Repudio de firmas electrónicas en Infraestructuras de Clave Pública

J. L. Hernández-Ardieta, A. I. González-Tablas y B. Ramos

***Resumen*—La firma electrónica como evidencia de no repudio ha adquirido un enorme respaldo tanto legal como de la propia industria. Para poder desarrollar aplicaciones de firma electrónica se necesita la existencia de una Infraestructura de Clave Pública (PKI) que permita la emisión y gestión de certificados digitales. No obstante, garantizar el no repudio de un documento firmado es tarea difícil, aun cuando existe todo el marco tecnológico y legal necesario para ello. Dado que el no repudio es quizá una de las propiedades de los servicios de seguridad que mayor complejidad y requisitos conlleva, cualquier vulnerabilidad en los estándares subyacentes o error en la implementación concreta puede hacer repudiable cualquier firma, incluyendo aquellas realizadas con el DNI electrónico. El presente artículo analiza las principales vulnerabilidades y ataques existentes en un modelo de firma electrónica basado en PKI, y que pueden derivar en el repudio del compromiso adquirido por el firmante.**

Palabras clave— DNI-e, estándares (*standards*), firma digital (*digital signature*), firma electrónica (*electronic signature*), Infraestructura de Clave Pública (*Public Key Infrastructure*), Ley 59/2003, no repudio (*non-repudiation*), seguridad (*security*), vulnerabilidades (*vulnerabilities*).

I. Nomenclatura

CAdES – CMS Advanced Electronic Signature
CA – Certification Authority
ASN.1 – Abstract Syntax Notation 1
CA – Certification Authority
CRL – Certificate Revocation List
DTBS – Data To Be Signed
PKI – Public Key Infrastructure
RA – Registration Authority
SCA – Signature Creation Application
SCDev – Signature Creation Device
SSCDev – Secure Signature Creation Device
SD – Signer's Document
SDP – Signer's Document Presentation Component
TSA – Time Stamping Authority
VA – Validation Authority
XAdES – XML Advanced Electronic Signature

Este trabajo ha sido parcialmente realizado en el marco del proyecto SEGUR@, subvencionado por CDTI, Ministerio de Industria, Turismo y Comercio de España, dentro del programa CENIT, con referencia CENIT-2007 2004. (https://www.cenitsegura.es)

J. L. Hernández-Ardieta es el Responsable de Proyectos Especiales de Secuware S.L. Actualmente realiza la Tesis Doctoral en el Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento de Informática de la Universidad Carlos III de Madrid (correo e.: jlopez@gmail.com).

A. I. González-Tablas es Profesora Titular Interina de la Universidad Carlos III de Madrid, del Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento de Informática. (correo e.: anaisabel.gonzalez-tablas@uc3m.es).

B. Ramos es Profesor Titular de la Universidad Carlos III de Madrid, del Grupo de Seguridad de las Tecnologías de la Información y las Comunicaciones del Departamento de Informática. (correo e.: benja1@inf.uc3m.es).

II. Introducción

Nos encontramos en mitad de un intenso periodo de despliegue de aplicaciones y tecnologías orientadas a facilitar y promulgar el uso de la firma digital como mecanismo de autenticación y garantía de no repudio. La aprobación de la Directiva Europea de Firma Electrónica [1] y posteriormente la publicación de la Ley Española de Firma Electrónica [2] ha posibilitado que exista el marco legal necesario para otorgar la confianza y respaldo requeridos a dicho panorama tecnológico. Tal panorama se encuentra además fortalecido por la entrada en vigor en Marzo del año 2006 del Documento Nacional de Identidad electrónico (DNI-e) [3], mediante el cual la Administración Pública proporciona al ciudadano los medios tecnológicos necesarios para que pueda llevar a cabo transacciones electrónicas de manera segura, ya sea con la propia Administración o en otros contextos transaccionales diferentes.

Mediante el uso de la criptografía de clave pública [4] como base subyacente, la firma digital [5] se erige como principal solución para el aseguramiento del no repudio [6], entendiendo el no repudio como el servicio de seguridad que proporciona protección frente al falso rechazo de haber participado en una comunicación [7].

En [7] ISO enmarca el concepto de no repudio dentro de una comunicación electrónica. Sin embargo, en la práctica, la garantía de no repudio proporcionada por la firma digital aplica a los datos firmados que se envían en dicha comunicación, no a la comunicación en sí. Es obvio que unos datos firmados que se queden en posesión exclusivamente del firmante carecen de importancia, puesto que a efectos prácticos es como si no existieran. Por tanto, una vez que el firmante ha transmitido a la otra parte interesada los datos firmados junto con la firma digital correspondiente, está inevitablemente adquiriendo cierto compromiso, el cual además varía según el contexto concreto de la comunicación y

la semántica de los datos firmados. Esta variedad de compromisos se encuentra tanto en el mundo digital como en el caso de las firmas manuscritas. El firmante puede estar queriendo, mediante el acto de firmar (digitalmente o de forma manuscrita), certificar el envío o recepción de cierta información, aceptar los términos descritos en un documento, autorizar una firma previa sobre un documento, o simplemente dar fe de la existencia de determinados datos, entre otros. En cualquier caso, el compromiso adquirido por el firmante en tal comunicación no sería repudiable.

Sin embargo, el empleo de la firma digital no otorga plenas garantías de no repudio sobre la información firmada. En el caso de aplicaciones de firma digital enmarcadas dentro de Infraestructuras de Clave Pública (PKI), las vulnerabilidades de seguridad intrínsecas de éstas se traducen directamente a la firma digital, permitiendo al firmante repudiar el compromiso adquirido.

En presente artículo realiza un análisis detallado de los principales problemas de seguridad actuales no resueltos en PKI que pueden impedir garantizar el no repudio de los datos firmados digitalmente. Así mismo, el artículo se encuadra en el contexto de la Ley Española 59/2003 de Firma Electrónica así como los correspondientes estándares europeos e internacionales, empleando el marco legal y tecnológico más adecuado en este momento para el análisis de las vulnerabilidades y carencias de PKI y firmas electrónicas.

El artículo se divide como sigue: los aspectos relativos a las Infraestructuras de Clave Pública, tales como los conceptos básicos o una arquitectura modelo de ejemplo, se analizan en la parte III. Las normas de firma electrónica de interés para el correcto entendimiento del artículo se exponen en la parte IV. El marco legal existente respecto a la firma electrónica se expone en la parte V. La parte VI trata el concepto de no repudio, elemento central del presente artículo. La parte VII contiene un estudio en profundidad de las vulnerabilidades y posibles ataques que pueden llevarse a cabo contra aplicaciones de firma electrónica basadas en Infraestructuras de Clave Pública. Por último, se finaliza el artículo con las conclusiones de los autores.

III. Infraestructuras de clave pública

A. Descripción

La Infraestructura de Clave Pública (PKI) es un modelo de arquitectura jerárquica de entidades cuyo objetivo es la creación, emisión y gestión de certificados digitales X.509 [8]. PKI surgió como infraestructura de soporte para el uso de la criptografía asimétrica en Internet. De esta forma, PKI ofrece la base sobre la cual asentar otros servicios de seguridad basados en la criptografía asimétrica, tales como S/MIME [9], SSL[10]/TLS[11] o IPSec [12].

Un *certificado digital X.509* es una estructura de datos que permite asociar una clave pública a una identidad [13]. Dicha estructura contiene información relativa a la clave pública criptográfica, al titular en cuestión (identidad, información de contacto, país de procedencia, organización a la que pertenece, etc.) y al periodo de validez del propio certificado. Se emplea la notación ASN.1 [14] así como el estándar X.500 [15] para la definición de la estructura y los distintos campos de la misma.

Se denomina *Titular* al legítimo poseedor de un certificado. De esta manera los datos contenidos en un certificado se refieren al titular de éste. La posesión de la clave privada asimétrica correspondiente es la que le permite realizar firmas digitales.

