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>.

Presentation

Electronic Signature as the Key to Security in the Information Society

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

1 Introduction

There can be little doubt that the 21st century will be characterised by the development and consolidation of the so called *Information and Knowledge Society*. The positive effects arising out this should reach all areas of our society. But all the studies carried out on this matter agree that citizens, business people and government officials are still very wary of using information and communication technologies, the most important of which is currently the Internet. This lack of *trust* with regard to the transmission of information over computer networks is a serious obstacle on the path towards progress of important applications areas like e-Government and electronic commerce (e-Commerce). *Electronic signature* should enable us to raise the real level of security and the security perceived by the players involved in these new scenarios.

But electronics signatures also enable us to verify the source (*authenticity*) of information received over telecommunications networks, and ensure that it has not been manipulated along the way (*integrity*). This could already be achieved with conventional cryptography or secret key cryptography, but electronic signatures also ensure that the sender of an electronically signed message cannot subsequently deny having sent it (*non-repudiation* of source). Public key based electronic signature forms part of what has come to be known as *Public Key Infrastructure* (PKI). This infrastructure has led to the emergence of certification service providers (or certification authorities) without whom the large scale use of electronic signature would not be possible. Certification service providers issue *electronic certificates* which are electronic documents linking the identity of a person (or entity) to a signature verification public key which in turn are mathematically linked to a private key which should only be known to the rightful owner of the key pair.

In addition to *technological solutions* (in this case public key cryptography based electronic signature) it was necessary to establish a *legal framework* in order to maximise users' trust in the system. In the European Union countries current legislation considers an electronic signature as the equivalent of a handwritten signature (providing, of course, that it complies with certain requirements). Once provided with a suitable legal and technical legal framework, electronic signature should serve as a catalyst for the incorporation of electronic communications security solutions for transactions involving governments and enterprises, thereby benefiting the citizens that use it.

The Guest Editors

Javier López-Muñoz is a Doctor of Computer Engineering, attached to the Area of Telematics Engineering of the Dept. of Computer Languages and Sciences at the *Universidad de Málaga*, Spain. He lectures as an Associate Professor at the Higher School of Informatics Engineering and carries out research work as part of Malaga University's GISUM group (Software Engineering Group), in which he coordinates the security subgroup. His research is currently centred on the field of security in communication networks and electronic commerce, a field in which he has carried out part of his research work in various US university centres specialising in the subject. In GISUM he is the technical head of several research projects relating to practical aspects of ICT security, perhaps the most important of which is the international Global PKI project of Japan's Telecommunications Advancement Organization. He is also the technical director of the IST's CASENET project, part of the 5th Framework Programme of the European Union. He is co-editor of the "Security" section of ***Novática*** and was guest editor for the December 2002 monograph of ***Novática*** and ***Upgrade*** on "Security in e-Commerce".<jlm@lcc.uma.es>

Apol·lònia Martínez-Nadal is Professor of Commercial Law at the *Universidad de las Islas Baleares*, Spain, and a specialist in the legal study of electronic commerce in general and electronic signature in particular. She has participated in various national and European research projects on these matters, has given numerous lectures and seminars, and has authored a great many publications on these topics. She authored the first legal monograph published in Spain on electronic signatures in 1998, which ran into two further editions (2000 and 2001); she has also published the first legal monograph on the Spanish Royal Decree-Law 14/1999, which also ran into two more editions (2000 and 2001) and has drafted a systematic comment on the recent Spanish Law 59/2003 on Electronic Signature which is soon to be published. <dpramn0@uib.es>

Ahmed Patel is a Lecturer in the Department of Computer Science, University College Dublin, Ireland, and Head of the Computer Networks and Distributed Systems Research Group. His research interests span topics concerning international networking and application standards, network security, digital forensics, cybercrime investigations, high-speed networks, heterogeneous distributed computer systems and including distributed search engines and systems for the Web. He has published wellover hundred technical papers and co-authored two books on computer network security and one book on group communications. He is a member of the Editorial Advisory Board of the Computer Communications, Computer Standards Interface and Digital Investigation Journals.
<apatel@cnds.ucd.ie>

2 The Content of this Monograph

In the light of all the above, for the purpose of this monograph we have chosen a healthy selection of interesting articles, starting with an article which provides a panoramic introduction to the subject for all kinds of readers, specialist or otherwise, from ***Arturo Ribagorda-Garnacho***, *"Digital Signature at the Heart of Information Security Development: An Overview"*. He explains the concept of digital signature and justifies the need for public key certificates, rounding off with a description of the role played by certification authorities and, by extension, by Public Key Infrastructures as generators of trust in the system as a whole.

