Towards e-Government: The Security SOA Approach of the University of Murcia

Daniel Sánchez-Martínez
Information and Communications Engineering Department, University of Murcia, Spain
danielsm@um.es

Inmaculada Marín-López
Information Technologies and Advanced Communications Area (ATICA), University of Murcia, Spain
inmaml@um.es

Antonio F. Gómez-Skarmeta
Information and Communications Engineering Department, University of Murcia, Spain
skarmeta@um.es

Tomás Jiménez-García
Information Technologies and Advanced Communications Area (ATICA), University of Murcia, Spain
tomasji@um.es

Abstract

This paper describes the experience of the University of Murcia in the design and development of security SOA infrastructures for electronic government, which provide university community with secure and interoperable services.

1. Introduction

Nowadays, there is a diversity of governments in countries, regions, cities and public organizations that have been developing electronic government services to improve their citizens' quality of life since the beginning of the new century. Specifically in Spain, the *Act 11/2007, concerning Electronic Access of Citizens to Public Services* has been recently published. This act establishes a suitable regulatory context in which Public Administrations are able to simplify their internal processes and offer electronic services to citizens with all the legal guarantees. Different articles of this act stress the importance of the use of standard formats with the objective of making the interoperability between Public Administrations easy. The University of Murcia has been working to achieve these objectives for the last ten years, by building the technological and strategic infrastructures that support the different kinds of services offered to the university community.

This paper describes the experience of the University of Murcia in the development of these security infrastructures that make use of electronic government services from different available environments. The University of Murcia shows an heterogeneous scenario where several operating systems, servers and software exist. The students, teachers and staff of the University of Murcia can use the government services face-to-face, from a desktop computer or even from a mobile device, with the same efficiency and security characteristics. These services are developed with the aim of improving the internal management, offering add-value services and interoperating with other governments.

In order to reach these objectives, the University of Murcia has been working in different lines for the last years. On the one hand, several registry offices were opened so as to distribute electronic certificates to the university community. This action is feasible thanks to an agreement with "Fábrica Nacional de Moneda y Timbre" (FNMT), which is the main certificate service provider in Spain. In the last two years, over one thousand new certificates have been distributed to students, lecturers and administrative staff. Another important administrative action is the technical improvement of the University of Murcia smart card. This card is now able to store cryptographic credentials, thus enabling the use of electronic signature. On the other hand, multiple technological developments have been performed in order to secure the exchange of electronic documents, as well as store and preserve these electronic files.

In the first sections of the paper we review the most basic infrastructures of the University of Murcia for securing the electronic transactions and handling the electronic documents. We also describe the use of the smart card of the University of Murcia as the main security element to perform electronic authentication and signature. Next, in the last sections of the paper, we show some electronic government services developed for the staff, teachers and students. Finally, we introduce several initiatives about interoperable services for the exchanging of electronic information with other governments.

2. SOA Infrastructure

As far as e-government in the University of Murcia is concerned, the most relevant aspect to deal with is the design and development of a suitable infrastructure that allows the deployment of a ubiquitous, flexible and secure platform.

With the aim of obtaining such a platform, it has been designed on the basis of a service-oriented architecture (SOA) [1] using Web services and several standard technologies, such as WSDL [2], XML, SOAP, HTTP, etc.

2.1. Related work

In the development of our platform, we have considered the architectures proposed in [3, 4] as the basis for a global e-government architecture. However, from our point of view, these architectures need to improve some functional aspects.

On the one hand, the incorporation of a server-based signature protocol, as the one defined in [5] by the OASIS's Digital Signature Services Technical Committee, which supports different signature formats, such as XMLDSig [6], CMS [7], XAdES [8], CAdES, etc. Additionally, for timestamp purposes, a new profile we have defined, called UMU-TS, based on the OASIS DSS timestamp profile specification (OASIS-TS) [9] should be included in the architecture. This new profile has been designed in order to comply with this platform requirements.

On the other hand, the verification of evidences over long periods of time should be extended according to the components and protocols we proposed in [10].

2.2. SOA platform architecture

The initial set of services within the platform we propose is depicted in Figure 1.

Generally, these services support access control by means of authorization information management, for example, credentials, when required. Additionally, they provide the possibility of indicating the service policy, so that a service behaves in different ways depending on the parameters supplied. Next, we describe the functionality of each service.

2.2.1. Signature service. This is the core service in the e-government architecture. Its implementation is based on the OASIS's digital signature service protocol (DSS) and it supports, among others, the features we comment next:

- The most common signature standard formats, as well as advanced ones. Additionally, it could support new emerging standards.
- Different kinds of signatures, depending on their relationship with the signed data: detached, enveloping or enveloped.
- Multiple signers.
- The generation of server's digital signatures using different private keys.
- Optionally, the access to other services (certificate validation, timestamp, role management, etc.) in order to properly validate signatures, as well as extend previously generated signatures for long-term archival purposes.

