



EUNIS 2006 Elite Awards Entry

***“Clauer”* Project**



SUMMARY

AUTHORS	2
INTRODUCTION	2
ANTECEDENTS OF THE PROJECT	2
OBJECTIVES.....	4
RESOURCES AND ENVIRONMENTAL CONSTRAINTS	4
IMPLEMENTATION AND ACTUAL STATE OF THE PROJECT	5
RESULTS OF THE PROJECT, UTILISATION DATA AND IMPACT ON THE INSTITUTION	6
ANY PLANNED FURTHER DEVELOPMENTS.....	7
INTEROPERABILITY AND APPLICABILITY OF THE PROJECT TO OTHER INSTITUTIONS.....	7
CONCLUSSIONS.....	7
LINKS AND REFERENCES.....	7

AUTHORS

Modesto Jesús Fabra Valls, General Secretary.

José Pascual Gumbau Mezquita, Director of Rector's Technical Cabinet.

Manuel Mollar Villanueva, Professor of the Computer Languages and Systems Department.

Vicente Andreu Navarro, Organization Technician.

INTRODUCTION

This document describes the project “*Clauer*”, the Catalan word for “keyring”, an initiative of Universitat Jaume I (Castellón, Spain) intended to promote the use of digital signatures in administrative tasks and in formal relationships among community members through the design, implementation and delivery of a cryptographically protected USB flash memory device. This project is a part of the global e-administration initiative that the university is carrying on.

Universitat Jaume I, as a signer of Berlin Declaration on Open Access to Knowledge in the Sciences and Humanities, is committed to facilitate free access to any kind of knowledge generated within the institution, and in this particular case, allows EUNIS to publish any details of the project and share them with EUNIS community. Full information on the initiative is available on-line at <http://clauer.uji.es/en>.

ANTECEDENTS OF THE PROJECT

Universitat Jaume I from Castellón, Spain, counts since 2001 with a body of rules that regulates and fosters administrative proceedings held using exclusively the computer and communication infrastructure of the institution. Procedures with a high degree of complexity, such as those derived from the registering of students, have been done during the last years in telematic form and the number of procedures that are carried only by electronic means has been increasing year after year.

The traditional system of user and password, that has served to identify the users of the systems, has been considered sufficient to credit the identity, but it needs additional requirements to offer guarantee of integrity. That is why the implantation of mechanisms of

electronic signature is replacing the traditional method in those proceedings in which it is necessary to assure integrity of the information or that are addressed to groups that do not have user accounts in the corporate systems, as happens with services or goods external providers or with future students.

One of the main problems that faced the university when decided to incorporate mechanisms of electronic signature to its administrative proceedings was to obtain a critical mass of users with digital certificates. The “anchor applications” of digital certificates in Spain are those related to the Spanish Tax Agency, so using digital certificates that are suitable for operating with Tax Agency would give potential users an additional attractiveness. The possibility of constituting a Certification Authority of its own and deliver Universitat Jaume I digital certificates was, thus, discarded and hiring a third-party certification services provider was considered.

After a market research of main certification services providers that offered enough guarantees under Spanish law and whose certificates were admitted for use by Spanish government entities, an agreement was signed with Valencian Community Certification Authority, an organism depending of the Valencian Community regional government to distribute their certificates among university members. The terms of the agreement were very favourable to both institutions because it was made under the basis of mutual cooperation in developing and promoting the use of electronic signature with no monetary charge for the emission of software certificates. Obviously, the university assumed the costs derived of the emission of the certificates and the “in person” verification of the identity of the applicants, a mandatory procedure for the legal validity of them.

As stated before, obtaining a considerable mass of users with certificate was judged key for the success of the project, so the digital certificates could be delivered on a support more attractive than a plain floppy disk. Additionally, the problem of the mobility of students and professors between different equipment (free-access computer classrooms, teaching classrooms, their own computers...) made to consider unsuitable solutions that implied to equip computers with rather unusual devices (card readers, for instance). A possible alternative, the use of simple software certificates, which had to be installed in the system repository or in each program repository, was also discarded by its lack of security since its installation in computers of public access (free-access computer classrooms, *mediateca*...) supposed a considerable risk.

