VII JORNADAS SOBRE TECNOLOGÍAS DE LA INFORMACIÓN PARA LA MODERNIZACIÓN DE LAS ADMINISTRACIONES PÚBLICAS
A CORUÑA
15, 16, 17 y 18 de octubre de 2002
Palacio de Congresos y de la Ópera
www.tecnimap.com
Ponencias

# La Gestión de Identidad como solución de seguridad para la generalización de las iniciativas de Administración Electrónica.

**Jesús Romero**

*Gestor de Negocio e-Security*

*Ingeniero Superior de Telecomunicación por la Universidad de Valladolid*

## 1 Antecedentes y Escenario.

### 1.1. Introducción.

Con los proyectos de Administración Electrónica, ligados a la implantación de la Sociedad de la Información mediante la incorporación las nuevas tecnologías de la información y las comunicaciones, las distintas instituciones consiguen facilitar el acceso a los servicios y mejorar la calidad de los mismos.

Así, uno de los primeros pasos en la política de construcción de la Sociedad de la Información ha sido la incorporación de las TIC en la Administración que, con el propósito de acercarse al ciudadano, está avanzando en el compromiso de gestionar gran parte de los procesos administrativos a través de Internet.

Esta filosofía, que se expresó en la Cumbre de los Quince celebrada en Lisboa, pretende conducir a la denominada Administración Electrónica. La regulación por Decreto, en septiembre de 1999, de la firma electrónica y las directrices enmarcadas dentro del Plan InfoXXI han venido a reforzar esta apuesta.

El carácter de alta confidencialidad de la información que se maneja en este ámbito hace que la seguridad adquiera un carácter determinante en toda iniciativa de Administración Electrónica, en la que resulta primordial establecer los sistemas adecuados para identificar los dos extremos del proceso: de un lado, la Administración y de otro, el ciudadano.

### 1.2. Las arquitecturas de seguridad como solución a los problemas derivados de la conectividad.

La aparición de Internet y su adopción por las instituciones como soporte de las comunicaciones y servicios (correo electrónico, sitios web, etc.) trajo consigo hace ya unos años la necesidad de aislar y proteger los procesos y datos fundamentales de las distintas administraciones, para impedir accesos no autorizados desde la red.

Con la llegada de las primeras iniciativas de Administración Electrónica el problema se agravó, al convertirse Internet en el medio donde se desarrolla la relación de la Administración con los ciudadanos, con las empresas y entre las propias instituciones, con la consiguiente apertura de las Instituciones Públicas hacia el exterior permitiendo la integración de todos los actores en los procesos administrativos.

La solución tecnológica a este reto se superó con las denominadas arquitecturas de seguridad, en las que se incluyen, entre otros, los cortafuegos o “firewalls”, las sondas de detección de intrusiones, los antivirus de pasarela, los escáneres de vulnerabilidades y los correspondientes sistemas de gestión.

### 1.3. Las tecnologías de certificación como habilitadoras de los procedimientos electrónicos.

En el paso de la Administración convencional a la Electrónica, surgió la necesidad de una tecnología que fuera capaz de garantizar los mecanismos de seguridad necesarios (autenticidad, integridad, confidencialidad y no repudio) en las distintas iniciativas.

Como solución a esta necesidad y apoyándose en los algoritmos de criptografía asimétrica surgen las tecnologías de certificación, soluciones basadas el las Infraestructuras de Clave Pública (en inglés Public Key Infrastructure, PKI). Estas tecnologías ofrecen la arquitectura necesaria para el uso de certificados digitales, consiguiendo así la autenticidad, la

integridad (mediante el proceso de firma digital), la integridad (mediante el proceso de cifrado) y el no repudio (mediante el proceso de firma digital)

En la práctica, estas soluciones o su evolución brindan la posibilidad técnica de implantar servicios y mecanismos orientados a la Administración Electrónica, tales como: Cifrado y Firma electrónica, Intercambio seguro de información, Apertura en acto público, Sellado de tiempo, Firma colegiada y Voto electrónico.