Los certificados digitales los emiten entidades que se conocen como *Autoridades de Certificación* (CA). Dependiendo de las dimensiones de la implementación concreta de la arquitectura PKI, ésta puede diseñarse contemplando varios niveles de CA, donde siempre existe una CA raíz y tantos niveles de CA intermedias como se necesite. Cada CA emite los certificados digitales de las CA subordinadas, y son las CA del último nivel las que en última instancia emiten los certificados finales de los sujetos. Cuando una CA emite un certificado, genera la estructura ASN.1 en formato X.500 con la información anteriormente indicada y procede a firmar digitalmente dicha estructura. Obviamente, la CA posee un certificado digital propio que permite a terceros verificar la firma digital del certificado emitido haciendo uso la clave pública de la CA. Dicho certificado habrá sido a su vez emitido por una CA de nivel superior, y así sucesivamente hasta la CA raíz, cuyo certificado es auto emitido. El conjunto de certificados desde la CA que ha emitido un certificado final de sujeto hasta la CA raíz se conoce como *cadena de certificación*.

El proceso de identificación del solicitante se lleva a cabo por las *Autoridades de Registro* (RA), entidades encargadas de verificar la identidad del sujeto cuyos datos van a incluirse en el certificado. Se conoce como *solicitante* al sujeto que solicita un certificado digital a una Autoridad de Certificación.

Como se ha indicado anteriormente, un certificado digital posee un periodo de validez concreto, el cual depende de muchos factores, tales como la aplicación concreta que vaya a darse al certificado o los requisitos de emisión de la CA. Un certificado que se encuentra fuera de su periodo de validez se considera expirado, y por tanto cualquier uso con la clave privada asociada no tiene validez ni implicaciones para el titular del certificado. Así mismo, es posible que la clave privada se haya visto comprometida, o que el escenario para el cual se emitió el certificado haya dejado de ser válido (p. ej. el certificado se emitió para un empleado que ha dejado de formar parte de la plantilla de la empresa). PKI habilita un conjunto de mecanismos para la gestión de los certificados digitales [16]. Entre dichos mecanismos se encuentran los métodos de revocación de certificados, mediante los cuales el titular del certificado o una tercera entidad con autoridad para hacerlo anulan la validez del certificado digital, y por tanto de la clave privada asociada, antes que su periodo de validez expire. Mediante la revocación del certificado el titular se asegura que futuros usos de la clave privada no tengan validez, evitando un uso fraudulento o no autorizado en su nombre, en particular la firma electrónica de documentos. No obstante,

existirá un periodo de tiempo desde la solicitud de revocación hasta que esta información se hace pública y por tanto efectiva.

La información del estado de revocación de los certificados emitidos y gestionados por una CA se encuentra en las Listas de Revocación de Certificados (CRL). Una CRL es básicamente una lista firmada digitalmente por la CA correspondiente, donde cada posición contiene el número de serie del certificado cuya validez se ha revocado, así como el momento de revocación. Las CRLs se actualizan periódicamente, típicamente una vez cada 24 horas, incorporando a la lista la información de los certificados revocados desde la última actualización. Así mismo, el momento de la siguiente actualización se incorpora en la propia CRL. Consultando la CRL adecuada, cualquier entidad puede saber si el estado de un certificado es válido o no en un momento determinado.

En PKI existen también entidades llamadas *Autoridades de Validación* (VA) encargadas de validar tanto certificados digitales como firmas electrónicas, de forma que abstraen a los verificadores de las operaciones relativas a la obtención y consulta de la información de revocación. Una firma electrónica es válida si la firma digital se verifica correctamente en base a las propiedades criptográficas de la firma digital [5], y si el certificado digital es válido. En lo que a una validación de certificado se refiere, la VA puede realizar una validación completa o únicamente la validación del estado de revocación. Una validación completa incluye, además de la propia validación del estado de revocación, la comprobación de la integridad del certificado mediante la validación de la firma digital de la CA y la comprobación del periodo de validez del certificado. Es importante que la VA compruebe si el certificado era válido o no (en periodo de validez y estado de revocación) en el momento de generación de la firma, y no otro. Para acelerar el proceso de validación, y dado que las CRLs pueden llegar a tener tamaños del orden de Megabytes, la VA suele descargarse la CRL publicada por la CA a una Base de Datos local cada vez que ésta es actualizada. Todas las consultas a la CRL se realizan a dicha copia local, evitando por tanto los retardos derivados de su descarga. Dado que la CRL incorpora el momento de la siguiente actualización, la VA siempre sabe cuándo realizar una nueva descarga, evitando las consultas periódicas a la CA.

Por último, es necesario mencionar el papel que juegan las *Autoridades de Sellado de Tiempo* (TSA) [17] en estos procesos. Una TSA permite añadir una referencia temporal confiable a la información que se especifique. Estas referencias temporales se llaman sellos de tiempo y, en su formato más extendido, son estructuras de datos firmadas digitalmente por la TSA. Un sello de tiempo certifica que la información sellada existía antes de un instante de tiempo determinado. Esta referencia temporal, incluida en el sello de tiempo, se corresponde con el momento en que la TSA firma digitalmente la estructura de datos anterior. Sellar temporalmente una firma electrónica permite que ésta pueda ser correctamente verificada en un futuro, incluso cuando el certificado empleado ha expirado o ha sido revocado con posterioridad al momento de creación de la firma, ya que el sello de tiempo establece de forma fehaciente que la firma se generó antes de dicho momento temporal.

B. Arquitectura

La Fig. 1 muestra un ejemplo de arquitectura PKI que engloba a las entidades anteriormente descritas.

El proceso de generación del par de claves asimétricas puede variar, realizándose tanto por el propio solicitante como por la Autoridad de Certificación. En el primer caso, el solicitante deberá emplear algún tipo de software criptográfico para la generación del par de claves asimétricas. Independientemente del proceso empleado, el solicitante debe identificarse previamente ante la Autoridad de Registro, ya sea por vía telemática o presencialmente. Como puede observarse en la Fig. 1 existe una comunicación directa entre la Autoridad de Registro y la Autoridad de Certificación. Ambos roles pueden ser desempeñados por la misma organización, e incluso ser implementados por la misma infraestructura informática. No obstante, es habitual el caso donde ambas funciones se llevan a cabo por distintas entidades, en cuyo caso la Autoridad de Certificación requerirá información de la Autoridad de Registro para conocer los datos del solicitante del certificado.

Una vez que se ha realizado el registro correctamente, el solicitante accede a la Autoridad de Certificación para obtener el certificado digital. Cada certificado digital se emite con un conjunto de propósitos determinados – autenticación SSL, firma digital, intercambio de claves, etc. –, los cuales se especifican en lo que se conoce como *Política de Certificado* [18].

Para evitar un uso fraudulento de la clave privada por terceros no autorizados, el usuario deberá custodiar de forma correcta su clave privada durante el periodo de validez del certificado.

Si se ha empleado una tarjeta inteligente para el almacenamiento de clave privada y el certificado digital, la custodia es más eficaz, debiendo proteger únicamente la clave de uso de dicha tarjeta. En caso de que se emplee un soporte software (p. ej. fichero en formato PKCS#12 [19]), lo normal es importar esta información en el navegador Web o software específico de firma a usar. El acceso a las claves privadas gestionadas por el almacén de claves del navegador suele protegerse mediante una clave de acceso, lo cual impediría el uso indiscriminado de las claves de firma por usuarios no autorizados.

Cabe destacar que los procedimientos y normativa seguidos por la Autoridad de Certificación para la emisión y gestión de los certificados que emite, así como las obligaciones, responsabilidades y derechos de las partes implicadas, incluyendo al solicitante y futuro titular, se recogen en la *Declaración de Prácticas de Certificación* [18].

