>> Jorge Dávila

La Criptografía en el Esquema Nacional de Seguridad

Después de la publicación hace un año del Esquema Nacional de Seguridad, ya disponemos de una serie de guías que nos dan detalles de cómo se deben poner en marcha los sistemas de la administración pública española. En esta sección nos sumergiremos en los temas, algoritmos y procedimientos que constituirán las bases de nuestro futuro sistema de e-Administración.

Desde que a finales del siglo XX el planeta se lanzó al uso masivo e indiscriminado de las tecnologías de la información y las comunicaciones (TIC), se ha creado un nuevo espacio o dimensión, el ciberespacio, donde la impronta de la humanidad no ha tardado en aparecer y se han desarrollado conflictos, y lo que muchos consideran agresiones y 'ciberamenazas'. Dado que la entrega al 'ciberespacio' ha sido tan completa, no es descabellado pensar que esos conflictos en la "cuarta dimensión" puedan llegar a atentar contra la seguridad nacional, como quizás lo hayan entendido los anteriores gobiernos de Egipto, Libia o Túnez. Lo que sí está claro es que esta nueva dimensión cada vez afecta más a los derechos civiles y la justicia, a la prosperidad económica de la sociedad, al estado del bienestar y al normal funcionamiento de la sociedad y de las administraciones públicas.

Por si esto fuera poco, Internet y las relaciones telemáticas pueden suponer una revolución en el tipo, cualidades y calidades del servicio que la Administración puede prestar a sus administrados. Desde hace años se viene utilizando el concepto de «ventanilla única» unido al de los servicios de e-Administración; pero no ha sido hasta la aparición de la ley[1] 11/2007, de 22 de junio, "*de acceso electrónico de los ciudadanos a los servicios públicos*" cuando realmente se ha puesto en marcha esa posibilidad. En el artículo 42.2 de esa ley se establece que debe haber un Esquema Nacional de Seguridad (ENS) y otro de Interoperabilidad (ENI), y no es hasta que aparece el Real Decreto[2] 3/2010 de 8 de enero cuando se desarrolla esa obligación.

La madurez de un profesional en la seguridad de las TIC se puede medir por su preocupación, sensibilidad y maestría en la generación y gestión de las claves. Aquellos que ahorren esfuerzos en este punto, le están poniendo pies de barro a sus productos y la seriedad/seguridad nacional no debería construirse sobre tan frágil basamento.

Guías

En el Esquema Nacional de Seguridad se fijan cuáles son los principios básicos, los requisitos mínimos y las medidas de protección que son necesarias dentro de los sistemas de la Administración pública española. Asímismo, encarga al Centro Criptológico Nacional la confección de una serie de guías[3] que faciliten su mejor cumplimiento.

En esos documentos se hacen una serie de recomendaciones sobre cuáles deben ser los algoritmos y parámetros criptológicos a utilizar, cuáles son los organismos de acreditación y certificación de la seguridad que se consideran competentes, y lo que es bastante importante, cuáles son los algoritmos criptográficos acreditados que se reconocen como válidos dentro del ENS. Además de esto, en esas guías se establecen cuáles deben ser los mecanismos de identificación y autenticación de usuarios, cómo debe protegerse la confidencialidad, la autenticidad y la integridad de los datos, cómo se deben cifrar y proteger las claves criptográficas usadas en ello, y para terminar, cómo se debe firmar electrónicamente y dotar de referencias temporales (sellos de tiempo) a esa firmas.

La "*Guía/Norma de Seguridad de las TIC (CCN-STIC-807): Criptología de Empleo en el Esquema Nacional de Seguridad*" no se queda solo en eso, sino que acompaña a todo lo anterior de un nutrido grupo de anexos de carácter netamente pedagógico. La serie comienza con la Criptografía de Clave Simétrica en sus versiones de flujo (Anexo A) o de bloques (Anexo B), para continuar con la de Clave Asimétrica basada en el problema de la factorización, es decir, el RSA (Anexo C), o en la basada en el problema del logaritmo discreto[4] (Anexo D), en concreto hablando del algoritmo de ElGamal[5] y de los que utilizan Curvas Elípticas. Terminado el cifrado, se pasa al problema de las funciones *hash* o funciones resumen, y a la muy importante autenticación de usuarios (Anexo E), para luego introducir el no-repudio a través de las firmas digitales (Anexo F). Como último apéndice y dando la sensación de que está un tanto descolgado de los anteriores, la guía termina hablando de la generación de números aleatorios y pseudoaleatorios que es, claramente, la asignatura pendiente de nuestra comunidad de Seguridad TIC.

