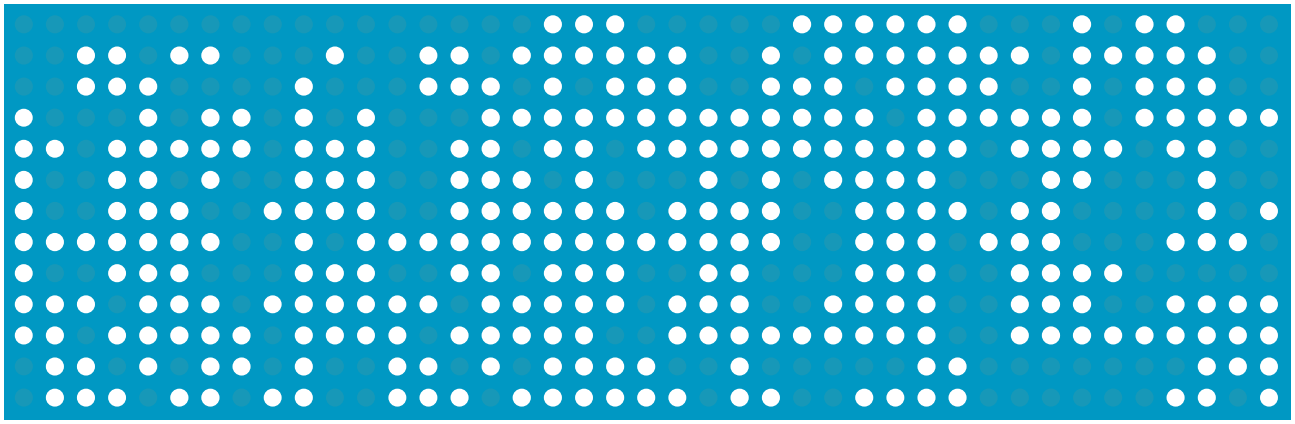
MINISTERIO
DE INDUSTRIA, TURISMO
Y COMERCIO

red.es
observatorio

ESTUDIO DE SERVICIOS PARA LA EMPRESA ASOCIADOS A LA IMPLANTACIÓN DEL DNI ELECTRÓNICO



red.es observatorio

Índice

red.es
observatorio

1. INTRODUCCIÓN

El Observatorio de las Telecomunicaciones y de la Sociedad de la Información, centro de referencia para el análisis y seguimiento de la Sociedad de la Información en España, ha liderado la elaboración de este estudio, que analiza los posibles **usos del DNIe en transacciones mercantiles privadas**, con la finalidad de elaborar un **conjunto de propuestas que sirvan de impulsoras de la Sociedad de la Información**.

Debido a la escasez de información de mercado, ya que España es un país pionero en este ámbito, y no existen experiencias comparables en otros países, se propuso una metodología basada en un análisis prospectivo. La prospectiva sirve de ayuda para la toma de decisiones en un ámbito tan novedoso, como el que nos ocupa, y por lo tanto, con un alto grado de incertidumbre. Por este motivo, para la elaboración de este análisis sobre el uso del DNI electrónico en transacciones mercantiles privadas, ha sido muy importante el papel de expertos que cuentan con una dilatada experiencia en el desarrollo de la Sociedad de la Información en diversos sectores de actividad.

Los expertos han intervenido en el proyecto de dos formas; mediante la realización una entrevista personales en las que se trataron temas directamente relacionados con su área de actividad o negocio, así como en grupos de trabajo, en los que se han reunido a los expertos conjuntamente, con el objetivo de recabar opiniones y consideraciones de personas de diferentes áreas de conocimiento y situar sus aproximaciones a la evolución de la tecnología en el marco de la evolución económica y social.

Los objetivos planteados para el proyecto se pueden resumir en:

- Compartir las iniciativas identificadas en el ámbito del DNIe aplicado a la empresa privada.
- Identificar nuevas iniciativas en este ámbito y reflexionar sobre las mismas.
- Avanzar en el análisis de la viabilidad de las distintas iniciativas desde el punto de vista:
    - Técnico, tanto a nivel software como hardware: disponibilidad de librerías, hardware necesario, infraestructura y servicios básicos, ect.
    - Operativo y de procedimiento: Análisis de la necesidad de reingeniería y diseño de procesos y operaciones tanto interno de la entidad que provee el servicio como de uso o aceptación del tipo de servicio.
    - Normativo y legal: Análisis de viabilidad según la normativa vigente, de necesidad de cambios normativos o necesidad de legislación que de cobertura a posibles nuevos usos.

Este estudio se ha centrado en los usos del DNIe en el sector privado, ya que en las Administraciones Públicas, ya existen gran cantidad y diversidad de servicios que se están ofreciendo a través de Internet de manera segura, haciendo uso de los certificados

de firma electrónica en general, y del DNIe. en particular. Es un hecho que muchos de estos servicios que necesitan de autenticación fuerte del usuario o de firma electrónica se ofrecen ahora utilizando el DNIe como elemento de autenticación o de firma.

En la dirección www.dnielectronico.es del Ministerio del Interior, Dirección General de la Policía y Guardia Civil, se ofrece una lista de servicios a los cuales se puede acceder utilizando el DNIe.

Es importante destacar, como se ha mencionado en los párrafos anteriores, el doble uso del DNIe como tanto como elemento de autenticación (Acreditación de la Identidad) como de de firma electrónica (Acreditación de la Voluntad). Esta versatilidad en el uso, derivada del carácter electrónico del DNIe, complementa los usos habituales del DNI tradicional, cuyo uso se limitaba a la Acreditación de la Identidad mediante su exhibición física.

La potencialidad del DNIe radica en esta ampliación de la funcionalidad tradicional que ofrece el DNI en entornos presenciales al mundo electrónico y que se sustenta en la incorporación de un chip criptográfico y la utilización de sistemas de clave pública (PKI, del inglés *Public Key Infraestructure*) que permiten, a través de la utilización de certificados digitales, ofrecer en entornos electrónicos servicios restringidos hasta ahora a los entornos presenciales.

Este aspecto se materializa en que el DNIe dispone de dos certificados electrónicos que permiten:

- **Autenticación**: autenticación fehaciente de la identidad del titular del DNIe, que permite asegurar su identidad en entornos no presenciales.
- **Firma electrónica reconocida**: con idéntica validez a la conferida a la firma manuscrita de acuerdo a lo establecido en la Ley 59/2003, de Firma Electrónica que permite, mediante el acto de la firma, acreditar la voluntad del firmante titular del DNIe.

Conviene destacar esta doble funcionalidad que ofrece el DNIe, ya que todos los posibles usos que se analizarán a continuación se basan, bien en una sola de estas características, o en ambas, con objetivos diferentes.

red.es
observatorio

2. CONCLUSIONES OBTENIDAS

Las conclusiones obtenidas tras las reuniones con expertos se enfocan hacia aspectos que se entienden, desde todos los sectores participantes, como determinantes para el uso masivo del DNIe. Igualmente, las entrevistas han puesto de manifiesto tanto algunas dificultades para la utilización masiva del DNIe, como la percepción de algunas lagunas sobre su aplicación en casos concretos. Esto se debe a que existen condicionantes operativos que no se encuentran, en la actualidad, suficientemente cubiertos, o bien la percepción por parte de los posibles actores promotores del DNIe no es clara, sobre todo desde el punto de vista legal.

Una de las primeras y más claras conclusiones que cabe destacar es que no se prevé, tras la implantación del DNIe, la aparición inmediata de nuevos actores, sino que los actores ya existentes operando en Internet, complementarán y mejorarán su oferta de servicios, tanto para sus clientes actuales como para no clientes, por lo menos hasta que el grado de despliegue e implantación del DNIe supere una cierta masa crítica.

Es decir, no se prevé una expansión en amplitud de nuevos servicios, sino en profundidad, por parte de las empresas que actualmente implementan servicios a través de Internet.

Esta situación es idéntica a la producida en las Administraciones Públicas, donde los primeros usos del DNIe se han asociado servicios ofrecidos previamente mediante la utilización de certificados digitales. En estos casos a la gama de certificados digitales, ya utilizados se ha añadido el DNIe. Es decir, no se han creado específicamente nuevos servicios sino que se ha incorporado el DNIe a servicios ya existentes.

No obstante, es necesario tener presente que el DNIe integra en un único soporte físico un mecanismo de identificación ampliamente utilizado en la vida diaria (ámbito presencial) y un mecanismo de identificación digital (certificado de firma electrónica). De esta forma, los ciudadanos españoles disponen de un mecanismo de Identidad Digital para operar telemáticamente con seguridad, facilidad de uso y, esto es muy importante, con la garantía del Estado. Se rompe así una importante barrera cultural al uso del certificado de firma digital al incorporarlo en un elemento de identificación presencial al que los españoles estamos completamente habituados lo que permite vislumbrar un despegue en el número de usuarios de servicios de la Sociedad de la Información tanto públicos como privados.

En esta línea, dos de los primeros sectores donde parece claro el uso del DNIe son el sector financiero y el de seguros. En el caso concreto de la banca, éste es uno de los sectores que más ha apostado por la utilización de nuevas tecnologías y por la diversificación de canales a través de los cuales ofrecer servicios a sus clientes.

En el caso de las empresas de seguros su uso es muy similar al planteado en banca, destacando la firma telemática de contratos de seguros, sin presencia física de las partes.

