novática
UPGRADE Revista de la Asociación de Técnicos de Informática

Novática, revista fundada en 1975 y decana de la prensa informática española, es el órgano oficial de expresión y formación continua de **ATI** (Asociación de Técnicos de Informática). ***Novática*** edita también ***Upgrade***, revista digital de **CEPIS** (*Council of European Professional Informatics Societies*), en lengua inglesa, y es miembro fundador de **UPENET** (*UPGRADE European NETwork*)

<http://www.ati.es/novatica/>
<http://www.upgrade-cepis.org/>

ATI es miembro fundador de **CEPIS** (*Council of European Professional Informatics Societies*) y tiene un acuerdo de colaboración con **ACM** (*association for Computing Machinery*). Tiene asimismo acuerdos de vinculación o colaboración con **AdaSpain**, **AI2** y **ASTIC**.

Coordinación Editorial, Redacción Central y Redacción ATI Madrid
Padilla 66, 3º, dcha., 28006 Madrid
Tlfn.914029391; fax.913093685 <novatica@ati.es>
Composición, Edición y Redacción ATI Valencia
Av. del Reino de Valencia 23, 46005 Valencia
Tlfn./fax 963330392 <secreval@ati.es>
Administración y Redacción ATI Cataluña
Via Laietana 41, 1º, 1ª, 08003 Barcelona
Tlfn.934125235; fax 934127713 <secregen@ati.es>
Redacción ATI Andalucía
Isaac Newton, s/n, Ed. Sadiel,
Isla Cartuja 41092 Sevilla, Tlfn./fax 954460779 <secreand@ati.es>
Redacción ATI Aragón
Lagasca 9, 3-B, 50006 Zaragoza.
Tlfn./fax 976235181 <secreara@ati.es>
Redacción ATI Asturias-Cantabria <gp-astucant@ati.es>
Redacción ATI Castilla-La Mancha <gp-clmancha@ati.es>
Redacción ATI Galicia
Recinto Ferial s/n, 36540 Silleda (Pontevedra)
Tlfn.986581413; fax 986580162 <secregal@ati.es>
Suscripción y Ventas
<http://www.ati.es/novatica/interes.html>, o en ATI Cataluña o ATI Madrid
Publicidad
Padilla 66, 3º, dcha., 28006 Madrid
Tlnf.914029391; fax.913093685 <novatica.publicidad@ati.es>
Imprenta
9 Impressió S.A., Juan de Austria 66, 08005 Barcelona.
Depósito Legal: B 15.154-1975 -- ISSN: 0211-2124; CODEN NOVAEC
Portada: Antonio Crespo Foix / © ATI 2004
Diseño: Fernando Agresta / © ATI 2004

Nº 169, mayo-junio 2004, año XXX

sumario

Monografía del próximo número: "Agentes Software"

Javier López Muñoz [1], Apol·lònia Martínez Nadal [2], Ahmed Patel [3]
[1] Universidad de Málaga; [2] Universidad de las Islas Baleares; [3] University College Dublin (Irlanda)

<jlm@lcc.uma.es>,
<dpramn0@uib.es>,
<apatel@ccvax.ucd.ie>

Presentación
La firma electrónica, clave para la seguridad en la Sociedad de la Información

1. Introducción

Con toda certeza el siglo XXI se caracterizará por el real desarrollo e implantación de la denominada Sociedad de la Información y del Conocimiento. Los efectos positivos que se derivan de la misma deben llegar a todos los ámbitos de nuestra sociedad. Pero todos los estudios realizados en relación a la materia coinciden en señalar que existe una fuerte desconfianza por parte de los ciudadanos, empresarios y responsables de las Administraciones Públicas, a la hora de utilizar las tecnologías de la información y las comunicaciones, de las que Internet es el máximo exponente en estos momentos. Esta desconfianza a la hora de transmitir información a través de las redes telemáticas se traduce en un serio freno en el camino hacia la Administración Digital (*e-Government*) y el comercio electrónico. La **firma electrónica** es uno de los elementos que debe permitir aumentar el grado de seguridad real, y percibido, por parte de los actores que intervienen en estos nuevos escenarios.

La firma electrónica permite comprobar la procedencia (autenticidad) de la información recibida a través de las redes de telecomunicaciones, y que no ha sido manipulada en tránsito (integridad). Estas propiedades ya se podían conseguir con la criptografía convencional o criptografía de clave secreta, pero, además, la firma electrónica permite garantizar que el emisor de un mensaje firmado electrónicamente no podrá negar a posteriori haber realizado tal acción (no repudio en origen). La firma electrónica, basada en la criptografía de clave pública, se enmarca en lo que se ha venido en llamar **infraestructura de clave pública** (PKI, *Public Key Infrastructure*). Surgen en esta infraestructura los prestadores de servicios de certificación (o autoridades de certificación), que son los sujetos que hacen posible el uso a gran escala de la firma electrónica. Para ello expiden **certificados electrónicos**, que son documentos electrónicos que vinculan la identidad de una persona (o entidad) a una clave pública de verificación de firma, la cual está relacionada matemáticamente con una clave privada que sólo debe conocer el lícito propietario del par de claves.

