Tools for spreading eAdministration at Universitat Jaume I

Manuel Mollar[1], Paul Santapau[2], J. Pascual Gumbau[3], Ricardo Borillo[4], Vicente Andreu[5]

[1]Universitat Jaume I, Avda. Sos Baynat, Castelló (Spain), mm@nisu.org. [2]santapau@uji.es. [3]gumbau@uji.es. [4]borillo@si.uji.es. [5]andreuv@uji.es.

Keywords
eAdministration, software tools, digital signature, e-authoring, e-polling.

1 EXECUTIVE SUMMARY

The present communication describes three tools developed by Universitat Jaume I which have a strategic value for spreading eAdministration initiatives within the institution. After assuming the importance of new technologies for University's governance and the use of digital signature as a key factor of success for the developing of electronically supported administrative procedures, our University has enforced eAdministration by developing a set of software tools. These tools are fully built under open code premises and are freely available for any institution which intends to use, adapt or improve them with a non-commercial objective.

TOOLS FOR eADMINISTRATION.

Generalized use of digital signatures is a requirement for a wide variety of procedures. Also, dealing with valid electronic documents -in substitution of the traditional ones in paper- has become a common task in this environment. Finally, universities frequently need to obtain feedback on the services they provide. These tools that we are hereby introducing are oriented towards helping to deal with these three basic aspects of eAdministration.

Cryptoapplet

It is a software module for carrying out digital signatures. Its operation is simple: given a data input and a configuration determined by a web server, a web browser digitally signs the data. Output formats supported by the applet are the following: raw, CMS/PKCS#7, DigiDoc format (XAdES-X-L), signed PDF. Use of certificates is transparent thanks to direct access to Microsoft CryptoAPI.

eAuthoring

It is a program designed to generate an electronically signed PDF document using any application with printing capabilities. In addition, it allows classifying and storing of the documents in a local folder or in a remote repository. Signatures generated can be checked by commonly used software such as Adobe Acrobat Reader.

eSurvey

The objective of this project is to develop a software environment that allows on-line polling or realisation of surveys. The system has been designed for being anonymous (based on "blind signature"), untraceable (through a controlled latency network) and with some fault-tolerance features. Implantation is simple and low cost: users only need a java empowered web browser.

CONCLUSIONS

The tools presented are being used in different contexts and administrative workflows. Beta versions of the products are available from University's website. At the moment these tools are totally operative.

2 INTRODUCTION

Universitat Jaume I has assumed, and also established in its organizational strategies, the importance of new technologies for University's governance. Some steps have been taken by the institution in the last few years to reinforce this fact. The present communication describes three tools developed by Universitat Jaume I which, in our opinion, have a strategic value for spreading eAdministration initiatives within the institution, but also can be integrated and applied in other public or private organizations.

Besides this, Universitat Jaume I is aware that most of concerns related to the use of electronic means in relationships among University and students, professors, administrative staff or general public, address the importance on security and the need of establishing guarantees on the identity of people involved in these relationships. For this reason, our institution promoted the use of digital signature and considered it as a key factor of success for the developing of electronically supported administrative procedures.

After performing an educational task on University's members about the use of digital signature, and providing with digital certificates to the whole community, Universitat Jaume I tries to go one step beyond by enforcing eAdministration. through the generalisation of three new tools. This tools, which will be described in the present paper, have been designed with the target of incorporating them to everyday tasks, not only by technicians but also by common users.

Following the pledge exposed in University's Statutes, the tools for spreading eAdministration are fully developed under open source premises and are freely available for any institution which intends to use, adapt or improve them with a non-commercial objective. Universitat Jaume I will be glad to contribute to any project which can profit from the integration of the tools introduced in this paper. Nevertheless, some restrictions apply for the distribution: for public non-profit organizations, we require being informed under which conditions the distribution is performed and which modifications are made to the original software; and for private companies, an agreement should be signed. This agreement has no cost unless the software has to be customized using University's own resources.

3 THE SET OF TOOLS.

An analysis of eAdministration processes reveals that generalized use of digital signatures is a requirement for a wide variety of procedures. It contributes to generate confidence among the users of the systems and to provide legally valid evidence of transactions that have been performed on them, proving the identity of the people involved and the exact time in which they took place.

