Uso de la identidad digital en la Universidad de Zaragoza. Algunas experiencias del sistema LEFIS UNIZAR PKI

Fernando Galindo[1], Javier García Marco[2], Pilar Lasala[3]

Universidad de Zaragoza

Resumen

Se presenta las principales características de varias experiencias, relacionadas con el uso de la identificación digital que permite el sistema **LEFIS UNIZAR PKI**, que tienen el fin de promover la puesta en aplicación de la Ley de Acceso de los Ciudadanos a las Administraciones Públicas y la Ley de Firma electrónica. Las experiencias han sido realizadas por el Grupo de Investigación "Protección de datos y firma electrónica" en actividades desarrolladas como resultado de proyectos de I+D+I con financiación obtenida de la Unión Europea, el Estado Español, la Comunidad Autónoma de Aragón, empresas y otras instituciones.

1 Introducción

Con investigaciones de carácter interdisciplinar cuyos orígenes se remontan a 1984[4], el Grupo de Investigación "Protección de Datos y Firma Electrónica"[5] trabaja desde la Universidad de Zaragoza (desde 1997) considerando como objetivo de las

[1] cfa@unizar.es. Departamento de Derecho Penal, Filosofía del Derecho e Historia del Derecho. Universidad de Zaragoza

[2] jgarcía@unizar.es. Departamento de Ciencias de la Documentación e Historia de la Ciencia. Universidad de Zaragoza

[3] lasala@unizar.es.- Departamento de Métodos Estadísticos. Universidad de Zaragoza

[4] Se encuentra una historia de las actividades del grupo en F. Galindo, 'From legal thesaurus to e-signatures', en A. Paliwala (ed.) *A history of legal informatics*, LEFIS Series vol. 9, Zaragoza, Prensas Universitarias, 2010, pp. 203-224

[5] http://www.lefis.org/index.php?option=com_content&task=view&id=173&Itemid=511

mismas el impulso de la confianza y la calidad en los sistemas de identificación digital extrayendo propuestas y planteamientos a partir de las experiencias que genera el sistema **LEFIS UNIZAR PKI** que se presenta resumidamente en este trabajo. El sistema es parte constitutiva de varias actividades y proyectos de alcance internacional, cuyo contenido se resume aquí en cuanto son claros ejemplos de las consecuencias del uso de la tecnología de clave pública que es base de los contenidos regulativos de las Leyes de Acceso de los Ciudadanos a las Administraciones Públicas y Firma electrónica.

El presente trabajo realiza lo siguiente: consigna una breve caracterización del grupo (2), reseña las notas básicas del sistema de identificación digital **LEFIS UNIZAR PKI** construido (3), muestra los datos básicos de actividades y proyectos originados a partir de experiencias habidas con la utilización del sistema (4) y concluye (5).

2 Presentación del Grupo

Reconocido como Grupo de Investigación por el Gobierno de Aragón en noviembre de 2003, el Grupo de Investigación Consolidado "Protección de Datos y Firma Electrónica" trabaja, como su nombre hace ver, en el desarrollo, gestión y análisis de sistemas de identificación digital que permitan operar en Internet de forma segura, confiable y legal. El Grupo, de carácter interdisciplinar, ha colaborado y colabora en el desarrollo y puesta en marcha de sistemas de identificación capaces de proporcionar seguridad y confiabilidad de acuerdo con el ordenamiento jurídico vigente, atendiendo a las virtualidades del desarrollo tecnológico propio de la sociedad del conocimiento y a su efectiva implantación, por una parte en la práctica de las Administraciones Públicas en relación a la prestación de servicios a los ciudadanos mediante el uso de Internet, y, por otra, en el desenvolvimiento del comercio electrónico.

Financiado por medio de las subvenciones obtenidas en concursos públicos existentes para proyectos de investigación europeos, nacionales y autonómicos, y por convenios y contratos de I+D realizados con empresas y Administraciones Públicas, el Grupo de Investigación viene centrando su actividad en varias líneas de trabajo que se concretan en lo siguiente:

- elaboración de propuestas de normas, códigos de práctica y documentos de seguridad sobre protección de datos personales y firma electrónica
- construcción de aplicaciones sobre comercio y administración electrónica
- construcción de sistemas criptográficos
- análisis de los sistemas de información de las Administraciones Públicas en el contexto de la Sociedad de la Información
- desarrollo de estrategias de inclusión digital en el ámbito del e-GOV (Gobierno electrónico), y
- desarrollo y puesta en acción de campus virtuales de ámbito global.