En ese sentido, los servicios inicialmente planteados para el entorno financiero son:

Uso del DNIe	Condicionantes críticos	Disponibilidad temporal
Autenticación en operaciones de banca electrónica		Corto plazo
Firma de operaciones o contratos en banca electrónica		Corto plazo
Autenticación de usuario y firma de operaciones en cajeros	Disponibilidad de librerías DNIe para cajeros	Corto/medio plazo
Uso en TPVs: autenticación de usuario y firma de operación	Disponibilidad librerías DNIe para TPVs Disponibilidad de teclado para introducción del PIN	Medio plazo
Usos en oficinas, en modo presencial	Revisión de los flujos de trabajo internos de las entidades	Largo plazo

El sector de las telecomunicaciones móviles también ha mostrado un gran interés en la utilización del DNIe, sobre todo en las posibilidades que abre, combinado con certificados software que se descarguen en el teléfono móvil para la firma electrónica en este tipo de dispositivos.

Uso del DNIe	Condicionantes críticos	Disponibilidad temporal
Solicitud de un certificado que se descargue en el móvil – firma en el móvil	El certificado software debe ser emitido por un prestador de servicios de certificación reconocido	Corto plazo / medio plazo
Autenticación y firma de operaciones en servicios a través de Internet.		Corto plazo

Desde el punto de vista de la empresa, también se aprecia un interés en el uso del DNIe en los procedimientos internos de la empresa:

Uso del DNIe	Condicionantes críticos	Disponibilidad temporal
Control de acceso - tarjeta de empleado	Adaptación de los tornos de acceso a lectura con chip ¿Necesidad de introducción del PIN?	Largo plazo
Firma en flujos de trabajo internos	Adaptación de los procedimientos internos de la empresa al tratamiento electrónico de la información firmada	Medio plazo
Uso para voto telemático en los consejos de administración		Corto /medio plazo

Además de los anteriores, separados por entornos concretos, durante las reuniones con los expertos han aparecido otros posibles usos del DNIe:

Uso del DNIe	Condicionantes críticos	Disponibilidad temporal
Uso del DNIe como tarjeta de control de acceso físico: Edificios públicos, aeropuertos, eventos deportivos, espectáculos etc.	Necesidad de disponer de un teclado y lector orientado al usuario para introducir el PIN, sí como librerías específicas para su uso en tornos, etc.	Corto / Medio / largo plazo en función del sistema de control de acceso
Identificación en sistemas de juego on-line	Analizar la legislación sobre juego on-line	Medio plazo
Compra de entradas	Disponibilidad de kioscos de recogida de entradas con lector de tarjetas chip y teclado para introducción del PIN	Corto / medio plazo
Firma de contenidos digitales	Definir el formato de la firma para su	Medio Plazo

	reconocimiento como prueba de autoría del contenido digital	

Las reuniones con los expertos, no sólo han permitido definir un grupo de usos del DNIe sino que han puesto sobre la mesa retos en la utilización del mismo o aspectos en los que es necesario avanzar para conseguir un mayor grado de utilización del DNIe y su universalidad como método de autenticación y firma electrónica

Necesidad de introducción del PIN alfanumérico para acceso a cualquier dato de los certificados	Este aspecto dificulta la utilización del DNIe en elementos que no dispongan de un teclado alfanumérico. Podría plantearse que para el acceso al certificado de autenticación no fuese necesario el PIN y sólo lo fuese para la firma
La existencia de dos certificados puede causar confusión en el usuario	Este punto sólo puede mitigarse mediante campañas de divulgación de lo que significa el DNIe y la autenticación vs la firma, así como que las aplicaciones que hacen uso del DNIe detecten qué certificado necesitan en cada operación y no dejen esa decisión a criterio del usuario.
Falta de librerías para algunos entornos de uso como TDT, PDAs, TPVs, etc.	Este punto debe solucionarse bien mediante el desarrollo por parte de la DGPyGC de librerías para todos los entornos demandados por el mercado o bien mediante la liberación de la información necesaria para que las empresas del mercado que lo deseen desarrollen los *drivers* necesarios
Diferencia entre los periodos de caducidad del soporte físico del DNIe (tarjeta) y de los certificados almacenados en el chip criptográfico.	Esta diferencia de periodos de caducidad puede causar confusión en los usuarios o hacer que se les caduque el certificado porque no recuerden su fecha de caducidad. Para resolver este tema sería necesaria una modificación legal del texto que recoge la duración del DNI y/o de la ley de firma que especifica el plazo en el cual la

	renovación de certificados debe ser presencial. También podría paliarse esta limitación si la DGPyGC enviará algún tipo de comunicación (similar a lo que hace tráfico cuando se aproxima la caducidad del carné de conducir) anunciando que los certificados del DNIe están próximos a caducar. De lo contrario la responsabilidad de recordar el periodo de renovación de los certificados recae en el usuario.
Desconocimiento general de la funcionalidad del DNIe	Esto puede reducirse mediante campañas de divulgación del contenido del DNIe, de los certificados que contiene y su objeto, de su funcionalidad y de en qué entornos puede utilizarse.
Desconocimiento jurídico sobre el tratamiento de la información firmada digitalmente y la custodia de la prueba electrónica, así como de que se ha realizado la validación del certificado	Existe desconocimiento entre muchos actores sobre el modo en que deben tratarse los documentos firmados electrónicamente y su conservación en el tiempo, así como el tratamiento de los registros de auditoria en el caso de las validaciones de certificados. En general, no se tienen claros los requisitos legales que deben cumplirse y sería necesaria una campaña de divulgación en este sentido.
Preocupación por la capacidad de proceso de las entidades de validación del DNIe	Ante la previsible explosión en el uso del DNIe, existe cierta preocupación sobre si las entidades de validación actuales (MAP y FNMT) serán capaces de responder a un crecimiento exponencial del número peticiones de validaciones de certificados, así como los tiempos de respuesta de estos servicios. Está prevista la incorporación de, al menos, una tercera entidad de validación (Red.es).
No disponibilidad de acceso a los datos que aparecen impresos en el exterior del DNIe	La utilización del DNIe está limitada a los datos que se pueden obtener de los

(fotografía, huella, etc.)	certificados electrónicos, que son nombre y apellidos, número de DNIe y fecha de nacimiento. No están disponibles el resto de datos que se encuentran en el chip en un área protegida.

En apartado sucesivos de desarrollan en más profundidad cada uno de esta ideas.

red.es
observatorio

3. ANÁLISIS DETALLADO DE LOS OBJETIVOS CONSEGUIDOS

A continuación se detalla con mayor profundidad cada uno de los posibles usos detectados y que aparecen resumidos en el apartado 2 de este documento. Para cada uno de los usos del DNIe propuestos se realiza un análisis que contempla:

- Descripción del uso o funcionalidad propuesta.
- Consideraciones y actores actuales, previo al uso del DNIe.
- Descripción del uso mediante la utilización del DNIe.
- Condicionantes técnicos.
- Condicionales legales.
- Condicionantes operativos y de facilidad de uso de la solución.
- Conclusión sobre el uso concreto.

3.1. Autenticación en banca electrónica

Actualmente la mayoría de entidades financieras ofrecen a sus clientes servicios de banca electrónica con acceso autenticado mediante un par usuario y contraseña. Además lo habitual es que un usuario disponga de parejas usuario y contraseña diferentes para cada entidad con la que opera.

La autenticación mediante el par (usuario, contraseña) es uno de los mecanismos de autenticación más utilizados en la identificación de usuarios a través de medios electrónicos, informáticos y telemáticos. Este mecanismo se apoya en un sistema basado en “lo que sé” en el que el usuario se identifica mediante el uso de un “nombre de usuario” y una “contraseña” que previamente ha memorizado. Por lo tanto, el único elemento de autenticación utilizado en este caso, es algo que el usuario “conoce”. Este hecho implica, en un principio, que la única forma de obtener la contraseña del usuario sería mediante el uso de alguna técnica o engaño para conseguir que el usuario la revele. Este tipo de técnicas conocidas como “Ingeniería Social” han de ser tenidas muy en cuenta con ataques a este método de autenticación.

No solamente la ingeniería social es la única debilidad relacionada con este tipo de autenticación, sino que también existen otro tipo de debilidades (ataques del tipo “fuerza bruta”, phising, etc.) que están sufriendo cada vez más las entidades financieras.

Algunas entidades añaden lo que se denomina una autenticación mediante dos factores, complementando el par usuario y contraseña con una tarjeta de claves, por ejemplo, con lo cual se pasa de mecanismos basados en “lo que se” a mecanismos de doble factor basados en “lo que se” y “lo que tengo”.

El DNIe permite incrementar el nivel de seguridad en las operaciones de acceso, ya que proporciona una autenticación basada en “lo que tengo”, el propio DNIe, y “lo que se”, el PIN, y basada en certificados digitales almacenados en el chip del DNIe. Además este mecanismo que aporta universalidad desde el punto de vista del usuario, ya que es una solución que podría utilizarse en las diferentes entidades financieras con las que trabaje utilizando el mismo soporte, el DNIe y su PIN.

Por lo tanto, el método de autenticación en banca electrónica mediante el DNIe aporta, a las entidades financieras, un mayor nivel de seguridad y permite paliar ataques mediante ingeniería social o phising, además de la utilización de certificados, y desde el punto de vista del usuario, le permite mantener un solo método de autenticación en las diferentes entidades con las que opere.

