

E-Firma

Problemas de seguridad y privacidad asociados al DNI electrónico

1. Introducción

El pasado viernes 4 de abril se aprobó la Ley de Firma Electrónica, como marco regulador que habilitará el uso de la firma electrónica y los sistemas de identidad electrónica, en las relaciones con la Administración y entre particulares. Esta Ley permite el uso de la firma/DNI electrónico por parte de las personas físicas y jurídicas. Esta legislación está en consonancia a lo que se dice en el informe de la comisión "De la Sociedad de la Información", también conocida como comisión "Soto" y su intención es la de usarlo como motor para lograr el despegue de la sociedad de la información, e-gobierno y e-comercio. Conclusiones con las que estamos de acuerdo en parte, pero que como marco amplio, es necesario matizarlas y acotarlas. Al margen de que que estemos de acuerdo con lo que establece la comisión "Soto" y de la conveniencia de una legislación habilitante para la firma electrónica, el uso del DNI electrónico y de la firma digital, no es algo baladí y requiere un profundo estudio tecnológico y de oportunidad, evitando creer ciegamente en todo lo que nos dicen los fabricantes de estos dispositivos. En una decisión tan trascendental, por su alcance social y por el precio de la solución, sería conveniente contar con el asesoramiento de expertos independientes, que ayuden a tener una idea más imparcial del problema y faciliten la toma de decisiones.

Con el presente documento no queremos decir que la plataforma tecnológica elegida en España para el DNI electrónico no sea segura o inadecuada, simplemente queremos señalar los posibles riesgos, y vulnerabilidades de un sistema de este tipo, para que sean tenidos en cuenta por los responsables de su implementación. Por ello, tampoco pretende ser un documento definitivo, más bien el germen para un estudio más detallado y profundo, que de la mano de expertos independientes, permita obtener un sistema de DNI/Firma electrónica completamente seguro, estándar, compatible y satisfactorio para los ciudadanos.

2. Marco tecnológico probable

Parece ser que el marco tecnológico elegido en España para el DNI electrónico se basa en el uso de tarjetas inteligentes y según reza en la página web de la Fábrica Nacional de Moneda y Timbre (FNMT), estarán fabricadas en torno al chip SLE66CX320P de la empresa alemana Infineon Technologies, empresa relacionada con Siemens. Este chip que tiene un coste aproximado de 12 euros por tarjeta fabricada, cuenta con el certificado de evaluación de "alta seguridad" para el nivel E4 del "Information Technology Security Evaluation Criteria" (ITSEC) y está clasificado como de altas características, los de alta seguridad tienen la denominación SLE88CX720P. Según el fabricante este chip ha sido sustituido por otro más moderno, con la denominación SLE 66CX322P que tiene unas prestaciones similares. Aquí la primera alerta, en una aplicación de este tipo, no cabe una implementación que en función de la economía, sea razonablemente segura, o que se sacrifiquen determinados requisitos de seguridad, para lograr otras capacidades tecnológicas. El DNI digital debe ser completamente seguro y en el caso de dejar de serlo, debería dejar de usarse hasta que vuelva a serlo.

Este chip que pertenece a la familia 66Plus de Infineon. Se trata de un procesador de 16 bits fabricado con tecnología de 0,25 micrones. Está especializado en tareas criptográficas, por lo que puede procesar los algoritmos RSA con claves de hasta 2048 bits, en menos de 290 microsegundos, o trabajar con DES, triple DES y con criptografía de curvas elípticas. En su interior integra una gran cantidad de dispositivos, como un generador de números aleatorios por hardware, lógica de seguridad antimonitorización de datos y claves, una unidad de manejo de memoria (MMU), un generador de frecuencias (PLL), cifrado/descifrado DES/triple DES por hardware, dos temporizadores de 16 bits, un circuito de comprobación de redundancia cíclica (CRC) y la lógica de interrupciones del dispositivo. Para almacenamiento de datos y programas, cuenta con 32 Kb de memoria EEPROM, 64 Kb de memoria ROM y 3 Kb de RAM. Entre sus medidas de seguridad destacan un número de identificación único para cada chip, un dispositivo de encriptación/descriptación de memoria para la RAM, ROM y EEPROM, un generador de números aleatorios por hardware verificable internamente, una disposición de elementos optimizada para dificultar el acceso a los componentes, contramedidas para el análisis de fallos diferencial, la alimentación diferencial o de análisis simple de potencia y un blindaje activo con detección de ataques.

Además de lo que acabamos de decir, según cuenta el fabricante en la página http://www.silicon-trust.com/redirect.asp?path=/background/backgr_overview.htm, si en lugar del SLE66CX320P usamos un chip como el

Copyright 2003 Hispalinux

Se permite la copia y redistribución por cualquier medio y su traducción a cualquier idioma siempre que sea de forma íntegra incluyendo el autor y esta nota.

