



Comunicación

050

E-ADMINISTRACIÓN EN LA UNIVERSIDAD DE MURCIA, INFRAESTRUCTURAS Y SERVICIOS

Daniel Sánchez Martínez

Analista de proyecto e-Administración
Universidad de Murcia

Francisco José Corral Agüero

Jefe de proyecto e-Administración
Universidad de Murcia

Tomás Jiménez García

Director de ATICA
Universidad de Murcia

Palabras clave

e-Administración, PKI, firma electrónica, sellado de tiempos, servicio Web, tarjeta inteligente, dispositivos móviles, registro telemático.

Resumen de su Comunicación

En esta comunicación se describe el caso práctico de la Universidad de Murcia en cuanto al diseño, implantación y puesta en marcha de infraestructuras y servicios seguros de Administración electrónica, tanto para la propia comunidad universitaria, como para sus relaciones con terceros.

E-ADMINISTRACIÓN EN LA UNIVERSIDAD DE MURCIA, INFRAESTRUCTURAS Y SERVICIOS

1. Introducción

El nuevo escenario de Administración electrónica existente en la actualidad representa una excelente oportunidad de implantación de servicios dentro de las Universidades, fundamentada en la capacidad de innovación tecnológica que las define.

La Universidad de Murcia se ha caracterizado por una continua preocupación tecnológica en la última década, cimentada en iniciativas como el carné universitario, el desarrollo de una PKI interna, las aulas de libre acceso o la implantación de redes inalámbricas.

Además, hace un año, la Universidad firmó un convenio con la Fábrica Nacional de Moneda y Timbre (FNMT), prestador de servicios de certificación (PSC) reconocido, convirtiéndose en autoridad de registro (RA) de la misma. Este acuerdo posibilita el desarrollo de servicios de Administración electrónica basados en el uso de firma electrónica reconocida, y con plena validez jurídica (equiparable a la firma manuscrita).

En este artículo se describirán, en primer lugar, las iniciativas que la Universidad de Murcia ha emprendido durante este último año con el objetivo de conseguir una Administración electrónica operativa tanto para la propia comunidad universitaria, como para terceros que tengan que relacionarse con ella.

A continuación se analizarán las infraestructuras de servicios Web desarrolladas para la parte servidora, y las tecnologías de integración de la tarjeta inteligente de la Universidad de Murcia con ordenadores personales y dispositivos móviles. Ambos elementos conforman la arquitectura fundamental de la plataforma de e-Administración.

Posteriormente se describirán los primeros servicios desarrollados y los beneficios que la comunidad universitaria obtiene. Para acabar se obtendrán algunas conclusiones del trabajo realizado durante este primer año y se analizarán ciertos caminos aún por explorar.

2. El proyecto e-Administración

En mayo de 2005 la Universidad de Murcia aprobó el plan estratégico “Hacia la Administración Electrónica”, el cual supone tanto una clara declaración de intenciones en busca de la modernización en los procedimientos y comunicaciones administrativas dentro de la propia Universidad y en sus relaciones con terceros, como una apuesta decidida por el uso de las tecnologías de la información para conseguir ese fin.

Como objetivos fundamentales del plan se han establecido los siguientes:

- Racionalizar los sistemas de acceso a la información y su utilización por parte de los órganos y unidades administrativas, facilitando su almacenamiento y consulta en condiciones óptimas de seguridad.
- Prestar un mejor servicio a los miembros de la comunidad universitaria y, en general, a la sociedad, permitiendo una comunicación más fluida a través de medios técnicos seguros y con la adecuada validez jurídica.
- Conseguir una importante reducción del coste económico y ambiental que conlleva una actividad administrativa basada en el papel, de manera que los actos y trámites se generen en soporte digital y se comuniquen por medios telemáticos.

• Simplificar las relaciones con el resto de las instituciones públicas, especialmente por lo que se refiere al intercambio de información y, en general, para permitir una mayor eficacia en la recíproca cooperación y asistencia necesaria para el ejercicio de las respectivas competencias.