3.1.1. Utilización del DNIe como método de autenticación

El proceso de autenticación utilizando el DNIe como método de acceso sería el siguiente:

- El usuario accede a su servicio de banca electrónica donde se le solicita el acceso con certificado (con el DNIe).
- El usuario introduce su DNIe en su lector de tarjetas y se le solicita que teclee su PIN de usuario.
- La entidad financiera accede a los datos del certificado de autenticación del DNIe y comprueba que el usuario está dado de alta en el servicio y valida su PIN.
- Realiza una validación del certificado del usuario para comprobar que no se encuentra revocado.
- En función del resultado anterior permite o deniega el acceso a la aplicación de banca electrónica.

Para poder efectuar un acceso a banca electrónica mediante el DNIe tal como se describe en este apartado anterior es necesario tener en cuenta algunas consideraciones.

3.1.2. Condicionantes técnicas

Desde el punto de vista del usuario, es necesario que éste disponga de un lector de tarjetas chip en su equipo para poder acceder a los datos electrónicos del DNIe. Además del lector, con sus librerías instaladas, es necesario descargarse e instalarse un software proporcionado por la DGPyGC que permite el acceso a los datos del DNIe.

Este software contiene las librerías criptográficas que permiten el acceso a los datos del chip del DNIe, y que deben instalarse para el sistema operativo y navegador de los que disponga el usuario. Actualmente están disponibles las librerías que aparecen en la página oficial del proyecto, www.dnielectronico.es, para los sistemas operativos: Windows, GNU/Linux y Mac OS.

La necesidad de que el usuario disponga de un lector de tarjetas chip, que cumpla las especificaciones PC/SC, se ha planteado tradicionalmente como un reto o dificultad para el despliegue de este tipo de tecnologías basadas en tarjetas chip. Sin embargo, desde nuestro punto de vista, más que un problema de coste o de disponibilidad (actualmente en el mercado existen diferentes tipos de lectores a un coste asequible), se trata de un problema de falta de información del usuario, que no entiende porqué debe adquirir un periférico con su ordenador sin un uso claro hasta la fecha.

El progresivo despliegue del DNIe, así como de las tarjetas financieras EMV que también disponen de chip, habituará a los usuarios al uso de estas tecnologías y parece previsible que en cuanto se perciban las posibilidades que ofrecen estas tecnologías, el coste del lector no debe ser un problema, incluso pueden aprovecharse campañas, tanto de la Administración como de las entidades financieras, para ofrecer lectores a los ciudadanos sin coste o a coste simbólico.

Por parte de las entidades financieras, es necesario que desarrollen su módulo de control de acceso a banca electrónica para que permita el acceso con certificados y disponer además de un mecanismo de validación de los certificados del DNIe así como de conectividad con la entidad de validación del mismo.

Actualmente, como entidades de validación de los certificados del DNIe se encuentran el Ministerio de Administraciones Públicas (MAP), orientado a transacciones en el entorno de la Administración y la Fabrica Nacional de Moneda y Timbre (FNMT), que ofrece servicios al entorno privado. Parece aconsejable que exista el menos un tercer validador del DNIe para poder absorber el tráfico previsto cuando se complete el despliegue del DNIe en todo el territorio nacional.

Otro aspecto a tener en cuenta es el formato de la validación del certificado, ya que si la validación se realiza a mediante el protocolo OCSP, y el resultado es un *token* OCSP, existe inquietud en el entorno financiero sobre la validez jurídica de este tipo de respuestas, en caso de litigio.

Una posible solución a este problema pasaría por que el *token* OCSP devuelto como resultado de la validación de un certificado del DNIe, fuese firmado e incluyese un sello de tiempo de la entidad emisora (entidad de validación).

3.1.3. Condicionantes legales

Desde un punto de vista legal, debe recogerse en los contratos con los usuarios la posibilidad de utilización del DNIe para acceso a los servicios de banca electrónica, y establecerse las responsabilidades de cada una de las partes.

Por el usuario:

- Custodiar su tarjeta DNIe y su contraseña.
- Comunicar a la entidad emisora de la tarjeta y los certificados, es decir a la DGPyGC, cualquier pérdida, robo o compromiso de las claves, pera proceder a la inmediata revocación de los certificados.

Por la entidad:

- Comprobar la vigencia del certificado en el momento de la transacción.

3.1.4. Condicionantes de uso

Desde el punto de vista de la operatividad de la solución y de su facilidad de uso, este método de autenticación facilita el proceso de autenticación al usuario, ya que éste no debe recordar un par usuario y contraseña sino tan sólo la contraseña o PIN del DNIe. Además aporta universalidad, ya que si se populariza el acceso a servicios digitales con autenticación a través del DNIe, el usuario sólo debe recordar su PIN de acceso al DNIe y no una contraseña por cada servicio como ocurre en la actualidad.

Por parte de las entidades financieras, este método de autenticación no supone una gran modificación en sus procesos operativos actuales, por lo que su implementación no debiera ser problemática.

Un aspecto a prever por parte de las entidades financieras es que si un usuario decide acceder a los servicios de banca electrónica a través de este método, y por algún motivo no dispone coyunturalmente de él (perdida, deterioro del chip o simplemente en caso de viaje y no tener acceso a un lector), debe plantearse si se va a permitir el acceso mediante un método alternativo al servicio sin el DNIe o se le va a negar el acceso al mismo.

3.1.5. Conclusiones

De acuerdo a lo expuesto en los apartados anteriores, el acceso a los servicios de banca electrónica a través del DNIe se plantea como un uso factible, relativamente sencillo de implementar y que podría comenzarse a ofrece a corto plazo por parte de las entidades financieras (algunas entidades incluso han empezado a ofrecer ya el servicio).

3.2. Firma de transacciones o contratos en banca electrónica

Al igual que en el caso anterior, la firma de transacciones en operaciones de banca electrónica es un servicio que se ofrece por parte de las entidades financieras mediante la introducción de una contraseña o clave de operaciones generalmente distinta de la contraseña de autenticación.

En el caso de los contratos, lo que se ofrece a través de los servicios de banca electrónica es la posibilidad de pre-contratar con la opción de imprimir el contrato correspondiente, firmarlo en modo manuscrito y enviarlo por correo a la entidad financiera. Es decir no se puede cerrar el ciclo de contratación on-line.

La incorporación de la firma electrónica reconocida que ofrece el DNIe aporta mayores garantías de seguridad en el caso de la firma de operaciones y permite cerrar el proceso de contratación en un sólo paso, ya que la firma electrónica del DNIe tiene la misma

consideración que la firma manuscrita de acuerdo a la legislación vigente de Firma electrónica.

3.2.1. Utilización del DNIe para firma electrónica

La utilización del DNIe para firmar electrónicamente transacciones o documentos se desarrollaría, una vez accedido el servicio de banca electrónica correspondiente:

- Se le presenta al usuario el documento a firmar o los datos de la transacción junto con un botón de firmar.
- El usuario pincha el botón de firmar lo que genera la firma electrónica del documento. En el proceso de generación de la firma debe validarse la vigencia del certificado que aporta el usuario.
- Se presenta al usuario la posibilidad de almacenar la transacción firmada o la huella electrónica de la transacción y en el caso de un documento el almacenamiento del mismo.

3.2.2. Condicionantes técnicas

Al igual que en el apartado anterior, es necesario que el usuario disponga de un lector de tarjetas instalado con sus librerías, así como las librerías criptográficas del DNIe (ver consideraciones al respecto en el apartado 3.1.1).

La entidad financiera debe disponer de un software de firma electrónica que realice la operación de la firma y almacene el resultado de acuerdo al formato de firma que se decida (por ejemplo Xades).

En el momento de la firma es necesario comprobar la vigencia del certificado, por lo que aplica lo comentado en el apartado anterior 3.3.1.

3.2.3. Condicionantes legales

Desde un punto de vista legal, el certificado de firma electrónica del DNIe tiene la consideración de certificado reconocido, por lo que la firma electrónica generada por el DNIe tiene la consideración de firma electrónica reconocida. Por su parte el chip del DNIe está certificado de acuerdo a la norma *Common Criteria* como dispositivo seguro de creación de firma, lo que hace que se cumplan los requisitos que establece la ley de firma Electrónica para reconocer la misma validez en una firma electrónica que en una manuscrita.

Un aspecto a tener en cuenta y, que se ha visto reflejado en las mesas de trabajo, son los requisitos legales que deben aplicarse a la custodia de los documentos o contratos firmados electrónicamente y cómo se solventa la problemática de almacenamiento y verificación que su larga su larga vigencia temporal conlleva. Este aspecto es

especialmente importante si se plantean operaciones financieras a largo plazo como pueden ser créditos.

Es necesario establecer las garantías de los documentos firmados electrónicamente durante toda el tiempo que sea preciso. Para ello existen diferentes soluciones algunas de las cuales pasan por la selección de entidades externas o terceros de confianza que realicen la función de custodia segura de documentos y realicen las operaciones de re-firma necesarias según se vayan agotando los periodos de seguridad criptográfica de las claves. No obstante, se perciben en las entidades financieras muchas incertidumbres en todo lo relacionado con estos procesos sobre todo desde el punto de vista legal.

Otro aspecto a considerar es que el DNIe no contiene una dirección electrónica que permita la remisión segura de datos, ni permite la lectura de los datos externos (domicilio), lo cual dificulta la notificación necesaria en transacciones.

3.2.4. Condicionantes de uso

Desde un punto de vista de facilidad de uso, por parte del usuario no es necesario más que introducir su PIN en el momento de la firma, así como tener la posibilidad de almacenar el documento firmado o recibirlo por correo electrónico, mientras que por parte de la entidad, es necesario incorporar la capacidad de tratar documento electrónicos firmados en el flujo de trabajo de la entidad, así como resolver el tema de la custodia anteriormente comentado.

