JUNTA DE ANDALUCIA

Consejería de Hacienda y Administración Pública

Plataforma @firma

Buenas prácticas de seguridad en los procesos de autenticación y firma

Versión: v01r06

Fecha: 25/09/2012

HOJA DE CONTROL

Título	Buenas prácticas de seguridad en los procesos de autenticación y firma		
Entregable	Documentación afirma v5		
Nombre del Fichero	20120925 Buenas prácticas de seguridad-v01r06		
Autor	DGPD		
Versión/Edición	v01r05	**Fecha Versión**	14/06/2012
		Nº Total Páginas	19

REGISTRO DE CAMBIOS

Versión	Causa	Responsable	Área	Fecha
v01r00	Primera versión del documento	DGPD	SCAE	15/05/2012
v01r01	Revisión del documento	DGPD	SCAE	31/05/2012
v01r02	Revisión del documento	DGPD	SCAE	04/06/2012
v01r03	Revisión del documento	DGPD	SCAE	04/06/2012
v01r04	Revisión del documento	DGPD	SCAE	13/06/2012
v01r05	Revisión del documento	DGPD	SCAE	14/06/2012
v01r06	Revisión del documento	DGPD	SCAE	25/09/12

CONTROL DE DISTRIBUCIÓN

Nombre y Apellidos	Cargo	Área
Manuel Perera Domínguez	Jefe de Servicio de Coordinación de Administración Electrónica	DGPD / SCAE
José Ignacio Cortés Santos	Gabinete de Administración Electrónica	DGPD / SCAE
Francisco Mesa Villalba	Gabinete de Administración Electrónica	DGPD / SCAE

ÍNDICE

1 Objeto y contenido....4
1.1 Organización del documento....5
2 Descripción General....6
2.1 Sobre la plataforma @firma....6
2.2 Métodos de autenticación....6
3 Riesgos y vulnerabilidades....7
3.1 Riesgos generales....7
3.2 Riesgos de la autenticación....8
3.2.1 Autenticación anónima....9
3.2.2 Suplantación de identidad....9
3.2.3 Secuestro de sesión....10
3.3 Riesgos específicos del uso de la fachada de tickets....11
3.4 Riesgos específicos del uso del cliente de firma (firma mediante servicios web)....12
3.5 Riesgos específicos en el proceso de firma....14
4 Buenas prácticas....15
4.1 Desconfiar de todos los valores externos....15
4.2 Desconfiar del flujo de proceso....15
4.3 Utilizar identificadores de sesión seguros, únicos y específicos....15
4.4 Generar un identificador de sesión nuevo en cada autenticación....15
4.5 Comprobar que los parámetros asociados son correctos....16
4.6 No aceptar múltiples autenticaciones con los mismos parámetros....16
4.7 No aceptar certificados de prueba....16
4.8 Desconfiar de que el proceso de firma electrónica se ha realizado correctamente en el entorno del cliente....16
5 Lista de comprobación....18

1 Objeto y contenido

Este documento define una serie de buenas prácticas de seguridad en la implementación de los procesos de autenticación y firma electrónica con certificado electrónico utilizando los mecanismos que proporciona la plataforma @firma de la Junta de Andalucía.

En primer lugar se describen brevemente las características técnicas de estos componentes. Posteriormente se comentan los principales riesgos de seguridad inherentes a este tipo de proceso. Finalmente se exponen una serie de recomendaciones y buenas prácticas para conseguir una implementación más segura.

Este documento no es un manual de integración con la plataforma @firma. El objetivo de este documento es comentar específicamente los problemas de seguridad que pueden derivarse de una integración incorrecta de dichos componentes en las aplicaciones y servicios.

El contenido de este documento es principalmente técnico y está dirigido al personal encargado del desarrollo de aplicaciones y servicios que utilicen los componentes de @firma. Por tanto, se asume el conocimiento por parte del lector del funcionamiento básico de dichos componentes.

1.1 Organización del documento

El contenido y organización del documento es el siguiente:

1. Descripción general sobre la plataforma @firma y, concretamente sobre los mecanismos que proporciona de autenticación.

2. Riesgos y vulnerabilidades, tanto generales como específicos de cada método de autenticación, así como las vulnerabiliades de firma de usuario.

3. Buenas prácticas, tanto de carácter general como de carácter específico de uso de los mecanismos de autenticación y firma electrónica.

4. Lista de comprobación, como referencia para comprobar la correcta implementación de la autenticación y firma con @firma.

