UPGRADE
The European Journal for the Informatics Professional
http://www.upgrade-cepis.org
Vol. V, No. 3, June 2004

UPGRADE is the European Journal for the Informatics Professional, published bimonthly at <http://www.upgrade-cepis.org/>

UPGRADE is the anchor point for **UP**ENET (**UP**GRADE European NETwork), the network of CEPIS member societies' publications, that currently includes the following ones:
- MONDO DIGITALE, digital journal from the Italian CEPIS society AICA
- NOVÁTICA, journal from the Spanish CEPIS society ATI
- PRO DIALOG, journal from the Polish CEPIS society PTI-PIPS

Publisher
UPGRADE is published on behalf of CEPIS (Council of European Professional Informatics Societies, <http://www.cepis.org/>) by NOVÁTICA <http://www.ati.es/novatica/>, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática <http://www.ati.es/>).
UPGRADE is also published in Spanish (full issue printed, some articles online) by NOVÁTICA, and in Italian (abstracts and some articles online) by the Italian CEPIS society ALSI <http://www.alsi.it> and the Italian IT portal Tecnoteca <http://www.tecnoteca.it/>.
UPGRADE was created in October 2000 by CEPIS and was first published by NOVÁTICA and INFORMATIK/INFORMATIQUE, bimonthly journal of SVI/FSI (Swiss Federation of Professional Informatics Societies, <http://www.svifsi.ch/>).

E-mail addresses for editorial correspondence: see "Editorial Team" above
E-mail address for advertising correspondence: <novatica@ati.es>
Upgrade **Newslist** available at <http://www.upgrade-cepis.org/pages/editinfo.html#newslist>

ISSN 1684-5285

Next issue (August 2004):
"Software Agents"
(The full schedule of **UP**GRADE is available at our website)

Electronic Signature and Digital Identity

Guest Editors: Javier López-Muñoz, Apol·lònia Martínez-Nadal, and Ahmed Patel

Joint monograph with NOVÁTICA*

Mosaic

UPENET (UPGRADE European NETwork)

* This monograph will be also published in Spanish (full issue printed; summary, abstracts and some articles online) by NOVÁTICA, journal of the Spanish CEPIS society ATI (Asociación de Técnicos de Informática) at <http://www.ati.es/novatica/>, and in Italian (online edition only, containing summary abstracts and some articles) by the Italian CEPIS society ALSI and the Italian IT portal Tecnoteca at <http://www.tecnoteca.it>.

Electronic Signature Today: A Manufacturer's Wiewpoint

Francisco Jordan-Fernández and Jordi Buch i Tarrats

The purpose of this article is to present the view of Safelayer, a company that specialises in PKI (Public Key Infrastructure), of the current situation of PKI and electronic signature technologies. It takes a look at the technology, the business and the market involved, and finishes off by looking at some real cases that the company has been involved in.

Keywords: Certification Authority, Digital Identity, Electronic Signature, PKI, Public Key Infrastructure, Trusted Third Parties, TTPs.

1 Introduction

The Internet and electronic transactions have become established as the new way to interact. Based on a new technology, able to automate transactions by electronic means without the use of paper documents, it typically includes the exchange of information via e-mail, electronic data exchange, or the World Wide Web.

Various technological factors (the explosive expansion of the new communication technologies, and in particular the Internet explosion) plus business and economic factors (the electronic world creates opportunities for new services for customers, citizens, etc. thereby becoming a strategic necessity for companies and governmental bodies) have brought about a spectacular growth in this new way to transact over the Internet.

Due to its flexibility, ease of use and lack of explicit rules and restrictions, the Internet has become the most used platform and communication channel for electronic transactions. But it is precisely this absence of barriers and controls which restricts the use of the Internet as an open telematic network that makes it especially vulnerable to some serious risks which are threaten electronic communications. Unfortunately, the electronic systems and infrastructures that support electronic transactions are vulnerable to a wide range of threats from aggressors who can spy on and attack systems and the information transmitted during transactions. This is why the cornerstone of the development of our new Internet driven e-society is the trust we have in our governments, financial entities, enterprises, service providers and users of this new technology in general.

Public Key Infrastructure (PKI) and electronic signature (e-signature) are emerging as critical components of our new virtual Information Society. The ultimate control over the security of all the new technologies and services, whether Internet based or based on any other networks (in other words, cyberspace in general) is effectively dependent on the identification of the entities that are interacting within that space, and this is the principal mission of a PKI. The use of public key technology, electronic signature, digital certificates and the certification bodies (entities which issue the certificates) enable us to resolve a great many of the security problems that arise in a remote electronic transaction. What we like to call the e-signature effect predicts that this technology will be implemented in most of the infomedia services currently in existence and that it will enable the creation of new services which were previously impossible to set up for security reasons.