El apartado 4 da cuenta sucinta de algunas de las actividades que concretan el desarrollo de estas líneas.

3 El sistema de identificación digital LEFIS UNIZAR PKI

El núcleo central del desarrollo de las líneas de investigación expuestas está constituido por el sistema de identificación digital **LEFIS UNIZAR PKI**[6] diseñado, construido, experimentado y gestionado por el Grupo, de cuyas características básicas damos cuenta en este apartado.

a) Introducción

Poniendo en práctica varios proyectos (iniciados en 1997) se desarrollan en la Universidad de Zaragoza desde 2003 experiencias dirigidas a habituar a estudiantes de la Facultad de Derecho, la Facultad de Ciencias (Matemáticas) la Escuela de Ingenieros y la Facultad de Filosofía y Letras (estudiantes de Gestión de Sistemas de Información y Documentación) a la obtención y uso de certificados digitales de clave pública emitidos por la autoridad de certificación no reconocida LEFIS UNIZAR, establecida y gestionada por el Grupo de Investigación "Protección de datos y firma electrónica", como medio de identificación para acceder a cursos y materiales localizados en servidores propios de la Universidad y de otras instituciones. Las experiencias tienen como fin familiarizar a estudiantes y profesores en el contenido y la puesta en práctica de la Ley 11/2007, de 22 de

[6] http://lefis.unizar.es/pki

junio, de acceso electrónico de los ciudadanos a los Servicios Públicos y la Ley 59/2003, de 19 de diciembre, de firma electrónica.

En las experiencias han participado y participan profesores y estudiantes que realizan sus estudios y trabajo en los siguientes países y ciudades: Alemania (Münster), Argentina (La Plata), Brasil (Santa Catarina y Curitiba), Finlandia (Rovaniemi y Vaasa), Lituania (Vilnius), Polonia (Torun), Portugal (Beja), Reino Unido (Belfast y Leeds), Turquía (Estambul) y Uruguay (Montevideo). En cuanto a España, los estudiantes proceden de prácticamente todo el país una vez que de las actividades expresadas también son partícipes profesores y estudiantes de la Universidad de La Laguna y estudiantes que forman parte del Campus Virtual Compartido del denominado "Grupo 9 de Universidades" (formado por las Universidades de Cantabria, Castilla la Mancha, Extremadura, Islas Baleares, la Rioja, Navarra, Oviedo, País Vasco y Zaragoza).

b) Algunos datos

El número total de certificados de clave pública emitidos a profesores y alumnos en el periodo comprendido entre el 1 de octubre de 2007 y el 30 de septiembre de 2009 fue 626.

El número total de certificados emitidos hasta la fecha de hoy (12 de marzo de 2010) es 795[7].

Mediante el uso del correspondiente certificado digital, utilizado como medio de identificación, estudiantes y profesores han accedido en el curso 2008-2009 a 58 cursos y a material contenido en los mismos situados en la página Web del denominado Campus Virtual Compartido Derecho y Tecnologías de la Información[8].

En la actualidad (curso 2009-2010) se hacen pruebas de obtención y uso de certificados digitales de clave pública en 6 cursos impartidos por la Universidad de Zaragoza en la Facultad de Derecho, la Escuela de Ingenieros y la Facultad de Filosofía y Letras (el Máster de Gestión de sistemas de Información y Documentación). Uno de los cursos, justamente el que se ocupa de introducir a la

[7] https://lefis.unizar.es/pki/index.php?option=com_wrapper&Itemid=25

[8] http://www.lawict.eu

"Administración electrónica" es impartido en modalidad "on line" en el Campus Virtual del G9[9].

c) La infraestructura de clave pública

La Infraestructura de Clave Pública LEFIS UNIZAR[10] (**LEFIS UNIZAR PKI**) es un efectivo sistema de seguridad y garantía de las comunicaciones del Grupo de Investigación , cuyo objetivo incluye la protección de la privacidad e integridad de los datos, y la identificación de los emisores. Está desarrollado para su uso en aplicaciones concretas. La Autoridad de Certificación ha sido constituida y es mantenida por el mismo Grupo de Investigación, quien se encarga también de la emisión y revocación de certificados.