3.2.5. Conclusiones

La firma electrónica de transacciones o de documentos o contratos mediante el DNIe es un uso perfectamente factible del mismo que puede implementarse en el corto plazo por parte de las entidades financieras.

3.3. Autenticación de usuario y firma de operaciones en cajeros

La utilización del DNIe en los cajeros automáticos de las entidades financieras se basa en los dos mecanismos que ofrece el DNIe: la autenticación de usuario y la firma electrónica.

La autenticación de un usuario en un cajero a través de su DNI, permite ofrecer servicios de reintegro de efectivo sin disponer de una tarjeta financiera de la entidad propietaria del cajero, siempre que se disponga de una cuenta en dicha entidad.

Otra servicio que necesita autenticación de usuario es el denominado *Halcash*, con el que actualmente operan diversas entidades financieras. Este sistema permite enviar dinero a un cajero automático, de forma instantánea y gratuita, a cualquier hora y a cualquier lugar donde exista un cajero de las entidades adheridas al sistema.

El beneficiario del pago no necesita una tarjeta para retirar su dinero del cajero, sólo un teléfono móvil.

El funcionamiento es el siguiente:

- Se inicia la orden de pago a través cualquiera de los diferentes canales que la entidad financiera del ordenante tiene disponible: Internet, Banca Telefónica, cajeros, oficinas, teléfono móvil o a través de SMS. En todos ellos se debe indicar la cuenta de cargo, el importe a enviar, el concepto del pago, el número del móvil del destinatario y una clave secreta de 4 números escogida por quien autoriza el pago.
- Se comunica al destinatario, por el medio que desee, la clave secreta que ha elegido.
- El destinatario recibirá en su móvil un SMS indicándole el nombre del pagador, el importe recibido y, por seguridad, una segunda clave, también de 4 dígitos.
- El destinatario podrá acudir a cualquier cajero de las entidades asociadas al servicio y, presionando el botón de *Halcash* que figura en ellos, retirar el dinero gracias a la introducción de: su número de móvil, las 2 claves recibidas y el importe enviado. Todo ello sin necesidad de utilizar ninguna tarjeta ni ser cliente de la entidad.

El destinatario dispone de 10 días a partir de la fecha de envío para retirar el dinero. Si el dinero no es retirado por cualquier motivo se devuelve el importe enviado a la cuenta del ordenante

La utilización del DNIe del receptor de la operación simplificaría la misma, ya que el titular que autoriza el reintegro, sólo tendría que indicar el DNIe del receptor de la misma, y en el cajero donde el receptor acude a por el reintegro se verificaría su identidad mediante el DNIe.

Otra posibilidad que aparece con la utilización del DNIe en los cajeros es la de ofrecer servicios que requieran de firma electrónica, como firma de contratos de nuevos productos o servicios de la entidad, autorizar pago de tributos, etc. En definitiva cualquier transacción que requiera de una firma electrónica reconocida del usuario que realiza la transacción.

3.3.1. Condicionantes técnicos

El primer aspecto a contemplar es la necesidad de que los cajeros dispongan de lector de tarjetas chip. Aprovechando el proceso de adopción de la tecnología EMV para las tarjetas de débito y crédito, la mayoría de entidades financieras ya han incorporado el lector de chip a sus cajeros, por lo que esto no debería ser un problema.

Los cajeros de la mayoría de entidades financieras funcionan en base a la tecnología WOSA/XFS o J/XFS (*Windows Open System Architecture eXtension for Finantial Services o Java eXtensión for Financia Services*). Las librerías de que actualmente se dispone para el DNIe no contemplan su utilización en estos dispositivos, salvo que se pueda acceder a los periféricos del cajero, concretamente al lector de tarjetas, a través de *drivers* Windows como si se tratase de un lector USB, aspecto que es necesario analizar en detalle.

Al no existir librerías oficiales para estos entornos, no se puede utilizar el DNIe en cajeros hasta que no se disponga de las mismas.

Otro aspecto a tener en cuenta es que el PIN del DNIe es de tipo alfanumérico, con posibilidad de contener mayúsculas, minúsculas, números y caracteres especiales; los cajeros automáticos (salvo modelos concretos) no disponen de teclado alfanumérico, por lo que tendrían que desarrollarse módulos de teclado virtual para mostrar éstos en pantalla, y bien a través de pantalla táctil o moviéndose con las teclas laterales poder introducir el PIN del DNIe. Esto puede resultar especialmente molesto para los usuarios y, además, en caso de que el teclado no permita distinguir bien qué tecla se pulsa en cada momento, podrían producir errores en al introducción del PIN o incluso bloqueos.

Un aspecto estrictamente técnico a revisar es que la mayoría de cajeros detectan que tienen una tarjeta en la ranura leyendo la banda magnética de la misma y una vez detectada la banda, se tragan la tarjeta y se accede al detalle de los datos de la banda o del chip. En el caso del DNIe, al no llevar banda magnética, podría no activar el cajero y por tanto no tragar la tarjeta y no poder acceder a los datos del chip. Algunas entidades están incorporando lectores de tarjetas chip externos, que no se tragan la tarjeta completamente solventando estos problemas.

La utilización del DNIe en cajeros pasa por resolver la cuestión de la relación entre el titular del DNI y la cuenta contra la que desea operar. En el caso de las tarjetas de crédito y débito, la propia tarjeta identifica la cuenta asociada, además del titular, al que se valida mediante el PIN de la misma.

En el caso del DNIe se identifica al titular pero no se tiene constancia de contra qué cuenta quiere operar. Este punto se complica si estamos en una operación de intercambio, es decir cuando un cliente de una entidad utiliza un cajero de otra entidad; desde el cajero no hay manera de saber contra qué entidad debe operar una vez identificado el titular.

Sería necesario que existiera un intermediario que asociara DNIs con cuentas financieras, de modo que ante una petición en un cajero, éste preguntara al nodo de intermediación de DNIs contra qué cuenta debe operar el cajero y proceder a solicitar la autorización de la operación. Este nuevo intermediario, competiría con los actuales intermediarios de operaciones de débito y crédito que son Servired, 4b y Euro 6000.

3.3.2. Condicionantes legales

Dado que las operaciones a realizar en el cajero son las mismas que las indicadas en los apartados anteriores, autenticación y firma, aplican las mismas consideraciones legales que en los casos anteriores.

Un punto a destacar, específico de los Cajeros, es que en la mayoría de ellos la tarjeta desaparece de la vista mientras dura la transacción, es decir, el cajero se “traga” la tarjeta hasta que se finaliza la/s operación/es. Esto no presentaría mayor problema salvo en el caso de que por un malfuncionamiento del cajero, éste se quedara con la tarjeta, ya que en este caso se estaría reteniendo el DNI del usuario y una entidad financiera no tiene base legal para retirar un DNI, lo que podría ser motivo de litigio.

3.3.3. Condicionantes de uso

Desde un punto de vista de usuario, la necesidad de tener que introducir el PIN del DNIe tanto para autenticación como para la firma, puede provocar cierto rechazo si la pantalla del cajero no ofrece buena visibilidad o no se detecta con claridad qué tecla se está seleccionando en cada momento. Otro punto a analizar es la receptividad de los usuarios para utilizar el cajero para firma de operaciones o contratos nuevos, ya que no parece un terminal especialmente diseñado para ello, es más habitual utilizarlo para reintegros de efectivo.

3.3.4. Conclusiones

La utilización del DNIe en los cajeros está condicionada a la resolución de los puntos que aparecen anteriormente y en particular a disponer de librería adecuadas para su uso en cajeros, por lo que se podría plantear como un uso a medio plazo.

3.4. Autenticación de usuario y firma de operaciones en TPV

La utilización del DNIe en los Terminales Punto de Venta (TPV) presenta las mismas dificultades que en el caso de los cajeros, con la dificultad añadida de que en este caso es aún más complicado disponer de un teclado para poder introducir el PIN del usuario.

3.4.1. Condicionantes técnicos

Al igual que en el caso de los cajeros, la mayoría de entidades financieras ha migrado sus TPVs a chip debido a la adopción de la tecnología EMV, por lo que la necesidad de disponer de un lector de tarjetas chip en el TPV no debiera se un problema.

El problema radica en que no existen librerías específicas para el uso del DNIe en TPV, y éstos no soportan las librerías oficiales suministradas por la DGPyGC, por lo que el uso del DNIe en estos dispositivos está pendiente de la disponibilidad de dichas librerías.

Otro aspecto a resolver es la necesidad de introducir el PIN del usuario, alfanumérico, para el acceso a los certificados. Los TPVs no disponen de teclado, ni de una pantalla lo suficientemente visible como para plantearse un teclado virtual, por lo que las únicas opciones serían las de incorporar un teclado externo (si esto fuera posible) o la de utilizar un teclado de tipo análogo al de los teléfonos móviles sobre el numérico del TPV.

3.4.2. Condicionantes legales

Dado que las operaciones a realizar en el TPV son las mismas que en los apartados anteriores, autenticación y firma, aplican las mismas consideraciones legales que en los casos anteriores.

3.4.3. Condicionantes de uso

Los usuarios están muy acostumbrados a la operativa de tarjeta de banda magnética, por lo que cambio de modo de uso pudiera necesitar de un cierto tiempo de adaptación, en particular la necesidad de introducción del PIN.

