tecnim@p Sevilla 2006
30 mayo a 2 junio
060.es
24x7x365

Comunicación

305

GESTIÓN INTEGRADA DE IDENTIDADES EN EL MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES

Angel Valor Reed
Jefe de Servicio de Administración Electrónica
Área de Informática – Unidad de Apoyo
Dirección General de Seguros y Fondos de Pensiones
Ministerio de Economía y Hacienda

Fernando Rubio Ponce
Jefe de Área Informática
Subdirección General de Proceso de Datos
Ministerio de Trabajo y Asuntos Sociales

Angel Valor Reed
Fernando Rubio Ponce

Palabras clave

Gestión Integrada de Identidades; Sincronización de datos; Autenticación robusta; Directorio corporativo; PKI; Tarjeta inteligente; Single Sign-On.

Resumen de su Comunicación

Este estudio ha sido motivado por situaciones como las siguientes:

Situación 1:

Un nuevo empleado se incorpora a una organización. Con suerte, obtendrá acceso a todas sus cuentas (correo, directorio corporativo, RRHH, control de presencia) en una semana.
Un empleado malintencionado abandona la organización. Al ser los plazos iguales, podría utilizar sus accesos remanentes para causar problemas de seguridad.

Situación 2:

Un empleado cambia de cargo. Se modifican los registros correspondientes en el sistema de RRHH. Sus datos, sin embargo, permanecen inalterados – y erróneos – en el resto de sistemas.

Situación 3:

Un empleado precisa acceder a ocho aplicaciones corporativas. A partir de la tercera aplicación como mucho, reutilizará la misma contraseña o la escribirá en un cuaderno o fichero en su PC, sin protección. Lo que constituye un atentado a la seguridad.

La Gestión Integrada de Identidades (GII) permite resolver estos problemas, mediante:

- *La sincronización de datos de identidad.*
- *La autenticación robusta ante el directorio corporativo mediante PKI y tarjeta inteligente.*
- *El Single Sign-On.*

Entre las conclusiones del estudio destacan las siguientes:

1. La seguridad ya no está reñida con la comodidad del empleado.
2. Los directorios corporativos se están convirtiendo en proveedores centralizados de seguridad.
3. Las recomendaciones del estudio podrán servir de guía y referencia a aquellas organizaciones que apuesten por la GII. Ese es el objetivo de esta comunicación.

Angel Valor Reed
Fernando Rubio Ponce

GESTIÓN INTEGRADA DE IDENTIDADES EN EL MINISTERIO DE TRABAJO Y ASUNTOS SOCIALES

1. Introducción

La Gestión Integrada de Identidades (GII) es una estrategia que adoptan las organizaciones, por un lado, para lograr la consistencia de los datos de identidad de sus empleados, a través de su sincronización; y por otro, para garantizar la seguridad en los accesos de los empleados a las aplicaciones corporativas, a la vez que se aumenta la productividad de estos a través de un proceso de autenticación simplificado o de Single Sign-On.

Adicionalmente, la GII permite:

a. Cumplir con la legislación de protección de datos de carácter personal.
b. Reducir costes relacionados con la gestión de identidades, en particular de atención a empleados para la gestión de sus contraseñas, alcanzando a la vez una mayor eficiencia y comodidad en el acceso a los datos y aplicaciones corporativas.

La tormentosa relación entre seguridad y comodidad ha cambiado: ahora seguridad equivale a comodidad

Hace unos años las empresas no podían siquiera imaginar un escenario en que los empleados no tuvieran que recordar infinidad de contraseñas para autenticarse ante las múltiples aplicaciones corporativas. Utilizar una única contraseña para todas las aplicaciones –o guardarla/s en lugar distinto de la cabeza- equivalía necesariamente a pérdida de seguridad: "los hackers se concentrarán en desvelar esa única contraseña, con la seguridad de que, con paciencia, tarde o temprano la descifrarán y, en tal caso, el premio será grande: el acceso a absolutamente todas las aplicaciones del usuario-víctima".