Para la consecución de dichos objetivos se han establecido varias líneas de trabajo prioritarias:

- Puesta en marcha de las oficinas de registro, y distribución de la firma electrónica entre los usuarios de la comunidad universitaria, siendo el carné universitario el soporte de la misma.
- Desarrollo de infraestructuras que permitan hacer seguras las transacciones y los documentos intercambiados, dotándolos de autenticidad, integridad y confidencialidad en aquellos casos en los que se requiera.
- Desarrollo de infraestructuras que permitan gestionar los documentos electrónicos, en cuanto a su archivo digital, accesibilidad y conservación en el tiempo.
- Desarrollo de la tecnología necesaria para la realización de procesos de firma electrónica desde el tipo de dispositivo donde se encuentre el usuario final (PC o móvil) mediante el uso del carné universitario.
- Digitalización de los flujos y expedientes internos de la Universidad, apoyándolos en el uso de la firma electrónica. Algunos ejemplos inmediatos serían los flujos de validaciones de facturas, la firma de actas por parte del profesorado, los expedientes de contratación...
- Puesta en marcha de servicios destinados a los miembros de la comunidad universitaria y a terceros que se relacionen con la Universidad. Algunos ejemplos: Registro Telemático, Notificación Electrónica, Facturación Electrónica, Contratación Pública Electrónica...

En los siguientes apartados se describen las principales tareas que se están acometiendo en las líneas descritas.

3. Infraestructuras SOA

La primera línea de actuación fundamental en las iniciativas de e-Administración dentro de la Universidad de Murcia, ha sido el diseño y desarrollo de las infraestructuras adecuadas que permitiesen conformar una plataforma de trabajo ágil y segura.

Se analizaron los requerimientos que debía de cumplir la nueva plataforma de Administración electrónica, dividiéndolos en dos grupos fundamentales; requisitos en cuanto a la seguridad de las transacciones y requisitos en cuanto a la gestión de los documentos. El diseño de la plataforma se ha realizado sobre servicios Web y una arquitectura orientada a servicios (SOA). Este modelado ofrece una gran cantidad de beneficios:

- Los servicios Web hacen uso de XML para la descripción de los interfaces y el paso de mensajes, y utilizan protocolos estándar como SOAP y HTTP para el transporte de la información.
- Los servicios Web ofrecen una gran simplicidad en el desarrollo de aplicaciones, por el alto grado de compatibilidad de las mismas, y por la gran variedad de implementaciones y software de desarrollo existentes.
- Los servicios Web pueden ser registrados a través de UDDI, de forma que los clientes potenciales puedan localizarlos.

- La arquitectura SOA permite que los servicios web que la conforman puedan interoperar de forma simple y con bajo acoplamiento, proporcionando la extensibilidad de los mismos y su integración en otras aplicaciones distribuidas ya existentes.

Estos beneficios son esenciales para un entorno tan heterogéneo como la Universidad de Murcia, y en general para cualquier Administración, en donde existen multitud de sistemas operativos, servidores y software de diferentes características.

Los servicios Web y la arquitectura SOA hacen posible que todos esos elementos puedan interactuar a través de la plataforma común de Administración electrónica. En la figura 1 se puede observar el conjunto inicial de servicios diseñados dentro de la plataforma, y dividido en servicios de seguridad y servicios de gestión documental.

Además también descarga a los clientes de la complejidad de tener que implementar por sí mismos ciertas funcionalidades, dejando esta responsabilidad final al servicio. Este hecho es fundamental para el caso de los dispositivos móviles, que disponen de capacidades de procesamiento reducidas.

Por último, es necesario destacar que este tipo de modelo centraliza la seguridad y la gestión documental de la plataforma de Administración electrónica en los propios servicios Web, permitiendo que cualquier cambio de políticas, aceptación de nuevos formatos y estándares, o ampliación a nuevas funcionalidades, permanezca transparente a los clientes finales. A continuación se describe la funcionalidad de cada uno de esos grupos de servicios.