### 1.4. Nuevos retos de seguridad asociados a la generalización de las iniciativas de Administración Electrónica.

Dentro del proceso de modernización y actualización de los sistemas en el que está inmerso el Sector Público, numerosas Administraciones centrales, autonómicas y locales han implantado con éxito distintas iniciativas de Administración Electrónica. Por otra parte y a partir las planificaciones existentes, es de esperar que a corto/medio plazo se generalicen este tipo de iniciativas en todos los ámbitos, aumentando tanto el número de las mismas como su alcance.

Esta transición llevará asociada una gran cantidad de beneficios, a partir de la mejora de eficiencia y eficacia de procesos internos y del establecimiento de nuevas vías de comunicación y relación con el ciudadano, con las empresas y entre las propias instituciones. Ahora bien, la transición mencionada llevará también asociada una nueva problemática de seguridad a resolver.

Actualmente los sistemas de información internos de las distintas administraciones están formados por diferentes plataformas y aplicaciones, cada uno de los cuales presenta su propio sistema de seguridad. La diversidad de tecnologías y de sistemas de seguridad aumenta si se contemplan también entornos Internet y Extranet existentes en la actualidad.

Con la generalización de iniciativas de Administración Electrónica este problema de heterogeneidad empeorará, debido a la transformación drástica que sufrirán los sistemas de información para que puedan soportar las nuevas iniciativas internas o externas, transformación que consistirá en la aparición de nuevas plataformas tecnológicas y en el crecimiento sustancial de las ya existentes.

De esta forma, los ya complicados sistemas de seguridad actuales se verán directamente impactados al aparecer nuevas aplicaciones, nuevos sistemas y, en definitiva, nuevos recursos que proteger y a los que controlar y auditar su acceso. De forma análoga, la gestión de usuarios y de políticas corporativas de seguridad se hará inabordable en un entorno tan heterogéneo.

Todos estos cambios se traducirán en nuevos e importantes retos para los responsables de seguridad de las instituciones, al volverse inmanejable el ofrecer respuesta a las siguientes necesidades para los distintos entornos (Intranet, Extranet e Internet) con los recursos disponibles en la actualidad:

- Gestión unificada, centralizada y automatizada de usuarios.
- Gestión centralizada de las políticas de seguridad corporativa, incluyendo las políticas de contraseñas y de control de acceso.
- Agregación de identidades, mediante un sistema capaz de recoger y consolidar la información de perfiles y atributos utilizada en los sistemas de seguridad de las distintas aplicaciones.
- Provisión centralizada de recursos para las distintas identidades.
- Propagación de la identidad de los usuarios entre sistemas, con objeto de obtener la validación única.
- Implantación en las nuevas plataformas de sistemas de auditoría acordes al Reglamento de la LOPD.

En resumen, la generalización de las iniciativas de Administración Electrónica presentará una serie de problemas de seguridad, tanto en su gestión como en la operativa de los usuarios, que repercutirán negativamente en la eficacia y eficiencia de los procesos y que incrementarán los costes de explotación.

En las siguientes páginas se expone la visión de Indra sobre las tecnologías de Gestión de Identidad como solución al escenario planteado.

## 2 Infraestructura de Gestión de Identidad

### 2.1. Planteamiento de la solución.

Como solución a la problemática expuesta, se hace necesaria la definición de una infraestructura de seguridad robusta, de alta disponibilidad, escalable e integrada con los sistemas de información que denominaremos Infraestructura de Gestión de Identidad. Como requisito básico, dicha infraestructura deberá resolver la “cuádruple A”:

- AUTENTICACIÓN: soportando múltiples mecanismos de identificación de los usuarios que acceden a los recursos.
- ADMINISTRACIÓN: gestionando de forma centralizada los usuarios, recursos, políticas y reglas de acceso.
- AUTORIZACIÓN: implantando y gestionando los mecanismos de control de acceso a los recursos.
- AUDITORÍA: generando trazas detalladas de la actividad del sistema que sean suficientes tanto para la gestión del mismo como para la adecuación a las medidas del Reglamento de la LOPD.