Igualmente, por parte de los comercios es necesario una periodo de adaptación para acostumbrarse a tramitar otro tipo de transacciones en las que en lugar de presentar la boleta a firmar se le solicita al usuario que introduzca el PIN de su DNI.

3.4.4. Conclusiones

La utilización del DNIe en TPVs, debido a los problemas planteados anteriormente, no parece que sea operativa hasta medio/largo plazo.

3.5. Uso del DNIe en oficinas en modo presencial

El uso del DNIe no debe restringirse sólo a entornos telemáticos, sino que ofrece una serie de opciones también en el mundo presencial. El esquema que se plantea es la utilización del DNIe de los usuarios, cuando se personan en una oficina para realizar un trámite, de esta manera podría iniciarse el trámite de manera electrónica, almacenando la información generada por la entidad financiera en modo electrónico y realizando las firmas necesarias por parte del usuario como firma electrónica.

Esta utilidad del DNIe evitaría el almacenamiento de todos los expedientes asociados a un trámite, que suelen ir acompañados de fotocopias del DNI de los participantes, así como diversos formularios firmados. La realización de estas operaciones de modo electrónico disminuiría el tratamiento de papel en la entidad, y facilitaría el intercambio y la disponibilidad de la información entre sedes y oficinas de una manera mucho más ágil.

3.5.1. Condicionantes técnicos

Por parte de la entidad financiera, debe adaptarse el puesto de oficina para una relación interactiva entre el usuario y el empleado. Es decir, debería disponerse de al menos dos teclados con lector de tarjeta, así como de doble pantalla para que en todo momento el cliente entienda el proceso que se está llevando a cabo.

Igualmente, deberían modificarse las aplicaciones de relación con los clientes para que permitir la gestión electrónica de la información. Una vez completado el trámite y

solicitadas la/s firma/s electrónica/s necesarias, se podría entregar al cliente una copia impresa de la transacción o bien ofrecerle el envío en modo electrónico de la información.

3.5.2. Condicionales legales

Desde un punto de vista legal, el soporte de la firma electrónica es claro y el único aspecto a considerar, es la custodia electrónica de los documentos firmados. Es necesario contemplar que algunas operaciones financieras como los préstamos, por ejemplo, mantienen su vigencia en un plazo temporal muy amplio y debe resolverse la custodia longeva de los documentos firmados.

3.5.3. Condicionantes operativos

Desde un punto de vista operativo, la gestión de un trámite en modo electrónico aunque se produzca en un entorno presencial supone un cambio de percepción de la operación por parte de los usuarios, que están acostumbrados a la gestión del papel en las transacciones. Igualmente, el cambio en la forma trabajo de las entidades supone una revisión de los flujos de trabajo, diseñados para el almacenamiento de la información en formato impreso y no en formato electrónico.

3.5.4. Conclusiones

Si bien las mejoras que suponen esta modalidad de trabajo son evidentes, existe un cierto riesgo percibido por el cambio en la modalidad de trabajo pasando a la gestión electrónica, por lo que no parece que salvo alguna experiencia concreta se planteen este tipo de operaciones hasta un plazo medio/largo.

3.6. Uso para petición de certificados que se descarguen en el teléfono móvil

El incremento en la utilización de dispositivos móviles ha hecho plantearse, principalmente a las operadoras móviles, la posibilidad de utilizar el dispositivo móvil como elemento de autenticación y firma electrónica.

Es evidente que los dispositivos que se ofrecen actualmente en el mercado, salvo alguna rara excepción en forma de accesorio, no disponen de lector de tarjetas externo que permita insertar el DNIe en ellos. Por ello la utilización directa del DNIe en el móvil es imposible, en tanto bien los teléfonos incorporen un lector externo, algo que no parece probable de acuerdo a las tendencias de diseño de los móviles. Otra posibilidad es que el eDNI cambie de formato aproximándose al de una tarjeta SIM o bien se permita almacenar un certificado emitido por la Autoridad de Certificación de la Policía en una tarjeta SIM, algo que tampoco parece probable.

El planteamiento realizado por las operadoras móviles consiste en la utilización del DNIe como elemento de acreditación de la identidad para solicitar un certificado software a través de Internet, y que éste certificado se descargue en el teléfono móvil. Si la entidad de certificación emite un certificado de firma electrónica reconocida, es decir, es un prestador de servicios de certificación reconocido, el certificado descargado en el móvil tendría la consideración de certificado derivado y heredaría la fortaleza de registro de haberse realizado la petición del mismo mediante el DNIe.

De esta manera, se evita el procedimiento de registro presencial que está recogido en la ley de firma para la solicitud del DNIe y podría utilizarse el móvil como dispositivo de firma electrónica reconocida.

3.6.1. Consideraciones técnicas

La petición de certificado a través de Internet, sería una operación de autenticación y firma electrónica similar a la descrita en los apartados 3.1 y 3.2 de este documento.

Adicionalmente, la entidad emisora del certificado debería ser un prestador de servicios de certificación de acuerdo a lo establecido por la ley de firma electrónica.

Desde el punto de vista del usuario, sería necesario disponer de un terminal móvil con capacidad de gestionar certificados, bien en la tarjeta SIM, o bien a través de la tarjeta de memoria que estos dispositivos incorporan.

En cualquiera de los casos, tanto para la tarjeta SIM como para la tarjeta de memoria, éstas deben disponer de la capacidad de almacenamiento tanto de los certificados como de librerías criptográficas para la gestión de los mismos desde el dispositivo móvil.

Por otra parte sería necesario desarrollar aplicaciones que permitan la utilización de certificados en el teléfono móvil.

3.6.2. Consideraciones legales

Desde un punto de vista legal, al utilizarse el DNIe para solicitar el certificado, se hereda la fortaleza del registro del DNIe por lo que la operación de solicitud y firma de la solicitud sería equivalente a la presencial y, si la entidad de certificación que emite el certificado es un prestador de servicios de certificación reconocido, la firma electrónica emitida por el dispositivo móvil sería una firma electrónica reconocida, con todas las consecuencias que ello conlleva.

3.6.3. Consideraciones de uso

Los usuarios están bastante habituados a la utilización de dispositivos móviles por lo que esta nueva funcionalidad no debiera suponer ningún problema de uso.

3.6.4. Conclusiones

Dado que ya existen productos que permiten la gestión de certificados tanto en tarjetas SIM como en tarjetas de memoria, este uso podría ponerse en funcionamiento a corto / medio plazo por parte de las operadoras de teléfonos móviles.

3.7. Autenticación y firma de operaciones y contratos a través de Internet

Aunque este uso se planteó por parte de los operadores móviles, la autenticación y firma de contratos a través de Internet en otros entornos es similar a la planteada en el caso del sector financiero, desarrollada en los puntos 3.1 y 3.2.

Este tipo de utilidad del DNIe es aplicable a cualquier sector que opere en Internet y tenga necesidad de autenticar a sus usuarios y/o realizar operaciones de firma de transacciones, contratos, etc.

Entre los sectores a los que aplicaría esta funcionalidad podrían encontrarse los servicios de las operadoras móviles, las *utilities*, los servicios de agencias de viajes, líneas aéreas, etc.

3.8. Control de acceso de empleados

El DNIe podría utilizarse como tarjeta de control de acceso para empleados en empresas. De esta manera se evitaría la emisión de tarjetas específicas para controlar el acceso a las empresas. En algún grupo de trabajo se ha mencionado la posibilidad de que el DNIe dispusiera de un chip sin contactos, similar al que se incorpora al pasaporte, de modo que se pudiera utilizar la tarjeta como tarjeta sin contactos.

Actualmente, sin embargo, esta utilidad está limitada al control de acceso a través del chip con contactos y la utilización del certificado de autenticación para determinar la identidad de la persona que desea acceder.

Adicionalmente, al ser necesaria la introducción del PIN para el acceso a los datos del certificado, deberían proveerse de lectores de tarjeta chip con teclado en los puntos de control de acceso, lo que resta agilidad a la solución, si bien se simplifica el procedimiento de accesos ya que todos los empleados y visitas que dispongan del DNIe lo utilizarían para acceder a la sede correspondiente.

3.8.1. Condicionantes técnicos

La mayoría de los sistemas de control de acceso a instalaciones o edificios están basados en tecnologías sin contactos, por lo que sólo es necesario acercar o posar la tarjeta en el lector para que se verifique la identidad de la persona que quiere acceder y se le permita o deniegue el acceso.

Como el DNIe no dispone de tecnología sin contactos, deberían modificarse los lectores de los tornos o sistemas de fichaje, para permitir la lectura de los certificados del DNIe y a su vez, sería necesario disponer de una librería que permitiera su utilización en el dispositivo concreto en el que va instalado el lector.

Igualmente sería necesario que se dispusiera de un teclado para poder introducir el PIN de usuario, salvo que se dispusiera de una librería que no solicitara el PIN para la lectura de los datos del certificado de autenticación.

3.8.2. Condicionantes legales

Al ser un uso estrictamente privado entre el empleado y la empresa, y no utilizarse firma electrónica, sino sólo autenticación, debería resolverse en la normativa propia de la empresa.

3.8.3. Condicionantes de uso

Desde el punto de vista de los usuarios, si la empresa dispone de control de acceso basado en tecnología sin contactos, el utilizar el chip del DNIe con contactos puede considerarse como un paso hacia atrás que resta agilidad el proceso.

También se ha detectado que algunos empleados no ven con buenos ojos la utilización de un elemento que consideran personal en el entorno laboral, y consideran que la empresa debería proveerles de los elementos necesarios para el acceso al lugar de trabajo.

