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

Comunicación

405

EL TOKEN CDCARD: UNA SOLUCIÓN PARA GENERALIZAR LA FIRMA ELECTRÓNICA Y AUMENTAR LA SEGURIDAD EN LOS PROCESOS DE AUTENTICACIÓN

Manuel Mollar Villanueva
Profesor de Lenguajes y Sistemas Informáticos
Universitat Jaume I

Modesto Fabra Valls
Secretario General
Universitat Jaume I

José Pascual Gumbau Mezquita
Gabinete Técnico de Rectorado
Universitat Jaume I

Vicente Andreu Navarro
Técnico de Planificación y Organización
Universitat Jaume I

Manuel Mollar Villanueva
Modesto Fabra Valls
José Pascual Gumbau Mezquita
Vicente Andreu Navarro

Palabras clave

Autenticación, tokens, seguridad, firma electrónica, administración electrónica, PKI

Resumen de su Comunicación

En la presente comunicación se propone la utilización de credenciales o de certificados digitales y sus claves asociadas transportados mediante dispositivos extraíbles y universales como los discos USB o los CDROM como sistema sencillo de implementar que permite incrementar la seguridad en la autenticación.

El sistema, por su escaso coste, podría ser acometido por las administraciones, en especial las locales, para procesos de distribución generalizada de certificados digitales de firma electrónica, con lo que contribuiría a la consolidación de la administración electrónica.

En la comunicación también se da cuenta de una implementación de la solución propuesta efectuada en la Universitat Jaume I, mediante la cual se han distribuido más de 12.000 certificados digitales entre todo su personal y estudiantes, lo que ha permitido afianzar su plan de administración electrónica.

Manuel Mollar Villanueva
Modesto Fabra Valls
José Pascual Gumbau Mezquita
Vicente Andreu Navarro

EL TOKEN CDCARD: UNA PROPUESTA PARA GENERALIZAR LA FIRMA ELECTRÓNICA Y AUMENTAR LA SEGURIDAD EN LOS PROCESOS DE AUTENTICACIÓN

1. La problemática que se pretendía solucionar

No hay administración electrónica sin identificación fehaciente en la red. Y la firma electrónica constituye el sistema más depurado técnicamente y seguro jurídicamente. A medio plazo todos los ciudadanos dispondrán de un DNI electrónico con funcionalidades de firma electrónica, pero de momento los equipos no disponen de lector para utilizarlo y su reparto se efectuará a medida en que se renueven los DNI con lo que hasta dentro de 7 u 8 años no estará generalizado.

El proyecto de administración electrónica de la Universitat Jaume I pasaba por un reparto generalizado de firma electrónica entre la comunidad universitaria. Entre todo su personal y, también, entre todos los estudiantes, que no disponen de equipo fijo, sino que utilizan frecuentemente los ordenadores compartidos, por lo que la firma electrónica debía presentar facilidades de movilidad.

Otro de los objetivos perseguidos, común a todas las administraciones con servicios web y, en general, a cualquier entidad que opere en la red, era aumentar la seguridad, que hasta ese momento se apoyaba en usuario y contraseña. Como es de sobras conocido, la autenticación puede hacerse en virtud de algo que el otro sabe (las contraseñas), de algo que el otro tiene (por ejemplo las tarjetas), o de algo que el otro es (sería el caso de los dispositivos biométricos). Una autenticación segura requiere apoyarse, al menos, en dos de los tres factores y así ocurre cuando vamos al cajero electrónico con nuestra tarjeta (algo que nosotros tenemos) y además, introducimos nuestra contraseña (algo que nosotros sabemos). Sin embargo, en Internet, la mayor parte de operaciones se hacen con la utilización de una simple contraseña, lo que ha dado lugar a fraudes como el phishing, o usurpación fraudulenta de las contraseñas.

Existía una tercera restricción consistente en el parque informático. El existente en la Universitat Jaume I, pero también, en casa de los estudiantes de la universidad y de los ciudadanos españoles en general, integrado por equipos que salvo excepciones contadas tienen puerto USB y lector de CD Rom, mientras que no tienen lector de tarjetas.

En la presente comunicación se expone la solución que se adoptó desde el Consejo asesor de las TIC de la Universitat Jaume I. Su implementación ha permitido generalizar la firma electrónica entre la comunidad universitaria con más de 12.000 certificados digitales repartidos a petición de los usuarios.

2. La solución ofrecida

La solución ofrecida ha sido la definición de unos protocolos de autenticación (algunos basados en dos factores) cuyo funcionamiento se sintetiza en el apartado siguiente y que son distintos en atención al grado de seguridad que se requiere. También se ha desarrollado el software que los ejecuta.