La Infraestructura de Clave Pública permite la emisión de certificados a utilizar por los integrantes de la Universidad y por los participantes de la red LEFIS (Legal Framework for the Information Society)[11].

En el proceso de emisión de un certificado bajo la estructura de la **LEFIS UNIZAR PKI**, intervienen además, las Entidades de Registro. La primera Entidad está integrada por el grupo de profesores que constituye el Grupo de Investigación. Está desarrollado el sistema que permite la constitución de otras Entidades de Registro de la Autoridad de Certificación.

Para el diseño, construcción y gestión del sistema se utilizan las herramientas de software libre Open CA[12] y Moodle[13].

[9] http://www.uni-g9.net/

[10] http://lefis.unizar.es/pki

[11] http://www.lefis.org/

[12] http://www.openca.org/

[13] http://moodle.org/

4 Actividades

a) LEFIS

El sistema **LEFIS UNIZAR PKI** es uno de los elementos básicos de las actividades realizadas por el Grupo. Entre estas, una de las principales toma forma en **LEFIS** (Legal Framework for the Information Society)[14]. Se trata de una Red Temática, inicialmente financiada por el programa Sócrates, que participa desde 2003 en varios proyectos y programas apoyados por la Unión Europea, el Gobierno Español y gobiernos regionales de los lugares en donde están situados sus miembros, esto es toda Europa y Sudamérica, especialmente Argentina, Brasil, Chile y Uruguay. Hoy LEFIS es una activa red internacional con repercusión en toda la UE, Sudamérica, África y Asia: 127 instituciones, 348 personas participantes y 44 países, y con interés común en el Marco Legal de la Sociedad de la Información.

LEFIS UNIZAR PKI permite a los miembros de la red introducir información y acceder a zonas reservadas de la misma, situadas en la página Web de LEFIS, utilizando la infraestructura de clave pública. LEFIS es, desde finales de 2007, una marca registrada en el registro europeo de marcas y patentes.

b) APTICE

Otra actividad es el **Proyecto APTICE**[15], o lo que es lo mismo, la elaboración y puesta en práctica de un distintivo público de confianza en los servicios de la Sociedad de la Información y del comercio electrónico, creado por la Asociación para la Promoción de las Tecnologías de la Información y el Comercio Electrónico (APTICE), cuya aprobación fue realizada por el Gobierno de Aragón en diciembre de 2007. APTICE cuenta, además, con una PKI propia puesta a disposición de sus miembros (empresas e instituciones públicas) para la creación y mantenimiento de

[14] http://www.lefis.org

[15] http://www.aptice.org

sus propias redes de confianza. La PKI de APTICE ha sido elaborada a partir de la experiencia de **LEFIS UNIZAR PKI**.

c) PRIME

Las experiencias desarrolladas con la **LEFIS UNIZAR PKI** permitieron participar en las actividades del proyecto **PRIME** (Privacy and Identity Management for Europe)[16], desarrollado en el marco del Sexto Programa Marco de la Unión Europea FP6. El proyecto estaba destinado a salvaguardar la gestión de la protección de datos y la identificación digital en la Sociedad de la Información, de forma que los usuarios de los sistemas de información puedan actuar de manera segura manteniendo salvaguardada su esfera privada.

d) GERSOCO

Bajo el nombre de **GERSOCO** (Gobernabilidad y Estrategias de Regulación en la Sociedad del Conocimiento) y dentro del Plan Nacional de Investigación 2004-2007, el Grupo elaboró un modelo teórico de gobernabilidad ("Gobernanza" o "Governance") para la sociedad del conocimiento. Su objetivo consistió en analizar qué condiciones deben cumplir los instrumentos de regulación en una sociedad marcada por la omnipresencia de las nuevas tecnologías y por los intercambios jurídicos e informativos a través de redes de telecomunicación públicas, a partir de una concepción democrática de la gobernabilidad caracterizada por la orientación al ciudadano.