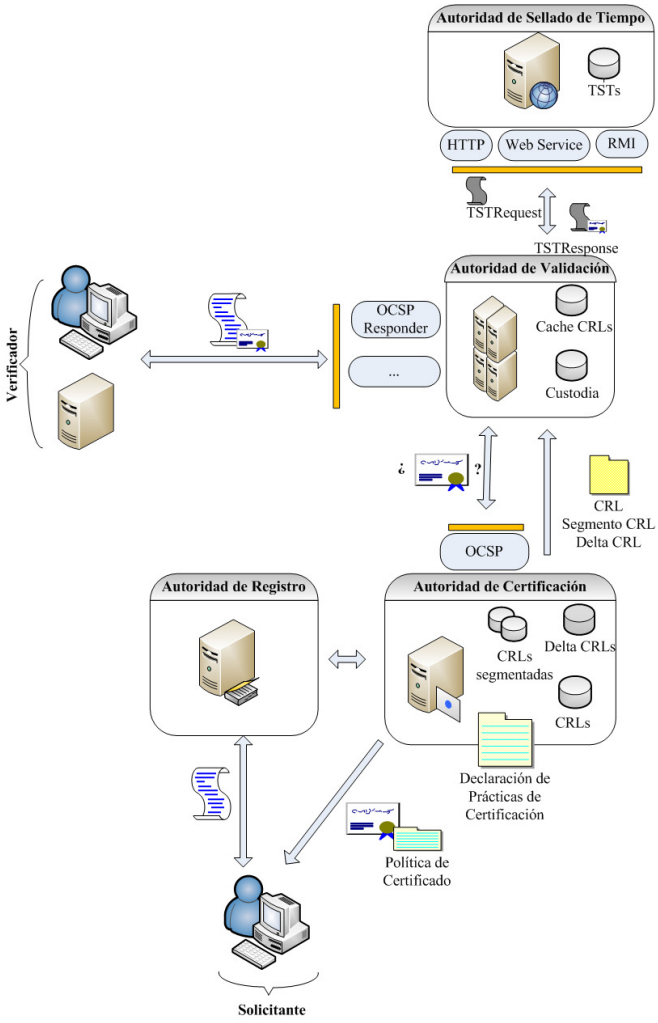

Fig. 1. Arquitectura genérica PKI

La arquitectura anterior muestra también un tercer actor llamado *verificador*, el cual desea validar bien un certificado digital bien una firma electrónica. Para ello accederá a los servicios publicados por una *Autoridad de Validación*, ya sea mediante una interfaz OCSP [20] u otras. Para poder validar el estado de revocación del certificado, la Autoridad de Validación deberá obtener la información de revocación de la Autoridad de Certificación pertinente.

Finalmente, la VA puede, a través de la *Autoridad de Sellado de Tiempo*, incluir un sello de tiempo en la firma electrónica validada. La VA podrá también incluir información adicional a la firma electrónica y proceder a su archivado y custodia, lo cual otorgaría a la firma electrónica la característica de firma longeva, pudiendo ser verificable en un futuro incluso posterior a la expiración del certificado de firma.

C. *La confianza como condición fundamental*

El elemento central sobre el cual gira PKI es la confianza. Para que terceros sujetos confíen en los proceso de firma electrónica y tengan garantías acerca de la validez de dichas firmas, es imprescindible que existan determinados requisitos:

- Confianza en la CA que emitió el certificado digital que contiene la clave pública de verificación. En este caso el prestigio de la CA como entidad es fundamental, así como los procedimientos y normativa llevados a cabo en la emisión y gestión de certificados digitales. Por ello, la evaluación de la Declaración de Prácticas de Certificación por parte del usuario es fundamental para adquirir un grado de confianza u otro.
- Confianza en el proceso de registro llevado a cabo por la RA. Los procedimientos de registro llevados a cabo por la RA pueden variar sustancialmente, y de ellos depende la confianza que se deposite en la relación clave pública-identidad. No otorga las mismas garantías un proceso de registro con identificación física del solicitante del certificado que uno telemático.
- Seguridad global que las distintas entidades de la PKI aplican en sus sistemas informáticos.
- Soporte empleado para el almacenamiento de la clave privada y del certificado digital. Un soporte hardware, como puede ser el DNI-e, siempre da mayores garantías de seguridad que un soporte software.
- Respaldo legal existente. El titular (signatario) y el usuario (receptor de la firma) del certificado depositarán su confianza en la PKI y los procesos que de ella se deriven si se encuentran respaldados por un marco legal adecuado.
- Terceros implicados. La seguridad y el grado de confianza en terceros (VA, TSA, etc.) que puedan intervenir en los procesos de la PKI es fundamental para aumentar o disminuir la confianza global en dicha PKI.
- Por último, y como requisito más fundamental, el entorno del firmante. Dado que un proceso de firma electrónica de usuario se puede considerar con un conjunto de etapas, desde la solicitud del certificado hasta la validación de la firma electrónica, el entorno del usuario, es decir, el eslabón más débil de la cadena de seguridad, supedita totalmente la confianza e incluso la propia validez de la firma electrónica.

A todo esto hay que añadir que la confianza es, ante todo, una sensación y percepción subjetivas de la persona, por lo que un mismo mapa de medidas de seguridad puede infundir distintos grados de confianza según la persona.

IV. Normativa de Firma Electrónica

Existen múltiples estándares relativos a firma electrónica y PKI, muchos de los cuales se han referenciado en la parte anterior. Esta parte IV en concreto describe brevemente dos normas europeas del organismo de estandarización CEN enfocadas a las aplicaciones de creación y verificación de firma electrónica. De esta forma se pretende ayudar a la

comprensión de ciertos ataques descritos en la parte VII.

La primera norma, denominada CEN CWA 14170 [21], modela un sistema de creación de firmas, especificando los requisitos de seguridad y ciertas recomendaciones que deben cumplir las Aplicaciones de Creación de Firmas (SCA) que se adhieran al modelo, y las cuales realicen firmas electrónicas avanzadas acorde a la Directiva Europea de Firma Electrónica (ver parte V) y que empleen un Dispositivo de Creación de Firmas (SCDev) hardware para tal fin.

Es importante resaltar que la norma indica que todos los datos manejados dentro de la SCA así como los transmitidos entre SCA y SCDev deberán serlo a través de canales seguros, protegiendo dichos datos frente a ataques de integridad o confidencialidad.

En la norma se define el DTBS como el conjunto de objetos que agrupan tanto el documento a firmar como los atributos adicionales que también se desean firmar. Los atributos firmados pueden englobar, entre otros, el identificador del certificado empleado, el tipo de documento a firmar o la referencia a la política de firma [22] a la cual se adhiere el firmante. El DTBS se compone internamente en SCA, por lo que todos los procesos llevados a cabo sobre dicha información, incluyendo el envío del DTBS correctamente procesado al SCDev, pueden considerarse seguros.

Por otra parte, aunque la Directiva Europea no establece requisitos para las aplicaciones de verificación de firmas, sí se indica que se debe asegurar que el proceso de verificación de la firma se lleva a cabo con ciertas garantías. Para ello, la segunda norma de interés, la norma CEN CWA 14171[23], establece los requisitos que deben cumplir las Aplicaciones de Validación de Firmas (SVA) tanto para la validación de firmas electrónicas básicas como avanzadas y reconocidas, acorde a la Directiva Europea. Esta norma diferencia entre las firmas cuyo periodo de vida sea corto y aquellas firmas longevas que se deban poder verificar más allá de los periodos de validez de los certificados digitales empleados. Los requisitos impuestos a las SVA variarán según soporten la validación de un tipo de firmas u otro.

V. Marco legal de la firma electrónica

Varios motivos impulsaron la redacción de la Directiva Europea de firma electrónica [1], entre los que se encuentran el aumento de la preocupación por la seguridad en las comunicaciones electrónicas y la iniciativa europea de comercio electrónico. La Directiva Europea fue por tanto una necesidad comunitaria cuyo principal objetivo era el impulso de la firma electrónica como medio de autenticación de usuarios en el ámbito telemático, más concretamente en el ámbito de las Administraciones Públicas nacionales y comunitaria. Pero sobre todo, el objetivo más ambicioso de la Directiva Europea fue atribuir a la firma electrónica, en su calidad de firma reconocida, la misma validez legal que la firma manuscrita. Así mismo, la Directiva establece los requisitos que deben cumplir los Prestadores de Servicios de Certificación que emiten certificados digitales reconocidos. Por otra parte existían en aquel momento un conjunto de normativas y leyes nacionales heterogéneas relativas a servicios de certificación que amenazaban con impedir la difusión y expansión de la firma electrónica entre los Estados miembro. Así pues se aprobó la Directiva Europea número 93 en Diciembre del año 1999 para establecer un marco comunitario para la firma electrónica.