4. Servicios de seguridad

En el primer grupo de servicios se encuentran aquellos que son responsables de garantizar la autenticidad, la integridad y el no repudio de las transacciones y documentos electrónicos involucrados en cualquier procedimiento de Administración electrónica.

Inicialmente se han considerado tres servicios básicos. Un servicio de firma que permita verificar las firmas de los documentos enviados por los clientes, y firmar ciertas transacciones de forma automatizada. Un servicio de sellado de tiempos que permita vincular un documento a un momento preciso del tiempo. Y un servicio de validación que permita comprobar la vigencia de los certificados electrónicos.

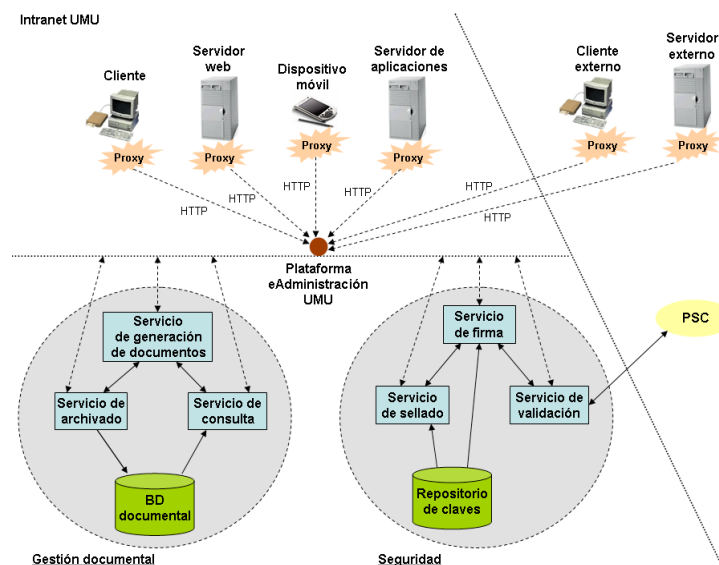


Figura 1. Plataforma SOA de Web services

Tal y como se describe en la figura 1, el servicio de sellado y el de validación pueden ser utilizados directamente por un cliente, o por el propio servicio de firma, que en un momento determinado puede necesitar ligar una firma a un instante temporal, o comprobar la validez del certificado incluido en una firma electrónica.

Se está estudiando la posibilidad de ampliar la arquitectura en el futuro con un nuevo servicio de cifrado, que complete la funcionalidad descrita.

5. Servicios de gestión documental

Junto al bloque de servicios de seguridad, se ha diseñado otro conjunto de servicios básicos relativos a la gestión documental de los procesos de Administración electrónica.

Inicialmente se han desarrollado tres servicios básicos, necesarios para poder trabajar con documentos electrónicos. Un primer servicio de archivado de documentos electrónicos en la base de datos documental de la Universidad de Murcia. Un segundo servicio de consulta de documentos electrónicos, que permite recuperar un documento electrónico de forma transparente al cliente final. Y por último un servicio de generación automática de documentos electrónicos, especialmente interesante para la producción de recibos y justificantes.

Adicionalmente se está analizando la posibilidad de incorporar nuevos elementos a la infraestructura, como un servicio de perfiles de autorización, que permita definir condiciones de acceso a ciertos documentos electrónicos; un servicio de gestión de expedientes electrónicos, que permita vincular varios documentos electrónicos entre sí; y un servicio de gestión de flujos, que permita definir las distintas etapas del ciclo de vida de un expediente o documento electrónico.

6. Arquitecturas cliente

Paralelamente al desarrollo de las infraestructuras de servicios que soporten todos los procesos propios de una plataforma de Administración electrónica, es fundamental diseñar e implementar la tecnología necesaria que haga posible la generación de firmas electrónicas en los clientes, de tal forma que un usuario pueda firmar un documento o una transacción en un momento determinado.

Para llevar a cabo este propósito es necesario tener en cuenta que las claves del usuario se encuentran contenidas en su carné universitario, y que por tanto deberán ser habilitados los mecanismos necesarios para que el proceso de generación de firma digital se realice en la propia tarjeta inteligente.