e) EGOBS

Otra de las actividades del Grupo de Investigación "Protección de Datos y Firma Electrónica" derivada de las experiencias desarrolladas a partir del diseño y gestión de **LEFIS UNIZAR PKI** es **EGOBS** (Internacional Electronic Government

[16] https://www.prime-project.eu/

Observatory, Observatorio Internacional de Administración Electrónica)[17], una iniciativa surgida a partir del proyecto Europeo ALFA Red de Gobierno Electrónico, que se desarrolló entre 2003 y 2006. Dicho Observatorio se está implantando en Suramérica, concretamente en Brasil, en la Universidad Federal de Santa Catarina, contando para ello con financiación recibida de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) para el periodo 2009-2012.

f) LAW&ICT SHARED VIRTUAL CAMPUS

En el marco del proyecto **LAW&ICT SHARED VIRTUAL CAMPUS** y utilizando las herramientas de identificación digital elaboradas por el Grupo, se ha desarrollado y puesto en acción un campus virtual europeo e iberoamericano que auxilia a la docencia impartida por el propio Grupo (que coordina el proyecto) y por las Universidades e instituciones participantes en el proyecto. La propuesta cuenta actualmente con 11 participantes, procedentes de 8 países europeos (Alemania, España, Finlandia, Lituania, Polonia, Portugal, Reino Unido y Turquía) y 1 participante de Brasil. El proyecto ha sido finaciado por la Unión Europea, programa Lifelong Learning.

g) Curso On Line y Encuentros sobre Gobierno electrónico e inclusión digital

Con financiación obtenida de la Agencia Española de Cooperación Internacional para el Desarrollo (AECID) para 2007 y 2009 el Grupo ha desarrollado e implantado un **Curso On Line sobre Administración Electrónica,** cuyos alumnos están situados en España (Zaragoza), Argentina (La Plata) y Brasil (Santa Catarina y Curitiba). En el curso participan profesores e investigadores de la Universidad Nacional de La Plata, la Universidad Federal de Santa Catarina y la Universidad Pontificia Católica del Paraná.

Igualmente, con financiación obtenida del Ministerio de Educación y Ciencia en el marco del Programa hispano-brasileño de cooperación interuniversitaria para el periodo 2007-2008, el Grupo organizó dos conferencias sobre Gobierno Electrónico e Inclusión Digital, celebradas en Brasil y Zaragoza en 2007, contando con

[17] http://www.egobs.org

participantes internacionales[18]. La acción fue el comienzo de la realización de actividades de investigación conjuntas entre el grupo español y un grupo de investigación de objetivos similares que trabaja en la Universidad Federal de Santa Catarina en Brasil.

h) LEFIS Series

Las propuestas teóricas y prácticas del Grupo en relación a las materias consignadas en este trabajo quedan recogidas en las publicaciones que sus miembros realizan. También se contienen en la denominada **LEFIS Series**[19] colección de publicaciones editada por Prensas Universitarias de Zaragoza que cuenta hasta la fecha con nueve volúmenes editados y dos en preparación. El contenido de los volúmenes en formato digital es accesible en el repositorio Zaguán [20] de la Universidad de Zaragoza desarrollado en software libre utilizando la herramienta Invenio[21] construida por el CERN de Ginebra[22]. El Grupo planea desarrollar un módulo de **LEFIS UNIZAR PKI** que forme parte del repositorio Zaguan.

5 Conclusión

La comunicación ha permitido presentar las numerosas implicaciones y consecuencias de los sistemas de identificación digital, que ya tienen la suficiente madurez como para mostrar que la extensión de su uso puede ayudar a cumplir los objetivos de la Ley de acceso electrónico. El Grupo de Protección de datos y firma electrónica está abierto a participar en cualquier tipo de iniciativa que esté interesada por la experiencia y actividades resumidas en este trabajo.

[18] Hasta el momento han sido realizados 8 encuentros. El próximo se realizará en Valladolid los días 28 y 29 de junio de 2010. Ver: http://www.infojur.ufsc.br/aires.rover/egov/index.html

[19] http://puz.unizar.es/catalogo/colecciones_libros.php?coleccion=40

[20] http://zaguan.unizar.es/

[21] http://cdsware.cern.ch/invenio/index.html

[22] http://cdsware.cern.ch/