SLE66CLX320P, que tiene características similares al anterior, se dispondría de la capacidad RFID (Radio Frequency Identification). Esta tecnología, que es la misma a la utilizada en los dispositivos antirrobo de los comercios, en las llaves con inmovilizador electrónico de los coches, o en los chips para la identificación de animales de compañía, permite interactuar con la tarjeta sin necesidad de un contacto físico con ella. Dependiendo del modelo, nos podemos encontrar ante un dispositivo con interfaz dual, es decir, al que se puede acceder mediante unos contactos ISO/IEC 7816 estándar, o mediante un interfaz multimodo sin contactos ISO/IEC 14443, compatible con los Tipos A, B y Felica. La distancia máxima con la que se puede interactuar con estos dispositivos, varía con la frecuencia de transmisión y otros factores, como el ruido electrónico, la presencia de masas metálicas, o la potencia y sensibilidad del emisor/interrogador, etc, pero puede variar entre 60 centímetros y 2 metros.

3. Una historia llena de fallos y mentiras

Como veremos, no es oro todo lo que reluce en torno a estos dispositivos y a pesar de las certificaciones, estándares y pruebas a las que se someten, tenemos ejemplos que nos hacen reflexionar sobre su seguridad y el censurable comportamiento de algunos fabricantes. Comencemos viendo los cuatro tipos de ataques básicos:

1 Ataques de acceso directo a bus. Estos ataques que podemos considerar de alta tecnología, requieren retirar la capa de protección externa para poder acceder directamente al chip con la intención de observarlo, manipularlo o interferir su funcionamiento normal.

2 Ataques de software. Estos ataques usan la interfaz de comunicación estándar del procesador y explotan las vulnerabilidades que pudieran haber en los protocolos, en los algoritmos o en su implementación.

3 Ataque basado de monitorización con una elevada resolución en el tiempo. Mediante el control de temperaturas, radiaciones electromagnéticas, tensiones, consumos o variaciones en los buses durante el funcionamiento normal del dispositivos, se pueden identificar estados, contenido de la memoria, etc.

4 Ataques por generación de fallos. Estos ataques intentan que los dispositivos entren en situaciones para las que no fueron diseñados, generando funcionamientos anómalos que permitan el acceso.

Ejemplos del éxito de algunos de estos ataques los podemos ver en la prensa diaria o en Internet. Veamos ahora algunos de los más famosos:

a) En el año 1.998 la North American GSM Alliance negó rotundamente la posibilidad de clonar las tarjetas inteligentes usadas en los teléfonos GSM. Ese mismo año, la Smartcard Developer Association y un grupo de investigadores de la Universidad de Berkeley, demostraron todo lo contrario. Más adelante, se logró clonar un teléfono de la Pacific Bell y el CCC (Chaos Computer Club) en Alemania, también clonó un teléfono GSM del operador D2. Aquí tenemos una de las constantes observadas en torno al uso de las tarjetas inteligentes en aplicaciones de seguridad, ante un fallo, se niega, Lo malo es cuando alguien lo demuestra como veremos en la siguiente historia.

b) En el año 2000 Serge Humpich, un ingeniero francés, descubrió que la clave de seguridad usada por las tarjetas de crédito de determinada entidad financiera francesa, parece ser que por reducir su precio, usaban un chip de seguridad de bajas prestaciones, con una clave de solamente 320 bits. Este ingeniero logró factorizar dicha clave en 4 años y descubrió que podía fabricar una tarjeta de crédito falsa, que funcionase con independencia del número secreto de los usuarios y obtener así dinero de los cajeros de forma fraudulenta. Consciente de la importancia de su descubrimiento, contactó con la corporación (GIE) que fabricaba estas tarjetas y les avisó del problema. En aquel momento nadie le hizo caso y la empresa mantuvo una agresiva campaña de información, sosteniendo que el sistema era completamente seguro. A la vista de ello, Serge demostró que decía la verdad haciendo una pequeña operación con una tarjeta falsa fabricada por él mismo. Desgraciadamente, lo único que consiguió fue una denuncia por fraude e intrusión y se expuso a una pena de siete años de prisión, así como a una multa de mas de un millón de euros. De nuevo nos encontramos ante la negativa de las empresas a reconocer los fallos y lo que es peor, ante el uso de un dispositivo no adecuado. Como podemos ver, la seguridad del sistema es la del eslabón mas débil, en este caso era una clave demasiado corta pero puede haber otros. En estos sistemas cuenta todo, desde el chip con sus prestaciones y sus sellos de seguridad, al tamaño de la clave, pasando por el tipo de encriptación, o el hardware y el software asociados. De nada nos sirve una tarjeta muy segura si, por ejemplo, no lo son las interfaces con los programas, que por desgracia, no siempre están bajo el control del fabricante o del explotador del sistema.

c) Otro hecho curioso lo tenemos en las negativas de las empresas a la hora de reconocer brechas de seguridad en sus dispositivos. Más adelante se han demostrado ciertas cuando las empresas han añadido medidas para evitar estas mismas vulnerabilidades que en su momento calificaban como imposibles. Por ello, los modernos chips disponen buses y memorias cifradas, células fotoeléctricas, blindajes electromagnéticos, reguladores de tensión, generadores de frecuencia aleatorios, reguladores de tensión o controles de temperatura y muchos de ellos, después de negar su necesidad o conveniencia. Pero ¿qué habría ocurrido si estas vulnerabilidades no se hubieran hecho públicas y se estuvieran explotando secretamente?. A pesar de los esfuerzos de las empresas, algunas de estas soluciones no se han mostrado tan seguras como pretendían inicialmente los fabricantes.