Este requisito de diseño implica la integración de las capacidades criptográficas del carné universitario en la arquitectura del sistema operativo de los clientes. En el diseño de esta solución de integración se han tenido en cuenta diversos factores que se describen a continuación:

- Debe integrar el carné universitario en clientes de la familia de sistemas operativos Windows (con gran penetración en la mayoría de los entornos administrativos), y también en clientes de la familia Linux (cada vez más presentes dentro de la Universidad de Murcia).
- Debe posibilitar el uso de la tarjeta inteligente de la Universidad de Murcia tanto en clientes fijos de escritorio (tipo PC) como en dispositivos móviles (PDAs o smartphones).
- Debe permitir el uso del certificado electrónico, de forma transparente al usuario, en los principales navegadores Web y clientes de correo utilizados a día de hoy dentro de la Universidad (Internet Explorer, Netscape, Mozilla y Firefox), tanto para procesos de autenticación de cliente en sesiones SSL, como para

firma de correo S/MIME.

- Debe ofrecer funcionalidad de alto nivel a los desarrolladores que necesiten incluir procesos de firma electrónica en aplicaciones o servicios finales, y soportando los principales estándares de firma actuales (CMS y XMLDSIG).

Atendiendo a estas necesidades se han diseñado dos arquitecturas, una de ellas responde a las necesidades de los clientes de escritorio tradicionales, y la otra a las de los clientes móviles.

7. Cliente PC

La arquitectura diseñada para este tipo de cliente se refleja en la figura 2 y está compuesta por tres elementos fundamentales: CSP, PKCS#11 y Crypto-Applet.

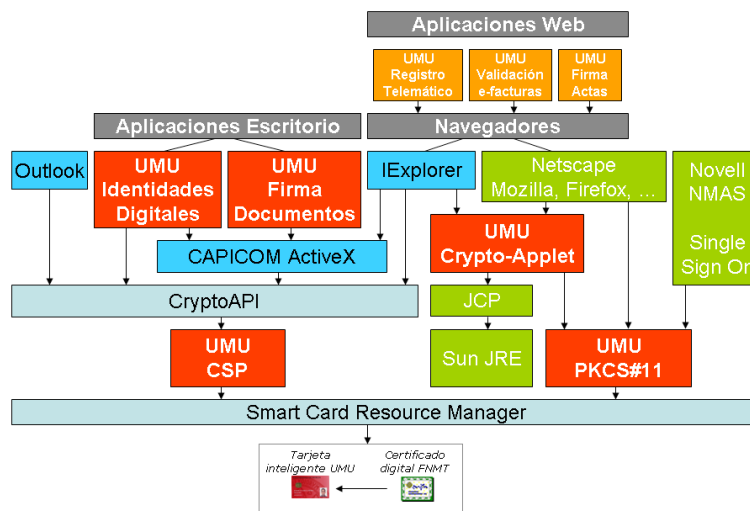


Figura 2. Arquitectura de componentes en cliente PC

UMU CSP

Este desarrollo es un proveedor de servicios de criptografía compatible con Microsoft Windows CryptoAPI, y que es capaz de interactuar con el certificado almacenado en la tarjeta inteligente de la Universidad de Murcia.

Se integra con aplicaciones Microsoft de más alto nivel como Outlook (posibilitando la firma de correo), Internet Explorer (autenticación de cliente en conexiones seguras) o con cualquier otro desarrollo cliente a través de Windows CryptoAPI y, opcionalmente, del componente CAPICOM ActiveX.

UMU PKCS#11

Este PKCS#11 representa un interfaz común entre ciertas aplicaciones cliente no Microsoft y el certificado de la tarjeta inteligente de la Universidad de Murcia.

Entre los navegadores que lo soportan se encuentran Mozilla, Netscape, Thunderbird y Firefox, permitiendo la autenticación de cliente basada en certificado y la firma electrónica de correos en aquellos casos en los que se incluye un gestor de correo.