Also, dealing with valid electronic documents in substitution of the traditional ones in paper and have them properly treated, classified and stored, has become a habitual task in this environment. The electronic documents must guarantee, at least, the same level of authenticity, integrity and availability that are customarily assigned to those papers which wear a handwritten signature scribbled on them.

Finally, universities frequently need to obtain feedback on the services they provide. Some quality assurance procedures require this feedback to be obtained in an anonymous way. This tool has been designed with that focus, but it could also provide a system for carrying elementary voting procedures in a quick and automatic way.

These tools that we are hereby introducing are oriented towards helping to deal with the basic aspects of eAdministration that we will explain in depth in the following paragraphs:

- Dealing with valid electronic documents:

  Dealing with electronic documents is a much harder issue than it appears at first glance. Finding the analogy with manually signed documents helps to give them the required level of validity, but also can lead to pay no attention to peculiarities of electronic documents. Electronically signed documents carry a digital signature, but also, they have attached a set of binary objects: user's certificate and public keys. In order to use that objects you need an environment for accessing and using the keys related to those that were used to create the signature. Most common operating systems such as Microsoft Windows, GNU/Linux and MAC-OS offer their own –and different- systems to access/use/store the certificates and their associated keys, but all of them imply trusting the host computer enough for installing those elements into the computer's HD. On the other hand, tools offered by the browsers to perform digital signatures are commonly limited in the output format they generate, so the real advantage of an advanced digital signature format is somewhat affected.

- Classification:

  When classified, the documents must offer an easy and programmatic way of getting the processed metadata information and also for verifying the signatures. For that task, advanced signature formats based on XML technology are becoming more and more used, constituting, in fact, a commonly accepted standard.

- Digital preservation and storing over the time:

  Digital documents are generated and recovered by software applications; this fact is a point to take into account because, either the application must be preserved attached to the digital document or the document must be stored in a format completely open and independent of the application.

  This is not a unique approach. Several others are being considered with the aim of avoiding obsolescence of digital objects: refreshment (copy of a digital object in new media or systems), migration (transfer of data to new environments), replication (generation of several copies of a digital object) or emulation (technique of providing contemporary systems with obsolete functionalities in order to regain access to data). But, although all these approaches must be seriously considered, the fact is that preserving data in formats like text, XML or PDF/A or any others with no dynamic components can suppose an advantage for future recovery of digital objects.

  Besides this, it cannot be ignored the fact that digital signatures are based on cryptographic mechanisms and that those mechanisms are, commonly, vulnerable to the pass of the time. This happens because the computational power of computers grows in a constant manner and researchers develop new techniques that reduce dramatically the amount of computational time required to break a specific algorithm. Thus, a kind of armour is needed for the signature. Again, XML advanced signature formats allow us to incorporate cryptographic mechanism to delegate the cryptographic strength on signed timestamps and, hence, remaining strong over the time.

  XadES-X-L or XadES-A are formats specifically designed for the representation of digital signatures and their preservation. Stored signatures and timestamps are validated and upgraded; generating new ones obtained from stronger keys and improved algorithms. Old cryptographic information (certificate status, OCSP response, timestamping,…) is ratified and keeps its validity, but is protected, from that time onwards, with a more reliable armour.

- Anonymous electronic procedures:

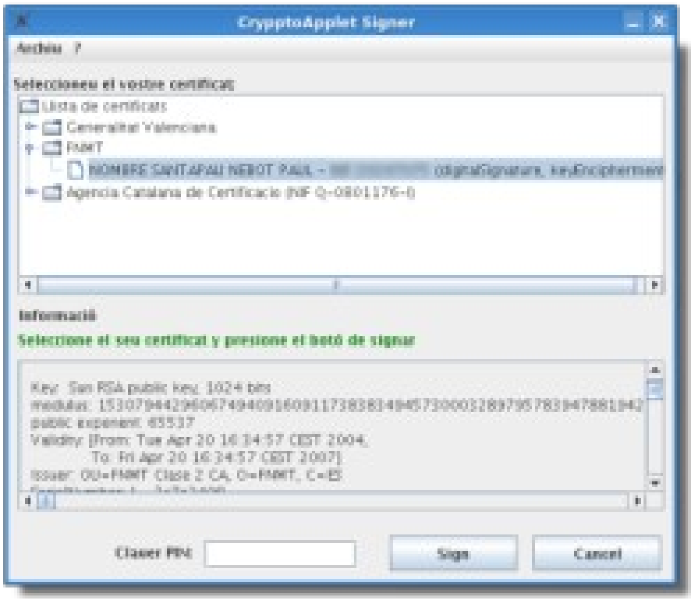
  Some procedures such as polling and voting in an anonymous way require some guaranties when subjects submitted to them act in the electronic world. Both of them require establishing mechanisms intended to control that a user cannot vote or submit a survey form more that once. But that control must be carried out in a way that respects the individual's anonymity: the whole procedure should not be traceable by any means avoiding that a concrete polling result could be associated with the person who issued a vote.