Dado el enorme alcance funcional de la infraestructura a construir y a partir de la complejidad tecnológica que presentará, se hace necesario abordar el problema por partes, diseñando una solución modular en la que cada uno de los módulos tenga entidad y sentido por sí mismo.

### 2.2. Descripción de los módulos.

A continuación se detallan los módulos necesarios para que, una vez integrados entre ellos y con los sistemas de información corporativos, proporcionen la "cuádruple A" dando así respuesta a las necesidades expuestas en el apartado anterior.

#### 1. Módulo Repositorio de Información.

Es la estructura sobre en la que se almacenará toda la información asociada a la Gestión de Identidades. Por razones escalabilidad y rendimiento se recomienda el uso de un directorio LDAP.

Así, en el Módulo Repositorio de Información se utilizará para almacenar y modificar las identidades y sobre él se definirá la estructura organizativa del sistema completo.

#### 2.- Módulo de Definición de Identidades.

Mediante este módulo se realizará la definición de las distintas identidades del sistema y su almacenamiento en el módulo Repositorio de Información. Dado el enorme volumen de usuarios que trabajarán en los nuevos sistemas el módulo

deberá ser capaz de manejar a la hora de definir identidades dos conceptos estrechamente relacionados que denominaremos “perfiles” y “atributos”.

Se define como perfil de identidad los arquetipos de usuario que vienen determinados por la operativa de los sistemas o por la estructura organizativa de la organización. Por otro lado se denominarán atributos al conjunto de permisos que el usuario tendrá sobre los recursos de los sistemas de información.

Además, para que el funcionamiento del sistema sea lo más productivo posible, el módulo dispondrá de la capacidad de definir identidades de forma automática a partir de la información contenida en repositorios corporativos ya existentes (lógicamente, siempre que éstos sean lo suficientemente estándar).

### 3.- Módulo de Provisionamiento y Gestión de Usuarios.

A partir de la definición de identidades realizada en el módulo anterior, este módulo se encarga de la gestión centralizada y automatizada de usuarios.

Así, el objetivo de este módulo es automatizar, según la política de seguridad corporativa, la asignación y administración de las habilitaciones y de los derechos de acceso a los recursos para los usuarios internos y externos.

El módulo de Provisionamiento y Gestión de Usuarios será el punto centralizado de definición de políticas relacionadas con el control de accesos, las contraseñas de usuarios y las propias identidades, encargándose de dialogar con los sistemas de información convenientes para implementarlas dichas políticas.

El módulo dispondrá de los procedimientos automáticos y de los “workflows” necesarios para gestionar las aprobaciones y notificaciones referentes a el aprovisionamiento de los mismos.

Por último, para garantizar la gestión correcta del sistema global y con objeto de poder cumplir las medidas establecidas en el reglamento de la LOPD, el módulo dispondrá de un motor de auditoría lo suficientemente granular y versátil como para poder acceder a los tipos de informe requeridos por el administrador (por usuarios, por recursos, por perfiles, por atributos, por fechas, etc.)

**4.- Módulo de propagación de identidad y control de acceso.**

Este módulo se encarga por una parte de propagar la identidad de los usuarios a través de todos los sistemas con objeto de obtener la validación única (Single Sign-On, SSO) y por otra de gestionar el control de acceso a todos los entornos corporativos (Enterprise Access Management, EAM).

El módulo dispondrá de los procedimientos automáticos necesarios para automatizar la resolución y gestión de las peticiones de acceso a los recursos, soportando esquemas múltiples de autenticación, control de acceso consistente y un nivel suficiente de granularidad.

En cuanto al Single Sign-On, el módulo proporcionará un punto (por ejemplo a modo de portal) en el que el usuario se valide de forma única, propagando la identidad de forma automática al resto de sistemas.