Finally, we need to bear in mind that PKI and e-signature technology is a strategic issue in our new information society at both a civil and a military level. This civil technology has become a vital platform for internal and external transactions of all our security forces and corps, not only at a national level but also at an international level of cooperation between states.

In the following points Safelayer Secure Communications, S.A., <http://www.safelayer.com/>, a company that specialises in PKI, sets out current situation of PKI and e-signature technologies. We present an up to date approach to the current technology, business and market, and finish off by looking at some real cases that the company has been involved in.

2 Reasons for Electronic Identity

The most frequent need for electronic identification is when we need to make a secure data exchange, the most common examples of which nowadays are web security applications, secure messaging and file protection. In all these systems

Francisco Jordan-Fernández is a Doctor of Telecommunications Engineering from the *Universidad Politécnica de Cataluña*, Spain. As associate professor at the same university he has participated in various national and international projects on security and PKI. In 1997 he was involved in the design and development of the SET (Secure Electronic Transaction) protocol of which an initial prototype was presented in 1998, the same year that he and a group of lecturers and students founded the company SET Projects S.L. In 1999 he co-founded Safelayer Secure Communications, S.A. in which he holds the position of vice-president of technology and is a board member. Safelayer is currently the leading PKI manufacturer in Spain and one of the most important in Europe, offering a complete range of PKI products.
<jordan@safelayer.com>

Jordi Buch i Tarrats is a Telecommunications Engineer and product marketing manager at Safelayer Secure Communications S.A. <jbt@safelayer.com>

it is necessary to securely identify who is allowed to access sensitive information before providing it, while at the same time identifying the author of that information. The solutions used in virtual banking are a clear example of the need for digital identification, one in which the client requires assurances that he is about to make an electronic transaction with his bank and not with some other entity impersonating it.

Digital certificate technology currently provides the most commonly used method of expressing digital identity in a trustworthy manner. In a way a digital certificate is like an identity card: it tells us who and what we are. Digital certificates can be given to individual people or groups of people and also to systems. The former can have digital certificates for authentication purposes with which a digital signature can be created or data protection provided. The latter can have digital certificates whose basic purpose is to achieve secure authentication, but also serves to receive protected information and to generate authenticated information.

While it is true that since 1997 a great many predictions have been made as to when the "*Year of PKI*" – the technology on which identification, digital signature and data protection is based – would finally come, it is expected to be gradually incorporated into applications over the next few years. The integration of PKI security services in all applications in an easy, simple and secure way will be a key factor in cost reduction.

2.1 Electronic Signature Today

Along with the assurances provided by electronic identification mechanisms based on digital certificates, we need to have assurances that the electronic data is authentic, has not been manipulated and is irrefutable. These assurances are provided by electronic signature which from a legal point of view can have the same validity as a handwritten signature.

The most important benefit electronic signature brings to e-commerce and all electronic transactional systems is that they cannot be repudiated. This service provides evidentiary value that proves that the data has been created by a specific entity and has not been altered since the date of its creation, thereby guaranteeing its irrefutability. Examples of types of data that require such an assurance are payments for purchases made by e-mail, bank balances, certificates of academic qualifications, medical prescriptions, or the plans of a building stored in a database.

Therefore, as this technology obviates the need to keep a hard copy of electronic documents, we can expect the use of electronic signature to be critical from the traditional viewpoint of cost reduction and process optimization. And the strategic benefits are not limited to the elimination of paper. Electronic signature also reduces risk and makes it possible to engage in e-business.

2.2 The Protection of Data

Electronic identification based on digital certificates also makes it possible to protect information and electronic communications. Examples of confidential data are the personal information of employees, an organization's customers, the company's business plans, etc. Electronic data is protected by encrypting it for the entities who will have exclusive access to it.

3 Need for the Public Key Infrastructure

Public Key Infrastructure, or PKI, facilitates both the control of entities (people or machines) by means of digital certificates, and the security services which guarantee the authenticity of those entities, their integrity, and the non-repudiability and confidentiality of data.