Universitat Jaume I has developed tools that solve each one of the problems above mentioned. In first place, ***CryptoApplet*** and ***eAuthoring*** provide the user with the level of abstraction needed when dealing with digital certificates and key stores. Moreover, those tools generate as an output an advanced digital signature format which allows the former to work with XML signatures and the latter with signed PDF documents. In second place, ***eSurvey*** is a technically complex project, with a difficult implementation, but is intended to be easily usable by common users to carry out surveys or voting procedures over the internet in an anonymous way.

Cryptoapplet

It is a software module for carrying out digital signatures. Its operation is simple: given a data input and a configuration determined by a web server, a web browser digitally signs the data. Output formats supported by the applet are the following: raw signature, CMS/PKCS#7, DigiDoc format (XAdES-X-L), signed PDF.

Management of digital certificates to be used for performing signatures is completely transparent for the user through direct access to CryptoAPI -in case of using Microsoft Internet Explorer- or PKCS#11 -in case of using Mozilla Firefox, whether on Windows or GNU/Linux-. The only requirement for *Cryptoapplet* to be used is having installed in the system a Java Virtual Machine (version 1.5 or higher).



Seleccioneu el vostre certificat:

```
Llista de certificats
  Generalitat Valenciana
  FNMT
    NOMBRE SANTAPAU NEBOT PAUL - [redacted] (digitalSignature, keyEncipherment
  Agencia Catalana de Certificacio (NIF Q-0801176-I)
```

Informació

Seleccione el seu certificat y presione el botó de signar

```
Key:  Sun RSA public key, 1024 bits
modulus: 15307944296067494091609117383834945730003289795783947881942
public exponent: 65537
Validity: [From: Tue Apr 20 16:34:57 CEST 2004,
           To: Fri Apr 20 16:34:57 CEST 2007]
Issuer: OU=FNMT Clase 2 CA, O=FNMT, C=ES
```

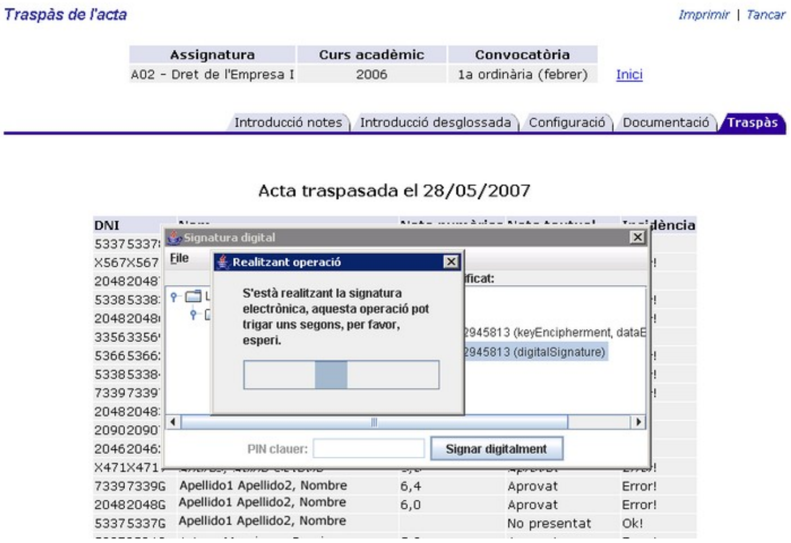
Clauer PIN:

Figure 1. An image of cryptoapplet

The formats and the way in which signatures are performed using your own X.509 digital can be checked at http://proyectostic.uji.es.