Poco antes de la aprobación de la Directiva Europea de firma electrónica se publicaba en España el Real Decreto-ley 14/1999 [24] por el cual se regulaba a nivel nacional el empleo de la firma electrónica como medio de autenticación y no repudio. Dado que la Comisión Europea exigía en el artículo 13 de la Directiva que cada Estado miembro realizara una adecuación de su legislación para dar cumplimiento a lo establecido en dicha Directiva, el Parlamento Español optó por reformar el Real Decreto-ley 14/1999 y por ello publicó la Ley Española 59/2003 de firma electrónica en Diciembre del año 2003 [2].

La Ley 59/2003 es una transposición de la Directiva Europea adecuada a la realidad nacional española, donde además se incorpora una mención al DNI-e, documento cuya expedición se regula a su vez en el Real Decreto 1553/2005 [3]. No obstante, la base fundamental de la Directiva y la Ley Española de firma es la misma, especialmente en relación a las definiciones de firma electrónica y las implicaciones jurídicas de ésta.

En ambas legislaciones se considera una firma electrónica (básica) como “datos en formato electrónico adjuntados o asociados de manera lógica a otros datos en formato electrónico y que sirven como un medio de autenticación”. Un mero nombre de remitente al final de un correo electrónico o una dupla usuario-clave de acceso podrían considerarse firmas electrónicas.

Así mismo, tanto la Directiva Europea como la Ley Española definen otros tipos de firma electrónica, como son la firma electrónica avanzada y la firma electrónica reconocida. A estas últimas se les atribuye otras propiedades además de actuar como mecanismo de autenticación, como son la capacidad de detectar modificaciones en el mensaje firmado, estar asociada de manera única al firmante, ser capaz de identificar al firmante y haber sido creada por medios mantenidos bajo el exclusivo control del firmante. Además, una firma electrónica reconocida ha de haber sido creada mediante un dispositivo seguro de creación de firmas (SSCDev) y el firmante debe haber empleado un certificado calificado como reconocido, el cual debe cumplir determinadas características. En particular, la firma electrónica reconocida tiene respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

No obstante, la Directiva Europea, en su art. 5.2, y la Ley Española, en su art. 3 disposición novena estipulan básicamente que no se negará validez jurídica a una firma electrónica por el mero hecho de no ser reconocida. Es decir, en la práctica, una firma electrónica básica o avanzada pueden tener las mismas implicaciones legales que una firma reconocida. Cualquiera de ellas impide que el firmante repudie

el compromiso adquirido ante los datos firmados. Evidentemente cualquier parte puede impugnar la autenticidad de una firma electrónica, para lo cual deberá seguir un proceso legal u otro dependiendo de si se trata de una firma electrónica básica, avanzada o reconocida (Ley 59/2003 art. 8 y 10).

A pesar de la neutralidad tecnológica con la que se define la firma electrónica, en la práctica sólo la firma digital basada en criptografía asimétrica y certificados digitales es capaz de proporcionar los requisitos que se exigen. El objetivo de dicha neutralidad no es otro que evitar que la normativa legal deba modificarse si en un futuro surge otra tecnología o fundamento criptográfico que aporte dichas propiedades.

VI. NO REPUDIO

El no repudio es un término ampliamente usado en el ámbito de la seguridad informática. Tal y como se ha adelantado en la parte I, aunque ISO define no repudio como el servicio de seguridad que proporciona protección frente al falso rechazo de haber participado en una comunicación [7], en la práctica el no repudio aplica a los datos firmados y transmitidos en la comunicación.

En los protocolos de seguridad donde se necesita asegurar el no repudio de las operaciones realizadas por los participantes se genera lo que se conoce como evidencias electrónicas. Una evidencia es información que, ya sea por sí misma o asociada a otros datos, se emplea para establecer una prueba sobre determinado evento o acción [25]. ISO define en [6] evidencias de no repudio a partir de técnicas criptográficas asimétricas, es decir, mediante la aplicación de firmas digitales. Así mismo, una evidencia de no repudio debe cumplir los siguientes requisitos [26]:

- Que un tercero pueda verificar el origen o autoría de la evidencia.
- Que un tercero pueda verificar la integridad (no modificación) de la evidencia.
- Que la validez de la evidencia no se pueda repudiar.

Las firmas electrónicas en conjunción con el uso de certificados digitales cumplen claramente los requisitos anteriores.

Para un documento firmado, el no repudio significa que el firmante, desde el momento que realiza la firma digital, es responsable del compromiso adquirido sobre dicho documento [27]. Este compromiso incluye, aunque no está limitado a, conocimiento de existencia del contenido, estar de acuerdo con dicho contenido o establecimiento de un contrato legal.

Por otra parte, no puede entenderse no repudio sin autenticación, aunque si a la inversa. Un sujeto podría autenticarse en un sistema informático sin la obligatoriedad de adquirir un compromiso en la comunicación. Por el contrario, todo sujeto que, de alguna manera, se compromete en una comunicación, revela su identidad ante el otro extremo del canal, pudiendo corroborarse que el sujeto es realmente quien dice ser.

Dado que a lo largo del artículo nos referiremos principalmente a firma electrónica en vez de a firma digital, conviene resaltar el diferente significado entre ambas. Firma digital se considera el resultado matemático de aplicar determinadas operaciones criptográficas [5]. Por el contrario, si tomamos como referencia la Directiva Europea o la Ley Española de Firma Electrónica (ver parte V), una firma electrónica se define como “datos en formato electrónico adjuntados o asociados de manera lógica a otros datos en formato electrónico y que sirven como un medio de autenticación”. Como puede observarse la definición de firma electrónica es neutral desde el punto de vista tecnológico, y no dependiente de la criptografía.

Independientemente del término empleado, y en caso de necesitar garantizar el no repudio de determinados datos firmados, se deberá poder, mediante la validación de la firma digital o electrónica, corroborar la identidad del firmante, detectar cualquier modificación de los datos firmados y tener la certeza que sólo el firmante ha sido capaz de generar dicha firma [2].

VII. VULNERABILIDADES Y ATAQUES ACTUALES

Esta parte del artículo realiza un breve repaso sobre las principales vulnerabilidades y ataques posibles a día de hoy sobre firmas electrónicas dentro del marco de las infraestructuras de clave pública. La gravedad y facilidad de ciertos ataques pone de manifiesto cómo el grado de confianza de los usuarios en las firmas electrónicas y PKI puede verse seriamente dañado.

De cara a la identificación de los ataques se ha tomado como hipótesis que el ordenador personal o corporativo del firmante es un elemento de no confianza, por lo que no se puede asegurar que esté libre de software malicioso que pueda intervenir en los ataques descritos. Por el contrario, cualquier otra entidad involucrada, como pueda ser una CA, VA o TSA, sí se considera una entidad de confianza; por ello se supone que los procesos llevados a cabo por éstas no pueden verse afectados por software malicioso, y que por tanto operan conforme a lo estipulado.

En el presente artículo se considera *software malicioso* al cualquier programa informático (p. ej. virus, troyano o similar) que tiene como objetivo comprometer la seguridad del proceso de firma llevado a cabo en el ordenador del firmante.

A. Entorno del Firmante

Esta sección desglosa los ataques más relevantes centrándose en el entorno del firmante.