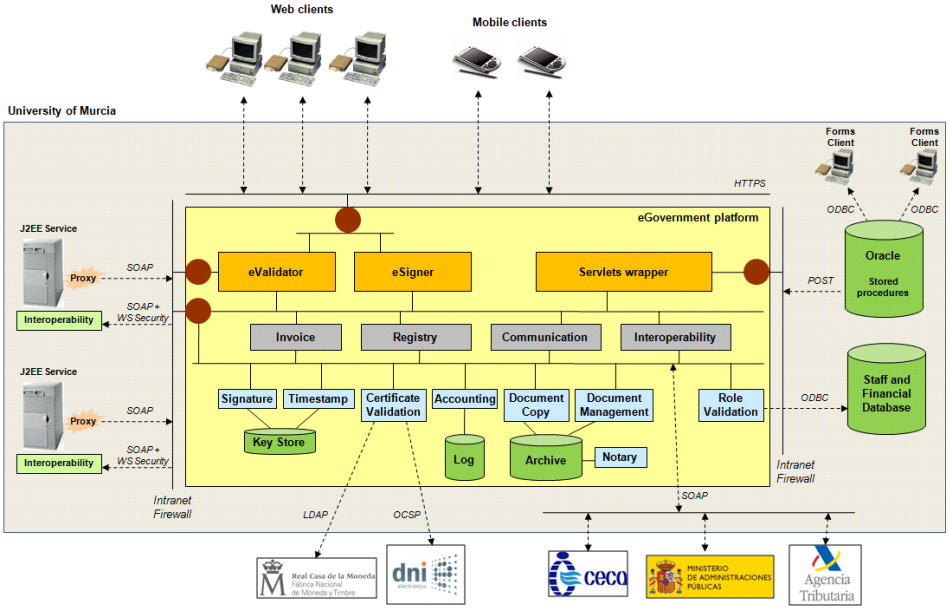

Figure 1. SOA-based framework for the e-Government infrastructure at the University of Murcia

This service ensures the authenticity and integrity of exchanged electronic documents. Besides, some signature operations can be made ubiquitously, from different and possible mobile environments, so that the keys used can be shared between different users or applications within the same organization.

2.2.2. Timestamp service. Timestamp service implementation is based on UMU-TS profile we have defined. This service has the following characteristics:

- Generation of existing timestamp standards and formats, such as RFC3161 [11] and OASIS DSS, as well as new emerging ones.
- Verification of timestamp tokens previously generated by this service and provision of information contained within them.
- Optionally, inclusion of new attributes into a timestamp token, thus extending the information included in it.

The timestamp service provides transactions non-repudiation by means of a timestamp token. This timestamp token, which is issued by a TimeStamp Authority (TSA), guarantees that a transaction was executed at a specific time.

2.2.3. Certificate validation service. The certificate validation service [10] is in charge of validating the certificates used in each transaction, thus ensuring the truthfulness of the signed documents. It mainly supports the following features:

- Validation of certificates issued by different Certificate Service Providers (CSPs).
- Support for different certificate validation mechanisms and protocols (CRLs [12], OCSP [13], SCVP, DCVP, etc.).
- Provision of the validation information obtained from the specific mechanism.

Currently, the supported certificates are those issued by FNMT and those included in eDNI (Spanish Identity Card); the supported validation mechanisms are CRLs and OCSP.

2.2.4. Role validation service. This service is in charge of checking if a civil servant played a given role at a specific time. In this manner, it could be ensured that an administrative transaction was performed by a University civil servant with a proper position.

2.2.5. Document copy generation service. A document copy is an electronic receipt which is delivered to citizens after the processing of an administrative procedure, as a proof of execution. It is a printable electronic document generated from the original signed document associated to the specific administrative procedure. Additionally, it includes a code that uniquely identifies the original signed document together with other information related to the signer (identification number, signing role, signing time, etc.) and other security features (electronic signature and barcodes) which guarantee its authenticity and integrity, not only in electronic format but also in printed paper.
The target of the document copies generation service is to create an electronic receipt from the original signed document and the inclusion of the aforementioned characteristics within that receipt.

2.2.6. Accounting service. The accounting service receives usage information from the rest of services deployed on the e-government platform. It registers the received information in a database, so that it could be retrieved later on in order to accomplish auditing processes. In this manner, usage statistics related to the e-government services can be obtained.

