tecnimap Murcia 2004

15

LA IDENTIDAD DIGITAL COMO HERRAMIENTA DENTRO DE LA ADMINISTRACIÓN ELECTRÓNICA. FUNDAMENTOS CLAVE

Eduardo López
Director de Tecnología
Grupo SIA

Oscar García
Business Sales Consultant. Área de Seguridad
Grupo SIA

Javier Jarauta
Business Sales Consultant. Área de Seguridad
Grupo SIA

INTRODUCCIÓN

El objetivo primordial de la Administración Electrónica es conseguir ampliar el número de servicios a usuarios (ciudadanos, funcionarios, clientes, proveedores), mejorar su experiencia de uso, disminuir el coste de explotación y a la vez minimizar los riesgos. La Identidad Digital es el útil que permite establecer la representación de las personas dentro de los procesos informáticos.

Para conseguir maximizar los beneficios y minimizar tiempos y costes de implantación consideramos que hay que establecer una arquitectura que permita independizar la identidad digital de las aplicaciones que pueden hacer uso de ella, mediante el uso de infraestructuras de servicio. Infraestructuras basadas en estándares y que permitan la implantación de políticas de gestión y control. Además, el seguimiento de estándares permite la interoperabilidad entre aplicaciones e independizar a su vez el servicio de las marcas concretas de tecnología. La idea fundamental es que la gestión de la Seguridad no se haga al nivel de las aplicaciones sino a través de las infraestructuras de servicio que asegure que las definiciones, políticas de control y cumplimiento se realicen de forma homogénea entre múltiple aplicaciones.

Es interesante considerar que, siguiendo las indicaciones de los analistas del Gartner Group, la problemática de Gestión de Identidad están cada vez más relacionada con la Gestión de los Accesos (derechos) que corresponden a dichas identidades.

IDENTIDAD DIGITAL

Entendemos identidad digital como el conjunto de elementos necesarios para garantizar (dentro de lo razonable), la identidad a través de medios electrónicos, así como todos los elementos que permiten gestionar y proporcionar funcionalidad en este medio.

Actualmente la identidad digital incluye principalmente los siguientes elementos:

- Certificados digitales (incluido su soporte físico)
- Firma electrónica
- Gestión y propagación de derechos.
- Simplificación de identificación en múltiples entornos (SSO)

ÁMBITOS DE UTILIZACIÓN

Para poder aprovechar la identidad digital en las organizaciones es fundamental considerar el ámbito de utilización. Esto es así debido a que ni las funcionalidades ni la gestión requerida o proporcionada a los distintos colectivos es la misma.

Esta diferencia va a marcar distintas estrategias en la aproximación al problema. Los colectivos que deben considerarse a priori podrían dividirse en tres círculos de actuación que requieren distintos tipos de gestión:

- Círculo externo: Ciudadanos. En ámbitos G2C, B2C interactúan esporádicamente con la organización (o al menos deben tener una puerta abierta para ello). Este colectivo es el más numeroso y harán uso preferente de certificados y posiblemente de firma electrónica.
- Círculo interno: Empleados / funcionarios de un organismo o institución, utilizan los sistemas de información de forma habitual. La organización puede obtener beneficios

económicos directos de la mejora de la eficiencia de este colectivo como resultado del uso de la identidad digital.

- Círculo "cercano": Colectivo que mantiene relaciones frecuentes con la organización. Tendrán necesidades intermedias entre los dos anteriores, además de poder tener especial relevancia la relación "servidor-servidor" mediante la cual se relacionan directamente dos sistemas de información distintos.

PANORAMA DE LA SITUACIÓN ACTUAL

Es evidente que el DNI Electrónico en España va a constituir un hito fundamental y pionero para dotar a una inmensa mayoría de ciudadanos con un medio de identificación digital. Este despliegue de certificados electrónicos va a ser un elemento facilitador y dinamizador para la generación de nuevas aplicaciones en el ámbito de interacción de los ciudadanos con la Administración, y de clientes con empresas.