2 Descripción General

2.1 Sobre la plataforma @firma

La información actualizada sobre la plataforma @firma de la Junta de Andalucía está disponible en la siguiente dirección: *http://www.juntadeandalucia.es/haciendayadministracionpublica/ae*

2.2 Métodos de autenticación

La Plataforma @firma de la Junta de Andalucía ofrece a las aplicaciones dos métodos de autenticación mediante certificado electrónico:

- Método nativo basado en servicios web.
- Fachada de autenticación de tickets.

El método nativo de autenticación basado en servicios web utiliza el cliente de firma electrónica como componente de autenticación mediante la obtención del certificado electrónico contenido en una firma electrónica previamente validada.

La fachada de autenticación de tickets es un componente software de la plataforma @firma de la Junta de Andalucía que no requiere la utilización del cliente de firma electrónica y basa el proceso de autenticación en el establecimiento de una conexión SSL bidireccional con el navegador del usuario.

El mecanismo de autenticación propio de la versión 4 de la plataforma, basado en la redirección HTTP y datos de respuesta cifrados con 3DES, se considera obsoleto y se debe evitar su uso.

3 Riesgos y vulnerabilidades

Como en cualquier aplicación expuesta a posibles atacantes, en las aplicaciones que usan los componentes de autenticación de @firma existen una serie de riesgos de seguridad que conviene conocer y gestionar.

No debe suponerse en absoluto que la mera utilización de certificados electrónicos hace segura, sin más, a una aplicación informática o servicio de administración electrónica, algo especialmente cierto en el caso de entornos web y disponibles en Internet, en los cuales resultan de especial consideración los riesgos asociados a las interacciones telemáticas e intercambios de información realizados en el entorno.

Aunque la plataforma @firma ofrece mecanismos de seguridad para limitar estos riesgos, en la aplicación cliente es posible cometer errores susceptibles de ser aprovechados y causar problemas de seguridad. Al margen de la propia seguridad de la plataforma es fundamental realizar una implementación segura en todas las partes y funcionalidades de la propia aplicación o servicio.

En los siguientes apartados se relacionan los principales riesgos que se deben conocer.

- **Riesgos generales**: aquellos relacionados con cualquier tipo de aplicación web.
- **Riesgos de la autenticación**: aquellos específicamente relacionados con los mecanismos de autenticación.
- **Riesgos específicos**: los riesgos concretos de la autenticación de tickets y de la firma mediante el cliente de firma.

3.1 Riesgos generales

Los principales riesgos de seguridad en aplicaciones web suelen estar relacionados con la manipulación y uso de los valores de los parámetros externos.

Hay que considerar como valor externo a cualquiera que sea obtenido fuera del ámbito local de la aplicación, por ejemplo:

- Parámetros de las peticiones GET.
- Campos en las peticiones POST.

- Cabeceras de las peticiones. Por ejemplo: “Referer”, “User-Agent”, etc.
- Dirección IP del cliente.

La mayoría de los ataques se basan en la manipulación o falsificación de estos parámetros, por lo que se debe prestar especial atención a cómo se usan.

Como se comentará en el apartado de buenas prácticas se debe aplicar siempre el principio de desconfiar de cualquier valor externo. Es fundamental validar y procesar de forma segura todos los valores que se obtengan externamente.

Otros riesgos a tener en cuenta son los relacionados con el flujo de ejecución de la aplicación. En este caso, un atacante intentará hacer un uso no “habitual” de la aplicación, saltándose pasos de comprobación, realizando peticiones a componentes “desactivados” y en general intentando “confundir” a la aplicación para evitar las comprobaciones.

Como en el caso de los valores externos, tampoco se debe confiar en que el usuario siga un flujo de ejecución normal. Si la aplicación no responde correctamente a este comportamiento es posible que un atacante evite mecanismos de comprobación y llegue a partes de la aplicación a las que no debería llegar.

Como referencia sobre los principales tipos de ataque a aplicaciones web se recomienda consultar los siguientes documentos:

- OWASP Top Ten:
  https://www.owasp.org/index.php/Category:OWASP_Top_Ten_Project

- OWASP Testing Project:
  https://www.owasp.org/index.php/Category:OWASP_Testing_Project

3.2 Riesgos de la autenticación

Los principales riesgos de cualquier componente de autenticación son los siguientes:

- Autenticación anónima.
- Suplantación de identidad.

- Secuestro de sesión.