El resultado es la autenticación a través de unas credenciales o la creación de la firma electrónica a partir de los certificados digitales y sus claves asociadas, que son incorporados y transportados con seguridad mediante un soporte extraíble y universal (por ejemplo, un disco USB o un CDROM) susceptible de ser utilizado en múltiples equipos. El soporte o dispositivo extraíble se convierte en una herramienta que permite el fácil almacenamiento, transporte y uso seguro de certificados digitales y sus llaves privadas asociadas, y de credenciales para autenticación y se evita tener que instalar los certificados en el disco duro del equipo.

Es decir, el usuario puede autenticarse y crear su firma electrónica a partir de su certificado insertando su memoria USB, o colocando su CDROM en el lector de su ordenador.

Para las entidades que implementan la solución (Ayuntamientos, empresas, etc.) el sistema ofrece múltiples formas de autenticación según la seguridad requerida. Así, según la necesidad, puede utilizarse la cartera de credenciales incorporada en el dispositivo extraíble que es consultada desde el servidor al que trata de acceder, con las debidas restricciones. O también puede efectuarse una autenticación mediante el certificado digital que incorpora y que se utiliza directamente desde el dispositivo. Si se opta por este sistema el coste de un reparto generalizado de dispositivos es muy reducido (el coste de grabar un CDROM es de céntimos de euro) con lo que un Ayuntamiento o una entidad bancaria podrían utilizar este sistema y distribuir generalizadamente la firma electrónica de forma gratuita entre los ciudadanos o sus clientes, sin tener que soportar un coste excesivo ni trasladarles el coste que tendrían otros sistemas como las tarjetas criptográficas.

Como ya se habrá advertido, la solución que se describe no consiste en utilizar un dispositivo con capacidad (autonomía) criptográfica para generar y utilizar internamente las llaves. Consiste en definir y emplear protocolos de autenticación que utilizan los certificados que transporta un dispositivo extraíble e insertado en el equipo desde el que se efectúa el acceso.

En todo caso, permite generar firma electrónica avanzada apoyada en un certificado reconocido (en caso de que el certificado que se distribuya lo esté) con seguridad. De este modo, gracias al reducido coste y a la facilidad de uso, podría generalizarse la firma electrónica avanzada apoyada en un certificado electrónico reconocido, que es el tipo de firma electrónica más extendido, mediante procesos de distribución masiva.

3. Los distintos niveles de seguridad que se alcanzan con los protocolos de autenticación propuestos

La solución propuesta permite implementar diversos protocolos de autenticación, tanto basadas en secretos compartidos incluidos en el token (el identificador del dispositivo y las credenciales), como en la utilización de cualquier certificado digital (con formato PKCS#12) que pueda incorporarse.
Cuando se utiliza una contraseña para proteger la credencial o el certificado se alcanza una autenticación fuerte apoyada en dos factores (la posesión del token más la contraseña).
Las principales opciones son las siguientes:

3.1. Posesión del dispositivo

El usuario se autentica con la simple posesión del dispositivo, concretamente mediante el identificador único que cada uno de ellos incorpora. La universitat Jaume I lo ha implementado mediante el desarrollo de un sistema de control de acceso al ordenador, de modo que, en aquellos equipos que tienen el software instalado, el sistema operativo se bloqueara si el dispositivo no se inserta en el equipo. La autenticación se realiza mediante webservices.

La seguridad específica es muy baja y el sistema únicamente es utilizable en situaciones muy peculiares como el caso en que se ha utilizado en que los usuarios de una sala con varios equipos compartidos se acreditan físicamente en la entrada pero se requiere identificar el equipo concreto que utilizan una vez dentro para cumplir con la LSSI.

3.2. Credencial sin contraseña

Similar al anterior, éste método permite poner condiciones, como ser accedido desde una página web con una determinada URL. Esto lo hace apto para autenticación muy básica en páginas web pero añade funcionalidades como el control del lugar desde el que se accede.

3.3. Credencial con reto

Aplicable para autenticación remota sin cifrar (p. e. páginas web no seguras).
Cuando el usuario envía su identidad al servidor, éste generará un número (reto) y lo envía al usuario, quien lo encripta con su credencial y lo envía encriptado al servidor. El servidor lo desencripta y verifica que es el mismo que envío.

3.4. Credencial con contraseña

La autenticación se efectúa con entrega de la credencial cifrada con una contraseña. Si la credencial es de naturaleza aleatoria (recomendado) resulta prácticamente imposible obtener la contraseña a partir de la credencial cifrada, protegiendo contra el robo o extravío del dispositivo.

3.5. Credencial con reto y contraseña

Es una combinación de los anteriores.