d) Un caso más cercano lo tenemos en simulación, manipulación y copia de las tarjetas inteligentes usadas para controlar el acceso a los contenidos de televisión vía satélite. En Internet es fácil encontrar información detallada sobre su funcionamiento y sobre sus vulnerabilidades. Sobre este tema se ha hablado largo y tendido en muchos medios de comunicación y se ha llegado a decir que la competencia o los mismos fabricantes de las tarjetas filtraron la información que permitió piratear lo que en teoría era completamente seguro. La magnitud del fraude ha sido tal, que uno de los operadores no tuvo más remedio que cambiar sus tarjetas por otras que no presentasen los errores que se estaban explotando en ese momento, pero ¿pueden tener otros errores?, el tiempo lo dirá. De hecho estas tarjetas no son imposibles de criptoanalizar teniendo los medios adecuados y hay que señalar, que esta misma plataforma pasó por varias versiones de la tarjeta hasta que se logró una relativamente segura. Lo que está claro es que a lo largo de su corta historia, estas tarjetas no han sido todo lo seguras que decían sus fabricantes o explotadores y este hecho puede ser demoledor para en el caso de DNI electrónico.

4. Uso y funcionamiento

Para poder usar estas tarjetas debemos contar con un interfaz de bajo coste y adecuado, que permita comunicarse con la tarjeta y su uso asociado a sistemas informáticos. Mediante este interfaz podremos acceder a las claves públicas y privadas y a los datos contenidos en la tarjeta, mediante sistema operativo de gestión, que en el caso del DNI electrónico, ha sido desarrollado por la FNMT. Pero por el momento no sabemos si se utilizará un chip con tecnología RFID de la que ya hemos hablado, aunque hay rumores de que sí se usará. De todos modos no sabemos si solamente se identificará la tarjeta, o se podrá acceder a todas sus funciones de forma vía radio. Lo que está claro es que esta tecnología está disponible y aunque tiene sus ventajas, como veremos, también tiene sus riesgos para la intimidad de los usuarios.

En estas tarjetas la autenticación del usuario se realiza sobre la misma tarjeta, al igual que lo hacen las tarjetas de la televisión digital, que tampoco requieren el acceso a un servidor para autenticar el usuario. Podemos decir, simplificando las cosas, que una tarjeta inteligente es una llave en sí misma y se convierte en un dispositivo prácticamente autónomo a la hora de firmar o certificar la identidad del usuario. Esto significa, que su seguridad parte de la dificultad que debe haber para su clonación o manipulación. Posteriormente a la autenticación del usuario, se puede generar una firma digital mediante un procedimiento que puede ser una clave o un sistema biométrico. Hay que señalar que estas tarjetas permiten establecer áreas de memoria y jerarquías de claves, pudiendo usar una clave para autenticación del usuario y otra distinta para la generación de la firma, o para la realización de otras operaciones.

Antes de seleccionar una tarjeta inteligente para una determinada aplicación, hay que hacerse una serie de consideraciones como ¿qué aplicación se le piensa dar?. Está claro que no es lo mismo una aplicación financiera o una aplicación que necesita de una alta seguridad como un DNI electrónico, que una tarjeta para dar acceso a las instalaciones de una empresa, o para el pago de las llamadas en las cabinas de teléfono, de hecho, debería haber una tarjeta distinta para cada entorno. Una vez que tengamos claro el uso, podemos plantearnos la tecnología que deseamos utilizar. Una vez seleccionada la tarjeta, nos podemos plantear otros temas como la interfaz de acceso, el hardware asociado, o el sistema operativo que se usará internamente. Pero ante todo, debemos considerar la enorme diferencia que hay entre un mal llamado DNI electrónico y uno tradicional. Un DNI tradicional sirve para acreditar nuestra identidad ante terceros, pero no es capaz de firmar por nosotros. Sin embargo, el DNI electrónico, además de acreditarnos electrónicamente, es posible que sea capaz de señalar nuestra presencia remotamente y puede firmar en nuestro nombre mediante la autenticación adecuada del usuario. Este hecho tan trascendental, además se debe reflejar en toda la legislación asociada a su utilización y aunque parezca algo imposible o improbable, el usuario debe estar protegido ante los posibles malos usos de la tecnología, tanto por parte de los delincuentes como de la Administración, quedando bien claro lo que se puede y lo que no se puede hacer con el DNI digital.

Mientras que la pérdida o sustracción del DNI tradicional no supone un riesgo grave para el usuario ya que normalmente requiere su presencia para su utilización, puesto que es autenticado mediante la firma y la fotografía presentes en el documento, no es así con un DNI electrónico. En este caso, si se ve comprometida su seguridad, el DNI electrónico puede

ser usado por un tercero sin nuestro consentimiento, o conocimiento y con total independencia de nosotros, con el riesgo que ello supone. Además, debemos tener en cuenta que el DNI electrónico, por su naturaleza intrínseca, tendrá muchos más usos y funciones que las que tiene ahora un DNI tradicional, de hecho es lo que se pretende. Con ello aumentarán considerablemente los ámbitos de aplicación, el interés por el producto y sus funcionalidades y paralelamente, las áreas con un riesgo potencial para los usuarios.