Another part of PKI's responsibilities is the provision of trustworthy services. Trusted Third Parties (TTPs) are responsible for ensuring the unique binding of entities with the socio-economic data certified by those entities, for uniquely binding a particular date with some particular data, or for providing evidentiary confirmation that those bindings continue to be valid over time. There are currently already a great many operational infrastructures: among others our company participates in the following infrastructures in Spain: CATCert (of the *Generalitat de Catalunya* – the Catalunya Regional Government), Izenpe (the Basque Country Regional Government), Ceres (Mint of Spain – FNMT), Plan Director CIS (the Ministry of Defence), Firmaprofesional (Professional Colleges), Camerfirma (Chambers of Commerce), CajaMadrid's (savings bank) Intranet, etc.

3.1 Basic Infrastructure

At the core of the basic PKI infrastructure is the Certification Authority (CA). This entity requires the services of a series of systems to enable it to manage digital certificates; i.e. to register users, renew certificates, revoke certificates, publish certificates and recover encryption keys if they are lost.

As we will see, no universal infrastructure exists, nor will one ever exist, but just as occurs in the case of physical identification, each infrastructure is contextualized according to the socio-economic sector and geographical location. It is very normal for users to have certificates issued by different infrastructures depending on the context they wish to access.

The Registration Authority (RA) plays an important role in the trustworthiness of the infrastructure. Its critical importance is due to two reasons:

- Firstly, the trustworthiness of the data included in the certificate depends on the security of the procedures used and on who is running the entity. For example, the inclusion of a professional attribute in the certificate must be backed up by the relevant professional college, whereas a person representing an enterprise and the powers of attorney he or she might have depend on the Chambers of Commerce or on the person's employment status within the enterprise itself.
- Secondly, because the issue of certificates must be done in a way that is simple, secure and integrated into corporate procedures. Different media (disc or smart card) will provide different levels of system security and user-friendliness, but certificates must be issued in the most automated way possible, for example, when the infrastructure is integrated transparently into existing corporate procedures. Certificates can thus be issued individually (personally or remotely via a telematic network) or automatically by

obtaining the required data from databases containing the users' credentials and creating certificates in automated batches.

3.2 Advanced Infrastructure

Advanced services are those providing additional services over and above the management of digital certificates. These include services that guarantee the validity of digital certificates or the validity of digital signatures. Other services can also be included, such as the notarisation of electronic documents.

Services checking the status of digital certificates are strategic in business processes which require an assurance that the status of a digital certificate has been checked during the digitally signed data acceptance process (for example, electronic transaction orders). The Validation Authority (VA) supplies the proof of validity (revoked or unrevoked certificate) of a given digital certificate at a particular moment, and takes responsibility for its responses.

The Time Stamp Authority (TSA) guarantees the time and binds it to some specific data by issuing time stamps. The purpose of time stamps is to guarantee the permanence of digital signatures by providing proof of the moment when the signature was created. Examples of systems requiring time stamps are Government services which need to certify delivery dates (records of receipts), electronic notary services or submission of tender deadlines, among others.

4 Applications: The e-Signature Effect

No one can be in any doubt that all our habits and processes that nowadays require paper will in the near future be served by bits and byes. By then society will be reaching such a degree of efficiency that economies (fuelled by unheard of margins and growth rates) and social habits (services, leisure, culture, etc.) will be totally transformed. Clearly, at this point in time, PKI is the only technology that can make the change from paper to bits and bytes a reality.

At present it is abundantly clear that PKI and e-signature are ***not*** applications but rather pure infrastructure. In the past PKI technology was marketed and acquired as an application, and this led to a frustrating situation for customers since once PKI had been implemented they discovered that there was no point using it while users had a digital identity but had no end applications that made use of that digital identity. The first and most widely used application that made use of digital identity was the secure web application in which web servers had a digital certificate which was normally named after the security protocol they used, i.e. SSL/TLS (Secure Socket Layer/Transport Layer Security). A Certification Authority is clearly a PKI application but it has no use outside the creation of the infrastructure itself. It is of no direct use for the majority of users; it is involved only indirectly via the certificates it issues.

Something akin to what has happened with PKI is now happening with new technologies like XML and WebServices. Like PKI these technologies are infrastructure, not applications: that is to say, they have no real use for end users; rather they are mechanisms and protocols which facilitate the creation of and dialogue between applications. As an infrastructure they are ideal for the deployment of applications which will make intensive use of Web environments in particular and the Internet in general. However, if we pause for thought we will realize that while XML technologies are newcomers on the scene, the universe of IT applications is truly ancient by comparison and that the current state of computing affairs is nothing more than a succession of active applications, most of which are not even connected to the Internet and, needless to say, none of them were designed with the Internet in mind. However, it is undeniable that the new XML technologies combined with EAI (Enterprise Application Integration) tools facilitate the integration of legacy applications with new and modern Internet based web application environments.