1) Compromiso de la clave privada

El hecho que una firma digital actúe como evidencia de no repudio implica que sólo el firmante pueda haber realizado dicha firma. No obstante, gran parte de esta afirmación depende de la correcta protección de la clave privada. A continuación se muestran ciertas vulnerabilidades y ataques que pueden comprometer la clave privada del firmante:

a) Generación del par de claves

En caso que sea el solicitante quien genere mediante un software específico el par de claves en su ordenador, es posible que durante o después de la fase de generación un software malicioso hospedado en su ordenador capture la clave privada de firma. Todo dependerá del nivel de seguridad que posea dicho software de creación de claves.

b) Almacenamiento y custodia del par de claves

Suponiendo una generación segura del par de claves, aun así es posible que un software malicioso pueda acceder al repositorio donde se almacena la clave privada del firmante y por tanto obtener una copia, aun cuando generalmente estos almacenes se encuentran cifrados.

Así mismo, es responsabilidad del firmante almacenar la clave privada en un soporte seguro. Ya sea un soporte software o hardware, siempre acaba existiendo una contraseña de acceso a la clave privada. Mientras que en un soporte hardware la clave privada no puede extraerse, en un soporte software sí, por lo que se está supeditando la seguridad global de la PKI a la calidad de dicha contraseña de acceso.

c) Generación de una firma electrónica en cliente

Una clara vulnerabilidad al respecto es la relacionada con el libre acceso a las claves de firma en los navegadores Web. Como ejemplo, cabe mencionar el caso en el cual una vez que el firmante ha realizado la importación de la clave privada y el certificado correspondiente en el almacén del navegador, normalmente no se ofrece ninguna opción para exigir la inserción de la contraseña cada vez que se vaya a emplear la clave privada. A lo sumo se habilita una opción para avisar al usuario que cierto software está solicitando acceso a dicha clave, pudiendo rechazar o aceptar la operación. Se permite así que cualquier usuario con acceso al ordenador donde se ha importado la clave privada del firmante pueda realizar firmas electrónicas en su nombre. Incluso en el caso que sea el usuario legítimo quien esté haciendo uso del navegador Web, si no se habilita la opción de aviso anteriormente mencionada, un software malicioso podría estar llevando a cabo cuantas firmas electrónicas deseara.

Así mismo, existe la posibilidad que el ordenador del firmante esté infectado por un *keylogger* [28], por lo que la captura del PIN o clave de acceso por parte del software malicioso es totalmente factible. En este caso, la vulnerabilidad afecta tanto si el firmante custodia la clave privada en un soporte software o hardware.

2) Ataque por modificación/sustitución de documento

Este tipo de ataque se centra en la fase de generación de una firma electrónica en cliente y teniendo en cuenta la aplicación de la norma CEN CWA 14170 [21], descrita en la parte IV.

Aunque los datos a firmar (DBTS) se manejan de forma segura tanto a nivel interno en la Aplicación de Creación de Firmas (SCA) como entre el SCA y el Dispositivo de Creación de Firmas (SCDev), siempre existe una etapa ajena al SCA que consiste en la selección del documento a firmar, y que posteriormente se enviará al SCA para su procesamiento. Esta etapa se cubre por un software ajeno al SCA, y cuyo nivel de seguridad puede ser totalmente nulo. Aunque la norma indica que debe existir cierto control sobre los canales no seguros de entrada/salida con los procesos externos al SCA, no se puede asegurar que un software malicioso pueda intervenir en la etapa de selección del documento.

Los posibles ataques a realizar por el software malicioso incluyen la modificación o la sustitución completa del documento. Sería este documento alterado de manera no autorizada el que se enviaría al SCA, y el cual se incluiría en el DTBS.

Como contramedida, el modelo mostrado en la norma incluye un componente llamado Componente de Presentación de Documento de Firmante (SDP) cuya finalidad es mostrar al usuario el documento previamente seleccionado así como los atributos adicionales que desea firmar. Sin embargo, existen múltiples variables que hace muy difícil la aplicación de estos requisitos de seguridad, como pueden ser:

- El formato del Documento del Firmante (SD): dado que existen infinidad de tipos de documentos, el SDP debería ser capaz de mostrar adecuadamente todos los SD de acuerdo su formato.
- SD con tipo de contenido sensible o no sensible: la norma identifica estos dos tipos de contenidos de SD, donde el primero se corresponde con aquellos formatos en los cuales una incorrecta presentación del contenido puede derivar en una diferente interpretación del mismo, es decir, la semántica depende de la presentación.

3) Ataques mediante inclusión de código oculto

El escenario de este tipo de ataque es el mismo que en el caso anterior, donde la norma CEN CWA 14170 se emplea como marco de referencia.

En este tipo de ataque el software malicioso residente en el ordenador del firmante incorpora al Documento del Firmante (SD) cierto código que modificará la interpretación/visualización del SD acorde a determinados parámetros deseados. Dado que el contenido en sí del SD no se modifica una vez realizada la firma electrónica, ésta continuará siendo válida aun con el código oculto del atacante.

Un ejemplo de un ataque mediante código oculto es la incorporación de una macro en un documento Word. Supongamos un documento contractual donde el firmante acepta pagar una cantidad determinada por un servicio dado. Si el atacante incorpora una macro en el SD que permita la modificación (visual) de dicha cantidad en base a la fecha de apertura del SD, el firmante puede estar aceptando el pago de una cantidad X en el momento de la firma y en cambio que el verificador visualice un cantidad diferente en el momento de la verificación de la firma del documento. Y el contenido de tal documento no se habría visto modificado en ningún momento, tomándose la firma como válida.

Para evitar este tipo de ataques, la norma indica que el SDP debe, además de poder mostrar al firmante el SD de forma

correcta, detectar cualquier código oculto incluido en el SD. El problema radica en que, al igual que en el apartado VII-A-2 anterior, es muy difícil desde un punto de vista técnico que una SCA cumpla estos requisitos de seguridad, por lo que la detección de cualquier código oculto es, en la práctica, imposible.

B. Protocolos y estándares

Esta sección se centra en vulnerabilidades de los protocolos y estándares actuales de firma electrónica y PKI, incluyendo aquellas vulnerabilidades pertenecientes al modelo de arquitectura y servicios de PKI.

1) *Incertidumbre sobre el estado de revocación del certificado*

Una de las mayores complejidades en los sistemas de firma electrónica es conocer con certeza el estado de revocación de los certificados digitales en el momento de creación de la firma. Esta problemática se debe al retardo existente desde que el titular de un certificado digital (o una entidad con autoridad para hacerlo) realiza la solicitud de revocación del certificado hasta que la Autoridad de Certificación publica la información de revocación actualizada. Este retardo provoca un periodo de incertidumbre donde la Autoridad de Validación puede tomar como válido un certificado digital cuya solicitud de revocación está todavía procesándose por la Autoridad de Certificación.

A continuación se muestran dos ataques que aprovechan el periodo de incertidumbre descrito:

- Repudio de firma por parte del titular del certificado

El legítimo poseedor del certificado desea poder repudiar, en caso que le interese, la firma electrónica de un documento dado.

Para ello, realiza la solicitud de revocación del certificado inmediatamente antes de firmar el documento. El firmante aplica así mismo un sello temporal a la firma electrónica generada haciendo uso de una TSA. Debido al retardo en la actualización de la información de revocación, la VA tomará la firma y el certificado como válidos respecto al momento indicado por el sello de tiempo. El firmante podrá más adelante, y una vez actualizada la información de revocación, probar que el certificado estaba revocado en el momento de creación de la firma, desligándose de cualquier responsabilidad legal respecto al documento firmado.

- Suplantación de identidad

En este caso, el atacante desea beneficiarse, en nombre del titular del certificado, de las ventajas obtenidas de la firma de un documento electrónico cuyas cláusulas sean de aplicación inmediata o temprana (p. ej. Transferencia bancaria, descarga de software de pago, acceso a servicios de pago, etc.).