La tecnología seleccionada para el DNI electrónico debe ser segura y flexible, para que dicha seguridad tenga continuidad en el tiempo. Por otra parte, el hecho de incorporar un chip, no debe eliminar la posibilidad de ser utilizado como DNI tradicional, por lo que deberá disponer todo lo necesario para actuar de este modo. Además, siempre que se establezca un sistema de gestión basado en el DNI electrónico, debe haber un procedimiento alternativo tradicional, para que su uso mayoritario no suponga un problema para los usuarios que tengan menos recursos, una reducida capacitación técnica o simplemente, no lo quieran utilizar en su faceta electrónica. Del mismo modo, se debería permitir al usuario, limitar los usos y funcionalidades que desea obtener con su DNI electrónico, hecho que sí se contempla para las personas jurídicas en la legislación vigente. Por ejemplo, el DNI electrónico se podrá utilizar ante un notario para la firma de escrituras públicas y otros documentos, pero este no es un uso del que sea necesario disponer a diario. El sistema debería permitir que el usuario pudiera activar o desactivar las operaciones que desea que se puedan realizar con su DNI electrónico o establecer un límite en la cuantía de las operaciones. De esta forma, en caso de fallo de seguridad, su uso estaría limitado a una serie de acciones definidas por su usuario. Estas opciones además de una medida de seguridad, sería una forma de limitar el abuso que se pudiera hacer con su uso por parte de empresas o instituciones.

5. Problemas de compatibilidad

Si se desean lograr los objetivos marcados por la comisión "Soto", es muy importante que estas tecnologías sean compatibles con la mayor parte del hardware y del software disponible en la actualidad. La única forma de conseguirlo es basando todo el hardware y el software relacionado en estándares abiertos y convenientemente publicados para general conocimiento. Tanto las administraciones como las empresas, deben ser capaces de realizar aplicaciones/hardware que utilicen estos dispositivos de autenticación y firma, con libertad y sin problemas derivados de especificaciones secretas, o de las patentes asociadas. Como es lógico, tanto el hardware como el software, deberá estar debidamente homologado y certificado por la Administración europea, y en especial, comprobando que no suponen un riesgo para la seguridad, libertad o la intimidad de los ciudadanos. En algunos casos, incluso se debería legislar su uso y tenencia, como por ejemplo, en el caso de las interfaces o los lectores remotos.

Los usos básicos del DNI digital serán la firma de documentos de correo electrónico, el acceso a información personal, la realización de transacciones en la red con la Administración o las empresas, etc. Por ello, es necesario garantizar, o como mínimo, facilitar la compatibilidad del hardware y del software asociado con todos los sistemas operativos y aplicaciones informáticas actuales y futuras. Lo que también funcionaría como un elemento de seguridad adicional, puesto que de descubrirse una vulnerabilidad en un determinado sistema operativo o programa, hasta su solución por el fabricante, se podría utilizar otro alternativo. Evidentemente, este objetivo no está al alcance de las administraciones europeas, pero como se ha dicho antes, de nuevo la solución pasa por la publicación de los estándares y de la información necesaria, para que los fabricantes puedan desarrollar el hardware y el software que sea necesario. No cabe duda que el monopolio sobre el uso del DNI electrónico, es algo que interesa a muchas empresas, por lo que las presiones comerciales no deben acabar limitando el uso del DNI electrónico a determinadas plataformas de hardware o software y en especial, si son propietarias. Es importante que haya competencia y libertad de elección en el hardware y en el software cuando se habla de un elemento básico y de uso tan generalizado como el DNI electrónico.

6. Problemas de seguridad

6.1 Seguridad por el oscurantismo/hardware

La seguridad basada en el oscurantismo tecnológico no son garantía de una seguridad absoluta, puesto que se con mayor o menor esfuerzo, se puede hacer ingeniería inversa y a partir de los resultados obtenidos, manipular o crear circuitos, que emulen el funcionamiento de estos dispositivos. Es más, si la seguridad se basa en el secreto de las especificaciones, tarde o temprano pueden haber filtraciones de información que comprometan el sistema completo. Ya hemos visto en los ejemplos que los sellos criptográficos de hardware no siempre han sido seguros y hay medios técnicos avanzados, que aunque caros, permiten analizar y manipular las criptotarjetas, aunque no siempre hay que recurrir a ellos, como ejemplo podemos poner las tarjetas de prepago para las cabinas de teléfono. En este caso, ante la dificultad de colonar o emular un sello criptográfico válido, se ha utilizado el de una tarjeta gastada y se le ha añadido una memoria manipulable, simulando a

la perfección una tarjeta que tiene permanentemente todo el saldo disponible.

6.2 Fallos no detectados

El hecho de que no se informen o conozcan fallos de seguridad en dispositivo, no significa que no existan, incluso en ocasiones, que no se estén explotando con éxito por los delincuentes. El no tener en cuenta este hecho puede ser muy peligroso para los usuarios, ya que es posible que ante un eventual problema y una reclamación judicial, que los peritos de la Administración, por desconocimiento de las vulnerabilidades, declaren que el sistema es completamente seguro. Esta situación, cuanto menos sorprendente, puede suponer un serio problema para los perjudicados, que pueden ser conscientes de las consecuencias, pero no de los medios o de la tecnología utilizada para lograrlo. Aunque hablaremos de ello más adelante, este hecho es especialmente preocupante cuando se compra una tecnología propietaria y protegida mediante secretos comerciales, que como se ha demostrado en algunos casos, puede ser insegura inadvertida o intencionadamente y las empresas en base a sus intereses comerciales, no reconocer los fallos de su sistema.