Existen dos elementos relativos a la disponibilidad que pueden ser relevantes: por un lado, la disponibilidad de sistemas de lectores en los hogares, y por otro lado que el ciudadano recuerde el PIN de uso de las tarjetas.

En cualquier caso el DNI electrónico (y otros documentos equivalentes para residentes de otras nacionalidades) constituirán el elemento universal de identificación, pero esto no implica que tenga que ser el elemento de uso profesional, como por ejemplo para funciones de Single Sign On dentro las organizaciones (empresas, administración).

PROYECTOS DE IDENTIDAD DIGITAL

Actualmente existen proyectos de gran calado en identidad digital tanto en organismos públicos como privados.

Estos proyectos requieren la intervención de diferentes actores:

- Prestadores de servicios de certificación y/o infraestructuras de clave pública propias de cada organización.
- Integradores especializados
- Proveedores de software / equipos de desarrollo.
- Directorios corporativos (complementados con gestión de identidades y/o gestión de privilegios)

Todos ellos son imprescindibles para potenciar el uso de la identidad digital.

Estos proyectos actualmente en funcionamiento, no solo responden a la necesidad de tratos con terceros, sino que responden a importantes ahorros de coste internos en las organizaciones.

Alguno de los proyectos más emblemáticos y con repercusión internacional son los de la Agencia Tributaria y los de la Gerencia Informática de la Seguridad Social. A nivel de uso interno existen numerosas iniciativas dedicadas a resolver funciones internas de confidencialidad y autenticación como correo electrónico seguro, acceso remoto, sistemas de firmas administrativas,... en numerosas empresas y organismos del país.

FIRMA ELECTRÓNICA

La firma electrónica está experimentando importantes avances actualmente en España. Uno de los principales motores de este desarrollo es la Administración Electrónica. La gran mayoría de las administraciones públicas están ya incorporando firma electrónica a multitud de procedimientos existentes principalmente para los ciudadanos, aunque también es significativo el impacto interno de cara a los funcionarios.

Es especialmente significativo el proyecto de AEAT para la presentación de la declaración de la renta (con amplia difusión de certificados de FNMT).

Aunque en muchos los casos se ha estado implantando firma en aplicaciones puntuales, actualmente ya se están desarrollando/implantando infraestructuras que permiten la generalización de la firma en la gran mayoría de los procesos existentes en el organismo. Estas infraestructuras proporcionan firma a múltiples aplicaciones reduciendo los costes de adaptación de cada una de ellas.

Funcionalidades e Infraestructuras

FUNCIONALIDADES

Autentificación

La Autentificación se refiere a los mecanismos necesarios para la identificación. Hablamos de identificación física (por contraste con la digital), en aquellos casos en los que la identificación se realiza de forma presencial.

La Autentificación puede realizarse electrónicamente siempre que la persona cuente con certificados confiables que eviten el proceso físico.

En relación con el tema objeto de este documento, la adaptación de los sistemas de identidad digital no pueden, en ningún modo, sustituir la identificación física sino complementarla debido a la distinta casuística a la que deberá enfrentarse (pérdida de certificados, público en general que no quiere/puede acceder a la identidad digital, etc...).

No obstante, complementar la mayoría de procedimientos existentes con mecanismos de Autentificación digital proporcionará el primer paso para mejorar la calidad del servicio con mecanismos de identidad digital.

La Autentificación electrónica es una funcionalidad que será compartida por todos los colectivos. Por ello, es recomendable para todo organismo que incorpore esta funcionalidad que se independice de tecnologías o marcas específicas. Aunque es evidente que actualmente los certificados de FNMT (clase 2) tienen una difusión mayor que cualquier otro dentro de nuestro país, y que en un próximo futuro será el DNI el certificado más implantado, las aplicaciones deben admitir un amplio rango de certificados sin suponer un impacto significativo en su complejidad.