Para poder llevar a cabo este ataque, el atacante debe haber obtenido previamente la clave privada del titular del certificado (ver apartado VII-A-1). Suponemos que el titular del certificado detecta el compromiso de la clave privada y procede a la solicitud de revocación del certificado. Si el atacante firma el documento inmediatamente después de la solicitud de revocación, es muy probable que la CA no haya actualizado todavía la información de revocación, tomándose la firma y el certificado como válidos. Si la ejecución de las cláusulas recogidas en el documento firmado se produce antes que la información de revocación se actualice, el atacante habrá obtenido su beneficio sin que el titular del certificado pueda haber repudiado ante las partes implicadas el compromiso adquirido.

Para disminuir ese periodo de incertidumbre, la solución más ampliamente instaurada en el mercado consiste en aumentar la frecuencia de actualización de la CRL. Sin embargo, esta solución provoca que las Autoridades de Validación deban descargarse con mayor frecuencia las CRLs, lo cual tiene un grave impacto en el rendimiento de los sistemas así como en el consumo de ancho de banda de la red.

Para paliar el impacto del aumento de la frecuencia de publicación de la CRL, se han ideado otros métodos de actualización de la información de revocación de las CRLs, como CRLs segmentadas [29], Delta CRLs [30] o servicios OCSP Reponder [20]. No obstante, por mucho que se mejore el rendimiento de los métodos de actualización y de consulta del estado de revocación de los certificados digitales, el periodo de incertidumbre que impide asegurar con total certeza la validez de un certificado, y por tanto de una firma electrónica, continúa presente.

A día de hoy, la única solución propuesta que permite averiguar con total seguridad si el estado de un certificado es válido o no en un momento determinado consiste en aplicar lo que se conoce como periodo de gracia [23].

El periodo de gracia permite a las Autoridades de Validación consultar la información de revocación totalmente actualizada respecto a un momento de tiempo dado. Para ello la VA deberá esperar (periodo de gracia) a la próxima actualización de la CRL antes de consultar la información de revocación, asegurándose que cualquier revocación previa ha sido convenientemente actualizada en dicha CRL. No obstante, no es una solución carente de desventajas. La principal de ellas es el retardo forzado que debe aplicar la Autoridad de Validación antes de comprobar el estado del certificado y, por tanto, antes de responder a la petición de validación del certificado. Esta solución resulta por ello inviable en escenarios donde el tiempo de respuesta ha de ser mínimo.

2) *Retardos en el sellado de tiempo*

Para poder conocer el estado del certificado en el momento de generación de la firma, y no otro, es necesario aplicar sellos temporales como garantía de referencia de tiempo, empleando para tal fin los servicios habilitados por las TSAs [17].

Dada la necesidad de conectividad con la TSA para la obtención el sello de tiempo, el proceso de sellado de la firma se realiza normalmente por parte de la VA una vez que se ha comprobado que tanto la firma como el certificado son válidos en el momento de verificación. Obviamente existirá una diferencia de tiempo entre el momento real de generación de la

firma por parte del firmante y el momento en que la VA valida la firma y, por tanto, solicita el sello de tiempo a la TSA. Por ello se aconseja a las Aplicaciones de Verificación de Firmas (SVA) que dicha diferencia de tiempo sea la menor posible, a fin de otorgar la máxima fiabilidad a la firma electrónica [23].

Sin embargo, independientemente de que la SVA valide y solicite el sello de tiempo a la TSA en un momento inmediatamente posterior a la creación de la firma, seguirá existiendo inevitablemente un retardo entre la solicitud y la creación del sello de tiempo. Es durante ese periodo de tiempo cuando el firmante puede haber emitido una solicitud de revocación del certificado, y que ésta haya sido procesada convenientemente por la CA (aunque no publicada). El resultado sería que la VA está sellando temporalmente una firma electrónica en un momento de tiempo donde el certificado está revocado, cuando tras el proceso de validación se consideraba válido.

Esta vulnerabilidad, que afecta tanto a la fase de validación de la firma electrónica como de extensión y custodia de la misma, debilita uno de los pilares que se emplean para la generación de firmas longevas, como es el sello de tiempo. El sistema podría estar archivando firmas no válidas que además se hayan aplicado a documentos electrónicos con gran implicación legal o contractual.

3) Vulnerabilidad de OCSP

El servicio de estado de certificado en línea [20], OCSP por sus siglas en inglés, se ideó con el objetivo de abstraer a los verificadores de las complejidades inherentes a la validación de certificados digitales, principalmente aquellas relativas a la obtención y consulta de la información de revocación, en concreto las CRLs.

El estándar OCSP básicamente define el formato de los mensajes de petición y respuesta con el objetivo de conocer el estado de revocación de un certificado, así como alguna otra información adicional. Se exige que las respuestas estén firmadas por el servidor OCSP, es decir, la entidad que publica el servicio OCSP. Las peticiones pueden ir o no firmadas por el sujeto solicitante.

Cada petición incluye fundamentalmente la siguiente información:

- Resumen (*hash*) del nombre distintivo del emisor del certificado a validar.
- Resumen (*hash*) de la clave pública contenida en el certificado del emisor del certificado a validar.
- Número de serie del certificado a validar.

El servidor OCSP empleará los dos primeros campos para discernir de qué Autoridad de Certificación consultará la información de revocación para la validación del estado del certificado.

Cada respuesta contiene los siguientes datos, entre otros:

- Identificador del certificado (número de serie)
- Estado del certificado (válido, revocado o desconocido)
- Intervalo de validez de la respuesta, indicando la próxima actualización de la información de revocación

La vulnerabilidad del protocolo OCSP radica en el sentido que se le atribuye a "válido" en una respuesta. "Válido" implica que el certificado no estaba revocado, es decir, que no se ha encontrado en la información de revocación, lo cual no significa que sea un certificado que se haya emitido por la Autoridad de Certificación indicada en la petición. Dado que el servidor OCSP consultará la información de revocación empleando el número de serie de la petición, si el solicitante indica un número de serie correspondiente a un certificado emitido por una Autoridad de Certificación distinta a la indicada en la petición, dicho certificado nunca se encontrará en la información de revocación de la Autoridad de Certificación consultada, aunque el certificado esté realmente revocado.

A través de esta vulnerabilidad es posible que un sistema de archivo longevo extienda firmas electrónicas con información de revocación errónea.

C. Algoritmos criptográficos

En esta sección se muestran algunos ataques que aprovechan vulnerabilidades propias de los algoritmos criptográficos (fundamentalmente algoritmos de clave pública y funciones resumen) que se emplean en PKI para la generación de firmas electrónicas o emisión de certificados digitales. No es objeto de esta sección realizar un estudio matemático al respecto, sino mencionar las vulnerabilidades existentes y cómo éstas se podrían explotar por un atacante.

Los ataques y vulnerabilidades aquí descritos afectan a la fase de generación de una firma electrónica en cliente.

1) Ataques por colisión

Relativo a las funciones resumen, la principal vulnerabilidad es la probabilidad de ocurrencia de una colisión. Ello permitiría al atacante sustituir el documento firmado por el documento manipulado, manteniendo la validez de la firma. Para evaluar la fortaleza de una función resumen es fundamental establecer el umbral de tiempo necesario para encontrar una colisión. Este umbral variará dependiendo del escenario concreto. Por ejemplo, en un entorno donde los documentos firmados tienen una validez de horas, el umbral puede situarse en días. Por tanto, aunque el tiempo necesario para encontrar una colisión se reduzca a 1 día, la función resumen aplicada al escenario anterior podría seguir considerándose segura.

No obstante, los tiempos necesarios para encontrar colisiones en las funciones resumen más empleadas en los sistemas de seguridad se han ido reduciendo en los últimos años, gracias a nuevas técnicas de criptoanálisis [31]-[34]. Aunque en la mayoría de los casos los ataques se reproducían en entornos de laboratorio específicos, la fortaleza de funciones resumen ampliamente usadas se ha puesto en entredicho, obligando a los organismos correspondientes a "descatalogar" dichas funciones en pro de nuevas propuestas [35].