3.6. Credencial protegida con contraseña general (4 niveles)

Los cuatro modos anteriores pueden exigirse cumulativamente entre sí. Además, previamente puede solicitarse la contraseña maestra del dispositivo.

3.7. Certificado sin contraseña

La autenticación se efectúa mediante un certificado digital incorporado en el dispositivo que no va protegido. Se trata de un método poco recomendable que sólo tendría sentido en caso de utilizar certificados no genéricos, es decir, emitidos para el propósito de ser usados en este contexto. De lo contrario, en caso de que se extraviara el dispositivo se podría utilizar el certificado incorporado y no protegido con contraseña para otros efectos.

3.8. Certificado con contraseña

Se trata de un método robusto y de uso universal que permite al usuario que dispone de un certificado digital genérico autenticarse en múltiples servidores y generar la firma electrónica con la clave privada del certificado. El certificado se protege con la contraseña del dispositivo (lo más normal) o con una propia.

3.9. Certificado con doble contraseña

El certificado puede protegerse también con la contraseña del dispositivo y con una propia permitiendo así su utilización para transportar certificados que den acceso a servicios de gran valor.

Manuel Mollar Villanueva
Modesto Fabra Valls
José Pascual Gumbau Mezquita
Vicente Andreu Navarro

4. Su implementación en la Universitat Jaume I. El proyecto clauer

4.1. Dispositivos

Para el proyecto de distribución generalizada de certificados digitales desarrollado en la Universitat Jaume I se eligió inicialmente un disco USB. Al proyecto se le denominó clauer (llavero en valenciano), al tratarse de un dispositivo que permitía almacenar y transportar las claves. El atractivo que representa en sí mismo el dispositivo ha sido un aliciente para el usuario, permitiendo una rápida distribución masiva de certificados. Dado que el disco USB es un dispositivo de lectura/escritura y para evitar que el usuario destruyera accidentalmente la información sensible, el disco se particionó de modo que la mayor parte se dedica a una partición de datos (vfat) y una pequeña parte se reserva para ser gestionada por el software desarrollado que permite añadir/eliminar certificados o cualquier otra información mediante las herramientas apropiadas.

Para reducir el coste en relación con otros repartos masivos se modificó el software para que pudiese utilizar un CD ROM como dispositivo. Esto permitirá a aquellas entidades que deseen utilizarlo el reparto de mini CDs o CD Cards como tokens de identificación.

En este caso, se trata de un CD con una imagen iso9660 (un disco de datos normal) que contiene uno o varios archivos de nombre CRYF_000.cla, CRYF_001.cla, etc. que internamente tienen la misma estructura que se almacena en la partición reservada del disco USB. Al tratarse de un dispositivo de sólo lectura, no existe el riesgo de borrado accidental por el usuario. Su ventaja es el precio y la facilidad de transporte. El inconveniente es no poder modificarlo, incluida la contraseña maestra, que en caso de necesitar cambiarse (por exposición, por ejemplo), implica la destrucción del dispositivo y la grabación de otro CD.

4.2. Arquitectura

El dispositivo USB se formatea con una tabla de particiones, de modo que la cuarta partición es de tipo 105. Consiste en un tipo propio que indica que se trata de una partición con un sistema de archivos con "formato clauer". En el caso del CD, contiene archivos de nombre CRYF_XXX.cla cada uno de ellos con el mismo formato clauer.

Este formato consiste en una colección de bloques de 10240 bytes. El primero de ellos es un bloque identificativo que desempeña también el papel de directorio (muy simplificado). Después hay una zona, cuyo tamaño se determina al formatear, reservada para uso propio de las aplicaciones. El resto es una colección de bloques, cada uno de ellos marcado con un tipo. Los bloques pueden estar en claro o cifrados. Los bloques cifrados lo están con una contraseña global.
Las aplicaciones no pueden/deben acceder directamente al dispositivo/archivo, sino que deben hacerlo a través de un sistema operativo que corre con privilegios de administrador. El s.o. maneja el sistema de archivos y provee de funciones de entrada/salida. Las aplicaciones inician sesión contra el s.o. para realizar tres tipos de operaciones básicas:

- Lectura de bloques en claro.
- Lectura de bloques cifrados: el inicio de sesión requiere la contraseña global.
- Escritura: requiere la contraseña global.

El s.o. se encarga del cifrado/descifrado con la contraseña global de los bloques que lo requieran, de modo que las aplicaciones pueden manejar bloques cifrados sin hacer uso explícito de criptografía. Obviamente la información que se escribe puede ir a su vez cifrada por la aplicación, permitiendo el uso de doble contraseña.

El s.o. se accede a través del puerto tcp 3c9 sobre la ip 127.0.0.1 .
La librería de acceso librt. provee funciones para C / C++ que facilitan el acceso al s.o.. Las aplicaciones, módulos criptográficos, controles web, etc., la emplean para las operaciones de entrada/salida sobre el dispositivo.