Por motivos operativos, sí es recomendable contar con una lista actualizada de los PSC en los que la organización confiará.

Registro de personas

El registro (alta del usuario ya sea para su certificación o para cualquier tipo de alta en un sistema de información) requiere una Autentificación previa, así como proporcionar de forma fiable todos aquellos elementos que constituyen las propiedades o atributos de la persona.

El registro además puede exigir no sólo conocer la identidad del usuario sino también es posible que se requieran elementos adicionales referentes a la persona (poderes, etc...) o realizar procesos adicionales (fotografía in-situ, entrega de tarjetas, ...).

En esta función, el DNI electrónico puede ser un elemento fundamental de registro (de la misma forma en que lo es en el mundo físico) de personas sin necesidad de requerir acto presencial, son lo que se puede combinar con sistemas de autoservicio que pueden abaratar considerablemente las funciones de registro.

Certificación

La certificación permite proporcionar a un colectivo elementos específicos para la identificación digital. Esto, además de ser una ventaja, ya que puede incorporarse información adicional, resulta una necesidad en algunos casos.

El DNI electrónico resulta, por ejemplo, poco adecuado para un uso por parte de empleados. Los inconvenientes principales son:

- Utilización en procesos "triviales" (autenticación PC) => mayor compromiso de la seguridad del documento.
- Exige verificación externa "intensiva" de validación.
- Pérdida => proceso externo a la organización para la recuperación
- Uso intensivo de tarjeta => Degradación del documento.

Por estos, y otros motivos, recomendamos a cualquier organización que planee utilizar la identidad digital profundamente dentro de su organización (y en un amplio rango de funcionalidades), disponer de elementos propios de certificación con los que dotar a los empleados (y en algunos casos a terceros "cercanos").

Por contra, considerar desde una organización la certificación del público en general no resulta necesario considerando que ya existen entidades (a la que se sumará el DNI) que proporcionan un elemento de identificación suficientemente robusto y confiable, a la vez que eliminan la necesidad de procedimientos adicionales a un colectivo que, por otro lado, se ha definido con relaciones esporádicas con la organización.

Firma electrónica

La firma electrónica debemos entenderla como una funcionalidad adicional que puede incorporarse dentro de las aplicaciones y procedimientos existentes.

Mediante esta funcionalidad es posible garantizar (dentro de lo razonable), no sólo la identidad del firmante sino además la voluntad de firma de éste. Esta funcionalidad, como ya se mencionaba, debe ser utilizable por todos los colectivos. Esta necesidad marca la exigencia de utilizar elementos que permitan la universalidad de las soluciones utilizadas.

En lo que se refiere a los estándares, nos debemos atener a los que hoy por hoy resultan más extendidos (PKCS #7 y firma XML).

En lo que se refiere a los certificados, la organización debe ser capaz de reconocer y verificar firmas de cualquiera de los usuarios de las autoridades de certificación en las que se confía.

Respecto a la firma por servidores, si bien resulta imprescindible en toda organización que incorpore la identidad digital, debe mencionarse la importancia de mantener en condiciones

excepcionales de seguridad los certificados capaces de firmar (justificantes de entrega, sellado de tiempo, etc...), y en ningún caso delegar en estos servidores cierto tipo de responsabilidades (firma de contratos, aprobaciones de gastos, etc...).