Dado que la experiencia dicta que lo que un día se considera

seguro, al cabo de un tiempo deja de serlo, ¿qué ocurre en el lapso de tiempo desde que se encuentran vulnerabilidades en los algoritmos instaurados en el mercado hasta que se empiezan a emplear nuevas propuestas más robustas? Evidentemente ese lapso de tiempo debería reducirse si se empiezan a tomar medidas tan pronto como las investigaciones comienzan a demostrar el debilitamiento de los algoritmos actuales [35], pero siempre existirá una etapa de adaptación del mercado. Es durante ese tiempo cuando los atacantes pueden hacer uso de las vulnerabilidades publicadas, y comprometer así los esquemas de firma existentes en ese momento.

Los estándares ETSI de firma electrónica [36], [37] recomiendan añadir a la firma sellos tiempo periódicamente cada vez que se prevea un debilitamiento en los algoritmos criptográficos empleados, lo cual deriva en la composición de una firma electrónica extendida longeva. De esta forma, en caso de detectar que, por ejemplo, la probabilidad de encontrar una colisión en la función resumen empleada por el firmante se esté acercando al umbral de seguridad establecido, el sistema de archivo longevo deberá calcular e incorporar a la firma un nuevo sello de tiempo. Dicho sello de tiempo se deberá haber calculado sobre la firma digital y la información de revocación existente en la firma electrónica, y la TSA deberá haber empleado una función resumen y/o algoritmo de clave pública más robustos.

Aunque la solución anterior resuelve el problema para aquellas firmas que incorporan los datos firmados (firmas implícitas), no es así para las firmas que solamente incorpora el resumen de los datos firmados (firmas explícitas). En este último caso es posible que no se posea dichos datos, puesto que estén custodiados por un sistema externo no accesible en ese momento. Dado que los nuevos sellos de tiempo sólo pueden aplicarse a la información disponible, en dicha firma explícita sólo se estará protegiendo el resumen de los datos, no los datos en si. Por tanto, por mucho que incorporemos nuevos sellos de tiempo, si el atacante encuentra una colisión en un documento cuya firma se ha calculado de forma explícita (externo a la firma), dicho atacante podrá sustituir el documento firmado manteniendo la validez de la firma extendida, afectando a la extensión y custodia de la misma.

2) Debilitamiento de la longitud de clave

Por otra parte, los algoritmos criptográficos de clave pública también se someten a una evaluación continua por parte de la comunidad científica. Prueba de ello ha sido el continuo incremento de las longitudes de clave empleadas en los distintos algoritmos asimétricos, como puede ser RSA [5], donde se recomendó en 1999 la migración del uso de claves de 512 bits a 1024 bits. Actualmente encontramos sistemas que emplean tamaños de clave RSA de 2048 bits, como es el caso de la clave de firma o autenticación del DNI-e. Así mismo, la Autoridad de Certificación raíz del DNI-e emplea tamaños de clave RSA de 4096 bits para la emisión de los certificados de las CAs intermedias.

En este caso se aplica el mismo razonamiento que el expresado en el apartado anterior VII-C-1 Ataques por colisión. El lapso de tiempo desde que las implementaciones del mercado migran los algoritmos criptográficos empleados hacia versiones o propuestas más robustas puede provocar un periodo inevitable de ataques.

3) Ataques indirectos

Los ataques indirectos son aquellos que hacen uso de interfaces de entrada/salida al criptosistema para obtener información que pueda ayudar a descubrir la clave de cifrado [38].

Ejemplos de este tipo de ataque son:

- Basados en tiempo de ejecución: son aquellos ataques indirectos que se basan en el tiempo que necesita el algoritmo criptográfico para las operaciones de cifrado/descifrado.
- Basados en consumo de energía: en este caso el parámetro que se mide es la energía consumida por el dispositivo de cifrado para la realización de las operaciones.
- Basados en la señal de reloj: cuando el dispositivo de cifrado requiere de la entrada de una señal de reloj externa para su operación, el atacante puede aplicar modificaciones sobre dicha señal. De esa forma, el atacante puede monitorizar el comportamiento anómalo del dispositivo, y así obtener información útil para el descubrimiento de la clave.
- Basados en otras condiciones del entorno, tales como temperatura, radiación, etc.

Por tanto, independientemente del algoritmo criptográfico empleado para la generación de una firma, si el dispositivo o la implementación concreta no se encuentran diseñados para contrarrestar este tipo de ataques, el atacante podría descubrir la clave privada del firmante.

D. Respaldo legal: la doble cara de la moneda

En la parte V se han descrito de forma somera las principales legislaciones sobre los cuales se sustenta actualmente el marco legal de la firma electrónica en España.

El objetivo de todos ellos es muy claro: fomentar el uso de la firma electrónica como medio de autenticación y no repudio, respaldando las acciones y responsabilidades que de su uso se deriven. Un titular que lleve a cabo una firma electrónica reconocida sobre un documento dado obtendrá la misma validez legal sobre dicho documento que si de una firma manuscrita se tratase. Ello aporta innegablemente grandes ventajas, como puede ser la posibilidad de interactuar por vía telemática con la Administración Pública, con la comodidad que implica, o el ahorro de recursos materiales y tiempo en caso de la aplicación de facturación electrónica.

No obstante, existe un sentimiento generalizado en la comunidad de usuarios donde prima también el miedo ante tal respaldo legal. Tal y como se ha visto en esta parte VII del artículo, existen múltiples vulnerabilidades y posibles ataques

a un esquema de firma electrónica basada en certificados digitales. Por tanto, dado que tales ataques son posibles, la suplantación de la identidad del firmante o la sustitución del documento firmado también lo son. Si el firmante debe responder por las consecuencias legales de la firma de un documento electrónico, es posible que deba hacerlo ante un documento cuyo contenido fue maliciosamente modificado (ataque por modificación/sustitución de documento) o del cual no tenía conocimiento (ataque por compromiso de clave privada), entre otros.

¿Qué ocurre en estos casos? Evidentemente la figura del perito judicial es necesaria para evaluar las condiciones bajo las cuales se llevó a cabo dicha firma electrónica, pero no siempre se puede obtener una fotografía clara de lo sucedido. Se abre por tanto un espacio para la libre interpretación de lo ocurrido, donde la presunción de inocencia debería tener cierto peso en la decisión final, aun a pesar de las firmes y concisas cláusulas de la Ley actual de firma electrónica.

VIII. Conclusiones

Es innegable la importancia que ha adquirido la firma electrónica en la mejora de la seguridad de las transacciones y comunicaciones electrónicas. El respaldo legal y de las Administraciones Públicas sumado al impulso otorgado por los diferentes estándares europeos e internacionales ha posibilitado la proliferación de aplicaciones de firma electrónica que vemos hoy en día. La firma electrónica se posiciona así como el principal mecanismo de autenticación y evidencia de no repudio, garantizando que los compromisos adquiridos por el firmante respecto al documento firmado no sean repudiables.

Este panorama se complementa con la figura de las Infraestructuras de Clave Pública (PKI), las cuales juegan un papel fundamental en los escenarios de firma electrónica al permitir realizar la asociación de la clave de verificación de firma con la identidad del firmante.

Sin embargo, y al contrario de lo que las diversas leyes y estándares fundamentan, la firma electrónica no otorga plenas garantías de no repudio sobre la información firmada. El presente artículo ha demostrado cómo es posible llevar a cabo numerosos ataques de mayor o menor complejidad sobre un entorno de firma electrónica basado en PKI. En algunos casos el atacante puede aprovechar una vulnerabilidad incluso cuando el entorno de firma se adecua a los requisitos de seguridad de los últimos estándares y normativas. En la mayoría de los casos la principal causa es que existe una alta probabilidad de que la seguridad del entorno del firmante pueda estar comprometida, lo cual afecta directamente a la seguridad del proceso de generación de la firma. En otros casos se han detectado carencias en los estándares actuales de firma o PKI.