A continuación se describen cada uno de ellos. Hay que tener en cuenta que los posibles tipos de ataques comentados a continuación no tienen por qué ser siempre factibles, ni tampoco que la plataforma @firma sea especialmente vulnerable a ellos. El principal objetivo es conocer estos riesgos porque una implementación defectuosa sí que puede facilitar ataques reales.

En el apartado de buenas prácticas se ofrecen recomendaciones para eliminar o limitar estos riesgos.

3.2.1 Autenticación anónima

La autenticación anónima consiste en que un atacante consigue autenticarse usando unas credenciales que no permiten la identificación real del usuario.

Por ejemplo, si hablamos de autenticación mediante usuario y contraseña, una autenticación anónima sería si el atacante pudiese usar unas credenciales de prueba como usuario "test" y contraseña "1234". Este tipo de credenciales son habituales en entornos de desarrollo y no es raro que lleguen hasta los entornos de producción.

En el caso de la autenticación con certificado electrónico, la autenticación anónima se puede hacer utilizando cualquiera de los certificados de prueba que suelen proporcionar las entidades de certificación. Estos certificados son relativamente sencillos de conseguir y permiten a un atacante autenticarse en la aplicación sin revelar su identidad real.

3.2.2 Suplantación de identidad

En la suplantación de identidad un atacante consigue autenticar con las credenciales de un usuario real y existente.

Para el caso de los certificados digitales y en su forma más simple, el atacante necesitaría el certificado de la víctima. Si esto ocurre, y el certificado sigue siendo válido, no hay nada que la aplicación o la plataforma @firma puedan hacer. En este caso es responsabilidad del usuario la custodia de sus certificados.

Otros posibles ataques de suplantación de identidad se pueden producir si la aplicación utiliza parámetros adicionales para la identificación del usuario. Por ejemplo, una posible mala implementación sería la siguiente:

- Una aplicación utiliza los componentes de autenticación correctamente y el usuario es identificado por su certificado.
- Posteriormente, el componente de autenticación de la aplicación redirige el navegador del usuario a la página privada utilizando un parámetro que incluye el NIF.
- Esta página privada utiliza el parámetro que contiene el NIF para mostrar los datos asociados.

Esta implementación defectuosa permitiría a un atacante cambiar el valor del parámetro que contiene el NIF para suplantar la identidad de otro usuario. Si además, el atacante utiliza un certificado de prueba, puede hacer esto de forma completamente anónima.

3.2.3 Secuestro de sesión

Prácticamente todas las aplicaciones web gestionan las sesiones de usuario mediante un identificador de sesión que normalmente se transmite en una "cookie".

Desde el punto de vista de la autenticación, este identificador de sesión es tan importante como el propio certificado electrónico. Si un atacante consigue el identificador de sesión de otro usuario podrá identificarse ante la aplicación como este último, accediendo a la misma sesión.

Es conveniente recordar que el certificado electrónico solo asegura la identidad del usuario pero no ofrece protección adicional durante la vida de la propia sesión autenticada. Es muy importante asegurar todos los eslabones de este control de sesiones.

3.3 Riesgos específicos del uso de la fachada de tickets

La autenticación mediante tickets de @firma presenta sus propios riesgos a tener en cuenta.

El proceso más sensible desde el punto de vista de la seguridad es la redirección del navegador del usuario a la fachada de autenticación. Para implementar este paso se utilizan una serie de parámetros que incorporan los datos del ticket, el identificador de sesión, el identificador de aplicación, el código de error y la URL de retorno.

Estos parámetros se usan en peticiones GET durante la redirección del navegador, por lo que deben considerarse parámetros externos a la aplicación y por lo tanto inseguros.

Si la aplicación no procesa correctamente estos parámetros un atacante podría alterarlos y conseguir evadir los controles de seguridad.

El mecanismo de autenticación de tickets también depende de que se realicen una serie de pasos o procesos en un orden determinado. Las aplicaciones no deberían confiar en que estos pasos se ejecutan de forma ordenada ya que un atacante podría intentar manipular este flujo para evadir controles.

Por lo tanto, en la implementación hay que tener en cuenta los riesgos derivados de:

- La manipulación de los parámetros usados en la redirección del navegador.
- La alteración en el orden de ejecución del flujo de proceso.