Single Sign On

De forma simple la función de Single Sign On consiste en que mediante un solo proceso de identificación se puede acceder a varios recursos protegidos. En función de estos recursos, existen tres tipos básicos de Single Sign On :

- Aplicaciones Web, típicamente aplicaciones nuevas o aplicaciones dedicadas a usuarios externos. La función de Single Sign On la realizan los sistemas de portal. La identidad digital de certificados resulta una herramienta perfecta de identificación, pero para determinadas aplicaciones (acceso al ciudadano, determinadas solicitudes de bajo riesgo, aplicaciones para residentes o extranjeros,...) pueden ser suficientes sistemas básicos como usuario y clave de paso. En cualquier caso es importante que el sistema de control de acceso del portal permita combinar múltiples métodos de autenticación.
- Recursos de la red local (LAN), en este caso la función de Single Sign On viene controlada por los sistemas operativos de red. Todos trabajan con identidades digitales, y existe un claro interés en soportar los certificados más difundidos, así como el caso del DNI electrónico.
- Recursos IT tradicionales (legacy) en este caso, el Single Sign On de red no es suficiente dado que todavía existen numerosas aplicaciones (aplicaciones propietarias, de gestión, de bases de datos, ...) y plataformas (Unix, mainframe, AS/400, ...) que requieren su propia autenticación. Para ello se necesitan soluciones especificas de Single Sign On, que evidentemente tienen que estar preparadas para utilizar la identidad digital como herramienta de autenticación. Las soluciones más sofisticadas permiten acceder a los tres tipos de recursos de forma transparente.

Gestión de derechos

La identidad digital permite identificar y probar quién es quién, y en función de ello permitir el acceso al sistema. Pero no es una herramienta suficiente para determinar los derechos que dispone el propietario de la entidad en cuanto a acceso o capacidades en sistemas IT, dado que esos derechos son función del entorno y de las aplicaciones. Por otra parte la identidad tiene un carácter permanente (o al menos duradero) mientras que los derechos pueden cambiar rápidamente. Por último, la asignación y gestión de esos derechos no se hace en función del individuo sino del rol que juega en el sistema.

Todas estas características hacen que la gestión de derechos mediante el uso de certificados de atributos sea poco flexible y económica.

Nuestra propuesta para la gestión de derechos está basada en servicios que se dediquen a esta función como parte de la infraestructura. La industria, siguiendo los pasos de Gartner, empieza a asociar esta función con la gestión de identidad, bajo la denominación de IAM (Identity and Access Management)

INFRAESTRUCTURAS

Entendemos las infraestructuras como los componentes que permiten servir a múltiples aplicaciones y permiten independizar las aplicaciones de la herramienta de identidad que se utilice (desde el DNI electrónico, certificado de terceros, o usuario-password en determinados casos). Mención especial dentro de las infraestructuras merecen el tema de los estándares.

Infraestructuras de clave pública (PKI)

Como se comentó anteriormente la tarjeta inteligente del DNI electrónico no debería ser utilizado como tarjeta de Funcionario.

Para este propósito se puede utilizar una PKI diferente, que a su vez puede ser un PSC reconocido, o incluso una PKI interna. Por otra parte esta PKI puede estar dedicada a generar certificados para otras entidades aparte de los funcionarios, como puedan ser los contratistas, o servidores o aplicaciones

La alternativa de PKI interna frente a servicios de certificación externos es una discusión que puede venir determinada por una multiplicidad de factores, siendo los más relevantes la estructura de riesgos y responsabilidades, la organización interna, la flexibilidad requerida. Conviene tener en cuenta que siempre es posible combinar soluciones donde la infraestructura interna de PKI proporciona los certificados de identidad para funciones de trabajo (Single Sign On, correo, web services, firmas de transacciones internas o de empleado, criptografía para confidencialidad,...), mientras que una entidad externa puede aportar los certificados necesarios para la ejecución de firmas digitales avanzadas requeridas en procesos de representación o validez legal. La ventaja de esta aproximación es maximizar la flexibilidad, la usabilidad y por otro lado minimizar los costes y los riesgos.

Firma electrónica y Validación

Está claro que en la vida normal empleamos la firma sobre papel en multitud de procesos con distintos niveles de significación. Por ello es fácil prever que el número de servicios y aplicaciones que harán o hacen uso de firmas digitales continuará creciendo.