6.3 Condiciones de trabajo adversas

El uso de estos dispositivos en el mundo real, es un de sus grandes retos. En el caso del DNI electrónico estarán circulando millones de dispositivos que se verán sometidos a las condiciones de trabajo más variadas (alimentación o frecuencias inestables, espúreos, temperaturas, malos contactos en la interfaz, interferencias electrónicas, etc). En este exigente campo de pruebas, es muy fácil detectar vulnerabilidades y fallos. Ejemplos de ello los encontramos en muchos campos tecnológicos, uno de los más recientes, ha sido un fallo en una determinada serie de máquinas tragaperras, que ha permitido que algunas bandas organizadas utilicen una secuencia conocida, para obtener los premios de forma fraudulenta. Cualquier prueba u homologación, por exigente que sean, no se pueden comparar con el uso masivo de un dispositivo en las severas condiciones de la vida real y el escrutinio al que se verá sometido por parte de los usuarios. Es posible que se encuentren fallos y problemas que pasaron desapercibidos a los diseñadores y que pueden ser de difícil o imposible solución.

Dotar a toda la población española de un DNI electrónico, es un proyecto que puede necesitar tiempo, por ejemplo, en el caso de Bélgica, se estima que la migración durará unos 5 años. Durante este tiempo el mantenimiento de la seguridad se puede complicar con la convivencia de varias tecnologías, o por las distintas revisiones de un mismo producto, lo que provocará la necesidad de mantener un registro de versiones, usuarios y la localización de los mismos, por si hay algún fallo que obligue a cambiarles la tarjeta. Además, si se tiene en cuenta el coste de estas tarjetas criptográficas, que ronda entre los 5 y los 40 euros, al problema logístico de sustitución, se unen los problemas económicos. No cabe duda del enorme coste que puede suponer la sustitución masiva de tarjetas en el caso de observarse un fallo de seguridad que así lo aconseje. Hay que señalar, que dadas las características específicas y posibilidades de uso del DNI electrónico, la mera sospecha de un fallo de seguridad, debería ser suficiente para paralizar su utilización por los usuarios, hasta comprobarlo o subsanarlo. Aquí no son válidos los estudios estadísticos de vulnerabilidad y las consideraciones de que el fallo puede afectar a relativamente pocas personas, para estas personas, las consecuencias pueden ser terribles.

En el caso de producirse un fallo de seguridad, al realizarse la autenticación sobre la tarjeta, sin necesidad de acceso a ningún servidor, también será complejo, si no imposible, impedir cautelarmente las operaciones con el DNI electrónico, hasta que se solucionen los posibles problemas de seguridad de la plataforma. Señalemos que si se logran clonar los DNI electrónicos, o se rompen los sellos criptográficos, no será necesario disponer de las tarjetas originales, que pueden seguir en poder de los usuarios, lo que dificultará la detección del fraude. Incluso con un sello criptográfico de hardware, si se tiene acceso a la tarjeta original durante un determinado tiempo que depende del tamaño de la clave, se pueden establecer pruebas de desafío, como se hace con las tarjetas GSM, e intentar clonarlas, o emularlas, usando un hardware específico, distinto al original. Incluso se pueden usar sistemas mixtos utilizando en dispositivos caducados, perdidos o robados, para usar un sello criptográfico real, al que se le ha añadido la circuitería y la información necesaria, para que se comporte como un DNI electrónico válido.

6.4 Funcionamiento en el tiempo

Un proyecto de este tipo, dada su envergadura y problemas logísticos, debe estar pensado para perdurar en el tiempo. Al establecer estas tecnologías, se deben tener en cuenta los avances informáticos y en análisis criptográficos que puedan ser aplicables en cada momento. En el caso de un dispositivo como un DNI electrónico, que nos puede suplantar nuestra personalidad completamente y está capacitado para generar nuestra firma ante la Administración o terceros, no sirve que sea razonablemente seguro, o muy seguro, es indispensable que sea un sistema completamente seguro a cualquier nivel y además, debe mantener esta seguridad en el tiempo, sin que ello suponga un problema logístico o económico excesivo para la sociedad. Hay que tener en cuenta, dado el enorme número de dispositivos necesarios, los costes asociados a la posible necesidad de cambiar la infraestructura en el caso de producirse un problema de seguridad.

Debemos tener en cuenta la variabilidad y las incertidumbres del mercado del hardware y software en el tiempo. Por ello, es

Copyright 2003 Hispalinux

Se permite la copia y redistribución por cualquier medio y su traducción a cualquier idioma siempre que sea de forma íntegra incluyendo el autor y esta nota.

necesario resaltar la necesidad de un sistema abierto y libre que permita evolucionar y adaptarse al futuro, por improbable que pueda parecer, puesto que los costes asociados a los cambios tecnológicos pueden ser demasiado elevados. En todo caso, se debería partir de las suposiciones pesimistas en cuanto a esta evolución, para reducir el impacto de los costes en el futuro.