The *e-Signature Effect* is simply how Safelayer sees the integration of electronic signature in existing or new applications, and the subsequent *transformation of paper to bits and bytes*. It is not logical to think that all existing applications will be modified to incorporate electronic signature functions (although at one time that is exactly what was thought). It is more logical to expect e-signature to be incorporated either directly into applications, as happened with the *Y2K Effect* and the *Euro Effect*, or as a result of applications opening up to the Internet via XML/EAI. In the many and varied cases of e-signature integration it is likely that in some cases environmental limitations ruled out one of the two forms of integration, or else the E-signature effect was a result of a combination of the two.

Web service encryption and authentication applications (SSL/TLS), e-mail, and the signature of electronic web-based forms are already perfectly integrated into the e-signature effect, and currently account for most of the use of the PKI and electronic signature infrastructure, especially for web based use. However, there is a far more generic scenario in which the e-signature effect plays a role, one that is closely related to the document flows that we are so careful to manage in the paper world. This scenario is shown in Figure 1.

Like other pure PKI infrastructure companies, Safelayer has included tools in its technological and product strategy to make e-signature effect integration possible. This strategy is evidenced by the real applications that the company has developed or is currently developing which we list below:

- **Electronic Invoice:** According to a study carried out by the European Commission[1] the cost of an electronic invoice is between €0.27 and €0.47, as opposed to the €1.13 – €1.65 of a traditional invoice, a saving of up to 70%. But an electronic invoice also benefits both the issuer and the recipient as it allows the invoicing process to be automated thereby speeding up the process, improving security and reducing the number of incidents. For example, a large company which deals with thousands of customers and needs to keep up to date with the invoices generated by its day to day business (sending out, confirmation, etc.).

1. Source: Thomson EC Resources, Journal of Electronic Commerce, "Electronic Bill Presentment and Payment: The Next Step for the E-Commerce Market", by Thomas F. Horan.