La gran ventaja de la GII radica en que, efectivamente, cada usuario deberá recordar una ÚNICA contraseña. La diferencia está en lo que rodea a esa ÚNICA contraseña a recordar, que es muy distinto ahora respecto a lo que se tenía hace unos años. Las mejoras más notables tienen que ver con CÓMO SE ALMACENA esa contraseña y CÓMO SE PROVEE al sistema con ella. Hasta hace bien poco, la forma de ALMACENAMIENTO de la contraseña se dejaba a discreción del usuario, y aquí radicaba su enorme riesgo: en el mejor de los casos ese medio lo constituían sus neuronas. En el peor de los casos, a partir de la tercera contraseña a recordar, el empleado reasignaba la misma contraseña a las subsiguientes aplicaciones, o bien procedía a escribirlas en un cuaderno, una PDA o un fichero no cifrado en su ordenador, allanando considerablemente el camino a los hackers.

En cuanto a CÓMO SE PROVEEN esas contraseñas, la situación hasta hace poco consistía en su introducción manual desde el teclado del terminal de usuario: un software malicioso de lectura de teclado podría por tanto recuperar fácilmente la contraseña tecleada. Lo mismo podría conseguirse mediante un detector de variaciones del campo magnético que se produce al oprimir las distintas teclas (ataque TEMPEST).

La GII dota de seguridad a la autenticación de usuarios mediante el uso de tarjetas inteligentes (o llaves USB de testigos) que almacenan certificados digitales de usuario, provistos por una Infraestructura de Clave Pública (PKI). Este binomio implementa tres factores que hacen (prácticamente) inexpugnable la seguridad:

- **Algo que se sabe:** la contraseña o PIN que desbloquea la clave privada que se encuentra en el chip de la

tarjeta y que permite efectuar operaciones de cifrado y firma digital.

• **Algo que se posee:** el hecho de que el par clave pública-clave privada haya sido creado mediante un dispositivo seguro de creación de firma, garantiza que el único sitio físico en que se encuentra la clave privada es el chip de la tarjeta. La tarjeta inteligente, mediante un mecanismo tipo válvula (se permite la entrada a todo, la salida a nada), garantiza que esta clave en ningún momento abandonará el chip, realizándose todas las operaciones que requieren usar la primera dentro del segundo. La tarjeta, además, se encuentra bajo el único y absoluto control del usuario. Si un individuo malintencionado consigue la contraseña del usuario mediante, por ejemplo, un ataque TEMPEST, aún tendría que hacerse con la tarjeta para poder acceder a la clave privada; y al contrario, si la tarjeta cayera en manos de ese mismo individuo, éste aún tendría que conseguir la contraseña de desbloqueo de la clave privada para poder operar (y tendría que conseguir todo esto, antes de que la víctima comunicara la pérdida y se revocara el certificado).

• **Algo que se es:** aunque los dos factores anteriores de por sí ya hacen la vida del individuo malicioso bastante difícil, se puede añadir un último ingrediente que hace la seguridad francamente inexpugnable. Se trata de la biometría. Al personalizar la tarjeta inteligente de un usuario determinado, se puede almacenar en ésta, por ejemplo, la morfología de su huella dactilar, digitalizada. Adquiriendo los lectores de tarjeta apropiados, capaces de leer la huella dactilar, se puede garantizar adicionalmente que quien accede es quien dice ser. Es cierto que un hacker persistente podría conseguir la morfología ajena y, por ejemplo, realizar un implante de silicona que simulara las huellas dactilares, pero convendremos en que las probabilidades de burlar los tres factores de seguridad al unísono son ínfimas, sin contar con que el coste que ello supondría lo convierten en un sinsentido.