Identificación, autenticación y niveles

A la hora de hablar de los mecanismos de identificación, se indica que a cada agente hay que entregarle

[1] Ver http://www.boe.es/boe/dias/2007/06/23/pdfs/A27150-27166.pdf
[2] Ver http://www.boe.es/boe/dias/2010/01/29/pdfs/BOE-A-2010-1330.pdf
[3] Véase la serie de documentos CCN-STIC elaborada por el Centro Criptológico Nacional como parte del ENS (www.ccn-cert.cni.es)
[4] Ver http://en.wikipedia.org/wiki/Discrete_logarithm
[5] Ver http://en.wikipedia.org/wiki/ElGamal_encryption

un identificador único que le represente en la dimensión cibernética y se dice que este número pueden ser varios: DNI, pasaporte, secuencia alfanumérica cualquiera, certificado digital, etc.; pero a la hora de hablar de estos últimos, descarta netamente el uso de la función *hash* MD5 [6], hecho que se conocía desde hace tiempo [7].

En cuanto a la autenticación, en los sistemas clasificados como de «nivel bajo», se sigue aceptando el uso de números secretos de identificación personal (PINs) de al menos 4 dígitos, lo cual es del todo inseguro. Para mitigarlo, la guía recomienda que se utilicen políticas de bloqueo de PIN o de retardo incremental, según el número de intentos fallidos. Estas técnicas evitarán muchos de los ataques por fuerza bruta o diccionario pero no servirán frente a la "ingeniería social", ya que esta suele tener éxito con un número muy reducido de intentos.

Lo bueno de este punto (apartado 1.4.2) es que se descarta el uso de contraseñas, PINs o cualquier otra «clave concertada» cuando se trabaja en instalaciones cuya seguridad es de nivel medio o alto. En este caso, la autenticación deberá basarse en dos "factores" auténticos distintos, como pueden ser la posesión de un determinado *token* y poder mostrar una determinada característica biométrica.

No se sabe si por desdecirse o por dejar la puerta abierta a multitud de sistemas que se autentican mediante usuario y contraseña, el caso es que en ese mismo apartado se termina aceptando el uso de claves alfanuméricas concertadas cuya longitud sea superior a cuatro caracteres, pero generadas al azar o mediante un procedimiento pseudoaleatorio de confianza.

En el caso de las instalaciones clasificadas de Nivel Alto, la autenticación podrá hacerse mediante dispositivos físicos personalizados (se entiende que habrán de ser difíciles de falsificar) o mediante biometría acompañada de la presentación de un segundo factor (*token*). Aquí también se resiste la guía en abandonar las claves concertadas y las permite siempre que su longitud no sea inferior a ocho caracteres y su generación sea aleatoria. Si esta tolerancia con las *passwords* se debe a no poder desterrar ese procedimiento, es poco realista pensar que el usuario común se va a aprender en secreto y sin escribir en un papel una clave que satisfaga estas restricciones [8].

En el caso de las instalaciones de Nivel Alto, también se aceptan como sistemas de autenticación el protocolo RADIUS [9], el establecimiento de canales TLS [10], la infraestructura de autenticación EAP [11] e incluso el WAP [12] de la Wi-Fi Alliance. En este punto no se dice nada sobre la protección que haya de hacerse del canal a través del cual se realizan los diferentes protocolos de autenticación. Aunque la guía no lo dice, la autenticación debe hacerse a través de canales protegidos de la observación de terceros como, por ejemplo, dentro de canales SSL/TLS.

para ello no tengan menos de 2.048 bits de longitud en el caso del RSA, o de 224 bits en el caso de que se esté utilizando criptografía asimétrica sobre curvas elípticas.

En el caso de las instalaciones de Nivel Alto, se recomienda utilizar dispositivos hardware para construir las VPNs. En este caso, el nivel de entropía asegurada que deben tener las claves simétricas es de 128 bits para los cifradores simétricos, de más de 2.048 bits para el RSA, o más de 256 bits cuando se utilizan curvas elípticas.