On these reasons, it was decided to develop a new product, a device that was not available in the market at a reasonably inexpensive price (cryptographic USB tokens are considerably more expensive than general purpose ones), that allowed its non-onerous substitution by the users in case of deterioration or loss and that was easy to carry and to use with the habitual configurations of the equipment.

Besides this, as the formal request for digital certificates has a voluntary character, it was necessary to give the product an added-value by equipping the device with a double functionality: a general purpose storing device, and a hidden, not directly accessible by the operating system, and cryptographically protected partition used as a repository for digital certificates used in electronic signature transactions.

OBJECTIVES

The object of the project is the design and implementation, using personal and material resources of the University, of the device described above, the distribution of digital certificates in a way that allows its use in a flexible and safe form to all the members of the university community and the education of the staff and students in the use of electronic signature. In order to obtain it, a cryptographic software has been developed that allows to store certificates, to manage them and to use them on a USB flash memory device. The project enhances the mobility of students, since specific readers are not required, and allows a reasonably safe access to electronic services from shared-use computers (as happens in the case of classrooms and laboratories). The certificates stored in the device are seen as integrated in the system's general repository of certificates, so that their use is completely transparent.

The devices have been distributed throughout 2005 to the teaching and investigating personnel, to the administration and services staff, to undergraduate students, to doctorate and master students and to several others groups, having been emitted altogether around 14,000 digital user certificates. This objective has been reached thanks to the double functionality of the device, divided in a zone of general use and another cryptographic one, that has acted like and "anchor", since the application for digital certificates is, under Spanish law, a voluntary act.

Some side-effects must also be considered: some of the computer equipment has been updated because due to their obsolescence could not use the software libraries that have served as a base for the programs developed and, also, diverse programs that make use of the authentication by means of certificates or mechanisms of electronic signature have started up. Some of them are the following:

- Safe electronic mail
- Certified authentication in the access to the private part of the intranet.
- Certified password change on corporate servers (more than 20.000 incidences each year can be solved without human intervention).
- Certified update of personal data.
- Academic acts signature.

The device is also being used as a mean of weak authentication (without making use of the certificate for electronic signature) in certain applications, as access to shared computer equipment.

RESOURCES AND ENVIRONMENTAL CONSTRAINTS

The initiative has been promoted by University's Secretariat-General and the Vice-Rector for Infrastructures and Services, and has been coordinated by the Rector's Technical Cabinet and the Service for Planning and Organization.

The development of the device has been directed by teaching staff belonging to the Department of Languages and Computer Systems and has been integrally carried with own resources. A team of four programmers, in different phases and working under the orders of teaching and investigating personnel of the above mentioned department, has designed and implemented the software for the management and support of the “*clauer*”.

The incorporation of mechanisms of electronic signature to the administrative procedures has been developed by the University’s Service of Computer Science. The services of electronic certification and certificate emission have been provided by the Certification Authority of the Valencian Community following the agreement of collaboration subscribed in 2004.

For the processes of massive certificate emission (about 14.000 people have been identified in person and have got their digital certificates), the University has hired up to eight User Registry Point operators in charge of the tasks of identity verification, generation and recording of recognized software certificates on the device. The University has supported the cost of more than 14,000 USB flash memory sticks that serve as a support for the emitted certificates.

IMPLEMENTATION AND ACTUAL STATE OF THE PROJECT

The integration of the device in the existing systems has been possible thanks to the software developed by the university. In the actual phase of development, any memory flash USB is susceptible to be used, using the software provided by the University (and which is available for download from the official project webpage), for the certificate storage.

Among the different software modules built, perhaps the most important one is the CSP (Cryptographic Service Provider) designed to work with Microsoft CryptoAPI. This condition fulfills most of the computer park of the University after its recent update. Another module of software responds to standard PKCS#11 and allows the users of other systems and programs (as happens with Mozilla Firefox or Thunderbird, running either under Windows or under Linux) similar functionalities to those that can enjoy the users of Microsoft Windows systems. The project has tried to accomplish both standards *de facto* (CryptoAPI de Microsoft) and *de iure* (PKCS, Public Key Cryptographic Standards) and follow the principles of open-source code software. In spite of the pledge of the University towards the use of open-source software, nowadays, over 90% of administrative and teaching staff is using Windows as an operating systems, that’s why any development made internally must have this constraint in mind.