El UMU PKCS#11 permite además que otros productos de gran calado en el trabajo diario del PAS, como Novell, también se integren con la tarjeta inteligente de la Universidad de Murcia, posibilitando el arranque de sesión seguro a través del certificado de la tarjeta, y la utilización de la misma como único medio de autenticación en todos los servicios y aplicaciones que el usuario maneje.

UMU Crypto-Applet

Este applet de tecnología Java se convierte en un componente esencial para el desarrollo de aplicaciones web que necesiten utilizar los recursos criptográficos de nuestra tarjeta inteligente.

Este desarrollo se sustenta en el JCP (Java Cryptographic Provider) y en el uso interno del UMU-PKCS#11 como interfaz criptográfico de comunicación con la tarjeta. Proporciona a los navegadores con soporte Java una serie de métodos criptográficos de alto nivel que pueden ser invocados desde código script.

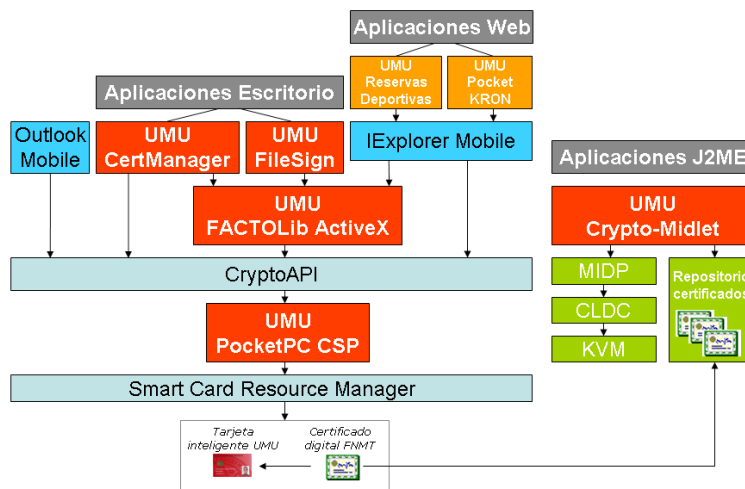


Figura 3. Arquitectura de componentes en cliente móvil

Cliente móvil

Para conseguir la integración de un dispositivo móvil dentro de los procesos de Administración electrónica, la Universidad de Murcia ha basado el diseño de la tecnología de integración y su posterior implementación en el trabajo realizado dentro del proyecto FACTO en colaboración con Telefónica Móviles España. La arquitectura de integración del carné universitario en el dispositivo móvil se puede observar en la figura 3.

A través de la arquitectura cliente descrita se ofrece al usuario final la posibilidad de acceder a los servicios de Administración electrónica de la Universidad de Murcia tanto desde un PC tradicional como desde un dispositivo móvil, manteniendo siempre las mismas características de seguridad en las transacciones.

8. Primeros servicios

Una vez desarrolladas las infraestructuras necesarias para dar soporte a los procesos de Administración electrónica, tanto en la parte servidor como en la parte cliente, la Universidad de Murcia ha puesto en marcha un catálogo inicial de servicios piloto, destinados tanto a los miembros de la comunidad universitaria, como a terceros con los que la propia Universidad se relaciona.

Validación de flujos

En primer lugar, la Universidad de Murcia ha iniciado la digitalización de sus flujos de gestión internos. Algunos de ellos ya disponían de una operativa telemática, pero carecían del soporte jurídico que proporciona la firma electrónica, y se fundamentaban en una identificación débil del usuario basada en contraseña.

El uso de este tipo de servicios telemáticos se restringía a una validez exclusivamente interna, y que en la mayoría de los casos implicaba una firma manual posterior sobre una documentación generada de forma automática e impresa. Se ha trabajado hasta el momento en tres campos fundamentales dentro de la Universidad: recursos humanos, gestión económica y gestión académica.