3.8.4. Conclusión

La utilización del DNIe como elemento de control de acceso a empresas podría considerarse un uso factible a corto / medio plazo, si bien para ser efectivo es necesario que se resuelvan los condicionantes técnicos mencionados anteriormente.

3.9. Firma en flujos de trabajo internos a la empresa

El DNIe permite realizar operaciones de firma electrónica en los flujos de trabajo internos de la empresa lo que agiliza la propia tramitación de los procedimientos internos de la empresa.

Para poder operar de esta manera, la empresa debe adaptar sus procedimientos internos a la tramitación electrónica y disponer de un sistema de gestión documental que permita la gestión y custodia de documentos electrónicos firmados digitalmente. Esto supone normalmente la adquisición de un sistema de gestión documental que se integre con los procesos internos de la empresa para conseguir una disminución de la gestión de información en formato papel.

3.9.1. Condicionantes técnicos

Desde un punto de vista técnico, la mayor complejidad de esta solución se encuentra en al integración del sistema de gestión documental con los procedimientos internos y la gestión de la validación de los certificados de usuario en cada transacción.

La utilización de la firma electrónica en el entorno empresarial hace si cabe más importante la necesidad de disponer de entidades de validación de certificados que soporten una utilización masiva del DNIe.

Un punto a tener en cuenta es que el DNIe identifica al usuario como persona física, pero no le identifica como representante o le asocia a su cargo en una persona jurídica (empresa o entidad). En muchos procedimientos internos de la empresa es necesario que la firma sea del cargo que tiene la responsabilidad para firmar, por lo que debe verificarse la capacidad de firma de la persona.

Este punto puede resolverse mediante la utilización de un directorio o repositorio común que almacena los atributos asociados al cargo de la persona, atributos a los cuales se podría acceder mediante el certificado de autenticación del usuario y una vez determinado si tiene capacidad de firma electrónica, se le permitiría o denegaría ésta.

El mantenimiento y la actualización de este tipo de sistemas de directorio resulta fundamental y crítico para asociar en cada momento a un usuario con su cargo o capacidad de firma.

3.9.2. Condicionantes legales

Desde un punto de vista legal, y al estar utilizando la funcionalidad de firma electrónica, este uso está amparado por la ley de firma electrónica que reconoce el DNIe como dispositivo seguro de creación de firma y le otorga la posibilidad de creación de firma electrónica reconocida.

Sería necesario regular a nivel normativo interno de la empresa en qué casos es necesario y/o obligatorio el uso del DNIe en los procedimientos internos de la misma.

3.9.3. Condicionantes de uso

Desde el punto de vista de los usuarios, la operación de firma electrónica con el DNIe es sencilla de realizar, sin embargo en algunas experiencias con otras tarjetas chip, se ha detectado que algunos empleados no ven con buenos ojos la utilización de un elemento de identificación que consideran de uso personal, como es el DNIe, en el entorno laboral y opinan que la empresa debería proveerles de los elementos necesarios para el acceso al lugar de trabajo.

3.9.4. Conclusión

La utilización del DNIe como método de firma en los procesos internos de la empresa podría considerarse factible a medio/largo plazo en función de la capacidad de la empresa en adaptar sus procedimientos internos a la tramitación electrónica.

3.10. Voto telemático en los consejos de administración

Este es un caso particular del punto anterior, donde aplica la firma electrónica a un procedimiento interno de la empresa, como es la votación en el Consejo de Administración, por lo que las consideraciones que aplican a nivel técnico, legal y de uso son similares.

Tan sólo destacar que en este caso es especialmente importante el disponer de acceso a la información sobre la capacidad de firma de una persona en el consejo de administración, es decir el mantenimiento de directorios o bases de datos que permitan asociar a una persona con el poder notarial correspondiente y pon ende su capacidad de firma.

3.11. Uso para control de acceso físico

El DNIe permite la identificación electrónica con certificado de su titular, lo que permite que se utilice el chip para acceder a los datos del mismo sin necesidad de tener que teclearlos.

Si se piensa en la gran cantidad de ocasiones en que debemos identificarnos en un punto de control de acceso y lo hacemos mediante la presentación del DNI o la presentación de otro tipo de pase que nos permita el acceso, podemos concluir que en estos puntos sería factible la identificación electrónica a través del DNIe.

En principio, y sin ser exhaustivos, este tipo de uso podría darse en:

- Acceso a edificios públicos que exigen autenticación.
- Acceso a eventos deportivos, congresos, ferias, etc.
- Acceso en aeropuertos, puertos, etc.

En cualquiera de los casos, es necesario identificar a la persona que desea acceder y decidir si se le permite la entrada o no a un determinado recinto, no obstante cabe diferenciar dos tipos de acceso:

- Acceso a entornos en lo que es necesario una autenticación fuerte, como puede ser aeropuertos o zonas de seguridad, donde si que aplica la utilización del DNIe con introducción del PIN del usuario.

- Accesos a espectáculos o eventos multitudinarios, donde prima la agilidad en el proceso de control de acceso frente a la seguridad y donde no sería aplicable la introducción del PIN del usuario por la lentitud del proceso.

Para realizar operaciones de control de acceso físico mediante el DNIe, es necesario disponer de elementos que permitan la lectura del chip del DNIe en función del tipo de acceso, bien a través de tornos o en accesos presenciales permitir el acceso.

En el caso de acceso a edificios, lo habitual es que se introduzcan los datos del visitante en un sistema de gestión de visitas que almacena durante un tiempo los datos de las personas que han accedido al edificio.

En el caso de acceso a eventos deportivos, congresos o ferias, lo que se pretende es evitar el tener que disponer de un pase específico, y que el torno o elemento que controla el acceso sea capaz de leer los datos del DNIe, consultar con una base de datos si debe facilitar el acceso, y permitir o denegar el mismo.

Para poder actuar de esta manera, es necesario que se pueda acceder a los datos del DNIe, en concreto al certificado de autenticación, sin necesidad de introducir el PIN del usuario, de lo contrario no resultaría un sistema ágil en caso de eventos multitudinarios.

3.11.1. Condicionantes técnicos

Para poder acceder a los datos del DNIe es necesario que los dispositivos de control de acceso dispongan de un lector de tarjetas chip, así como de las librerías necesarias para poder acceder al certificado del DNIe. Si los dispositivos son tipo torno o barrera es necesario desarrollar una librería específica para el dispositivo.

También es necesario que el sistema de control de acceso esté basado en DNIe y se sustituya la emisión de pases específicos por el uso del DNIe y la consulta a una base de datos.

En el caso de acceso a edificios, es necesario simplemente disponer de un lector orientado al usuario, así como de un teclado para introducir el PIN.

3.11.2. Condicionantes legales

Desde un punto de vista legal, es necesario cumplir con los requerimientos de la LOPD para el tratamiento de la información personal del usuario.

3.11.3. Condicionantes de uso

Para poder operar en controles de acceso de manera ágil, es necesario disponer de una librería que no haga necesario que el usuario teclee el PIN del certificado de autenticación, ya que de lo contrario se restaría agilidad al proceso y se provocarían colas de acceso.

3.11.4. Conclusiones

La facilidad para la utilización de estos servicios con el DNIe, depende del servicio concreto. Así y para el control de acceso a edificios dado que normalmente el sistema que lo gestiona ya es un sistema PC, sería relativamente sencillo lanzar este tipo de iniciativas.

En el caso de acceso a ferias, eventos o espectáculos deportivos, depende del sistema de control de accesos de que dispongan y de la disponibilidad de librerías específicas para dicho sistema, por lo que se puede plantear este tipo de uso del DNIe a medio / largo plazo.

Como acción específica en este uso del DNIe podría proponerse la utilización del DNIe como método de control de acceso en la Expo 2008 de Zaragoza, como escaparate internacional de uno de los usos del DNIe.

3.12. Identificación para la compra de bienes o servicios por Internet (entradas, vuelos, etc.)

La compra de bienes o servicios a través medios telemáticos es un servicio que ya se está ofreciendo actualmente. Normalmente está asociado al uso de tarjetas de crédito, pero podría ofrecerse también a través del DNIe, ya que bastaría con que la identificación del titular que compra, por ejemplo la entrada, por Internet se realizara mediante el DNIe, con lo que al recogerlas, bien en un kiosco o en ventanilla, el usuario podría también identificarse mediante el DNIe.

Esto permitiría separar el medio de pago de bien o servicio adquirido del sistema de identificación en la recogida del mismo.

3.12.1. Condicionantes técnicos

Desde un punto de vista técnico, sería necesario que el kiosco donde se recogen las entradas o la ventanilla, o el lugar donde se reciba el valor adquirido dispusiera de un lector de DNIe que accediera a los datos del certificado de autenticación y verificara que se corresponde con el usuario que realizó la adquisición de la entrada.

3.12.2. Condicionantes legales

No presenta ningún condicionante legal específico ya que simplemente se incrementa el nivel de seguridad respecto a un sistema que ya se está ofreciendo en al actualidad.

3.12.3. Condicionantes de uso

La operativa es sencilla, ya que basta con identificarse mediante el DNIe en el momento de la compra de las entradas y en el momento de la recogida.

3.12.4. Conclusiones

Este uso podría implementarse de modo sencillo a corto plazo.

3.13. Identificación en sistemas de juego on-line

El acceso a los sistemas de juego on-line está restringido, de acuerdo a la legislación vigente, a los mayores de 18 años, por lo que podría ser un requisito legal el acceso a estos sistemas de juego mediante el DNIe, ya que con éste es posible realizar la validación de la fecha de nacimiento del usuario que accede.