As a summary, the developed software modules are the following ones:

- Windows 2000/XP:
 - Base Software: contains the operating system of the device that is executed as a service in Windows. It contains the Cryptographic Service Provider (CSP) signed by Microsoft, the Certificate Store Provider and the ActiveX control to the device. It must be installed in any computer desired to operate with the “*clauer*”.
 - Manager for the device: allows formatting the USB stick, creating the partitions, establishing a PIN or password and importing the certificates.

- Clablock: system for access control to computers based on the “*clauer*”. It works at user level, so the modifications on the system are minimum. The authentication is made against webservices.
- Linux.
 - A PKCS#11 module for Firefox and Mozilla, adaptable to the navigators who support this model. It is scheduled to develop authentication libraries similar to those of Windows during 2007.
 - Several managing and debugging libraries used by the developing team (are available on-line at the developing team webpage <http://clauer.nisu.org>).

RESULTS OF THE PROJECT, UTILISATION DATA AND IMPACT ON THE INSTITUTION

Possibly, the most evident project’s indicator of progress is the index of penetration of digital certificates among members of the community: more than 75% of the students, 80% of the teaching and investigating staff and 95% of the administrative and services personnel have actually a digital certificate form electronic signature and encryption stored in an USB flash memory device which interacts directly with the system without need of installing them on every computer from which they are going to be used.

With this number of potential users, new applications which are being progressively designed and started up are expected to have a fast implantation phase. Besides this, community has experienced a considerable increase in the degree of alphabetization of its members in matters related to electronic signature, having also been detected an additional interest for applications that are external to the University (Tax Agency, Health System, Regional Government...) and that make use of digital signature.

Other collateral positive results have been the update of the computer park in order to allow a generalised use of the device (some obsolete equipment did not allow the interaction with the “*clauer*” and the design of specific modules was judged excessively expensive), the revision and selection of applications based on their capacity to use electronic signature (for example, electronic mail clients have been suppressed from the catalogue of desktop programs for not having signature and encryption functionalities).

The procedures that have proven taking benefit of the project, have done it for several different reasons:

- increase of its simplicity (services of authentication and change of passwords, more than 20,000 incidences during past year; if the certificate needs to be revoked or renewed it is possible to do it outside the University in anyone of the registry points the Certification Authority of the Valencian Community maintains all over the region)
- increase of the availability (web services are available 24x7...).
- avoiding in-person initiation in many proceedings (first term students can register themselves crediting their identity with digital certificate).

- guarantee of data integrity by eliminating intermediaries (academic acts signature).

FURTHER DEVELOPMENTS

The developing team is working in similar modules that will permit to use standard Compact Disks as a support for certificates, also interacting directly with the system with no need of installing them.

INTEROPERABILITY AND APPLICABILITY OF THE PROJECT TO OTHER INSTITUTIONS

The software generated within the scope of the project has been developed following the premises of open-source code and free use of the programs. All of them can be downloaded from the webpage of the project. Several initiatives are being started up for valid exchange of information between the University and the rest of public administrations, mainly in the aspects of delivery of certificates and public hiring. The cooperation between public administrations is evident from the very start of the project, since the University uses an organism belonging to the regional government as a supplier of certification services. The collaboration between the Valencian Community Certification Authority and the University has been constant in the last two years. Other agreements of cooperation are on the way to being signed with other organisms of public (Catalan Agency of Certification) and private nature (Camerfirma). The designed device allows to transport, with its factory default configuration, up to one hundred digital user certificates of diverse nature and origin. Additionally, the generated software products are offered freely for noncommercial uses.

CONCLUSIONS

The main conclusion that the experience leads to is, on one hand, there is a generalized ignorance of the matter and the mechanisms on which it is based, and on the other hand, there is a great feeling of distrust among users. One and another must be fought with a suitable alphabetization of the implied agents.

The main objectives of the project have been satisfied in their principal facets of innovation (a similar low-cost device did not exist), cultural aspects (generalization of the use of the electronic company/signature) and the possibilities of application to the management that are opened (academic acts, qualification certificates, exchange of information with other public administration, public hiring of goods and services...).

LINKS AND REFERENCES

- Institutional web page of the project: <http://clauer.uji.es/en>.
- Software developing group webpage: <http://clauer.nisu.org>.