Dicha propagación de identidad es tecnológicamente sencilla en los entornos web, los construidos sobre en servidores de aplicaciones y los basados en sistemas de autenticación LDAP. Para el resto de entornos serán necesarios trabajos de desarrollo para realizar la integración, por lo que es recomendable que la organización evalúe la relación coste/beneficio para cada uno de ellos.

Por último y al igual que el módulo anterior, incorporará las funciones de auditoría lo suficientemente granular y versátil como para poder acceder a los tipos de informe requeridos por el administrador.

**5.- Módulo de control del sistema.**

El último módulo establece la infraestructura necesaria para la operación de todos los módulos anteriores mediante la/s consola/s de administración.

Así, la misión de este módulo es consolidar en un entorno Web los interfaces necesarios para la operación del sistema global. Así, desde la/s consola/s mencionadas se realizarán de forma centralizada las tareas de configuración de módulos, modificación de políticas de seguridad, obtención de informes de auditoría, etc.

### 2.3. Beneficios de la solución propuesta.

Mediante el diseño e implantación de la Infraestructura de Gestión de Identidad, las instituciones satisfarán las necesidades de seguridad expuestas en el capítulo anterior:

- Gestión unificada, centralizada y automatizada de usuarios.
- Gestión centralizada de las políticas de seguridad corporativa, incluyendo las políticas de contraseñas y de control de acceso.
- Agregación de identidades, mediante un sistema capaz de recoger y consolidar la información de perfiles y atributos utilizada en los sistemas de seguridad de las distintas aplicaciones.
- Provisión centralizada de recursos para las distintas identidades.
- Propagación de la identidad de los usuarios entre sistemas, con objeto de obtener la validación única.
- Implantación en las nuevas plataformas de sistemas de auditoría acordes al Reglamento de la LOPD.

Por otra parte las instituciones disfrutarán de los siguientes beneficios adicionales:

- Incremento de la productividad y mejora de los procedimientos internos:
  - los usuarios trabajarán con sistemas de seguridad más cómodos y amigables gracias a la funcionalidad de Single-Sign On.
  - la disponibilidad de los sistemas de usuario aumentará al realizarse de forma automática la definición de identidades, la asignación de privilegios y la provisión de recursos.
  - la gestión y auditoría de los sistemas de información será más cómoda y efectiva, eliminando tareas rutinarias y permitiendo a los responsables técnicos dedicarse a tareas de mayor valor añadido.
- Reducción de costes:
  - la Infraestructura de Gestión de Identidad elimina la necesidad de numerosas herramientas comerciales que dan soluciones de nicho y de alcance limitado a las problemáticas planteadas.
  - se reducirá de forma drástica del número de llamadas a los sistemas de soporte a usuarios.

## 3 Conclusiones

Tal y como se ha descrito en el presente documento, la generalización de iniciativas de Administración Electrónica en las Administraciones Públicas, llevará asociados importantes desafíos de seguridad.

Para dar respuesta a los mismos, posibilitando la gestión y explotación segura de los sistemas de información y, por extensión, las propias iniciativas de Administración Electrónica, surgen lo que hemos denominado Infraestructura de Gestión de Identidad.

La tecnología de Gestión de Identidad está ya disponible, al poder encontrarse actualmente en el mercado distintos productos comerciales que dan solución a cada uno de los módulos de la arquitectura definidos en este documento. Por otro lado, las actuales Arquitecturas de Certificación son perfectamente integrables en las Infraestructuras de Gestión de Identidad.

Ahora bien, el diseño e implantación de una Infraestructura de Gestión de Identidad no es un trabajo sencillo. Una vez analizadas las necesidad corporativas y elegidos a partir de las mismas los distintos productos que aporten la solución para cada módulo, habrá que afrontar el proyecto de integración de dichos productos entre sí y con los sistemas de información corporativos. Dicho proyecto de integración será de alcance y dificultad considerables.