Por este motivo, no es lógico pensar que se deban desarrollar funciones de firma para cada aplicación. Por otra parte, no hay que olvidar que en el mundo electrónico cada operación de firma debería ir acompañada por su correspondiente función de validación (sea para que un ciudadano verifique la firma de un documento recibido, o de sus propias peticiones, o de que un servicio pueda comprobar la validez de una transacción firmada antes de aceptarla).

Nuestra propuesta va encaminada al uso de librerías seguras de firma, que además cumplan con el requisito de poder utilizar distintas procedencias de certificados, a la vez que distintos soportes, de tal forma que la aplicación (o el servicio de gestión de derechos) pueda determinar simplemente por configuración que sistema utilizar. Junto con el módulo genérico (multiaplicación –multisoporte) de firma, debe considerarse el servicio de Validación (encargados de comprobar la validez de certificados y funciones, key usage, CRL /OCSP, e información conectada con el sistema de gestión de derechos, como valor límite de la transacción,...). Además este servicio se puede ocupar de asegurar la integridad a largo plazo de las transacciones firmadas, o proporcionar servicios de notarización.

Single Sign On

Este es el servicio que permite el acceso a múltiples aplicaciones sin necesidad de autenticarse en cada una de ellas. Es una función dedicada a mejorar la usabilidad y experiencia de los usuarios. Existen dos infraestructuras distintas y complementarias :

- Web Single Sign On, tanto para acceso a portal de ciudadanos como a portal del funcionario (empleado)
- Aplicaciones internas dedicada a funcionarios, que permite el acceso no solo al entorno de red y las aplicaciones de Escritorio (Office), sino también de las aplicaciones y plataformas tradicionales (legacy) con sistemas propios de seguridad.

Infraestructuras de gestión de derechos (PMI)

Este servicio se ocupa de la determinación de a qué recursos tiene acceso una identidad determinada, proporcionando la autorización a través de múltiples aplicaciones. Este componente de infraestructura facilita de forma centralizada la creación de derechos, su administración y revocación.

Su funcionamiento además combina las posibilidades de uso de varias formas de autenticación y en función de ello otorgar derechos de acceso. Así por ejemplo un funcionario puede acceder al portal de funcionario mediante userid/password (por ejemplo desde su casa) para ciertas funciones de consulta, mientras que sólo puede acceder a aplicaciones o funciones sensibles si se autentica mediante el uso de la tarjeta de funcionario.

Este es un servicio que trabaja en combinación con el de Single Sign On.

POLÍTICAS DE CONTROL

A diferencia del mundo real, donde existe limitaciones físicas para ejecutar ciertas acciones, por ejemplo no se puede ir a cobrar un cheque a más de un sitio a la vez, en el mundo virtual esas limitaciones desaparecen, por lo que es muy importante que los elementos de infraestructura tengan la capacidad de implantar políticas de control que eviten el uso fraudulento del sistema, o que en cuanto se detecte pueda reaccionar para evitar su propagación. Por eso es importante la implantación y control del cumplimiento de las políticas. Por ejemplo el servicio de validación de firma puede rechazar firmas de rápida (múltiples) documentos a funcionarios no autorizados, mientras que se lo permite otros cargos. También podría evitar procesos de firmas rápidas de documentos que no lo permiten.

ESTÁNDARES

Los estándares sirven para asegurar la interoperabilidad entre servicios y aplicaciones. Aparte de los conocidos estándares de certificados electrónicos (X.509v3) y verificación, conviene prestar atención a los nuevos estándares dedicados a proporcionar seguridad en los entornos de procesamiento cooperativo (web Services) :

- XMLDSig : XML Digital Signatura, aplicación de firmas digitales en datos xml
- XMLEnc : XML Encryption, método para aplicar cifrado en datos xml

- SAML : Security Assertion Markup Language, destinado a proporcionar servicios de autorización para transacciones distribuidas. Describe los objetos para la decision sobre autenticación, atributos y autorización que pueden ser intercambiados y propagados entre infraestructuras de gestión de permisos (PMI) heterogéneas (o en múltiples dominios).
- XACML, XML Access Control Markup Language, suministra especificaciones para acceder a documentos XML, considerando los objetos (elementos dentro el documento), sujeto (usuario) y acción (lectura, escritura, creación, borrado).
- XKMS, XML Key Management Specification, protocolo de mensajería basado en xml para la intercambio de claves entre servicios Web.