2.2.7. Interoperability service. The interoperability service is conceived to make feasible the exchange of electronic documents and/or other information related to administrative procedures, between different services existing within the e-government infrastructure. This exchange is accomplished by using XML content and SOAP authenticated headers, as stated in WS-Security [14] standard, thus ensuring the authenticity and integrity of the exchanged data.

2.2.8. Document management service. The document management service has the responsibility for storing every electronic document generated within the University into a local documentary database. Before archiving a document, this service checks that it includes validity data, that is, one or more extended electronic signatures for long-term archival purposes.

2.2.9. eValidator service. This service validates both electronic documents and document copies. This validation is based on the security features included in both types of documents.

Regarding a document copy, the eValidator service uses the information included in it in order to validate the original signed document.

Once the eValidator service has checked the validity of a document, it is able to offer additional information related to the processing state of the associated procedure.

2.2.10. eInvoice service. The eInvoice service is aimed at receiving Facturae-compliant invoices. After receiving an invoice, this service checks if it conforms to Facturae schema and if it includes a valid XAdES-EPES/T signature. Then it temporarily archives that invoice and, after 24 hours, the service will extend it to XAdES-X-L format and will archive it again for long-temp periods.

3. Client architectures

Additionally to the development of the SOA infrastructure, which gives support to all processes involved in the e-government platform, we have also developed some applications at client side. They allow end users to generate digital signatures and authenticate themselves, by means of digital certificates, in order to make their transactions in a secure way.

In the design of the e-government client architecture, these key principles have been taken into account:

- Users must be able to use their UMU smart cards in the e-government client applications, from both Windows and Linux operating systems.
- Client applications should be capable of using digital certificates to user authentication and S/MIME mail signing purposes. This must be done in a seamless way for the user. The credentials could be stored in the UMU smart card or locally, in the client certificate repository, in order to use them with the main browsers and mail clients available in the University of Murcia (Internet Explorer/Outlook, Netscape, Mozilla Firefox and Thunderbird).
- The architecture should offer high level functionality to developers who need to include digital signature processes to end services or applications, and it also must support the most extended signature standards (CMS and XMLDSig).

Bearing in mind the aforementioned requirements, we have designed the client architecture shown in Figure 2.

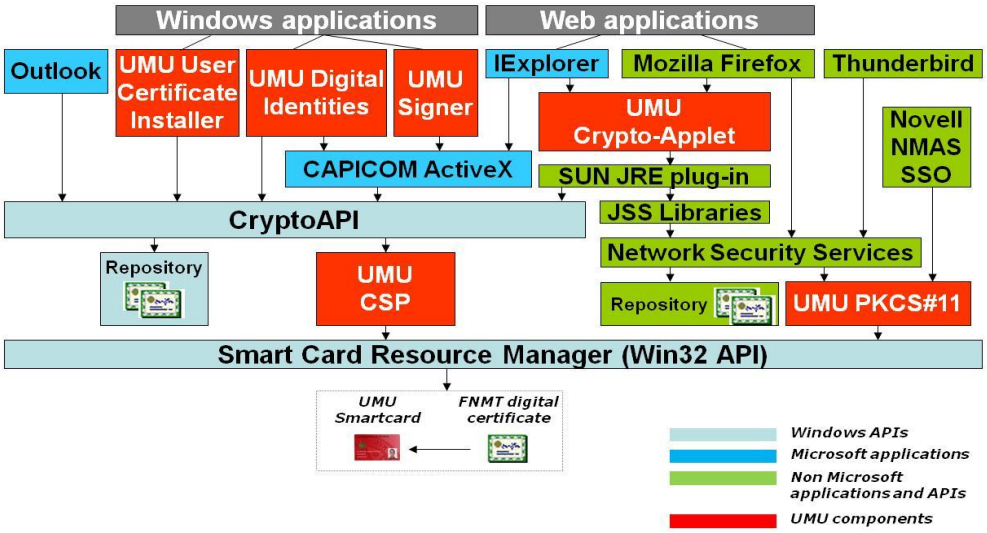

Figure 2. Security client architecture

This architecture consists of three main components: CSP [15], PKCS#11 [16] and Crypto-Applet.

Firstly, we find the UMU CSP component, which allows a client to use cryptographic operations to manage the credentials stored in his UMU smart card.

Secondly, we find the UMU PKCS#11 component. This module can be integrated with several tools that use NSS libraries, like Mozilla, Netscape, Firefox or Thunderbird, to provide analogous capabilities as UMU CSP.

