## Hacia la interoperabilidad de la autenticación de la identidad

# Un problema de confianza

**Recuerdo con ternura cuándo conseguí mi primer certificado digital software, que sólo me servía para hacer la declaración de la renta. No le encontré otro uso y me costó más esfuerzo conseguirlo de lo que posteriormente me ahorró; pero no me importó, porque significaba pasar al selecto club de usuarios de certificado digital. Durante muchos años fue mi único certificado y sólo me servía para autenticarme ante la Agencia Tributaria.**

**ROBERTO GIL NAVALÓN**
Jefe de Unidad en el Área de Seguridad de la Información de la Subdirección General de Tecnologías de la Información y Comunicaciones del Ministerio de Defensa.

En la actualidad, probablemente todo aquel que lea este artículo disponga de varios certificados, algunos en *smart card*, y casi todos para un solo uso. Y aunque tengamos muchos, debemos sentirnos afortunados, porque cada certificado nos ahorra varios procesos de alta y muchas contraseñas, con sus consecuentes cambios periódicos.

Parecía que el DNI nos iba a ahorrar tener varios certificados y, al menos para nuestras gestiones en la Administración Electrónica, así ha sido. Sin embargo, el hecho de que el uso del DNI en la vida profesional sea voluntario, entre otras cosas, nos lleva a que no exista un modelo de certificado tipo. Cada sistema en que necesitemos autenticarnos, tiende a proporcionarnos uno distinto. Esta situación nos lleva a acumular muchos certificados que podríamos considerar, cuanto menos, prescindibles.

La única solución para que no necesitemos un certificado distinto para interactuar con cada servicio es asegurar una verdadera confianza común. ¿Son todos los certificados igualmente confiables? La respuesta es claramente negativa.

Dejando aparte la Administración Electrónica, que tiene sus propios retos y soluciones, la necesidad de que nuestros aliados en organizaciones internacionales o nuestros socios empresariales entren en nuestros sistemas críticos nos lleva a tener que admitir certificados mutuamente reconocidos. No tiene sentido que cada proveedor de servicios genere un certificado distinto (no digamos ya, usuarios y contraseñas), sino a replantearnos el problema de la confianza electrónica de prestadores externos.

### Confianza en la autenticación electrónica.

Que todos los certificados digitales no son exactamente


iguales se intuye cuando vemos la diferencia de precios entre los prestadores. Tampoco el hecho de que los certificados sean más caros significa necesariamente que deban ser mejores.

Del mismo modo, la diferencia entre los certificados la percibimos como clientes cuando leemos correo electrónico seguro o nos descargamos un control de ActiveX firmado. También al entrar en un portal si se nos advierte de que el certificado del sitio no es de confianza. Nuestra navegación nos depara estos avisos porque cada desarrollador incorpora una lista de certificados raíz de confianza precargados. Para establecer esa lista, por ejemplo Microsoft, ha generado una selección mediante su Programa de certificados raíz de Windows **(1)** . Nosotros, al utilizar su producto, salvo que realicemos modificaciones, confiamos también en la selección que ha realizado. Delegamos nuestro criterio de confianza.

No existe un baremo que pudiésemos considerar estándar para establecer nuestra confianza en los certificados digitales. Ésta se basa en un mercado abierto, donde los prestadores exponen sus *Declaraciones de Prácticas de Certificación* y donde los clientes juzgan por ellos mismos o confían en terceros. Y esto puede ser un problema para la Administración, porque debemos establecer qué criterios utilizaremos para confiar en un prestador y qué razones aduciremos para denegar la confianza a otros.

A esto debemos sumar que nuestro reto es la autenticación y que, si bien la normativa de firma electrónica se encuentra muy desarrollada, la de su hermana menor, la autenticación electrónica, no lo está en la misma medida. Prueba de esta descompensación es la extraña paradoja de disponer de una ley de firma y de un Catálogo de Prestadores de Certificación de Firma Electrónica en la Administración, cuando lo que realizamos casi en exclusiva, en nuestras acciones de Administración electrónica, es la autenticación. Esta situación cambiará cuando se apruebe el nuevo Reglamento Europeo, con él, la autenticación cobrará el papel que le corresponde.

### La confianza en el acceso a nuestros sistemas

Si necesitamos que nuestros socios entren en nuestros sistemas avalados por una Autoridad de Certificación (CA) externa, probablemente nos interese considerar el nivel de confianza que podemos depositar en la entidad que genera los certificados y en los soportes en que éstos se proporcionan.

La confianza en una CA debería establecerse en función de varias consideraciones. Entre ellas, principalmente en si implementa las medidas adecuadas cuando evalúa las solicitudes de certificado, si revoca los certificados no válidos y los publica adecuadamente o si mantiene un nivel de seguridad acorde con la misión que desempeña.

Quizás la última consideración ha sido habitualmente obviada. Probablemente, por la complejidad que conlleva su verificación, pero recientes incidentes, como el caso de DigiNotar **(2)** , han aumentado drásticamente su importancia.