2. Tipos de Administración Electrónica: i) Documental; ii) de Gestión de Identidades

En aras de la claridad en la exposición que sigue, estableceremos una distinción entre los dos tipos posibles de Administración Electrónica:

1. Administración Electrónica Documental: relacionada con el quehacer diario de las unidades administrativas. Su característica distintiva es el uso del certificado de usuario para firmar y cifrar digitalmente documentos. Consta, entre otras, de las siguientes facetas:

a. La firma digital y el cifrado de todo o parte de los expedientes administrativos, así como de los flujos de información que se establecen entre los ciudadanos y la administración.
b. El intercambio telemático de datos entre la administración y otras entidades.

2. Administración Electrónica de Gestión de Identidades: tan importante como la anterior, aunque tradicionalmente se le ha prestado menos atención. Es la faceta de la Administración Electrónica que permite que un empleado de la Administración se autentique de manera robusta, mediante mecanismos de PKI, ante el directorio de trabajo, de modo que el acceso subsiguiente a las aplicaciones corporativas (incluyendo a las utilizadas para el ejercicio de potestades y que por tanto implican Administración Electrónica Documental) se beneficie de esa autenticación fuerte, garantizando en todo momento la autenticidad, integridad, confidencialidad y no repudio. Para que sea una realidad, la Administración Electrónica de Gestión de Identidades requiere la implantación de un mecanismo de Single Sign-On (SSO), que sustituya el mecanismo habitual de presentación de credenciales de usuarios, por separado, ante cada una de las aplicaciones corporativas, por un mecanismo basado en la **confianza**, por parte de las aplicaciones, en la autenticación robusta que provee el directorio. En definitiva, la única contraseña que deberá recordar el usuario es la que desbloquea su clave privada. Existen dos métodos para alcanzar el SSO, un método elegante pero intrusivo con las aplicaciones; y un método menos elegante pero no intrusivo con las aplicaciones. Ambos serán discutidos en la sección dedicada al SSO.

A día de hoy, el cuadro típico en las organizaciones es una incipiente Administración Electrónica Documental y una inexistente Administración Electrónica de Gestión de Identidades. La Administración Electrónica de Gestión de Identidades requiere de un decidido impulso por parte de la Administración, pues sólo a través de ella se puede garantizar el cumplimiento de los requisitos ACID para el ejercicio de potestades por parte de la primera.

Los apartados restantes de esta comunicación están dedicados al estudio de las fases necesarias para hacer una realidad la Administración Electrónica de Gestión de Identidades, también conocida como Gestión Integrada de Identidades en el contexto global de las organizaciones.

Como resultado del estudio llevado a cabo en el MTAS, ha quedado claro que las fases por las que se debe transitar son:

Fase 1: Sincronización de orígenes de datos de identidad de empleados.

Fase 2: Gestión del acceso de empleados a recursos de información, mediante:

- Autenticación robusta ante el dominio de trabajo mediante PKI y tarjeta inteligente.
- Single Sign-On.

Los apartados siguientes están dedicados a la discusión de estas fases y etapas.

3. Fase 1: Sincronización de orígenes de datos de identidad de empleados

Desafortunadamente, el cuadro típico en las organizaciones es el de varios repositorios inconexos con los mismos tipos de datos de identidad de empleados, pero que, al ser administrados de manera independiente, resultan desiguales dependiendo del almacén de que se trate. Dar de alta y de baja cuentas de usuario conlleva esfuerzos que consumen mucho tiempo y que son en la mayoría de los casos redundantes. Por otro lado, tener muchos repositorios de usuarios, uno por aplicación, en lugar de uno centralizado, lleva a la desesperación de estos últimos, que se ven en la necesidad de recordar múltiples alias y contraseñas para las distintas aplicaciones. Y esto empeora según la organización crece. El resultado es un aumento de costes y pérdida de productividad, pérdida de seguridad y pérdida de una visión global del empleado a nivel de la organización.