4.3. La creación de firma electrónica

La firma electrónica se crea mediante los datos (claves criptográficas privadas) que el dispositivo incorpora.

Los certificados y sus llaves se almacenan en el sistema de archivos con su correspondiente tipo y buscando la máxima compatibilidad. La forma habitual de protección de la llave privada es mediante la contraseña global del dispositivo, aunque existen diversas combinaciones.

El empleo de llaves y certificados se realiza a través del CryptoAPI de Windows o de PKCS#11 de modo que es totalmente transparente para el usuario. En el caso del CryptoAPI, el manejo de llaves y certificados queda totalmente integrado en el sistema, gracias a la instalación de un Cryptographic Service Provider (CSP) y de un Certificate Store Provider, que permiten hacer uso de la firma electrónica con el certificado que transporta el dispositivo desde todas las aplicaciones que emplean CryptoAPI.

4.4. La cartera de credenciales

Además, al dispositivo extraíble se le dota de una colección de credenciales para acceso condicional. Cada credencial se define mediante un nombre, una condición (expresión regular) y un valor, preferentemente 100% aleatorio.

La cartera puede guardarse en claro o cifrada con la contraseña maestra del dispositivo. Cada valor de credencial puede a su vez ir cifrado, lo cual si es aleatorio, es sólo una interpretación, que permite cambiar la contraseña incluso en dispositivos de sólo lectura, cambiando, en lugar del valor, el resultado del cifrado en los servidores donde se autentique. El control ActiveX permite acceder sólo a las credenciales cuyo nombre se conozca previamente (no permite listar la cartera) y contrastará la condición de la credencial contra la URL de la página que usa el control. De este modo, incluso en autenticación ante una página web con credencial sin contraseña, el token está protegido contra servidores hostiles.

4.5. El software desarrollado

En la implementación efectuada por la Universitat Jaume I se ha desarrollado software para Windows y Linux.

La mayor parte del software se ha desarrollado para Windows dado su mayor impacto en el colectivo de usuarios. Concretamente para este sistema operativo se ha desarrollado el siguiente software:

Software base

Contiene el sistema operativo que se ejecuta como un servicio de Windows, el Cryptographic Service Provider (CSP) firmado por Microsoft, el Certificate Store Provider y el control ActiveX criptoClauer. Debe instalarse siempre que se desee operar con el dispositivo.

Gestor para dispositivos USB.

Permite formatear un disco duro USB, creando una partición de datos (nº 1) y una partición con formato clauer (nº 4). También permite eliminar la partición nº 4.
A través de este gestor pueden transferirse certificados y sus llaves correspondientes al dispositivo, a partir de ficheros con formato PKCS#12 (ficheros con extensión .p12 o .pfx).
También es el encargado de manejar la contraseña global del dispositivo.

Gestor para CD.

Realiza funciones similares con los archivos que serán grabados en el CD. Permite guardarlos o grabarlos en un CD.

Clablock.

Sistema de control de acceso al ordenador basado en el clauer. Funciona a nivel de usuario, por lo que las modificaciones sobre el sistema son mínimas. La autenticación se realiza contra webservices.

Para Linux actualmente está disponible el sistema operativo y un formateador. Está en desarrollo un PKCS#11 para firefox y posiblemente para otros navegadores, con fecha prevista de terminación de Junio de 2006.

4.6. Distribución gratuita y liberación del código

El software diseñado se distribuye gratuitamente dentro y fuera de la comunidad universitaria, estando prevista también la liberación del código después de un periodo de carencia, dentro de la apuesta por el software libre que efectúa la Universitat Jaume I.

Los programas también se licencian gratuitamente para su distribución (siempre que sea gratuita) por parte de entidades y empresas mediante la suscripción del oportuno convenio.

4.7. El equipo de desarrollo

El desarrollo del software con el que la Universitat Jaume I ha implementado la solución propuesta se ha efectuado por varios programadores dirigidos por el autor principal de la presente comunicación quien también ha definido los protocolos de autenticación basados en la cartera de credenciales y la arquitectura del desarrollo.

Concretamente, el equipo ha sido el siguiente:

- Mauro Esteve (Ene 2005 -): Gestor del USB, gestor del CD, ClaBlock.
- Rafa Forcada (Dic 2003 – Sep 2005) Sist Operativo y formateador USB v1 para Windows.
- Paul Santapau (Oct 2005 -) S.O. Linux, formateador USB Windows y Linux, PKCS11 para Linux.
- Juan Segarra (Dic 2003 -) S.O. CD, LibRT, CSP y Store para Windows.