Entendiendo por autenticidad de una información el poder comprobar que su fuente es quien realmente la elaboró, y que la integridad de una información se refiere a la comprobación de que lo recibido no ha sido alterado en su tránsito hasta nosotros, la guía solicita que, incluso a Nivel Bajo, se pueda comprobar la autenticidad del otro extremo para evitar ataques activos de suplantación). En sistemas de Nivel Medio, la autenticidad e integridad será la que proporcione la VPN que se exige como protección de la confidencialidad, y lo mismo ocurre con las instalaciones de Nivel Alto.

Confidencialidad, integridad, autenticidad y sello de tiempo

La confidencialidad solo preocupa en instalaciones clasificadas de Nivel Medio o Alto. Para las primeras, se exige el uso de Redes Virtuales Privadas (VPNs), tanto IPsec como las que se establecen a nivel de aplicación mediante el uso de conexiones SSL/TLS. Dado que estas redes utilizan cifrado para proteger la confidencialidad, la guía especifica claramente que la resistencia mínima que debe asegurarse para instalaciones de Nivel Medio es de 112 bits de entropía real y certificada. Dado que en el establecimiento de esos canales confidenciales simétricos se suele utilizar criptografía asimétrica, la guía indica sabiamente que las claves que se vayan a utilizar

Entendiendo por autenticidad de una información el poder comprobar que su fuente es quien realmente la elaboró, y que la integridad de una información se refiere a la comprobación de que lo recibido no ha sido alterado en su tránsito hasta nosotros, la guía solicita que, incluso a Nivel Bajo, se pueda comprobar la autenticidad del otro extremo para evitar ataques activos de suplantación (ataques *Man-in-the-middle* [13]). En sistemas de Nivel Medio, la autenticidad e integridad será la que proporcione la VPN que se exige como protección de la confidencialidad, y lo mismo ocurre con las instalaciones de Nivel Alto.

En las instalaciones de Nivel Alto se requiere que la información esté permanentemente cifrada. En estos casos, el estado natural de la información es el criptograma, tan-

[6] Ver http://www.win.tue.nl/hashclash/rogue-ca/

[7] Stevens, M.; Lenstra, A.; de Weger, B.: "Target Collisions for MD5 and Colliding X.509 Certificates for Different Identities" en http://eprint.iacr.org/2006/360.pdf

[8] Algunos ejemplos de 8 caracteres podrían ser: LICn:-k6 -Y'/k"if db6Ue~KM /%4-;.9g Y&6L=JPT PV&gT&p8 La entropía esperada en estos casos sería de solo 52 bits.

[9] Ver http://en.wikipedia.org/wiki/RADIUS

[10] Ver http://en.wikipedia.org/wiki/Transport_Layer_Security

[11] Ver http://en.wikipedia.org/wiki/Extensible_Authentication_Protocol , RFC3748 y RFC 5247

[12] Ver http://en.wikipedia.org/wiki/Wi-Fi_Protected_Access

[13] Ver http://en.wikipedia.org/wiki/Man-in-the-middle_attack

to cuando se transporta de un lado a otro, como cuando se almacena, que no es más que un transporte de un lugar del tiempo a otro en el futuro. En este caso, las claves utilizadas para el cifrado no deben tener una resistencia inferior a los 128 bits de entropía real.

Independientemente de la seguridad que ofrezca, toda clave secreta debe estar protegida durante su ciclo de vida; es decir, desde su misma generación, como durante su transporte, en su custodia mientras se utilice, y en su almacenamiento posterior hasta su destrucción final.

En el caso del Nivel Medio, el proceso de generación de las claves debe hacerse completamente desconectado de cualquier red y las claves que se hayan retirado de uso deben almacenarse en dispositivos también aislados hasta su destrucción. En estos casos, el acceso a cualquier componente del sistema tendrá que tener una resistencia igual o superior a los 122 bits de entropía. En los sistemas de Nivel Alto, se mantiene la misma filosofía pero se sube el umbral mínimo hasta los 128 bits.