Además de las soluciones tecnológicas (en este caso la firma electrónica basada en la criptografía de clave pública) era preciso el establecimiento de un marco jurídico para generar el máximo nivel de confianza por parte de los usuarios. En Europa, y más concretamente en España, la legislación vigente equipara la firma electrónica (evidentemente con el cumplimiento de unos determinados requisitos) a la firma manuscrita. Siendo así, y disponiendo por tanto de un adecuado marco jurídico y técnico, la firma electrónica podrá servir como catalizador para la incorporación de las tecnologías de seguridad de las comunicaciones electrónicas en la actividad de las Administraciones Públicas y de las empresas, con el consiguiente beneficio para los ciudadanos.

2. El contenido de esta monografía

En concordancia con lo expuesto anteriormente, para este monográfico hemos seleccionado un buen número de artículos de interés, comenzando con un artículo que introduce la materia para todo tipo de lectores, espcializados o no, a cargo de ***Arturo Ribagorda Garnacho***, "*La firma digital como soporte de confianza de la Sociedad de la Información"*, donde se explica el concepto de firma digital y se justifica la necesidad de los certificados de clave pública, concluyendo con la descripción del papel de las Autoridades de Certificación y, por extensión, de las Infraestructuras de Clave Pública como soporte de confianza de todo el sistema establecido.

El primer bloque de artículos tiene un carácter técnico, comenzando con el artículo *"La Declaración de Prácticas de Certificación de la FNMT-RCM"* de ***Josep Lluís Ferrer Gomila*** y ***Magdalena Payeras Capellà***, en el que se profundiza en las Declaraciones de Prácticas de Certificación como elemento esencial a la hora de establecer un marco adecuado para el uso de la firma electrónica y se comentan las declaraciones de prácticas de certificación de la FNMT-RCM, uno de

Nota del Editor de Novática: por razones de espacio no se incluyen en esta monografía los artículos "*Creating a Cross-Domain Public Key Infrastructure: The Keystone Project*", de ***Ahmed Patel***;"*Firma electrónica y documentos digitales: la confianza como prerrequisito*", de ***Petr Švéda*** y ***Václav Matyáš***; y "*Firma Electrónica: análisis comparativo de la legislación europea e internacional*", de ***Nadina Foggetti***, que fueron seleccionados por los editores invitados.

Estos artículos han sido publicados en el número 3/2004 de ***Upgrade***, <http://www.upgrade-cepis.org>, en inglés, y serán publicados en próximos números de ***Novática***, en castellano.

Editores invitados

Javier López Muñoz es Doctor Ingeniero en Informática, adscrito al Área de Ingeniería Telemática del Departamento de Lenguajes y Ciencias de la Computación de la Universidad de Málaga. Desarrolla su actividad docente como Profesor Titular en la ETS de Ingeniería Informática y su labor investigadora dentro del grupo GISUM (Grupo de Ingeniería del Software) de esta universidad, donde coordina el subgrupo de Seguridad. Su actividad investigadora está centrada en el área de Seguridad en Redes de Comunicación y en Comercio Electrónico, habiendo realizando parte de esa labor de investigación en varios centros universitarios de E.E.U.U. especializados en la materia. En GISUM es responsable técnico de varios proyectos de investigación relacionados con los aspectos prácticos de Seguridad de las TIC, entre los que destaca el proyecto internacional Global PKI de la Telecommunications Advancement Organization de Japón. Asimismo, es Director Técnico del Proyecto CASENET de IST dentro del V Programa Marco de la Unión Europea. Es co-editor de la sección de "Seguridad" de *Novática*, habiendo sido editor invitado de la monogarfía de su número 160 sobre "Seguridad en e-Comercio".

Apol·lònia Martínez Nadal es Profesora Titular de Derecho Mercantil y especialista en en el estudio jurídico del comercio electrónico en general y de la firma electrónica en particular. Ha participado en distintos proyectos de investigación nacionales y europeos sobre estas materias, ha impartido numerosas conferencias y seminarios y es autora de numerosas publicaciones sobre estos temas; en concreto, es autora de la primera monografía jurídica publicada en España sobre firma electrónica en 1998 y que ha sido objeto de dos ediciones posteriores (2000 y 2001); ha publicado también la primera monografía jurídica sobre el Real Decreto-Ley 14/1999, objeto también de dos ediciones (2000 y 2001) y ha elaborado un comentario sistemático de la reciente Ley 59/2003 de firma electrónica de próxima aparición en el mercado editorial.