De forma concreta, algunos posibles errores de implementación son los siguientes:

- Aceptar más de una vez la URL de retorno de autenticación.
- No comprobar que los parámetros “ticketId” y “webSessionId” se corresponden con la sesión de usuario.
- No comprobar correctamente el valor del parámetro “resCode”.
- Utilizar valores de “webSessionId” débiles y/o fácilmente predecibles.

3.4 Riesgos específicos del uso del cliente de firma (firma mediante servicios web)

Las aplicaciones que se integran con @firma pueden realizar la autenticación de certificados electrónicos de usuarios mediante el uso del "cliente de firma". El proceso a seguir es el siguiente:

1. La aplicación envía al navegador del usuario un documento HTML que contiene:
   a) Código javascript necesario para la carga del cliente de firma.
   b) Código javascript que invocará los servicios ofrecidos del cliente de firma para la realización de una firma electrónica de una cadena de texto HASH aleatorio, generada desde la propia aplicación.
   c) Un formulario HTML que será enviado al servidor de aplicaciones una vez realizada la firma electrónica, conteniendo entre sus parámetros el resultado de la firma y la codificación en BASE64 del certificado empleado en el proceso.
2. Cuando la aplicación es invocada una vez realizada la firma, deberá invocar los servicios web de @firma que permitan asegurar:
   a) La vigencia del certificado electrónico empleado en el proceso.
   b) Los datos firmados coinciden con la cadena de texto HASH aleatorio remitida originalmente desde la aplicación.

Una incorrecta implementación del proceso anteriormente descrito puede hacer vulnerables a las aplicaciones afectadas. En concreto, los problemas más habituales son:

1. No se verifica la firma electrónica realizada: las aplicaciones "confían" en la firma electrónica realizada por el cliente de firma. La ausencia de la comprobación de la transacción de firma puede hacer que la aplicación sea atacada si se le remite un certificado electrónico de usuario, sin necesidad de contar con su clave privada. Los certificados electrónicos (sin clave privada) son fácilmente accesibles y es precisamente la clave privada la que garantiza la integridad del proceso. Por tanto es un error confiar en que el proceso de firma se ha realizado sin comprobar que efectivamente así ha sido.
2. Se establece un texto fijo o incluso vacío para realizar la firma con el cliente. Dado un certificado electrónico y una cadena de texto, el resultado de la firma será siempre el mismo.

Por tanto, si esta cadena de texto es "fija" se podría desarrollar una aplicación "maliciosa" que haga a los usuarios firmar los mismos datos que se firman en la aplicación a atacar. En estas circunstancias, una vez conocido el resultado de la firma éste sería enviado a la aplicación a atacar y se tendría acceso incluso si ésta realizara el proceso de verificación de firma.

3.5 Riesgos específicos en el proceso de firma

Las aplicaciones que remitan contenido al usuario para que éste lo firme haciendo uso del "cliente de firma" deben verificar la integridad de la firma realizada y también que los datos firmados son coincidentes con los remitidos originalmente para su firma.

De no realizarse esta verificación, un usuario malicioso podría reemplazar los datos a firmar por otros distintos, firmarlos, y remitir el resultado de la firma de los datos alterados. La aplicación que no realizara la comprobación, aceptaría la firma en una situación en la cual no podría garantizarse el no repudio por parte del usuario final ya que lo firmado no coincide con lo establecido por la aplicación.

4 Buenas prácticas

Para limitar al máximo los riesgos comentados anteriormente se recomienda una serie de buenas prácticas. Ninguna de ellas, por sí sola, ofrece una garantía plena de seguridad, pero es importante implementar todas las "capas de defensa" posibles para limitar y dificultar los posibles ataques.

4.1 Desconfiar de todos los valores externos

Como norma general se debe desconfiar de todos los valores externos, incluso aquellos proporcionados por la propia plataforma. Se deben implementar comprobaciones sobre la integridad, tipo de datos, formato y validez de cada parámetro antes de usarlo.

4.2 Desconfiar del flujo de proceso

Implementar controles para detectar posibles usos incorrectos del flujo de proceso. Específicamente se debe controlar que todos los pasos previos se han completado de forma correcta.

4.3 Utilizar identificadores de sesión seguros, únicos y específicos

Para el parámetro "webSessionId" se debe utilizar un valor seguro, aleatorio y único a cada usuario y petición de autenticación. Las aplicaciones normalmente utilizan el propio identificador de sesión como valor de este parámetro. Aunque esto no es un problema de por sí, se debe utilizar un valor distinto, generado con un algoritmo aleatorio seguro. De esta forma se establece una capa de seguridad adicional frente a posibles filtraciones de este parámetro.