Dentro de los flujos de recursos humanos, se ha añadido el soporte de la firma electrónica a los procesos de gestión de ausencias, controlados por la aplicación de recursos humanos de la Universidad de Murcia KRON. Un usuario del PAS puede solicitar una ausencia laboral de forma telemática, firmando la solicitud con su carné universitario. Posteriormente su superior o superiores podrán validar o desestimar la misma, firmando la solicitud del trabajador o generando un documento de desestimación alternativo. Esta vista de la aplicación KRON está disponible tanto desde clientes PC como desde clientes móviles (Pocket-KRON).

De forma similar en cuanto al soporte de seguridad se refiere, se ha añadido firma electrónica a los flujos de validaciones y desestimaciones de facturas de la aplicación JUSTO de gestión económica. Este flujo permite elevar la validación de las facturas que llegan a la Universidad de Murcia desde sus distintos proveedores hacia el responsable de la misma y los responsables de gestión económica de la propia Universidad. Soporta la validación de facturas en formato papel (se digitalizan mediante escaneo) y en formato electrónico (mediante el servicio JUSTO-FE para proveedores de la Universidad de Murcia). La vista de la aplicación se encuentra disponible en entorno PC y en entorno móvil (Pocket-JUSTO).

En este ámbito se ha procedido a digitalizar un flujo de especial trascendencia para el PDI de la comunidad universitaria. Se trata del flujo de firma de actas, que está formado por un único paso, pero que tiene una gran importancia dentro de la gestión de la propia Universidad. El servicio de firma de actas se integra dentro del portal SUMA (campus virtual de la Universidad de Murcia) que ya utiliza todo el PDI.

Registro telemático

La aplicación de Registro Telemático es otra de las iniciativas de la Universidad de Murcia para su catálogo de servicios de Administración electrónica. Este servicio se plantea varios objetivos fundamentales:

- Ofrecer al usuario de la comunidad universitaria la posibilidad de presentar instancias de distinta naturaleza de forma telemática.
- Establecer las medidas de seguridad necesarias para garantizar la autenticidad e integridad de las instancias presentadas, así como el no repudio y la veracidad temporal de las mismas.
- Posibilitar que el usuario pueda comprobar el estado de tramitación de sus instancias registradas, también de forma telemática.
- Integrar estas instancias telemáticas dentro de los flujos de validaciones y desestimaciones existentes dentro de la gestión académica de la Universidad de Murcia.

Hasta el momento han sido desarrollados dos servicios fundamentales, la presentación de una instancia básica (sin documentación adjunta) y la comprobación de una instancia presentada, ambos en entorno Web.

En el proceso de presentación de una instancia básica el usuario rellena y firma digitalmente un formulario con la información de la instancia, generándose un documento criptográfico contenedor de la instancia, su firma y el certificado utilizado para realizar la misma.

Ese documento se envía al servidor, que verifica la firma de la instancia, su integridad y autenticidad. Una vez realizadas todas estas comprobaciones, añade un sello de tiempo al documento en el que se incluyen la fecha y hora de presentación de la instancia y el número de asiento en el registro, procediendo a continuación al almacenamiento del documento en base de datos. Este proceso se observa en la figura 4.

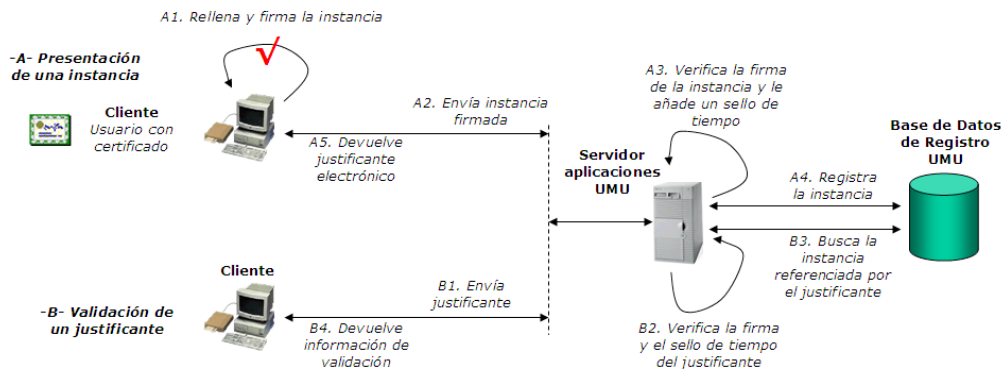


Figura 4. Registro telemático

Además, este documento firmado inicialmente por el usuario y sellado posteriormente por la Universidad de Murcia, es devuelto al usuario, posibilitando que lo descargue en su ordenador a modo de justificante electrónico para posteriores comprobaciones.