6.5 Puede llegar a ser un objetivo probable y codiciado

La existencia de un dispositivo de autenticación y firma, con la garantía del Estado, puede ser un buen revulsivo tecnológico, como pretende la comisión "Soto", una tecnología que anime a empresas e instituciones a diseñar productos y servicios basados en él. Por ejemplo, es posible que las empresas de crédito, sustituyan sus tarjetas actuales, por el DNI electrónico, como medio de autenticación de un usuario ante un cajero automático. Esto significa que también serán importantes los intereses económicos y la cuantía de las operaciones que rodearán al uso de estos dispositivos. Por lo tanto, cuanto mayor sean sus posibilidades de uso y las cuantías económicas que se muevan, su copia, manipulación, simulación, estudio y decodificación, se convertirán en objetivos prioritarios para las mafias tecnológicas. Estas mafias con expertos muy cualificados y dotados de grandes medios materiales, como ya lo han hecho con otras tecnologías que les han interesado, pondrán su punto de mira en estos dispositivos. Estas mafias, en caso de romper la seguridad de las tarjetas, intentarán mantener en secreto los posibles fallos de seguridad, aprovechando el desconocimiento de las vulnerabilidades por parte de las autoridades para trabajar impunemente. Incluso es posible que los técnicos de la Administración que pudieran actuar como peritos en juicios y pleitos, protegieran inadvertidamente a los delincuentes por el desconocimiento de lo que ocurre realmente.

6.6 Las políticas de generación de claves

Si queremos que los usuarios tengan confianza, hay que evitar que la clave pública y privada no estén nunca al mismo tiempo en poder de la Administración. Lo adecuado sería que fuera el usuario el que generase sus claves, y posteriormente fueran activadas y autenticadas por la Administración. Es importante garantizar que no hay puertas traseras y que no se usan tecnologías de "key scrow" en torno a todo lo que rodea a un producto tan importante y estratégico como el DNI electrónico. La seguridad del depósito de claves, se basa únicamente en la integridad de los funcionarios que las custodian, pero como personas humanas que son, no están exentas de defectos, errores y otras pasiones. Para la generación remota de claves se podrían utilizar aplicaciones certificadas, basadas en una tecnología basada en software libre denominada Live y se está desarrollando actualmente en Hispalinux. Esta tecnología permite arrancar un sistema operativo y unas aplicaciones certificadas, desde una unidad de CDROM. lo que garantiza la integridad del software.

6.7 Tecnología externa

Dada la importancia y la envergadura económica que supone el proyecto de dotar a todas las personas físicas y jurídicas de España de un DNI electrónico, consideramos especialmente importante que los chips de dichas tarjetas, sean fabricados en España, con tecnología propia, o licenciada, que sea perfectamente conocida y auditada, que evite la inclusión inadvertida o premeditada de vulnerabilidades y que permita su modificación en caso necesario.

Es necesario darse cuenta de que si no se hace de este modo, la Administración confiaría en lo que le dice una determinada empresa con sus intereses, alianzas, patentes, desarrollos y negocios. En cierta medida, se haría responsable, de avalar la seguridad de una tecnología que no controla y de la que es posible que no conozca todos sus detalles y secretos. Ni que decir, el daño que se produciría en la imagen del Gobierno y en el avance de la Sociedad del Conocimiento, del e-comercio y de la e-administración, si después de lanzar un producto como el DNI electrónico, al poco tiempo se revelase inseguro, incompatible o poco útil tecnológicamente. Por ello, insistimos que es indispensable que esta tecnología sea perfectamente conocida y controlada por la Administración que la implementa. Aquí, la independencia, tecnológica es fundamental, como en la fabricación de la moneda, hay riesgos no admisibles, que van más allá de la seguridad, por ejemplo, no se pueden dejar de suministrar chips, cambiar de tecnología, o modificar las compatibilidades y estándares, por problemas de patentes, convenios comerciales o quiebras empresariales.

La administración debe tener la certeza de que no hay, ni habrá, puertas traseras, llaves maestras para las claves, fallos de seguridad intencionados, ni nada que pueda poner en peligro la seguridad del sistema por un fallo de fabricación o la simple revelación de un secreto por parte de un empleado del fabricante de los chips. Recientemente se ha producido una reclamación judicial de una plataforma digital europea, acusando a otra plataforma, de desvelar un fallo de seguridad en su sistema criptográfico, lo que ha sido aprovechado para acceder a sus contenidos sin pagar. Esta información partió de un empleado de la empresa que fabricaba los chips criptográficos usados en las tarjetas, que vendió esa información a la empresa de la competencia, que a su vez, la hizo pública a través de los foros en Internet. Pero, si no somos independientes tecnológicamente, tampoco hay nada que nos garantice que una tecnología propietaria, que no controlamos y aparentemente segura, deje de serlo en el futuro por fallos en la fabricación, o por la inclusión de vulnerabilidades de forma maliciosa. De todos modos, ¿quién garantiza que la empresa que fabrica los chips no fabrica clones de los que ya se han fabricado? Es posible que la empresa sea seria y ponga los medios, pero no se puede descargar toda la seguridad de un

Copyright 2003 Hispalinux

Se permite la copia y redistribución por cualquier medio y su traducción a cualquier idioma siempre que sea de forma íntegra incluyendo el autor y esta nota.

sistema de DNI electrónico, en la fidelidad y buen hacer en los empleados de una empresa, posiblemente extranjera, posiblemente el riesgo sea remoto, pero un estado moderno no puede ser cautivo de ello.

