



Cam*erfirma*

Certificado Digital

DFIRMA WEBSECURE

TABLA DE CONTENIDO

1.	<i>Dfirma WebSecure</i>	3
2.	<i>Ventajas</i>	3
3.	<i>Características</i>	4
3.1.	Applet de acceso	4
3.2.	Página de verificación	4

1. Dfirma WebSecure

Dfirma WebSecure es un paquete que permite la autenticación mediante certificados digitales en cualquier web que disponga de tecnología de servidor (PHP, JSP, ASP, .NET).

El sistema se basa en los siguientes componentes:

- Una página Web donde se incluye el **applet de acceso**, que será el encargado de realizar todas las operaciones para la firma electrónica del ticket de acceso.
- Una página Web de **verificación** del ticket firmado recibido. Durante la verificación se comprobará la validez del certificado y la integridad de los datos firmados.
- Objeto de usuario que contendrá todos los datos del certificado y los incluidos en el ticket firmado que podrá ser utilizado en el resto de la Web.

2. Ventajas

Las ventajas de un sistema de acceso con certificado digital como el propuesto son innumerables, dotando de una total seguridad de acceso a cualquier Intranet/Extranet:

- Máxima seguridad de acceso a la Web.
- Mejor control de las sesiones del usuario pues se solicita de nuevo el certificado digital si el usuario cierra sesión o ésta caduca automáticamente tras cierto tiempo, aunque se queden abiertos los navegadores.
- No es necesario modificar, ni configurar las propiedades del servidor Web
- El control de las sesiones con certificados por el servidor Web directamente es muy deficiente en comparación con el sistema Dfirma, evitando cualquier agujero de seguridad.
- Instalación y **puesta en marcha muy sencilla**.
- Se integra totalmente **en la página Web** de la empresa.
- Funciona en cualquier sistema operativo y navegador Web con soporte para **Java** y javascript.
- Permite utilizar certificados instalados en el almacén de **certificados de Windows**.
- Es posible utilizar cualquier certificado emitido por una Autoridad de Certificación reconocida (Camerfirma, PKI de la GVA,...).
- Será posible integrar la autenticación con el DNI Electrónico.
- Utilización de certificados digitales tanto hardware PKCS#11 (USB criptográficos, tarjetas smartcard,...) como software PKCS#12, instalados en el PC del usuario.

3. Características

3.1. Applet de acceso

Para una total seguridad del sistema, el applet de acceso debe colocarse en una página bajo SSL.

El sistema dispondrá de un applet y un código javascript que podrá ser incluido en la página web del cliente.



Este applet, consistirá en un botón de acceso, que al pulsarse demandará al usuario el certificado con el que desee acceder al sistema. Para ello se mostrará una ventana con todos los certificados válidos que el usuario tiene instalados en dicha máquina y que hayan sido emitidos por una entidad en la que el sistema confía.

Una vez el usuario haya seleccionado el certificado deseado, se le pedirá la contraseña del mismo, en el caso de que haya instalado el certificado, con el nivel de seguridad alto si es un certificado de software o siempre que sea un certificado hardware, y se procederá a la firma del ticket de acceso.

El ticket de acceso a firmar contendrá la siguiente información:

- Session_id: Parámetro que identificará unívocamente la sesión del usuario que está accediendo.
- IP: Dirección IP del usuario que está accediendo al servidor.
- HOSTNAME: dirección Web desde donde está accediendo al servidor.

Adicionalmente se podrán incluir otros campos a medida del cliente, como por ejemplo claves.

Una vez el applet haya conformado el ticket, procederá a la firma electrónica con el certificado suministrado. Esta firma se realiza en el PC del usuario. Una vez firmado el ticket es enviado a la página de verificación de Dfirma, desarrollada en la tecnología correspondiente.

3.2. Página de verificación

La página de verificación estará desarrollada en la tecnología disponible en el servidor Web, ya sea PHP, JSP, ASP o .NET (DfirmaVerify.php, DfirmaVerify.jsp, DfirmaVerify.asp o DfirmaVerify.aspx).

Si todas las verificaciones son correctas, se encapsulará toda la información del certificado (clave pública, número de serie, CN, emisor, CIF,...) y del ticket en un Vector, que será introducido en la sesión del usuario. Una vez finalizado el proceso se accederá a la página indicada por la empresa, que realizará el resto de comprobaciones requeridas para el acceso, como por ejemplo la consulta en la base de datos si existe el usuario, perfiles, grupos a los que pertenece,...

El vector podrá ser utilizado durante la sesión en cualquier página de la Web de la empresa. Una vez se invalide la sesión el vector será borrado automáticamente y no se podrá acceder a la plataforma, a no ser que se firme de nuevo el ticket.

De esta forma se evitan las deficiencias existentes que presentan los servidores Web ante el manejo de los certificados digitales para el acceso a las plataformas, que no vuelven a demandar al usuario el certificado para la autenticación si se dejan abiertos los navegadores, aún habiendo cerrado la sesión.