) 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 of putting security services in a layer fully independent from the application one.

The Security Backbone therefore 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.

We now give some detail on the functions executed by the subsystems in the Security 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.

Authorization service. This subsystem takes care of the initial set-up of functions in the security layer. 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. 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.

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.

Documentation subsystem. A dedicated subsystem of the Security Backbone [ACN+01c, AMN+02a, AMN+02b], 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.

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.

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.

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 [AFG+03, AFN+03].

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 single functional 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 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, . . .).

Also, advances in lower level protocols for communication (e.g. IPv6) or PKI-based approaches to interorganizational security infrastructures 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 thinks it may contribute to spread further the use of digital government services for those areas where security is a primary concern.

6. Conclusions

In this paper we have described the deployment of a distributed digital government architecture dealing with the issue of Electronic Identity Cards in Italy.

We have presented 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.

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

[ACN$^+$99a] 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.

[ACM$^+$01] 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.

[ACN$^+$99b] 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.

[ACN$^+$02] 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.

[ACN$^+$01a] 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.

[ACN$^+$01b] 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.

[ACN$^+$01c] 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.

[AFG$^+$03] 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.

[AFN$^+$03] 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.

[AGN$^+$01] 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.

[AMN$^+$01] 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.

[AMN$^+$02a] 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.

[AMN$^+$02b] 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.

[ElMI01] 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.

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

[NTV99] 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.

[TCDE00] IEEE TCDE Bulletin, Special Issue on Data Cleaning, 23(4), Dec.2000.

[Law63] Law n.63, 17/mar/1993.

[Law1228] Law n.1228, 24/dec/1954.

[Law26] Law n.26 28/feb/2001.

[MD02] Ministerial Decree of 23/apr/2002 of the Ministry of Interior.

PROBLEMS RUNNING UNTRUSTED SERVICES AS JAVA THREADS

Almut Herzog
Dept. of Computer and Information Science
Linköping University, Sweden
almhe@ida.liu.se

Nahid Shahmehri
Dept. of Computer and Information Science
Linköping University, Sweden
nahsh@ida.liu.se

Abstract A number of Java environments run untrusted services as Java threads. However, Java threads may not be suitably secure for this task because of its problem with safe termination, resource control and thread isolation. These problem areas have been recognised by the research community and are comprehensively addressed in the not yet implemented Java Isolate API. Meanwhile, Java threads continue to be used for running untrusted code.

This paper examines the risks associated with Java threads that run untrusted code and presents existing research solutions. Requirements for a secure execution environment are presented. The requirements are contrasted by recommendations and problems when using Java threads for running untrusted code.

Keywords: Java, server, security, thread, untrusted code, termination, requirements for a secure execution environment

1. Introduction

There are a number of server environments or *containers* that run untrusted Java code: Applets in web browsers, servlets in web servers, Enterprise Java Beans (EJB) in their EJB containers, OSGi bundles in their framework—to name a few. In all the examples, the untrusted code must adhere to a certain API. In all scenarios the code comes from different sources and was developed without knowledge about other code that runs in the same container. Normally all named containers make use of Java threads to run the untrusted code.