En pocas palabras, lo que se busca con la sincronización de orígenes de datos es que, por ejemplo, el apellido o cargo de un empleado permanezca igual y correcto en el almacén de RRHH, el directorio corporativo, el directorio de correo y el sistema de control de presencia. Para ello, para cada dato de identidad, se declara uno de los almacenes como dominante sobre el resto y, al cambiar el dato en aquel, una aplicación traslada las modificaciones al resto de manera transparente.

Además de gestionar y coordinar los datos de identidad provenientes de diferentes orígenes de datos, una aplicación de sincronización de datos permite combinar esa información en una vista lógica, simple, modificable por un administrador a través de una interfaz web, que representa toda la información sobre un empleado dado en la organización.

Existen en el mercado varios productos de sincronización de datos. A la hora de escoger uno, las funcionalidades a las que habrá que prestar mayor atención serán:

1. La variedad de orígenes de datos que permite conectar. El producto debe ser capaz de operar con los principales sistemas de directorio corporativos, los principales sistemas de bases de datos del mercado,

los principales directorios de correo, ficheros planos, etc.

2. El producto debe traer desarrollados, listos para comenzar a ser usados después de una configuración básica, piezas de software conocidas como agentes gestores que permitan, por un lado, importar los datos modificados externamente en los orígenes de datos y, por otro, exportar a aquellos los datos modificados dentro de los repositorios propios del producto en virtud de sus tareas de sincronización. La organización debe prestar atención a si el producto dispone del tipo de agentes gestores apropiados para las aplicaciones comerciales corporativas existentes (de directorio, correo, de base de datos, etc.) y en caso contrario, a la facilidad para lograr esa conectividad mediante un desarrollo a medida.

Uno de los resultados más visibles de la sincronización será la inmediatez con que se proveerán las cuentas de los nuevos empleados. Con un solo "clic", el usuario obtendrá todas las cuentas que precisa para comenzar a trabajar. En el caso de empleados que abandonan la organización, de manera inmediata se podrán desactivar todas sus cuentas, lo que representa un hito importante en la seguridad de la organización.

4. Fase 2: Gestión del acceso de empleados a recursos de información

Acabamos de analizar la sincronización de datos de identidad de empleados, que podríamos definir como una fase preparatoria de aquella que concentra el grueso de las actividades de gestión de identidades: la de gestión del acceso de los empleados a los recursos de información.

Esta fase busca claramente la seguridad, y a través de ésta, la comodidad y aumento de productividad de los empleados. Se consigue en primer lugar, a través de la autenticación robusta de los empleados ante el dominio de trabajo, mediante la implantación de una infraestructura de PKI que haga posible el uso de certificados X509.v3 en tarjeta inteligente. En segundo lugar, a través de la implementación de un mecanismo de Single Sign-On que sustituya el mecanismo habitual de autenticación ante cada aplicación por separado, por uno en que cada aplicación confíe en la autenticación robusta del directorio corporativo para permitir el acceso.

Autenticación robusta ante el dominio de trabajo basada en PKI

Los pasos para implementar la autenticación robusta ante el dominio de trabajo son los siguientes:

1. Tomar las medidas que garanticen que los usuarios pueden comenzar sesión en el dominio de trabajo únicamente si se autentican a través de sus tarjetas inteligentes, mediante los correspondientes lectores. Los principales proveedores de tarjetas inteligentes y lectores los acompañan de software certificado para su gestión e integración con las APIs criptográficas de los sistemas operativos subyacentes. Entre otras funcionalidades, este software garantiza que todas las operaciones con certificado (firma, cifrado, interacción con el directorio) se realizan desde las tarjetas inteligentes. Por otro lado, es preciso efectuar un trabajo de configuración para que el software de tarjetas y lectores pueda dialogar con el directorio corporativo.