6.8 Seguridad remota y limitaciones

También se deben tener en cuenta las limitaciones impuestas por estas tecnologías y los escenarios probables en los que se desarrollarán los usos por parte de los usuarios. Partiendo de la base de que una firma manual no es igual que una firma electrónica y que es complicado asociar el trazo manual, a la introducción de una palabra de paso de una longitud determinada. En primer lugar, aún estando a la vista, las firmas son complicadas de falsificar, mientras que una clave de 8 cifras, una vez conocida, puede ser introducida por cualquiera, una vez en posesión de la tarjeta adecuada. Recordemos que una simple cámara de vídeo, o un teclado manipulado, además de la ingeniería social pueden servir acceder a las claves previamente al robo de la tarjeta.

Aquí también hay que tener en cuenta, las limitaciones que tienen los usuarios a la hora de establecer y recordar las contraseñas de seguridad. Estas se deberían poder crear por el usuario, para facilitar su recuerdo, pero sobre una base de control de su calidad y caducidad periódica. Si se quiere que el sistema sea seguro y funcional, es indispensable iniciar una campaña de concienciación, educación y uso que minimice los fallos de seguridad derivados del mal uso o de la aplicación de técnicas de ingeniería social sobre los usuarios. Una solución alternativa a las contraseñas pueden ser los sistemas biométricos, de los que hablaremos más adelante. En ocasiones, estas tarjetas se usarán en ámbitos no controlados, como el hogar o en instalaciones no vigiladas, en los que cabe la posibilidad de coacción o amenaza. Por ello, la limitación voluntaria de la operativa posible con la tarjetas criptográficas, puede ser una buena medida de seguridad y de confianza para los usuarios. De todos modos, los desarrollos reglamentarios deberán tener en cuenta todos estos problemas y limitaciones, defendiendo al usuario ante estos casos y contemplando su posibilidad, aunque sea remota. No se debe legislar pensando en que el sistema es seguro y que siempre lo será, es necesario estar preparados para el caso de que no sea, o que deje de serlo en un determinado momento, protegiendo a los usuarios ante cualquier eventualidad.

6.9 Problemas derivados de la autenticación biométrica

Ante los problemas del uso de contraseñas y su relativa baja seguridad, parece ser que la alternativa más fiable son los sistemas biométricos. La mayoría de ellos se basan, por su simplicidad de implementación en la lectura de la huella dactilar, pero aunque dicha huella es única para cada usuario, lo cierto es que este sistema ya ha sido atacado con éxito. En el año 2002 un matemático Japonés usando materiales de bajo coste y de fácil acceso, logró, clonar y usar con éxito una huella dactilar presente en un vaso de cristal. A pesar de lo rudimentario de su método, logró un éxito del 80% en la falsificación. Por ello, también hay que ser cuidadosos a la hora de seleccionar un sistema biométrico, puesto que son caros y de complicada sustitución si falla y a fecha de hoy tanto el de huellas dactilares como el basado en la lectura del fondo de ojo, se han demostrado vulnerables. En la actualidad, uno de los más fiables y de más fácil implementación sería uno basado en la firma del usuario, que firmaría sobre una superficie sensible con un puntero especial. En este caso, los parámetros de velocidad, presión, tamaño del trazo y forma de la firma, lograrían identificar al usuario con un menor margen de error y sería más complicado de falsificar, puesto que en este caso la forma de la firma es un parámetro más a medir, pero no el único.

7. Consideraciones sobre los derechos de los usuarios

7.1 Uso y abuso de la detección remota

La detección remota puede ser útil para evitar falsificaciones y automatizar algunos procesos, como el control de accesos, cuando no es indispensable verificar la identidad de la persona que porta el dispositivo, o ya se ha realizado anteriormente mediante otros procedimientos. No obstante, mal utilizada esta tecnología, puede atentar seriamente la intimidad de los ciudadanos. Por ejemplo, colocando detectores en la entrada de comercios o instalaciones, se pueden controlar hábitos y costumbres, desarrollando una publicidad personalizada similar a la que se puede ver en la película "Minority Report". Con ello también proliferarán las bases de datos, oficiales o extraoficiales, con información detallada sobre los movimientos y preferencias de los usuarios, a la espera de casar el número de la identificación remota, con los datos personales del usuario y lograr así una identificación completa. Esta tecnología debería limitarse o eliminarse ya que se presta al uso y al abuso por parte de particulares, la Administración o incluso las fuerzas de seguridad del estado. Como norma general, se debería evitar que se hiciera uso de ninguna de las funcionalidades del dispositivo, sin conocimiento y autorización expresa del usuario que lo porta.

5.2 Problemas con la información contenida

Copyright 2003 Hispalinux

Se permite la copia y redistribución por cualquier medio y su traducción a cualquier idioma siempre que sea de forma íntegra incluyendo el autor y esta nota.

Si el DNI electrónico acaba en su evolución natural, conteniendo datos adicionales sobre el usuario, como información médica, históricos de transacciones, o información adicional a la que ahora consideramos como indispensable en un DNI tradicional, será muy complicado para el usuario controlar los accesos a dicha información y el contenido de la misma. Una vez que se ha introducido el dispositivo en una interfaz de lectura, estas funciones de lectura y escritura se pueden realizar sin que el usuario tenga conocimiento de ellas y es posible que sin que haya dado su autorización expresa para ello. Este motivo, se deben limitar los datos contenidos en el DNI y la información que contiene se debería poder consultar de forma transparente por los usuarios y evitando el almacenamiento de información sensible que se pueda utilizar fuera del ámbito establecido para ello, sin conocimiento y consentimiento expreso del usuario.