Finally, we highlight our UMU Crypto-Applet component. With this development, members and clients of the University of Murcia can perform CMS, PDF and native XML digital signatures (not only basic XMLDSig but also XAdES signature), using their Internet Explorer or Mozilla Firefox browser, by means of JavaScript calls. This applet checks what specific browser the client is using; if it is Internet Explorer, it accesses to MSCAPI Java provider in order to make the digital signature; if it is Mozilla Firefox, the applet accesses to NSS to perform the signing process. Moreover, the application behavior is transparent whether the selected certificate is associated to a CSP or PKCS#11 module.

4. Main applications

This section describes the main e-government applications in the University of Murcia supported by both security SOA infrastructure and client architecture previously outlined.

The first one is the Electronic Registry. This application facilitates the sending of electronic forms and documents to the University from an electronic service, and with the same validity as the physical

registry. It provides an electronic way of receiving official documents with high security characteristics, like authenticity, integrity and non-repudiation of the performed transactions. It also offers the final user the state checking of the forms and documents registered through the electronic validation service. Moreover, these electronic documents are integrated inside the workflows of the University, getting a complete electronic processing between the different users that play a role in the lifecycle of the document.

Another important application is the Express Payment Service. The main objectives of this service are the development of a system to digitalize invoices and other financial documents in printed paper, and the establishment of a work-flow to validate these new electronic documents, based on electronic signature processes. The main benefits offered by this service are the avoiding of paper in the administrative procedure and the speeding up of the financial payments. Other important extensions to this project are the reception of electronic invoices sent by a provider, the development of an OCR to simplify the integration of paper invoices, and the establishment of agreements with financial entities to exchange electronic documents.

Finally, one of the most accepted applications is the Publishing of Exam Announcements and Marks Service. This service has some important benefits to the university community. First, a lecturer is able to generate the two main official documents (exam announcements and exam marks) related to each one of the subjects he teaches through the e-learning portal of the University of Murcia (a.k.a. SUMA). Then the lecturer performs a digital signature process with a qualified certificate. Afterwards, the students receive authentic copies from these electronic documents via e-mail or SMS notification instantly, so they can know these academic issues without any delay. Moreover, these copies are printed and published on the official notice board of the Faculty in order to provide the students with the choice of the communication channel (physical or electronic). Finally, both exam announcements and exam marks documents can be checked and validated by anybody through the electronic validation service and the interoperability services previously outlined. Figure 3 depicts the different entities involved in this service.

5. Interoperability services

The University of Murcia is focused on different projects in order to provide real interoperability processes inside the University and in its relationship with other organizations. This effort has the aim of avoiding the use of paper and speeding up the exchange of electronic documents. Next, we comment these projects.

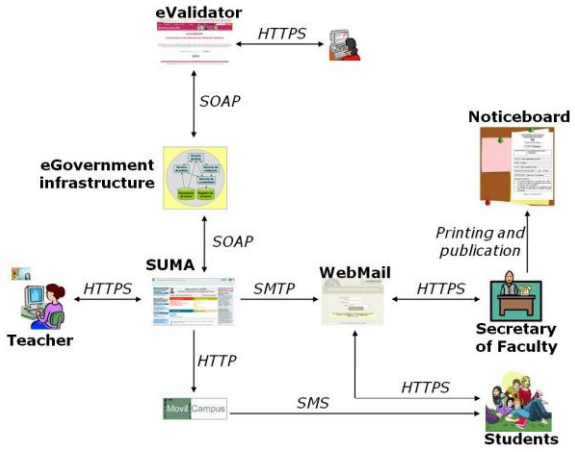

Figure 3. Publishing of exam announcements and marks service

Firstly, the Ministry of Public Administration offers a network, called SARA, which provides a SOA platform to other Public Administrations that have intranet access to this network. The services offered by SARA are related to generation and validation of timestamp tokens from different Time Stamping Authorities (TSAs), validation of electronic Spanish Identity Document (DNIE) as well as digital certificates issued by all Spanish Certificate Authorities, and checking that a person is included in a specific population census. The University of Murcia interoperates with this network for the purposes of requesting information to other external entities, that the Ministry of Public Administration has direct access to, thus acting as a bridge between the University and those external entities.

Secondly, the Spanish Confederation of Savings Banks or CECA offers a service that is in charge of sending accounting documents to other entities. These accounting documents must have been created according to a standard format, which includes one or more advanced XAdES compliant signatures. Particularly, the University of Murcia sends payment orders to CECA in order to authorize economic transfer payments, from the University's banks account to other providers' bank account.

Finally, the National Agency for Tax Administration, along with the Ministry of Industry, has defined a standard format of representing electronic invoices called Facturae. The University of Murcia has adopted this specification in order to make the reception of supplier invoices easy. In this sense, the University is able to receive invoices, which have been created according to Facturae, from different suppliers. Another standard supported by the University of Murcia is UBL-Invoice.