2. Como resultado del punto anterior, se establecerá el siguiente proceso:

   a. El empleado enciende su ordenador. En lugar de usuario y contraseña, se le solicita que introduzca su tarjeta inteligente. Una vez introducida, se le solicita el PIN de desbloqueo de su clave privada.
   b. Superadas las comprobaciones, el certificado en la tarjeta se compara con aquel que se encuentra en el correspondiente objeto del usuario en el directorio corporativo. Sólo en caso de coincidencia, se autentica al usuario ante el dominio de trabajo.
   c. A partir de este momento, sólo algunas aplicaciones muy críticas podrían volver a pedir el PIN del

usuario, por ejemplo, antes de firmar documentos muy importantes que impliquen el ejercicio de potestades. El resto de aplicaciones confiará en la autenticación robusta que les expone el directorio corporativo.

Damos por sentado que la organización ya tiene implantada una PKI para la Administración Electrónica Documental. En aras del ahorro de costes, la situación ideal sería re-utilizar esa PKI para la Administración Electrónica de Gestión de Identidades.

Las preguntas que hay que plantearse en este punto son: ¿Son las políticas de certificación de la Autoridad de Certificación de la PKI existente suficientemente flexibles como para permitir, en principio, su uso para la autenticación robusta? En caso afirmativo, será necesario negociar con esa Autoridad una nueva política de certificación titulada "Autenticación Robusta de usuarios", para, a continuación:

1. Crear los nuevos certificados de los usuarios una vez éstos los soliciten.

2. Que los usuarios certifiquen su identidad ante la Autoridad de Certificación, obteniendo el correspondiente código de descarga de las claves.

3. Que los usuarios descarguen, desde el portal de la Autoridad, sus nuevas claves y certificado a su tarjeta inteligente.

4. Que los usuarios, a través de las herramientas de administración de tarjetas, efectúen las tareas de administración necesarias para el uso del nuevo certificado para autenticación robusta ante el directorio de trabajo.

Si la autoridad actual no es flexible con el uso de atributos de los certificados para la creación de nuevas políticas de certificación, la organización tendrá que estudiar decisiones que podrán ir desde la coexistencia de dos PKIs (cuyos certificados, eso sí, compartirían una misma tarjeta inteligente) hasta la renuncia al contrato con la primera Autoridad de Certificación, en favor de una segunda, más flexible, que haga posible la máxima "una política de certificación para cada funcionalidad".

Por último, la organización podría incluso erigirse en Autoridad de Certificación, mediante la adquisición de una plataforma al efecto, que hiciera posible la creación de políticas de certificación, gestionara la creación y descarga de certificados, creara y gestionara las listas de revocación, estableciera relaciones de confianza para certificados de otros proveedores, etc. La ventaja de esta opción es su total flexibilidad e inmediatez. Además, estas plataformas suelen venir provistas de software y herramientas que facilitan enormemente la integración, en las aplicaciones existentes, de la firma digital y el cifrado para la Administración Electrónica Documental. Su desventaja radica en la importante carga de gestión que trae asociada, sobre todo en lo que concierne a la relación con terceros: es necesario publicar y mantener actualizadas las políticas de certificación, establecer convenios con otras Autoridades de Certificación para reconocimiento mutuo de certificados, publicar a diario y posibilitar el acceso en régimen de 24x7 a las listas de certificados revocados, etc. Esta opción podría ser viable para una organización grande, como el MTAS.

Single Sign-On (SSO)

El SSO es el ingrediente que cierra el círculo de la Gestión Integrada de Identidades. No puede hablarse de SSO sin la autenticación robusta ante el dominio de trabajo que acabamos de analizar.