El acceso a los datos del certificado debería limitarse al dato de la edad, ya que no existe la obligación de identificar a un usuario de un casino, salvo para operaciones que superen un determinado importe, por lo que la identificación en el acceso podría considerarse una violación de la intimidad.

Si que es necesario, sin embargo identificar al titular receptor de un premio, por lo que la gestión de los usuarios debe ser diferente según se trate de controlar, bien el acceso, o bien la entrega de premios.

El acceso a las salas de juego on-line debería ser anónimo, salvo la verificación de la edad y la entrega de premios.

3.13.1. Condicionantes técnicos

Desde un punto de vista técnico, el acceso a los datos del certificado de autenticación o la identificación del titular tras la entrega del premio no presenta una dificultad añadida al uso habitual de certificados en Internet.

3.13.2. Condicionantes legales

La legislación sobre el juego on-line, es compleja, ya que depende del país que ofrezca el servicio de juego. En España los únicos juegos y apuestas de ámbito estatal son los que comercializan el Organismo Nacional de Loterías y Apuestas del Estado y la Organización Nacional de Ciegos, y la actividad sin autorización está prohibida.

Algunas Comunidades Autónomas están tratando de regular esta cuestión. Se trata pues de un tema complejo, y se está a la espera del desarrollo de su normativa regulatoria específica y del desarrollo de las competencias autonómicas en la materia.

3.13.3. Condicionantes de uso

Desde un punto de vista del usuario que accede a un entorno de juego on-line, puede estar condicionado por el anonimato en el acceso, y su derecho a preservar la intimidad, por lo que la introducción del DNIe como elemento para garantizar la edad podría verse como un aspecto negativo.

3.13.4. Conclusiones

Si bien desde un punto de vista técnico es relativamente sencillo implementar un sistema de control de edad basado en el DNIe, la complejidad en materia regulatoria sobre los juegos on-line y las posibles reticencias por parte de los usuarios a sentirse identificados con jugadores, hace plantear este servicio como factible a medio / largo plazo.

3.14. Firma de contenidos digitales

La firma de contenidos digitales mediante el DNIe permite garantizar la "paternidad" del autor de un contenido digital. Para ello debería establecerse qué formato de firma se exige para la verificación del autor del contenido y establecerse un sistema de almacenamiento de la composición firmada por un tercero de confianza que actuaría como garante de dicha autoría.

Un aspecto a destacar es que el DNIe permite firmar no sólo documentos sino ficheros o código que no se puede firmar de modo manuscrito. Esto permitirá la diferenciación entre ficheros válidos y no válidos para aplicarlo en temas de propiedad intelectual. Para ello además de la firma, sería necesario que se incorporara un sello de tiempo del momento en que se realizó la misma que debería estar emitido por un tercero de confianza que actuara de intermediario entre las partes en caso de litigio.

3.14.1. Condicionantes técnicos

Desde un punto de vista técnico, debe definirse el formato de la firma y la necesidad de que esta incorpore sellado de tiempo, para garantizar el momento en que se produce la firma. También habrá de definirse cómo se distribuirá el contenido digital junto con la firma, así como los mecanismos de inspección para determinar en caso de litigio la autoría del contenido.

Además de la propia firma de los contenidos digitales, sería necesario establecer la figura de una entidad de intermediación que almacenara las firmas de contenidos digitales, para, en caso de litigio sobre la autoría de un contenido digital concreto, disponer de un repositorio de contenidos digitales firmados, junto con el sello de tiempo en que se produjo la firma. Esta entidad podría también ofrecer a usuarios finales domésticos, servicios informativos sobre la autoría registrada de contenidos digitales.

3.14.2. Condicionantes legales

Debería establecerse los requisitos mediante los cuales se reconoce la autoría de un contenido digital, y las competencias de la entidad de intermediación que almacenaría los contenidos digitales firmados.

3.14.3. Condicionantes de uso

Desde un punto de vista de usuario final, debería concienciarse sobre la adquisición de contenidos digitales firmados, que garanticen la autoría del mismo y eviten plagios o copias, si bien por parte de los usuarios finales, está muy arraigada la descarga y utilización de material desde la red, sin respetar derechos de copia.

Por parte de los autores, debería fomentarse la firma digital de los contenidos, para asegurar la autoría del mismo.

3.14.4. Conclusiones

Si bien desde un punto de vista estrictamente técnico, la firma de un contenido digital sería relativamente sencilla de implementar, los condicionantes legales derivados de los derechos que adquiriría el autor por la firma y el establecimiento de la entidad de intermediación hacen que este uso del DNIe se plantee como posible a medio plazo.

3.15. Otros usos

A lo largo de las reuniones de trabajo, se han propuesto otros posibles usos del DNIe, que no se han desarrollado en un punto separado, bien por afectar a la relación entre empresas y ciudadanos con la administración, o bien porque no parece a priori que pudieran convertirse en usos diferenciales del DNIe:

- Utilización del DNIe para al pago de tasas portuarias.
- Utilización para asociar la identidad de los recién nacidos a sus padres.
- Pago de tasas y servicios universitarios, así como identificación de alumnos en entornos virtuales de campus universitarios.

4. RETOS PARA EL DNIE

Este capítulo identifica los retos cuya superación podría impulsar significativamente la utilización del DNI, así como aquellos aspectos detectados por los expertos como puntos de mejorables en el actual modelo de emisión y uso del DNIe.

4.1. Necesidad de introducción del PIN para cualquier acceso a los certificados

Las librerías disponibles en estos momentos para el uso del DNIe en entornos PC obligan a la introducción del PIN dos veces para cualquier acceso a los certificados, una para acceder físicamente al chip de la tarjeta, y otra para la firma o acceso al certificado de autenticación.

Desde el punto de vista de los usuarios, el hecho de tener que introducir el PIN de la tarjeta al menos dos veces para realizar una operación puede causar un cierto rechazo al uso del DNIe por incómodo (es un tema de usabilidad). También hay que tener en cuenta la casuística relacionada con el olvido del PIN, que desactiva el uso telemático del DNIe debiéndose implementar mecanismos rápidos y ágiles de reactivación del PIN.

Este aspecto también dificulta la utilización del DNIe en dispositivos que no dispongan de teclado alfanumérico o donde habitualmente sólo se hacen consultas de datos del DNI.

Una posibilidad para mitigar este problema, sería que el acceso a los datos del certificado de autenticación para consulta, se realizará sin necesidad de introducir el PIN y que éste se solicitara sólo para operaciones de firma electrónica o acceso autenticado, ampliando así sus usos potenciales. Este aspecto se considera esencial para poder utilizar en DNIe en entornos de nivel de seguridad medio donde no sea necesario la introducción del PIN.

4.2. Existencia de dos certificados en el DNIe

La existencia de dos certificados en el chip del DNIe puede causar confusión en usuarios no expertos en temas de certificación digital, y puede hacer que no tengan claro con qué certificado están firmando en cada momento, y cuál de ellos ofrece firma electrónica reconocida y no repudio.

Para solventar este problema es necesario trabajar en dos frentes:

- Campañas de divulgación para difundir el contenido del DNIe y la funcionalidad que ofrece cada uno de sus certificados. Según se vaya incrementando el conocimiento tecnológico de los usuarios, este punto dejará de ser motivo de confusión.
- Las aplicaciones que utilizan el DNIe deben ser capaces de diferenciar qué certificado necesitan para una autenticación y cuál para una firma y no dejar que la decisión de qué certificado utilizar quede en manos del usuario final.

4.3. Falta de librerías para algunos entornos

Actualmente están disponibles para el DNIe librerías para los sistemas operativos siguientes: Windows, GNU/Linux y Mac OS. Sin embargo cada vez es más frecuente el uso de otros dispositivos que no disponen de estos sistemas operativos y en los que no es factible, a fecha de hoy, el uso del DNIe, como por ejemplo:

- Decodificadores de Televisión Digital Terrestre (TDT).
- Agendas electrónicas tipo PDA.
- Terminales punto de venta (TPV).
- Cajeros automáticos no basados en PC.

Actualmente no es posible desarrollar aplicaciones que hagan uso del DNIe en estos entornos ya que ni existen las librerías adecuadas, ni está disponible la documentación necesaria para que cualquier desarrollador pueda desarrollar una librería a medida para alguno de estos entornos.

Como solución a este punto caben dos posibilidades:

- Que la propia DGPyGC, emisora del DNIe, bien a iniciativa propia o bien a través de la FNMT, desarrolle librerías para los entornos que sea necesario y se ocupe de su mantenimiento, como sucede ahora con las librerías para los entornos ya disponibles.
- Que se libere la documentación necesaria para que cualquier desarrollador pueda diseñar librearías que se adecuen a sus necesidades. En este punto, cabría la posibilidad de que la cesión de la información necesaria fuese pública, o bien se liberase mediante algún tipo de acuerdo de confidencialidad, así como que el resultado final del desarrollo tuviese que someterse a algún tipo de certificación (solución compleja y cara para las empresas desarrolladoras) o verificación de funcionamiento de acuerdo a un código de buenas prácticas de desarrollo (solución mas sencilla y económica).

4.4. Diferencia entre periodos de caducidad del soporte físico y de los certificados

El periodo de renovación de los DNI como soporte físico es de:

- 5 años hasta que el titular tiene los 30 años.
- 10 años entre los 30 y los 70 años.
- Permanente a partir esa edad.