APLICACIONES

ACCESO A APLICACIONES

El concepto de Ventanilla Única, se plasma en los correspondientes Portales de Aplicaciones. El elemento fundamental de autenticación será en su momento el DNI electrónico, pero como se ha comentado en el apartado anterior hace falta el servicio de infraestructura que proporcione el Logon Único y que además permita determinar a que aplicaciones tiene derecho qué persona, en función de su identidad y de la forma de autenticación (puede ser conveniente permitir el acceso desde entornos sin lectores de tarjetas - domicilios - a través de userid/password), .

Por otra parte en lo que se refiere a los funcionarios, el servicio de Single Sign On para acceder a sus aplicaciones de trabajo, sean de Web, red de área local o legacy, permite aportar mejor experiencia de uso a los usuarios, y constituyen proyectos de alta visibilidad en la organización

FIRMA ADMINISTRATIVA DE DOCUMENTOS

La firma digital es la función necesaria para avanzar hacia la oficina sin papel. Aplicaciones dedicadas a la efectuar la firma, se tienen que ver complementadas con las correspondientes funciones de verificación y de registro. Un sistema ágil y completo que permita consultar los documentos y peticiones firmadas y custodiadas por la administración es fundamental para lograr la confianza de los ciudadanos en un sistema sin tangibles como el papel.

Por otra parte para el funcionario resulta de gran ayuda aplicaciones de firma que le permita visar de forma rápida todos aquellos documentos que firma en función de su cargo y por requerimiento administrativo (porque así lo requiera las normas establecidas).

CORREO Y MENSAJERIA SEGURA

El correo electrónico es una de las utilidades informáticas más ampliamente utilizadas, y constituye un método muy común para el intercambio de información tanto dentro como fuera de la organización, siendo por tanto muy sensible a los riesgos de seguridad. Añadir una capa de seguridad a los correos requiere no solo la autenticación mediante la identidad digital, sino también la privacidad mediante encriptación. El problema en este caso reside en la gestión de las claves de criptografía. Además, el correo electrónico está sujeto a otros tipos de ataques como la dis-

persión de virus o la utilización de leguaje ofensivo o fuga de información confidencial. Por lo tanto hay que combinar las funciones de cifrado de información con la de filtrado de contenidos y virus.

La solución más eficiente para cumplir con estos requerimientos (gestion de certficados de receptores, filtrado de contenidos y virus) está basada en servidores de mensajería con interfaces a los servidores de correo más extendidos (Exchange, Lotus).

WEB SERVICES

La arquitectura de Web Services está dedicada a mejorar la eficiencia y automatización mediante la integración más fácil de los procesos que pueden correr en distintos departamentos o incluso organizaciones. Esto permite expandir el concepto de Ventanilla Única al de Gestor Único, de tal forma que una petición puede ser tratada de forma cooperativa entre múltiples aplicaciones pertenecientes al mismo o distintos organismos. Mediante Web Services se pueden obtener evidentes mejoras de integración, pero es necesario establecer la seguridad de los datos en transito, y la identidad de los peticionarios, es decir establecer el sistema de confianza para las transacciones. Para ello se están desarrollando el conjunto de estándares mencionados en el apartado anterior para poder autenticar, firmar, validar, encriptar mensajes xml, así como establecer los derechos permitidos cuando las transacciones pasan de servicio a servicio.