EL SSO es una estrategia para el acceso de los empleados a los recursos de información de la organización, que consta de dos facetas, dependiendo del punto de vista de quien mira:

a. Desde el punto de vista del empleado, SSO equivale sobre todo a comodidad y aumento de productividad: de repente ya no es necesario autenticarse ante cada aplicación corporativa por separado – con el SSO desaparecen las interfaces de autenticación y el empleado accede a las aplicaciones de forma transparente. Lo que ocurre realmente en la trastienda es lo siguiente:

- En el objeto del usuario en el directorio corporativo se encuentran almacenadas, cifradas con métodos que aseguran el absoluto control por el usuario, las credenciales que permiten el acceso a las distintas aplicaciones. Cuando un usuario intenta acceder a una aplicación particular, un software de SSO se encarga de establecer un diálogo con el directorio, recuperar y descifrar las credenciales y obtener el acceso a la aplicación en cuestión. Dependiendo de la organización, este software tendrá una u otra naturaleza, cuestión que discutiremos más abajo.

b. Desde el punto de vista de la organización, SSO equivale sobre todo a seguridad – sin SSO el empleado precisaba de decenas de credenciales para autenticarse ante las aplicaciones. Como hemos visto, tal situación no hace sino allanar el camino de los hackers hacia la consecución de esas credenciales y el acceso indebido a los recursos de la organización. Con el SSO, sólo es preciso recordar el PIN de la tarjeta – la autenticación robusta y el cifrado mediante técnicas de clave pública hacen el resto: las eventuales credenciales secretas de acceso a las aplicaciones se encuentran en el objeto del usuario en el directorio, y sólo éste, a través de la tarjeta, puede descifrarlas. De hecho, en la mayoría de las ocasiones esos secretos no son conocidos siquiera por el usuario – el software se encarga de coordinar ante las aplicaciones la definición y gestión de las eventuales contraseñas de acceso. Y bien, si no se conoce un secreto, es imposible desvelarlo a terceros. Ese es la filosofía de seguridad del SSO.

A continuación discutiremos las dos maneras que existen de conseguir el SSO. Cuál de las dos escoger, depende de las particulares condiciones de la organización:

Un método no excesivamente elegante, pero no intrusivo con las aplicaciones:

Método indicado en las organizaciones históricas, que no pueden permitirse una reingeniería de las aplicaciones corporativas. En estas organizaciones, cada sistema de información está inconexo del resto de sistemas, es decir, implementa de forma individual la autenticación de sus usuarios. Por tanto no existe manera de acceder al mismo como no sea suministrando un secreto (un par alias-contraseña, por ejemplo). Desde un principio, está claro que las aplicaciones no se podrán modificar y que solamente se podrá lograr el SSO "engañándolas" (de manera segura, eso sí). Los pasos para lograr este "engaño" son:

1. En cada PC de empleado se instala un software de SSO no intrusivo. Este software es una especie de "espía" con las siguientes funcionalidades:

a. Es capaz de "aprender" cómo las aplicaciones solicitan a los usuarios que se autentiquen. A través de scripts, y de un proceso de configuración más o menos sencillo, es posible instruir al software de SSO sobre el aspecto que tienen las ventanas de autenticación (y de cambio de contraseñas) de las distintas aplicaciones. A través de interfaces visuales, se muestra el sitio exacto de esas ventanas en que será necesario introducir las credenciales de autenticación. Finalmente, el usuario debe introducir, una única vez, esas credenciales.

b. El software de SSO tiene la capacidad de interactuar con certificados inteligentes provistos por PKI y tarjetas inteligentes, y con el directorio corporativo para la comprobación de la autenticación robusta. Con este arsenal a su disposición, los secretos introducidos por el usuario son almacenados cifrados en su objeto en el directorio corporativo, de modo que sólo este y ni siquiera los administradores tengan acceso a los mismos.

c. La próxima vez que el usuario intente acceder a una de las aplicaciones ya configuradas para SSO, tendrán lugar las siguientes acciones:

i. El software de SSO, que estará escuchando constantemente los eventos de apertura de ventanas, detectará la interfaz de autenticación de la aplicación.
ii. Comprobará el estado de autenticación del usuario en el directorio. En caso de estar autenticado robustamente, recuperará las credenciales apropiadas desde el objeto usuario en el directorio corporativo, las descifrará y las introducirá en los sitios apropiados del script previamente configurado. Con el resultado, "engañará" a la aplicación, simulando el envío por el usuario del formulario de autenticación. La aplicación permitirá el acceso al usuario a continuación. Para éste, se ha producido la magia, pues ni siquiera notará el complicado proceso que acaba de tener lugar entre bastidores.
iii. Es posible, y recomendable, delegar en el software de SSO la subsiguiente gestión de credenciales ante las aplicaciones: así, cada vez que la aplicación envíe una interfaz de cambio de contraseñas, se realizarán acciones similares a las que acabamos de describir. Como resultado, después del primer cambio, el usuario desconocerá totalmente las credenciales, lo que beneficiará a la seguridad.