Una vez decidido en qué Autoridades de Certificación estamos dispuestos a confiar, tenemos que considerar el soporte en el que el usuario recibe su certificado.

Si consideramos crítica la autenticación de acceso de entidades externas a nuestros sistemas, todos estaremos

de acuerdo en requerir autenticación fuerte. En lo que probablemente no coincidamos será en qué entenderemos por ello. Si observamos las distintas definiciones de autenticación fuerte observaremos que todas incluyen la mención al doble factor **(3)** y, algunas, a la necesidad de que intervenga algún mecanismo o dispositivo criptográfico.

No existe consenso en cuanto a si los certificados digitales en software pueden considerarse un mecanismo de autenticación fuerte. En este sentido, debe tenerse en cuenta la naturaleza replicable de éstos y que la confianza en ellos conlleva implícita la confianza también en la seguridad de los clientes en los que se instale y en la fortaleza de la contraseña para su uso.

La solución ideal al problema de la autenticación fuerte es la que implementa un dispositivo, normalmente una *smart card*, con chip criptográfico, a semejanza del DNI. En estas tarjetas la clave privada del certificado se aloja en el dispositivo y éste ha sido diseñado para impedir su extracción; en consecuencia, podemos estar seguros de que no existe ninguna otra copia de la clave privada. En la mayoría de tarjetas, incluso el par de claves público-privada, se genera en el chip de la propia tarjeta. A esta gran ventaja debemos sumar unas medidas de protección altas: bloqueo de la tarjeta tras varios errores consecutivos en la contraseña, medidas anti-manipulación, etc.

Si, tal como se ha sugerido, exigimos como instrumento de autenticación en nuestros sistemas, certificados proporcionados en una *smart card* **(4)** con chip criptográfico, el siguiente problema que debemos afrontar es encontrar el mecanismo para verificar en nuestro servidor que la solicitud de autenticación que recibimos procede de ese tipo de soporte. Y esta averiguación no es trivial.

A falta de atributos específicos en los certificados que indiquen si la clave privada reside dentro de una smart card , la única solución práctica es encontrar una relación entre ésta condición y el campo OID (Object IDentifier). El OID es una cadena numérica que identifica unívocamente el tipo de certificado emitido. Buscando el OID en la Declaración de Política de Certificación debería poder averiguarse si el certificado ha sido emitido en tarjeta criptográfica.

Lamentablemente, algunos prestadores no consideran relevante el distinguir con alguna característica, tal como el OID, si el certificado ha sido proporcionado en tarjeta *smart card* o en software. Esta información será cada vez más necesaria y esa decisión, a la larga, sin duda les penalizará. Este mercado se encuentra tan liberalizado que los servicios que requieran autenticación fuerte probablemente deban rechazar estos certificados.

Nuevo Reglamento de la Comisión No cabe duda de que necesitamos distintos mecanismos de autenticación para nuestras diferentes políticas de acceso y de que, cada vez más, vamos a tener que dar acceso colaborativo a nuestros socios en algunos sistemas que consideramos críticos.

Teniendo en cuenta la madurez del mercado de servicios de certificación, no tiene sentido que esa autenticación se realice con distintos certificados, proporcionados por quién provee el servicio. Tampoco es lógico admitir todo certificado que nos sea presentado.

Resulta también crítico establecer en nuestra política si requerimos condiciones al formato en el que se entrega el certificado al usuario. La situación ideal es que éste se entregue en una *smart card* con chip criptográfico, en cuyo caso debemos encontrar el método de verificar esta condición en el servidor. Es de esperar que esta información sea más accesible en el futuro.

En breve será de obligado cumplimiento el nuevo Reglamento sobre identificación electrónica y servicios de confianza, que nos deparará importantes avances en el reconocimiento mutuo de identidades electrónicas. ✱

**NOTAS**

**(1)** Para ser miembro del Programa de certificados raíz de Windows se exigen fuertes requisitos formales y de auditoría.*http://technet.microsoft.com/es-es/library/cc751157(en-us).aspx*

**(2)** En el verano de 2011, la prestadora de servicios de certificación Diginotar fue objeto de una intrusión en sus sistemas. Como consecuencia de ésta, se generaron certificados fraudulentos que fueron usados para ataques informáticos a terceros. La compañía Diginotar se declaró en bancarrota pocos meses después. *http://unaaldia.hispasec.com/2011/09/diginotar-la-tercera-revocacion-masiva.html*

**(3)** Descartando la biometría por el común rechazo del usuario, el doble factor requiere verificar algo que se sabe (contraseña) y algo que se posee (token). Tampoco hay acuerdo común en si el token debe ser físico (lo común) o si se admite en forma lógica.

**(4)** Existe un parámetro (QcSSCD, del perfil ETSI TS 101 862) que marca si la clave privada del certificado reside en un dispositivo seguro de creación de firma (DSCF). Sin embargo, ni todos los certificados de autenticación que residen un DSCF incluyen dicha extensión, ni todos las smart card que se encuentran certificadas como DSFC.