J. Lopez, et al., "Towards a Trustful and Flexible Environment for Secure Communications with Public Administrations", *First International Conference on Electronic Government (EGOV02)*, LNCS vol. 2456, pp. 211-214, 2002.
NICS Lab. Publications: https://www.nics.uma.es/publications

Towards a Trustful and Flexible Environment for Secure Communications with Public Administrations

J. Lopez, A. Maña, J. Montenegro, J. Ortega, and J. Troya

Computer Science Department, E.T.S. Ingenieria Informatica
Universidad de Malaga 29071 - Malaga, SPAIN
{jlm,amg,monte,juanjose,troya}@lcc.uma.es

Abstract. Interaction of citizens and private organizations with Public Administrations can produce meaningful benefits in the accessibility, efficiency and availability of documents, regardless of time, location and quantity. Although there are some experiences in the field of e-government there are still some technological and legal difficulties that avoid a higher rate of communications with Public Administrations through Internet, not only from citizens, but also from private companies. We have studied two of the technological problems, the need to work in a trustful environment and the creation of tools to manage electronic versions of the paper-based forms.

Keywords: Public Administrations, Secure Communications, Electronic Forms, Certification Authorities, Public Key Infrastructure

1 Introduction

Approaches to electronic versions of many of the paper-based administrative procedures between Public Administrations and citizens can bring meaningful benefits. These benefits concern accessibility and availability of documents, regardless of time, location and quantity.

Although there are some experiences in the field of e-government there are still some technological and legal difficulties that avoid a higher rate of communications with Public Administrations through Internet, not only from citizens, but also from private companies. Any type of digital transaction is influenced by typical open networks risks. Agents involved (public organizations, private companies and citizens) need to work in a trustful environment. This environment must satisfy the required security levels in such a way that privacy and authentication of digital information is guaranteed to senders and receivers OGIT96 [4]. Also there is a lack of software tools that help to create, distribute and manage in an easy and flexible way the electronic versions of paper-based forms, which is the usual way of interaction with Public Administrations. Clearly, these tools

must incorporate authenticity and integrity mechanisms that mimic those ones existing in the traditional paper-based documents [5].

In this paper we present the results of a research project that has focussed on the problems we have mentioned. We also show how the integration of the approaches produce a solution that enhance many of actual developments. Thus, the structure of the paper shows the two main works done in the project. Section 2 presents the design and development of a real hierarchical Public Key Infrastructure (PKI), which we consider the most convenient type of infrastructure for operation of any administrative procedure that involve a digital signature. Section 3 presents the design of a language for the description of electronic forms that allows the utilization of signed forms in all communications with Public Administrations. The paper finishes with conclusions in Section 4.

2 Development of a PKI based on new design goals

Digital signatures schemes are based on the use of public-key cryptosystems [3]. The reasons are that these schemes offer the same functionality than handwritten signatures, and also a high protection against fraud. However, the global use of any of those cryptosystems needs a reliable and efficient mean to manage and distribute public keys, by using digital certificates. Such functionality is provided by a Public Key Infrastructure, which is formed by a diversity of Certification Authorities. A PKI becomes essential because without its use public key cryptography is marginally more useful than traditional symmetric one [2].

Although addition of certification capabilities in commercial electronic mail programs is a very helpful feature, a detailed analysis shows that these schemes result not satisfactory for e-government applications. Some design features that may compromise the security of the systems have been detected. We summarize some of the most important ones:

- It is common in most of Public Administrators that users share the same computer system. Therefore, private keys belonging to different users are not completely "isolated". This drawback does not allow the appropriate use of a very important security service for e-government applications, the non-repudiation service [7].
- Certificates needed for a verification of documents that have been digitally signed must be obtained from sources that are external to the electronic mail programs. Therefore, it is very possible that users do not verify them properly (as they are not forced to). Moreover, use of Certificate Revocation Lists (CRLs) is constrained.

These considerations has taken us to develop our own PKI [11], that has the following features:

- Adapted to the multi-hierarchical Internet structure because this is the operational environment.
- Provides secure means to identify users and distribute their public keys.

– Uses a CAs architecture that satisfies the needs of near-certification so the trust can be based on whatever criteria is used in real life.
– Eliminates problems of revocation procedures, particularly those associated with the use of Certificate Revocation Lists.