Ahmed Patel es profesor del Departamento de Ciencias de la Computación del University College Dublín (Irlanda) y director del Grupo de Investigación sobre Redes Telemáticas y Sistemas Distribuidos. En el campo de la investigación sus intereses comprenden temas como estándares internacionales para redes y aplicaciones, seguridad de redes, actividades digitales forenses, análisis de delitos informáticos, redes de alta velocidad y sistemas distribuidos heterogéneos, así como motores y sistemas de búsqueda distribuida en la Web. Ha publicado más de un centenar de artículos técnicos y ha sido co-autor de dos libros sobre seguridad de redes telemáticas y de uno sobre comunicaciones grupales. Es miembro del Consejo Asesor Editorial de las revistas Computer Communications, Computer Standards Interface y Digital Investigation.

los prestadores más importantes radicados en España.

A continuación, ***Gemma Déler Castro*** y ***Juan Carlos Cruellas***, en "*Requisitos de funcionalidad y seguridad en firma electrónica* ", analizan el valor de la firma electrónica como símbolo de garantía y confianza en el mundo virtual, y profundizan en el hecho de que para su correcta implantación y funcionamiento sea necesario que los productos, servicios y sistemas cumplan con los requisitos funcionales y de seguridad además de que haya un proceso de formación de todas las partes que intervienen.

Posteriormente, ***Francisco Jordan Fernández*** y ***Jordi Buch i Tarrats***, en el artículo "*La firma electrónica hoy: visión de un fabricante* ", desarrollan la visión de la empresa Safelayer en cuanto a la situación actual de las tecnologías de PKI y firma electrónica, ofreciendo un enfoque sobre la tecnología, el negocio y el mercado, rubricado con referencias a casos reales ejecutados por la propia compañía.

Iñaki Echevarria Larrinaga, ***Oscar García Jimeno***, ***Juan A. Martín Zubiaur***, ***Víctor Llorente Gómez*** y ***Javier Areitio Bertolín***, en el artículo **"***Desarrollo de un Sistema Integrado de Gestión Documental con Servicio de Firma Electrónica Avanzada***"**, describen el diseño, arquitectura, funcionalidades y tecnologías utilizadas para el desarrollo de un sistema escalable, distribuido y tolerante a fallos que integra la gestión documental con una infraestructura de clave pública.

En el segundo bloque de la monografía se analiza el marco legal vigente en relación con la firma electrónica. ***Apol·lònia Martínez Nadal***, en su artículo *"La legislación española sobre el DNI en el contexto europeo"*, comenta como la reciente Ley 59/2003 de firma electrónica deroga al Real Decreto-Ley 14/1999 e introduce algunas reformas y novedades, que son analizadas en este artículo. De entre ellas, se dedica una especial atención al denominado DNI electrónico, que presenta indudables ventajas para los ciudadanos pero que genera también algunas dudas.

Posteriormente, ***Rafael Illescas Ortiz***, en su artículo *"La Ley modelo de la CNUDMI/UNCITRAL sobre las firmas electrónicas ""* describe cómo las Naciones Unidas establecieron el 2001 una Ley modelo para facilitar a los estados la elaboración de leyes nacionales sobre la firma electrónica dotadas de uniformidad internacional y validez global, y analiza esta Ley modelo, que ha servido como base para otras normas establecidas en algunos países latinoamericanos.

Enlazando con esto, ***Mariliana Rico Carrillo***, en su artículo "*Iniciativas legales sobre firma electrónica en Latinoamérica* ", repasa el contenido de las normas en ocho de los países latinoamericanos.

Finalmente, ***Nadina Foggetti***, en su artículo *"Firma Electrónica: análisis comparativo de la legislación europea e internacional"* compara el modelo de UNCITRAL con la Directiva Europea y describe las diferentes formas en que ésta última se ha implementado en diversos países europeos.

Agradecemos a todos los autores su valiosa colaboración y a los editores de ***Novática*** y ***UPGRADE*** la oportunidad de elaborar esta monografía, que esperamos sea de interés y utilidad para los lectores de ambas revistas.

Referencias útiles sobre "Firma electrónica"

Las siguientes fuentes, junto con las referencias que aparecen en los distintos artículos de esta monografía, permitirán a los lectores interesados conocer con más profundidad el tema objeto de la misma.

Sitios Web

- 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, FNMT-RCM). <http://www.ceres.fnmt.es/>.
- 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/Digital Signature.htm>.
- W3 Consortium, XML-Signature Syntax and Processing. <http://www.w3.org/TR/xmldsig-core>.

Libros

- **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.
- **Jalal Feghhi, Peter Williams, Jalil Feghhi.** *Digital Certificates: Applied Internet Security*, Addison-Wesley 1998.
- **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 (en prensa).

Congresos

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