6. Conclusions

This paper presents the main technical initiatives about electronic government services and SOA infrastructures that have been developed by the University of Murcia for the last years. These steps represent the beginning of a complete transformation of paper-based procedures into electronic ones. The figure 4 shows the evolution in the use (in transactions per month) of these electronic government services inside the University for the last months. The most important issues in this process are the improvement of the technical interoperability inside our University and the relationships with other public e-governments and organizations, through the use of secure services and standard data formats (like XAdES or Facturae).

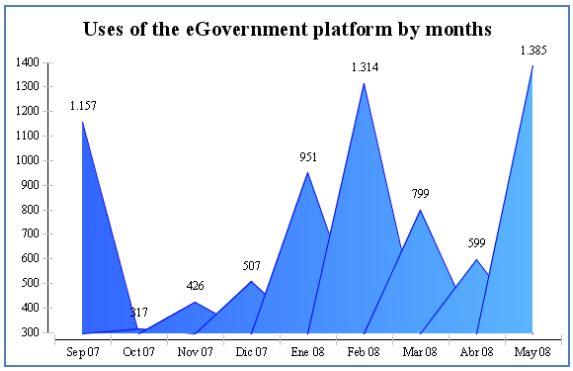

Figure 4. Use of electronic government platform

Moreover, the University has to face some important challenges yet. One of them is the preservation of the digital objects, particularly the electronic signatures. The University of Murcia is developing a preservation layer based on an initiative of an IETF working group called Long Term And Notary Services. This layer tries to generate the appropriate electronic evidences that guarantee the long term authenticity and integrity of the digital objects stored in the electronic archive.

Other interesting issue is the use of a mobile device as a secure signature-creation device. The University of Murcia, in collaboration with Telefónica, is working for the distribution of cryptographic SIM cards (CryptoSIM) inside the university community and the integration of mobile signature processes [17] in the electronic government platform. Searching for proper solutions, which cover different profiles of use, is essential for the development of a global electronic government scenario.

7. References

[1] OASIS. *SOA Reference Model Technical Committee*. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

[2] W3C. Web Service Definition Language (WSDL). W3C Recommendation, June 2007. http://www.w3.org/TR/wsdl20/

[3] A. Kaliontzoglou, P. Sklavos, T. Karantjias and D. Polemi. *A secure e-Government platform architecture for small to medium sized public organizations*. Electronic Commerce Research and Applications, September 2004.

[4] D.S. Gómez, A. Ruíz, L. Baño, C.I. Marín, A. F. Gómez. *Una infraestructura de Seguridad para una Plataforma SOA*. III Simposio Español de Comercio Electrónico, Junio 2005.

[5] OASIS. *Digital Signature Services (DSS) Technical Committee*. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

[6] W3C. *XML-Signature Syntax and Processing*. W3C Recommendation, February 2002.

[7] R. Housley. *Cryptographic Message Syntax (CMS)*. RFC 3852, July 2004.

[8] ETSI. *XML Advanced Electronic Signatures (XAdES)*. http://uri.etsi.org

[9] OASIS, *Time-Stamping Profile of the OASIS Digital Signature Service*. OASIS, June 2004.

[10] A. Ruiz, D. Sánchez, I. Marín, M. Gil and A. Gómez-Skarmeta. *ACVS: an Advanced Certificate Validation Service in Secure-Oriented Architectures*. ICIW 2008, June 2008.

[11] C. Adams, P. Cain, D. Pinkas, R. Zuccherato. *Internet X.509 Public Key Infrastructure Time-Stamp Protocol (TSP)*. RFC 3161, August 2001.

[12] R. Housley, T. Polk, W. Ford and D. Solo. *Internet Public Key Infrastructure, Part I: X509 Certificate and CRL Profile*. RFC 3280, April 2002.

[13] M. Myers. *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. RFC 2560, June 1999.

[14] OASIS, *Web Services Security (WSS) Technical Comittee*. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=wss

[15] *Cryptographic Service Provider*. http://msdn2.microsoft.com/en-us/library/aa380245.aspx

[16] PKCS #11 v2.20: Cryptographic Token Interface Standard. RSA Laboratories, 28 June 2004. ftp://ftp.rsasecurity.com/pub/pkcs/pkcs-11/v2-20/pkcs-11v2-20.pdf

[17] A. Ruiz, D. Sánchez, M. Martínez and A. Gómez-Skarmeta. *A Survey of Electronic Signature Solutions in Mobile Devices*. JTAER Vol.2 Issue 3, December 2007.