The main element in the hierarchy is the Keys Service Unit (KSU), which integrates certification and management functions. We use a scheme with various KSUs operating over disjoint groups of users, conforming a predefined hierarchy.

KSU hierarchy is parallel to the hierarchy of Internet domains. KSUs are associated to the corresponding e-mail offices. Every KSU is managed by a CA.

Additionally, it contains a portion of the certificates database to store the certified keys of its users. The third component is the key server, which receives requests and delivers the certificates. The key server manages a certificate proxy that keeps some of the recently received external certificates. The certified keys are managed solely by the corresponding CA; therefore, key updating and revocation are local operations that do not affect the rest of the system.

3 Description Language for eforms: A new design

Structured forms has been the traditional method of interaction with Public Administrations [6]. Moreover, the use of hand-written signatures in this type of documents has provided the necessary legal bindings for most of scenarios. Our previous study of common e-government applications has showed us that if paper-based forms have to be substituted by electronic forms, then these ones must have the following characteristics: integrity, or non-modification by external entities; non-repudiation, or non-deniability of agreements; and auditability.

Taking these features as a staring point, we have tried to design an appropriate language for the description of forms.

These reasons recommended us to try to design and develop our own Formal Description Language. Its name is FDL, and XML-like. To be more precise, it is based on XFDL [1].

The use of our own specific language, with its own tools, and completely adapted to XML [8, 9], introduces many advantages in comparison with traditional use of HTML [10].

The most important advantages are briefly summarized next:

– *Regarding forms status*: It is easy to add useful components not included in standard HTML, and it provided automatic data validation without programming specific code. Also, the definition of the structure of the fields where signatures are contained simplify the (automatic) process of signature verification, and finally, the particular design of our language, together with the standard where it relies on, facilitate creation of parsers that automatically translate forms to any other language.
– *Regarding forms management:* The signer can store a copy of a partially filled document and one or several persons can sign these forms.

FDL has two fundamentals concepts oppositely to HTML, the first notion is there are some extensions defined to distinguish different parts and formats in the same document, and the second one is the status of the form is preserved, thus our solution has been designed to organize any form in several pages while having data in memory continuously.

- *Regarding communication:* A proprietary format facilitates that the context of the signature is not lost.Moreover, the document is audited on its own. Oppositely to HTML, FDL provides a data structure and separates application, presentation and logic levels.

4 Conclusions

In this paper we have presented the results of a research project that studies the need of using security for communications over open networks, and the use of electronic versions of the paper-based forms to interact with Public Administrations.

We have shown the main features of the PKI specifically developed and the reasons for its design. Regarding the electronic forms we have designed a language for their description.

Modular design and development of those tools facilitates that the outcome of the work is integrated into e-government broader systems, and can be immediately applied to the social environment. These new solutions also help in establishing the basis for future design and development of schemes oriented to electronic forms signature in the communications with Public Administrations.

References

1. B. Blair, J. Boyer, "XFDL: Creating Electronic Commerce Transaction Records using XML", Computer Networks, n. 31, pp. 1611-1622, 1999.
2. W. Burr, "Public Key Infrastructure Technical Specifications (version 2.3). Part C: Concepts of Operations", Public Key Infrastructure Working Group, National Institute of Standards and Technology, November 1996.
3. W. Diffie, M. Hellman, "New Directions in Cryptography", IEEE Transactions on Information Theory. IT-22, n. 6. 1976, pp. 644-654.
4. European Commission, "Directive 1999/93 of the European Parliament and the Council on a Community Framework for Electronic Signatures", December 1999.
5. European Commission, "Directive on Certain Legal Aspects of Electronic Commerce in the Internal Market", February 2000.
6. "Improving Electronic Document Management", Guidelines For Australian Government Agencies, Australian Office of Government Information Technology, 1996.
7. "Non-Repudiation in Electronic Commerce", Artech House, 2001.
8. Extensible Markup Language (XML)" http://www.w3.org/XML
9. Canonical XML, Version 1.0, W3C Working Draft, September 2000. http://www.w3.org/TR/2000/WD-xml-c14n-20000907
10. HTML 4.01 Specification, W3C Recommendation, December 1999. http://www.w3.org/TR/html4/
11. J. Lopez, A. Mana, J. Ortega, J. Troya "Distributed Storage and Revocation in Digital Certificate Databases", Dexa 2000.