En lo que se refiere a la firma digital, en sistemas de Nivel Medio se aceptan cualesquiera de los métodos de firma reconocida que acepte la legislación vigente y que hagan uso de certificados reconocidos. Las claves RSA de firma no tendrán menos de 1.024 bits, y las funciones de resumen no tendrán nunca una resistencia inferior a la de la función SHA-1. Se rechaza expresamente la función MD5 o cualquier otra de resistencia similar o inferior. Las firmas que otorgan validez a los certificados de identidad no deberán tener longitudes inferiores a 2.048 bits en el caso de RSA, ni menos de 224 bits en el caso de utilizar curvas elípticas. Como función *hash* se aceptará cualquiera de la familia SHA-2.

En instalaciones de Nivel Medio, las firmas digitales deben ir respaldadas por el correspondiente sello de tiempo que dé fe de su existencia y perduración desde la fecha indicada en ellos. En las instalaciones de Nivel Alto se utilizarán cualquiera de los esquemas de firma que se aceptan para las de Nivel Medio, pero las claves serán más largas, de 2.048 bits en el caso del RSA, y de 256 a 283 en el caso de que se utilicen operaciones sobre curvas elípticas. En este caso, también es preceptivo acompañar a las firmas de su correspondiente sello de tiempo.

En las instalaciones de Nivel Alto se utilizarán Autoridades de Sellado de Tiempo (TSAs), que reciben el documento a sellar, se le añade la hora actual y se firma digitalmente. Para mayor seguridad del sistema, los distintos sellos pueden estar relacionados entre sí a través de lo que se conocen como esquemas enlazados. Las firmas de una TSA, en el caso de utilizar RSA, requieren claves de no menos de 4.096 bits de longitud y una función resumen de la familia SHA-2 con una seguridad mayor o igual a la de SHA-256. En los esquemas enlazados, la función de enlace no deberá tener, en cuanto a su "no-invertibilidad", una seguridad inferior a la de la función SHA-256.

Más de tres cuartas partes de la guía se consagran al desarrollo de siete anexos de carácter bastante académico, que intentan poner de manifiesto aspectos que son importantes cuando se trata de poner en pie una instalación real. Además de tratar los cifrados simétricos, asimétricos RSA o con Curvas Elípticas, los protocolos de cogeneración de claves y las funciones *hash*, en la guía también se educa en lo que a protocolos clásicos de autenticación de usuarios y a la firma digital se refiere.

Aunque en lo que respecta a la firma de documentos secretos y no secretos, el enfoque podría ser distinto al que se sigue en la guía, lo cierto es que en ese punto se habla de los sellos de tiempo y de los sistemas para generarlos.

Los sellos de tiempo y, sobre todo, el último apéndice que le sigue sobre la generación de bits aleatorios, son las aportaciones pedagógicas más importantes de esta guía. Nada de lo dicho en los apéndices anteriores puede considerarse útil si la clave no es segura; es decir, secreta y uniformemente aleatoria como sinónimo de «inimaginable».

Lo que se cuenta en la guía sobre los números y las secuencias aleatorias no es nuevo, pero sí es una novedad que se hable explícitamente de ello en un manual oficial como este. El problema de la generación de las claves, de su gestión y de su calidad, desde todos los puntos de vista, es mucho más serio de lo que muchos integradores o desarrolladores de equipos o sistemas se piensan. La madurez de un profesional en la seguridad de las TIC se puede medir por su preocupación, sensibilidad y maestría en la generación y gestión de las claves. Aquellos que ahorren esfuerzos en este punto, le están poniendo pies de barro a sus productos y la seriedad/seguridad nacional no debería construirse sobre tan frágil basamento. ■

En las instalaciones de Nivel Alto se requiere que la información esté permanentemente cifrada. En estos casos, el estado natural de la información es el criptograma, tanto cuando se transporta de un lado a otro, como cuando se almacena, que no es más que un transporte de un lugar del tiempo a otro en el futuro. En este caso, las claves utilizadas para el cifrado no deben tener una resistencia inferior a los 128 bits de entropía real.

Independientemente de la seguridad que ofrezca, toda clave secreta debe estar protegida durante su ciclo de vida; es decir, desde su misma generación, como durante su transporte, en su custodia mientras se utilice, y en su almacenamiento posterior hasta su destrucción final.

Jorge Dávila Muro
Consultor independiente
Director
Laboratorio de Criptografía
LSIIS – Facultad de Informática – UPM
jdavila@fi.upm.es