La solución no es trivial, pero un primer paso consiste en fortalecer dicho entorno de firma. Actualmente el Instituto Nacional de Tecnologías de la Comunicación está desarrollando varios perfiles de protección de acuerdo a la norma *Common Criteria* [39], y en los cuales se recogen los requisitos de seguridad que deben cumplir las aplicaciones de creación y verificación de firma que empleen el DNI-e como dispositivo seguro de creación de firmas.

Por otra parte es necesario subsanar las vulnerabilidades y carencias que sufren los estándares de PKI y firma, en tanto y cuanto son parte esencial del escenario. El artículo ha descrito algunas vulnerabilidades que impiden a la entidad verificadora de una firma conocer con certeza el estado de revocación del certificado en el momento de creación de la firma, permitiendo la suplantación de la identidad del firmante o la posibilidad de repudiar la firma generada, y, por ende, el compromiso adquirido.

Referencias

[1] Directiva Europea 1999/93/CE del Parlamento Europeo y del Consejo, de 13 de Diciembre de 1999, por la que se establece un Marco Comunitario para la Firma Electrónica. Diciembre 1999.

[2] Ley Española 59/2003, de 19 de Diciembre, de Firma Electrónica. Diciembre 2003.

[3] Real Decreto 1553/2005, de 23 de Diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica. Diciembre 2005.

[4] W. Diffie y M. Hellman. "New Directions in Cryptography". *IEEE Transactions of Information Theory*, vol. 22 (6), pp 644-654. ISSN: 0018-9448. 1976.

[5] R. L. Rivest, A. Shamir y L. Adleman. "A method for obtaining digital signatures and public-key cryptosystems". *Communicatios of the ACM*, vol. 21 (2), pp 120-126. ISSN:0001-0782. 1978.

[6] *ISO/IEC 13888-3 Information technology – Security techniques – Non repudiation – Part 3: Mechanisms Using Asymmetric Techniques*. ISO/IEC, 1997.

[7] *ISO 7498-2. Information processing system – Open systems interconnection – Basic reference model – Part 2: Security architecture*. International Organization for Standardization, 1989.

[8] R. Housley, W. Polk, W. Ford y D. Solo. *Internet X.509 Public Key Infrastructure. Certificate and Certificate Revocation List (CRL) Profile*. Internet Engineering Task Force – Request for Comments 3280. 2002.

[9] *IETF RFC 2633 – S/MIME Version 3 Message Specification*. Internet Engineering Task Force, Noviembre 1998.

[10] *IETF RFC Draft – The SSL Protocol, version 3.0*. Internet Engineering Task Force, Noviembre 1996.

[11] *IETF RFC 2246 – The TLS Protocol, version 1.0*. Internet Engineering Task Force, Enero 1999.

[12] *IETF RFC 2401 – The Security Architecture for the Internet Protocol*. Internet Engineering Task Force, Noviembre 1998.

[13] S. Santesson, M. Nystrom y T. Polk. *Internet X.509 Public Key Infrastructure. Qualified Certificates Profile*. Internet Engineering Task Force – Request for Comments 3739. 2004.

[14] *ISO/IEC 8824-1:2002. Information technology -- Abstract Syntax Notation One (ASN.1): Specification of basic notation*. International Organization for Standardization, 2002.

[15] *ITU-T Recommendation X.501: Information Technology – Open Systems Interconnection - The Directory: Models*. International Telecommunication Union, 1993.

[16] C. Adams, S. Farrell, T. Kause y T. Mononen. *Internet X.509 Public Key Infrastructure. Certificate Management Protocol (CMP)*. Internet Engineering Task Force – Request for Comments 4210. 2005.

[17] C. Adams, P. Cain, D. Pinkas, R. Zuccherato. *Internet X.509 Public Key Infrastructure. Time-Stamp Protocol (TSP)*. Internet Engineering Task Force – Request for Comments 3161. 2001.

[18] S. Chokhani, W. Ford, R. Sabett, C. Merrill y S. Wu. *Internet X.509 Public Key Infrastructure. Certificate Policy and Certification Practices Framework*. Internet Engineering Task Force – Request for Comments 3647. 2003.

[19] *PKCS 12 v1.0: Personal Information Exchange Syntax*. RSA Laboratories. 1999

[20] M. Myers, R. Ankney, A. Malpani, S. Galperin, C. Adams. *Internet X.509 Public Key Infrastructure. Online Certificate Status Protocol – OCSP*. Internet Engineering Task Force – Request for Comments 2560. 1999.

[21] *CEN Workshop Agreement CWA 14170 – Security Requirements for signature creation applications*. Comité Europeo de Estandarización (CEN). 2004.

[22] *ETSI TR 102 041 v1.1.1 Signatures Policies Report*. European Telecommunications Standards Institute. 2002.

[23] *CEN Workshop Agreement CWA 14171 – General guidelines for electronic signature verification*. Comité Europeo de Estandarización (CEN). 2004.

[24] Real Decreto-ley 14/1999, de 14 de Septiembre, de Firma Electrónica, Septiembre 1999.

[25] *ISO/IEC DIS 13888-1. Information technology – Security techniques – Non repudiation – Part 1: General model*. ISO/IEC JTC1/SC27 N1503, Noviembre 1996.

[26] J. Zhou y D. Gollmann. "Evidence and Non-repudiation". *Journal of Network and Computer Applications* vol. 20 (3), pp 267-281. ISSN:1084-8045. 1997.

[27] D. Lekkas, S. Gritzalis y L. Mitrou. *Withdrawing a declaration of Will: Towards a framework for Digital Signature Revocation*". Internet Research, vol. 15, nº 4, pp 400-420. 2005.

[28] A. Young y M. Yung. *Deniable Password Snatching On the Possibility of Evasive Electronic Espionage*. Proceedings of the IEEE Symposium on Security and Privacy vol. 4 (7), pp 224-235. ISBN: 0-8186-7828-3. 1997.

[29] D. Cooper. *A Model of Certificate Revocation*. Proceedings of the 15th Annual Computer Security Applications Conference, vol. 256. 1999.

[30] D. Cooper. *A more efficient use of Delta-CRLs*. Proceedings of the 2000 IEEE Symposium on Security and Privacy, pp 190–202. 2000.

[31] X. Wang y H. Yu. *How to Break MD5 and Other Hash Functions*. Advances in Cryptology – EUROCRYPT 2005, 24th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Lecture Notes in Computer Science, vol. 3494, pp 19-35. ISBN: 978-3-540-25910-7. 2005.

[32] H. Yu, G. Wang, G. Zhang1 y X. Wang. *The Second-Preimage Attack on MD4*. 4th International Conference on Cryptology and Network Security. Lecture Notes in Computer Science, vol. 3810, pp 1-12. ISBN: 978-3-540-30849-2. 2005.

[33] X. Wang, H. Yu y Y. Lisa Yin. *Efficient Collision Search Attacks on SHA-0*. Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference. Lecture Notes in Computer Science, vol. 3621, pp 1-16. ISBN: 978-3-540-28114-6. 2005.

[34] X. Wang, Y. Lisa Yin y H. Yu. *Finding Collisions in the Full SHA-1*. Advances in Cryptology - CRYPTO 2005: 25th Annual International Cryptology Conference. Lecture Notes in Computer Science, vol. 3621, pp 17-36. ISBN: 978-3-540-28114-6. 2005.

[35] *Timeline for Hash Algorithm Competition*. http://csrc.nist.gov/groups/ST/hash/timeline.html. National Institute of Standards and Technology.

[36] *ETSI TS 101 733 v1.7.3 Electronic Signatures and Infrastructures (ESI); CMS Advanced Electronic Signatures (CAdES)*. European Telecommunications Standards Institute. 2007.

[37] *ETSI TS 101 903 v1.3.2 XML Advanced Electronic Signatures (XAdES*). European Telecommunications Standards Institute. 2006.

[38] P. Kocher. *Timing Attacks on Implementations of Diffe-Hellman, RSA, DSS, and Other Systems*. Proceedings of Advances in Cryptology – CRYPTO '96. Springer-Verlag, pp. 104-113. 1996.

[39] Common Criteria. http://www.commoncriteriaportal.org