Terminaremos diciendo que las principales soluciones de este tipo son capaces de "engañar" a prácticamente cualquier tipo de aplicación, sea de naturaleza web, Windows, o de emulación de terminales.

Su principal ventaja radica en que no es preciso modificar las aplicaciones existentes para beneficiarse del SSO. Su inconveniente, la necesidad de instalar un cliente que consume recursos en cada PC que se vaya a beneficiar del SSO. Y la importante carga de configuración que traen asociadas (aunque las principales aplicaciones corporativas pueden ser configuradas de manera centralizada, basándose en el directorio corporativo, por un administrador).

Un método elegante, aunque intrusivo con las aplicaciones

Si la organización puede permitirse una reingeniería de sus aplicaciones corporativas, o si se trata de una organización de reciente creación, entonces sin dudas su elección debe ser esta. Los pasos para conseguir el SSO son los siguientes:

1. Diseñar una política de roles para el acceso a las aplicaciones corporativas: se debe diseñar tantos roles como distintas necesidades tengan los usuarios en el acceso a las distintas aplicaciones. Por ejemplo, el rol administrador tiene el máximo de privilegios ante todas las aplicaciones, en tanto el rol invitado tiene el mínimo de privilegios, limitados a la lectura de determinados registros. El diseño de esta política requiere de mucho sentido común, pues, si por un lado es recomendable afinar lo más posible los derechos que determinados usuarios pueden tener, no es menos cierto que una proliferación de roles puede ser contraproducente.

2. Diseñar un módulo de seguridad y exigir su uso por todas las aplicaciones corporativas: cuando una aplicación recibe una petición de autenticación por un usuario, la deriva a este módulo de seguridad. El módulo construye un testigo y lo pasa al usuario, reclamando de éste que lo devuelva firmado. A continuación se comprueba la firma con el certificado que el módulo recupera del directorio corporativo. En caso de éxito, se recupera la lista de roles del usuario y se pasa a la aplicación. En base a esta lista, la aplicación permite el acceso del usuario a unas u otras funcionalidades. La siguiente vez que el usuario requiera autenticarse ante una aplicación, le bastará con presentar al módulo de seguridad ese mismo testigo, aligerando así el proceso. Todo el mecanismo, por supuesto, es transparente para el usuario.

Terminaremos con una nota positiva: este método no es una quimera- ya ha sido implementado y está dando sus frutos en organismos como la Dirección General de Seguros y Fondos de Pensiones del Ministerio de Economía y Hacienda, donde todas las aplicaciones fueron sometidas a una reingeniería en el marco de

su Plan de Modernización.

5. Conclusiones

Los objetivos de este trabajo eran, en este orden, aclarar qué era la Gestión Integrada de Identidades, estudiar cuáles serían las principales fases y etapas por las que habría que transitar para su implantación en el MTAS y realizar una serie de recomendaciones sobre buenas prácticas para alcanzar los objetivos trazados.

Una vez concluido el trabajo, creemos que no solo se han cumplido esos objetivos, sino que las conclusiones y recomendaciones del mismo pueden ser de utilidad para las instituciones que, preocupadas por la seguridad y la productividad de sus empleados, proyecten hacer realidad la Gestión Integrada de Identidades. Si este trabajo sirve de inspiración o guía a algunas de esas instituciones, nosotros los autores nos damos por satisfechos.