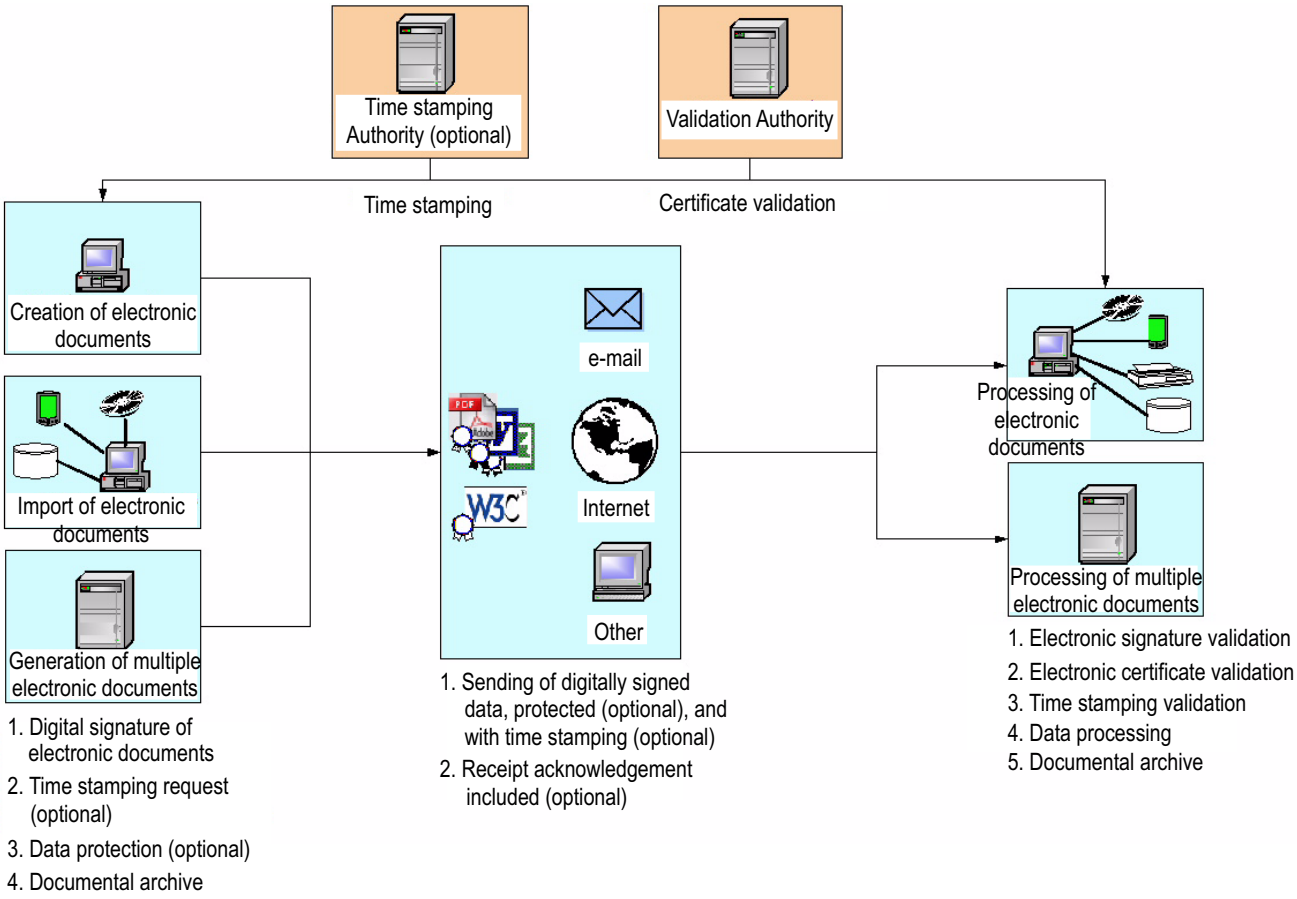

Figure 1: The e-Signature Effect and Documental Flows.

- **Human Resources and e-Recruitment:** In a temporary work agency the end-to-end time required to complete a traditional paper based recruitment process involving the candidate, the temporary work agency and the recruiting company up to the moment of signing the contract was, in the best of cases, 5 days. Using electronic methods, electronic signature and e-mail as the transport medium, the whole process could be completed in 5 minutes. Another ongoing experience concerns companies that have to renew contracts with their collaborators every so often. In most cases the use of traditional paper based procedures resulted in illegal situations as the collaborators nearly always ended up working for a long time without a valid contract. The introduction of electronic media, including electronic signature, makes it possible for the contracts to be drawn up and signed before the collaborators start work.
- **Electronic Certificates:** In their recent modernisation plan the Spanish Ministry of Justice has included the issue of electronic birth certificates, criminal records, etc., thereby providing a much faster and user-friendly paperless service. The citizen only needs to have access to the Internet to be able to apply for a certificate that a civil servant will issue and sign electronically before delivering it to the citizen electronically by e-mail or over the web. This is a typical example which could be extended to any kind of certified document or receipt.
- **Electronic Voting:** This is part of what is known as e-democracy and should not go unmentioned. It has not only been tried out by the Spanish Ministry of the Interior in the recent general elections on March 14, but it has also been used in shareholder meetings and other collective meetings which, as things stand now and given the present tyranny of the printed word, you either have to attend personally or have someone stand in for you to cast a proxy vote.

All the cases described above and many more, such as the fantastic success of the Social Security where more than 90% of the salaried workers pay their SS charges over the Internet, and the Tax Office which every year increases the number of internet contributors, only serve to confirm that the E-signature effect is already underway and that the transformation to the bit society is already underway, and all of this largely thanks to the existence of PKI and electronic signature technologies.

5 Conclusions

Our conclusion is that PKI and e-signature are already a reality and that the e-Signature Effect has already begun. As has occurred with all technological revolutions, society is being transformed and there can be no doubt that the future will be a digital one. Electronic signature is the 'wheel' of our digital civilization, and so far we have only seen the 'horse drawn carriage', but we are moving at breakneck speed towards a 'jet powered' paperless society; in other words, a digital society.

Sources

- Safelayer Secure Communications S.A. <http://www.safelayer.com>.
- IETF (Internet Engineering Task Force). <http://www.eitf.org>.
- ETSI (European Telecommunications Standards Institute). <http://www.etsi.org>.
- EESSI (European Electronic Signature Standardization Initiative). <http://www.ict.etsi.org/EESSI_home.htm>.
- W3C (World Wide Web Consortium). <http://www.w3c.org>.
- EAI (Enterprise Application Integration) Industry Consortium. <http://www.eaiindustry.org>
- Directive 1999/93/EC of the European Parliament and of the Council of 13 December 1999 on a Community framework for electronic signatures. <http://europa.eu.int/information_society/eeurope/2002/action_plan/pdf/esignatures_en.pdf>.
- Council Directive 2001/115/EC of 20 December 2001 amending Directive 77/388/EEC with a view to simplifying, modernising and harmonising the conditions laid down for invoicing in respect of value added tax. <http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_015/l_01520020117en00240028.pdf>.