The first block of articles are of a technical nature, describing practical experiences almost all of them. It starts with the article *"Creating a Cross-Domain Public Key Infrastructure: The Keystone Project"*, by ***Ahmed Patel***, where a scalable and robust architecture for the cross-domain Public Key Infrastructure (PKI) is described. Next, *"Certification Practise Statements: The National Mint of Spain's Experience"*, by ***Josep-Lluís Ferrer-Gomila*** and ***Magdalena Payeras-Capellà***, takes a close look at certification practices statements as a vital component of a proper framework for the use of electronic signature, and comments on the certification practices statements used by the Spanish National Mint (FNMT-RCM), one of the most important certification providers in Spain. ***Gemma Déler-Castro*** and ***Juan-Carlos Cruellas-Ibarz***, in *"Electronic Signature Functionality and Security Requirements"*, analyse the value of electronic signature as a symbol of assurance and trust in the virtual world, and focus on the fact that its widespread introduction and proper functioning depend on the compliance of its products, services and systems with functional and security requirements and the existence of a training process for all the parties involved. In the next article, *"Electronic Signature Today: A Manufacturer's Viewpoint"*, ***Francisco Jordan-Fernández*** and ***Jordi Buch i Tarrats*** present the vision that their company, Safelayer, has of the current situation of PKI and electronic signature technologies, giving their viewpoint on the technology, the business and the market, illustrated with references to actual cases that the company has been involved in. ***Iñaki Echevarria-Larrinaga***, ***Oscar García-Jimeno***, ***Juan A. Martín-Zubiaur***, ***Víctor Llorente-Gómez*** and ***Javier Areitio-Bertolín***, in their article *"Development of an Integrated Document Management System with Advanced Electronic Signature Service"* describe the design, architecture, functionalities and technologies used in the development of a scalable, distributed and fault tolerant system integrating document management within a public key infrastructure. Finally, ***Petr Švéda*** and ***Václav Matyáš***, in their article *"Digital Signatures and Electronic Documents: A Cautionary TaleRevisited"*, identify and analyse different types of trust and provide a broad overview of how they affect the use of digitally signed documents.

The second block of the monograph looks at the current legal framework relating to electronic signature in Europe. In her article *"Electronic Signature: An Analysis of the Main European and International Legal Regulations"*, ***Nadina Foggetti*** compares the UNCITRAL (United Nations Commission on International TRAde Law) Model Law with the European Directive and describes the various ways that the latter has been implemented in several European countries. In *"Electronic Signatures and Electronic Identity Card in the European Context and in Spanish Law"*, ***Apol·lònia Martínez-Nadal*** comments on the Spanish Law 59/2003 on electronic signature within the frame of the European legislation; she pays special attention to the what is known as electronic ID which, while it offers some undeniable advantages to citizens, also gives rise to a series of doubts and concerns. Next, ***Rafael Illescas-Ortiz***, in his article *"The UNCITRAL Model Law on Electronic Signatures"*, describes how in 2001 the United Nations created a Model Law to help states around the world to draft internationally uniform and globally valid national laws on electronic signature; the article goes on to analyse this Model Law which has served as a basis for legislations drafted in a number of Latin American countries. Finally, developing this theme, ***Mariliana Rico-Carrillo***, from Venezuela, in her article *"Legal Initiatives on Electronic Signature in Latin America"*, takes a look at the content of regulatory laws in place in several Latin American countries.

We close this presentation expressing our thanks to all the authors for their valuable collaboration and also to the editors of ***UPGRADE*** and ***Novática*** for the opportunity to produce this monograph, one which we hope will be both interesting and useful to readers of the two journals.

Translation by ***Steve Turpin***

Useful References on "Electronic Signature"

Readers interested in delving deeper into the subject of this monograph may like to consult the following sources, that complement the references provided by the authors of the papers included in this issue.

Books

Jalal Feghhi, Peter Williams, Jalil Feghhi.
Digital Certificates: Applied Internet Security, Addison-Wesley 1998.

Gail L. Grant.
Understanding Digital Signatures: Establishing Trust Over the Internet and Other Networks, McGraw-Hill Osborne, 1997.

Ben Hammond.
Digital Signatures, Osborne/McGraw-Hill, 2002.

Birgit Pfitzmann.
Digital Signature Schemes: General Framework and Fail-Stop Signatures, Lecture Notes in Computer Science 1100, Springer-Verlag, 1996

Fred Piper, Simon Blake-Wilson, John Mitchell.
Digital Signatures Security and Controls, Information Systems Audit and Control Foundation, 2000

A. Martínez Nadal.
Comentarios a la Ley 59/2003 de Firma Electrónica, Editorial Civitas (in Spanish; to be published soon.)

Events

- IWAP 2004 (International Workshop for Applied PKI), Fukuoka (Japón), 3-5 October 2004. <http://itslab.csce.kyushu-u.ac.jp/iwap04/>.
- 1st EuroPKI (European PKI Workshop: Research and Applications), Isla de Samos (Grecia), 25-26 June 2004. <http://www.aegean.gr/EuroPKI2004/>.

Web Sites

- Bitpipe, Digital Signatures Reports. <http://www.bitpipe.com/data/rlist?t=itmgmt_10_50_20_12_2&sort_by=status&src=findwhat>.
- CERES (CERtificación Española, National Mint of Spain, FNMT-RCM). <http://www.ceres.fnmt.es/> (in Spanish.)
- European Electronic Signature Standardization Initiative (EESSI), CEN/ISSS Electronic Signature Workshop. <http://www.ictsb.org/EESSI_introduction.htm>.
- Digital Signature Links. <http://www.qmw.ac.uk/~tl6345/>.
- Digital Signature Resource Center. <http://www.digitalsignature.be/d_vs_e.cfm>..
- Digital Signature Resources. <http://www.123-digital-signature.com/>.
- Digital Signature Standard (DSS). <http://www.itl.nist.gov/fipspubs/fip186.htm>.
- e-Commerce Law Resources. <http://www.bakerinfo.com/ecommerce/>.
- Electronic Privacy Information Center, Digital Signatures. <http://www.epic.org/crypto/dss/>.
- HIPAAdvisory. <http://www.hipaadvisory.com/tech/DigitalSignature.htm>.
- The PKI Page. <http://www.pki-page.org/>.
- W3 Consortium, XML-Signature Syntax and Processing. <http://www.w3.org/TR/xmldsig-core>.