4.4 Generar un identificador de sesión nuevo en cada autenticación

Es recomendable generar un identificador de sesión nuevo después de la autenticación que no tenga relación con el identificador de sesión generado al conectar con la aplicación. De esta forma se utiliza una sesión específica para la parte autenticada de la aplicación y se evitan algunos tipos de ataque de secuestro de sesión que utilizan vulnerabilidades existentes en la parte no autenticada.

4.5 Comprobar que los parámetros asociados son correctos

Se deben comprobar que todos los parámetros recibidos en el componente de retorno son correctos. Específicamente, que:

- El parámetro "resCode" no indica ningún error.
- El parámetro "webSessionId" corresponde al valor esperado.
- El parámetro "ticketId" corresponde al valor esperado.

4.6 No aceptar múltiples autenticaciones con los mismos parámetros

Después de aceptar una autenticación en el componente de retorno, los valores de los parámetros "webSessionId" y "ticketId" deben ser invalidados para que no se puedan volver a utilizar.

No se debe aceptar más de una vez la misma URL de retorno de autenticación para evitar ataques de secuestro de sesión.

4.7 No aceptar certificados de prueba

No se deben aceptar certificados de prueba porque esto facilita los ataques de forma anónima.

No existe una lista completa de los certificados de prueba emitidos por las distintas entidades de certificación, pero normalmente estos certificados utilizan valores de NIF conocidos, como 12345678Z y 00000000T. Aunque no resulta sencillo reconocer todos los certificados de prueba, filtrando por estos NIF habituales se consigue algo más de protección.

4.8 Desconfiar de que el proceso de firma electrónica se ha realizado correctamente en el entorno del cliente

No se debe confiar de las firmas realizadas en el entorno local del cliente. Todo proceso de firma realizado en el cliente debe ser verificado en el servidor.

Una vez realizada la firma electrónica, la aplicación deberá invocar los servicios web necesarios para comprobar la firma realizada, validando la autenticidad del certificado del firmante y su validez.

Adicionalmente, es indispensable comprobar que los datos firmados son coincidentes con los datos remitidos inicialmente por el servidor al usuario.

En el caso de realizar autenticación de usuarios mediante firma electrónica, la cadena a generar por la aplicación debe ser aleatoria y de una longitud elevada. No debe utilizarse una cadena vacía o de contenido estático.

5 Lista de comprobación

En este apartado se incluye una lista de comprobación para su consideración y referencia en la implantación de funcionalidades y servicios de administración electrónica basados en la plataforma @firma de la Junta de Andalucía.

#	Ámbito	Comprobación
1	Autenticación WS Autenticación tickets Firma electrónica	En cada parte del proceso de la aplicación comprobar el tipo, integridad y validez de los parámetros proporcionados.
2	Autenticación WS Autenticación tickets Firma electrónica	En cada parte del proceso, comprobar que los pasos anteriores han sido ejecutados correctamente.
3	Autenticación tickets	El identificador de sesión (webSessionId) es único y aleatorio para cada usuario y petición de autenticación.
4	Autenticación WS Autenticación tickets	El identificador de sesión debe ser diferente del identificador de sesión generado al conectar con la aplicación.
5	Autenticación tickets	Comprobar el valor del parámetro resCode, asegurandose que no contenga errores.
6	Autenticación tickets	Comprobar que el valor del parámetro webSessionId es el esperado.
7	Autenticación tickets	Comprobar que el valor del parámetro ticketid es el esperado.
8	Autenticación tickets	Una vez validado al usuario, evitar posteriores validaciones con el mismo valor del parámetro webSessionId.
9	Autenticación tickets	Una vez validado al usuario no aceptar la misma URL de retorno.
10	Autenticación WS Autenticación tickets	No aceptar certificados de prueba en aplicaciones de producción.

#	Ámbito	Comprobación
	Firma electrónica	
11	Autenticación WS	Asegurar que los datos que se envían para la firma son aleatorios.
12	Autenticación WS Firma electrónica	Los procesos de firma electrónica realizados en el equipo cliente del usuario de la aplicación, con el cliente de firma, deben ser validados en el servidor una vez que recibe el resultado de la firma, para verificar la validez del certificado electrónico empleado y que los datos firmados son coincidentes con los remitidos por la aplicación.
13	Autenticación WS Autenticación tickets Firma electrónica	Comprobar que el certificado utilizado no está caducado ni revocado.