This tool has been already adapted in the University Jaume I in a variety of procedures such as:

- Certificate of student’s academic file issued as an electronic document, digitally signed by the University as a guarantee of authentication and with full legal validity under Spanish laws.
- Electronic Registry Office, the digital version of Registry Offices, where official documents addressed to public entities are submitted, validated, registered and time stamped.
- Signature of “Actas Académicas”, professor’s official document in which assessment records are registered. An especially critic document in an academic environment because it carries the signature of the professor and his or her assessment on every student’s abilities.



Traspàs de l'acta

Assignatura	Curs acadèmic	Convocatòria
A02 - Dret de l'Empresa I	2006	1a ordinària (febrer)

Acta traspasada el 28/05/2007

S'està realitzant la signatura electrònica, aquesta operació pot trigar uns segons, per favor, esperi.

…ficat:

…2945813 (keyEncipherment, dataE…

…2945813 (digitalSignature)

DNI				…idència
53375337…				
X567X567				…!
20482048…				
53385338…				…!
20482048…				…!
33563356…				
53665366…				…!
53385338…				…!
73397339…				…!
20482048…				
20902090…				
20462046…				
X471X471…				…!
73397339G	Apellido1 Apellido2, Nombre	6,4	Aprovat	Error!
20482048G	Apellido1 Apellido2, Nombre	6,0	Aprovat	Error!
53375337G	Apellido1 Apellido2, Nombre		No presentat	Ok!

Figure 2. Signature of an academic digital document using cryptoapplet

Any organization can simply integrate the cryptoapplet in their own automatic procedures by following the guidelines provided in the webpage of the project.

eAuthoring

It is a program designed to generate an electronically signed PDF document using any application with printing capabilities. In addition, it allows classifying and storing of the documents in a local folder or in a remote repository. Signatures generated can be checked by commonly used software such as Adobe Acrobat Reader.

The aim of that tool is make easy the interoperability with the suppliers of the university in a way they only have to install a virtual printer in their windows systems and to have a digital certificate issued by a trusted certificate authority in order to interoperate with the university with electronically signed invoices.

eSurvey

The objective of this project is to develop a software environment that allows on-line polling or realisation of surveys. The system has been designed for being anonymous (based on “blind signature”), untraceable (through a controlled latency network) and with some fault-tolerance features. Implantation is simple and low cost: users only need a java empowered web browser.

In a wide and complex organization such as a University, voting for choosing among several options arisen or for electing representatives is a frequent activity. Many of these polling processes do not require the high degree of formality of an electoral process, and they could be quickly and safely performed through this application.

Also, many administrative tasks in public organizations or even quality-related processes, could benefit form the feed-backs provided by a tool that allows the realisation of surveys on the internet with, at least, as many guarantees of anonymity as the traditional methods used till now.

4 CONCLUSIONS

The tools presented are being used in different contexts and administrative workflows.

Cryptoapplet has been integrated in the University's ERP for performing advanced signatures in applications that require this guarantee and has been favourably received by specialized audience. More than one hundred developers and software engineers from both public and private organizations have subscribed the distribution list and are actively participating in it, suggesting improvements or demanding information for the integration of the tool in their own systems. It has also been discussed in electronic magazines specialized in new technologies.

The eAuthoring tool is being installed on personal computers' desktops and a culture of generating digitally signed and time stamped documents is being spread among teaching and administrative staff. This documents have the same legal validity that their equivalents on paper.

Survey tools are still undergoing final tests before being incorporated to University's integrated management systems. The deployment will be made in the next moths.

For those interested in this project, Beta versions of the products are available from University's website. Internal procedures are being reviewed in order to incorporate them to common workflows.

Completion of the present project proves that advanced tools for eAdministration, with complex cryptographic capabilities and a long term perspective, can be implemented under the principles of open source software.

5 REFERENCES

Project website (2008). *Universitat Jaume I – Open Source projects*. Retrieved May 15, 2008, from: http://projectestic.uji.es/.
Developing team website (2008). *Universitat Jaume I – NISU Computing Security Team*. Retrieved May 15, 2008, from: http://www.nisu.org/.