8. Recomendaciones

Por todo lo anterior, consideramos que se debe realizar un estudio minucioso de las distintas soluciones disponibles, que es necesario obrar con mucha cautela, puesto que el coste total de implantación es muy elevado por lo que sería deseable:

- a) Que antes de proceder a la implantación de esta tecnología se establezcan unos mínimos indispensables de alfabetización tecnológica y de acceso a la Sociedad del Conocimiento, que se deberán materializar en tantos por ciento de la población total.
- b) Que sea una solución abierta, basada en estándares internacionales y compatible con cualquier aplicación, plataforma o sistema operativo, permitiendo a los desarrolladores y fabricantes, la elaboración sus propias soluciones de software y hardware. La utilización de software libre y sus herramientas de seguridad, consideramos que son indispensables para lograr estos objetivos con eficacia, rapidez y economía. Teniendo en cuenta que los lectores no solo van estar conectados a PC's, sino que también se conectarán a otros dispositivos como TPV's, PDA's, Teléfonos, cabinas, etc, es indispensables elaborar planes para que los programadores puedan competir en igualdad cuidando los siguientes aspectos:

* **Libertad de acceso a las especificaciones**

* **Existencia de una interfaz de referencia, de libre acceso**

* **Necesidad de homologación de las aplicaciones desarrolladas**

* **Integración de expertos independientes en todas las fases del desarrollo y planificación.**

Además, dado el enorme factor de escala, mantener una tecnología propietaria sujeta a las presiones de los fabricantes, puede redundar en unos elevados costes de mantenimiento e implantación que acaben haciendo inviable su uso.

c) Que se base en una tecnología de la que la Administración conozca su funcionamiento a la perfección y sobre la que tenga la posibilidad de introducir modificaciones en caso necesario, sin tener que recurrir a la autorización o a la ayuda del la empresa que lo diseñó. En todo caso, no se debería adoptar ninguna solución que no estuviera disponible a través de un mínimo de dos fabricantes, evitando siempre, la firma de convenios de exclusividad o de acuerdos de no revelación.

d) Que igual que se desarrolla una legislación habilitante para el servicio, se desarrolle una reglamentación de protección del usuario, que contemple el mal uso, los abusos y los posibles fallos de seguridad de esta tecnología, aunque inicialmente se consideren improbables. En cualquier caso, se debería legislar la posibilidad de revocar las operaciones realizadas con estos sistemas dentro de un tiempo establecido legalmente.

e) Que el usuario pueda elegir los servicios que desea obtener con el uso de esta tecnología, dejando constancia oficial de los que se tienen activados o desactivados en un determinado momento. Al mismo tiempo se mantendrán los sistemas tradicionales, para aquellos usuarios que lo necesiten.

Copyright 2003 Hispalinux

Se permite la copia y redistribución por cualquier medio y su traducción a cualquier idioma siempre que sea de forma íntegra incluyendo el autor y esta nota.

- f) Que se elija una tecnología en caso de fallo de seguridad, se pueda desactivar su utilización a todos los niveles y que permita su actualización de forma remota, evitando o paliando, los problemas logísticos y los costes asociados a necesidad de una sustitución masiva. Estas actualizaciones deberá realizarse mediante un sistema tecnológico que sea seguro y verificable por el usuario, evitando que se realicen actualizaciones falsas o que dejen el dispositivo inoperativo. La tecnología debe permitir la realización de cambios en el software y en el tamaño de las claves, para garantizar su vigencia en el tiempo. Las tarjetas se deben poder desactivar a petición del usuario, en el caso de que sean robadas o perdidas.
- g) Que se eliminen las prestaciones que puedan suponer un riesgo para la intimidad o libertad de los usuarios, tales como información adicional almacenada, o el acceso y detección remota de los dispositivos.
- h) Que la generación de claves se realice mediante un método que garantice que solamente el usuario pueda tener la clave pública y privada al mismo tiempo y que garantice que no existen puertas traseras, debilidades en la longitud de las claves, o la existencia de claves maestras.
- i) Que necesiten una comprobación de seguridad, homologación y autorización administrativa previa, todos los servicios que se deseen implantar usando como base de autenticación y/o firma el DNI electrónico.
- j) Que todo el software y hardware asociado a estos dispositivos, esté certificado homologado y verificado por la Administración Europea. En algunas aplicaciones críticas se debería exigir el uso de esos dispositivos asociados a sistemas de verificación biométrica, como alternativo o complementario a las claves, preferentemente asociados a la firma manual, que a fecha de hoy, es el sistema que se ha demostrado como el más fiable.
- k) Garantizar que el ciudadano conoce y tiene la posibilidad de ajustar la "versatilidad" de su DNI electrónico, pudiendo deshabilitar en cualquier momento aquellos usos que no desee utilizar.

En este sentido, Hispalinux se ofrece para colaborar en la consecución de una Sociedad del Conocimiento Libre para todos.

Junta Directiva de Hispalinux