El segundo servicio que ofrece la aplicación Web es la comprobación de justificantes electrónicos. El usuario puede utilizar este servicio para comprobar que el justificante electrónico correspondiente a una instancia que presentó, y que tiene en su poder, es válido. El proceso de comprobación realiza una verificación de la firma y el sello de tiempo del justificante, muestra la información relativa al firmante y al asiento en el registro, y permite visualizar de nuevo la instancia básica presentada.

Ambos servicios se encuentran plenamente integrados con las aplicaciones de gestión interna de la Universidad, lo cual proporciona un gran beneficio en la agilización de los trámites tanto al usuario que presenta la instancia, como a los miembros del PAS que tengan que intervenir en el flujo de la misma.

9. Conclusiones y vías futuras

A lo largo de este artículo se han puesto de manifiesto las iniciativas técnicas, en cuanto a infraestructuras y servicios finales, que la Universidad de Murcia ha puesto en marcha en este último año con la ambición de caminar hacia una Administración electrónica plena.

En este momento la Universidad dispone de los medios humanos y técnicos necesarios para seguir ampliando su catálogo de servicios, y flexibilizar así la forma de trabajar de los miembros de la comunidad universitaria.

Sin embargo se trata tan sólo de un primer paso en el camino y todavía quedan una serie de desafíos técnicos y logísticos que afrontar en los próximos meses. Entre otros se pueden destacar los siguientes:

- La aparición del nuevo DNI electrónico emitido por el Ministerio del Interior a todos los ciudadanos espa-

ños, y que permitirá identificarse y realizar procesos de firma electrónica en transacciones telemáticas. La Universidad de Murcia está trabajando en colaboración con Telefónica Móviles España (a través del proyecto FACTO) para soportar este nuevo medio de identificación electrónico dentro de su plataforma de Administración electrónica.

- La interoperabilidad entre distintas plataformas de Administración electrónica de distintas organizaciones y naciones, es una de las grandes preocupaciones mundiales en torno al concepto de e-government. El lograr los mecanismos de gestión necesarios para poder compartir información entre la distintas Administraciones de forma ágil, controlada, segura y mediante métodos telemáticos es otro de los retos que la Universidad debe afrontar.

- Desde el punto de vista de la seguridad, también será fundamental afrontar en el futuro el problema de cómo asegurar que los elementos de seguridad de los documentos electrónicos mantengan su vigencia con el paso de largos periodos de tiempo.

- En cuanto a la gestión documental se refiere, la Universidad de Murcia debe analizar nuevos estándares como OAIS y PDF/A relativos a archivos digitales y documentos electrónicos y estudiar la viabilidad de adaptación a los mismos.

Son todos ellos elementos que será necesario resolver próximamente, de forma que iniciativas como la de la Universidad de Murcia no queden como elementos aislados, sino como una pieza más del puzzle de una Administración electrónica global.

10. Referencias

[1] M. Barnés, D. Gómez, A.F. Gómez-Skarmeta, M. Martínez, A. Ruiz and D. Sánchez. "An electronic signature infrastructure for mobile devices". ISSE Book 2005. July 2005.

[2] D. Sánchez, J.A. Cascales, R. Ferrando, F.J. Pérez. "E-Administración En La Universidad De Murcia", en Comunicaciones TECNIMAP 2004, Septiembre de 2004.

[3] ATICA, Universidad de Murcia. <http://www.um.es/atica>.

[4] OASIS, SOA Reference Model Technical Committee. http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=soa-rm

[5] RSA Laboratories. PKCS #11 v2.20: Cryptographic Token Interface Standard. 28 de Junio de 2004.