Sin embargo, el periodo de validez de los certificados electrónicos almacenados en el chip del DNIe es de 30 meses, tras el cual es preciso renovarlos. Además, la renovación de los certificados del DNIe debe efectuarse presencialmente en los centros de expedición

del DNIe, aunque puede hacerse de modo desatendido en los Puntos de Actualización del DNIe que existen en dichos centros de expedición. Para facilitar la renovación, la DGP tiene previsto incorporar kioscos o puntos de actualización del DNIe en las zonas 24 de comisarías y centros de expedición.

Como la fecha de caducidad de los certificados es inferior al periodo de validez normal del soporte del DNIe, es fácil que un usuario, si no lo utiliza frecuentemente, olvide que tiene que renovar sus certificados del DNIe.

Para evitar este problema es necesario concienciar a los usuarios sobre la caducidad de los certificados electrónicos, y la propia DGPyGC, emisora del DNIe, habría de adoptar medidas proactivas en este sentido encaminadas a facilitar al máximo la renovación de los certificados.

Una medida sencilla sería la notificación de la inminente caducidad de los certificados electrónicos del DNIe para que el usuario pudiese proceder a su renovación, de modo similar a como se hace con el permiso de conducir. Actualmente, esta notificación no está prevista y, además, la DGPyGC no almacena una dirección electrónica de los usuarios a los que les expide el DNIe por lo que la notificación debería realizarse por correo postal.

4.5. Desconocimiento general de la funcionalidad del DNIe

Este punto es similar al de desconocimiento de la utilidad de los dos certificados del DNIe, y es una percepción generalizada entre la población, que se ha manifestado frecuentemente durante las reuniones de trabajo. Es un hecho que existe un desconocimiento general sobre la funcionalidad que ofrece el DNIe que puede eliminarse progresivamente mediante campañas de divulgación sobre el contenido del DNIe, los certificados contiene, cuál es su propósito, en qué entornos puede utilizarse, y, esencialmente, en qué puede facilitar la vida de los ciudadanos.

La realización de campañas de difusión del DNIe para fomentar su uso, se ha planteado a lo largo del estudio como un punto vital. La Administración debería liderar la difusión y adoptar medidas legislativas, de promoción y beneficios, tanto para empresas como para usuarios. Estas campañas de difusión no deben centrarse en aspectos técnicos o de detalle de la tecnología del DNIe, sino con un enfoque de venta de sus beneficios por el uso y marketing del DNIe, que permita acostumbrar a los ciudadanos al uso del DNIe.

Otro aspecto fundamental es que el uso en servicios ofrecidos en las empresas sea sencillo para los ciudadanos y no requiera especiales conocimientos tecnológicos. Las propias empresas deberían colaborar en la difusión del uso del DNIe a través de los canales que permitan su uso, por ejemplo en banca y *utilities*, asesores fiscales y gestores, etc., que podrían ser precursores del uso del DNIe. Estos sitios podría publicitar que permiten el uso del DNIe mediante la inclusión de *logos* o marcas, algo similar a lo que se hace con el nivel de accesibilidad de la página.

4.6. Desconocimiento sobre las normas jurídicas aplicables al tratamiento de la información firmada electrónicamente

Aunque la firma electrónica está regulada por la Ley de Firma electrónica, existe cierta inseguridad entre los participantes en el tratamiento que debe darse a la información firmada digitalmente y, en particular, a los contratos y cláusulas de condiciones contractuales.

Aunque existen soluciones técnicas en el mercado que permiten tanto el tratamiento como el almacenamiento de documentos firmados electrónicamente, lo que no está claro en los servicios jurídicos de las entidades, es el tratamiento que debe darse a la custodia de documentos electrónicos firmados digitalmente, y su gestión a lo largo del tiempo, sobre todo cuando los periodos de tiempo son muy largos.

La presentación de pruebas en formato electrónico en caso de litigio hace que los servicios jurídicos de las empresas se muestren reticentes a la utilización de estas tecnologías en los diferentes ámbitos de la actividad empresariales.

4.7. Capacidad de proceso de los centros de validación del DNIe

Actualmente son dos los organismos públicos que ofrecen servicios de validación del DNIe el Ministerio de Administraciones Públicas (MAP), para los organismos de la Administración, y la Fábrica Nacional de Moneda y Timbre (FNMT) para el sector privado. Si se confirma la explosión de servicios que utilizan el DNIe que se prevé, existen dudas razonables acerca de la capacidad de estos centros de validación de los certificados del DNIe así como del nivel de servicio que ofrecerán. Esta preocupación se detecta principalmente en el sector privado.

Aunque actualmente sólo existen los dos centros antes citados, parece estar prevista la existencia de un tercero, el Ministerio de Industria (Red.es), aunque todavía no está operativo. La existencia de al menos tres centros permitiría configurar un backup en caso de que fallaran alguno de los actuales.

En cualquier caso, resulta esencial la realización de un estudio que permita elaborar un escenario de la demanda de los servicios de validación asociados al DNIe, que permita el dimensionamiento y evolución a futuro más adecuado para las infraestructuras de servicios de validación necesarias.

4.8. No disponibilidad de acceso a los datos biométricos

El acceso a los datos del chip del DNIe se limita a los datos que aparecen en los certificados de autenticación y de firma y que son el nombre y apellidos, número de DNI y fecha de nacimiento.

No está disponible el acceso a los datos biométricos como son la huella o la fotografía, ni tampoco el acceso al resto de datos que están impresos en el exterior de la tarjeta, como la dirección o datos de filiación.

En el caso de la huella digital, además, no está publicado el algoritmo de digitalización de la misma, por lo que el acceso y verificación de la huella no es posible.

4.9. Otros retos

Junto con el reto de conseguir una masa crítica de DNIe desplegada, se plantea que es necesario que se disponga de un parque de lectores entre los ciudadanos que permita el uso del DNIe. En este caso se plantean medidas similares a las adoptadas en el caso de la "ñ" de los teclados que se comercializan en España. Los equipos informáticos a comercializar deberían incorporar por requisito de industria un lector de tarjetas chip. Igualmente desde la Administración se debería establecer la obligatoriedad de que todos los equipos que se adquieran en concursos de la Administración, incorporen un lector de tarjetas.

En relación con este punto también se plantea que los propios impulsores de luso del DNIe promocionen la adquisición de lectores para los usuarios. Esto se podría orquestar mediante campañas, que podrían estar cofinanciadas por la administración, para la promoción del uso del DNIe a través de la adquisición de lectores, ligados a usos concretos del DNIe en las empresas.

En general se plantea que la promoción del DNIe debería ser conjunta entre la Administración y las empresas y que éstas se beneficien del uso del DNIe bien por incentivos fiscales, o por la realización de campañas cofinanciadas por al Administración. Es necesario vender los beneficios del DNIe tanto a las empresas como a los ciudadanos.

El DNIe resuelve la problemática de la autenticación y la firma electrónica para los ciudadanos españoles, pero por ejemplo no se contempla de momento la emisión de una tarjeta con chip para los extranjeros residentes en España. Estos disponen de una tarjeta similar al DNIe, pero sin chip.

Otro problema planteado, es que España es un país destino de un gran número de turistas. Si las empresas españolas ofrecen servicios en modo electrónico utilizando el DNIe deberían ser capaces de ofrecer esos mismos servicios a clientes extranjeros que dispongan de otros certificados electrónicos reconocidos.

Este aspecto, el determinar bajo qué política de certificación se ha emitido un certificado por un prestador de servicios de certificación extranjero, y por tanto, determinar si la firma electrónica de dicho certificado puede aceptarse como firma electrónica reconocida es complejo tanto desde el punto de vista jurídico, como desde el punto de vista técnico.

Por ejemplo sería necesario, en el momento de la firma, comprobar el estado de revocación del certificado, para lo cual debería disponerse de acceso directo a las listas de certificados revocados de la autoridad emisora o a un servicio OCSP, o bien que existiera un nodo de validación de certificados que hiciera las funciones de nodo de intercambio internacional.

5. ANEXO I. METODOLOGÍA DE TRABAJO

Ejecución de la Metodología

La metodología utilizada en el proyecto está basada en un análisis prospectivo cuya piedra angular ha sido el papel que han jugado expertos con una dilatada experiencia en el desarrollo de la Sociedad de la Información. Los expertos intervinieron en el proyecto de dos formas; mediante la realización de entrevistas personales en las que se trataron temas de su competencia directa en su área de actividad (empresarial, comercial, técnico, docente, etc.), así como en grupos de trabajo, en los que se reunió a los expertos de manera conjunta.

La metodología consistió en recabar opiniones y consideraciones de personas de diferentes áreas de conocimiento y en situar sus aproximaciones a la evolución de la tecnología en el marco de la evolución económica y social.

La metodología ha tenido dos fases una pre-prospectiva y otra post-prospectiva:

5.1.1. Fase I. Pre-prospectiva.

En esta fase se fijaron los objetivos principales, la metodología de trabajo, el horizonte temporal y la planificación, la orientación y las guías de actuación (documentos de trabajo, cuestionarios, estructura de los grupos de trabajo) y la elección del grupo de expertos.

El grupo de expertos se dividió en dos ámbitos, con el objetivo de buscar un equilibrio de perfiles profesionales de los expertos participantes, el ámbito 1**, Productos y servicios financieros y servicios profesionales (aseguradoras y asesorías)** y el ámbito 2, **Productos y servicios sobre comercio electrónico y sobre ocio y multimedia.**

Participaron un total de 10 expertos.

5.1.2. Fase II. Trabajo de campo.

Grupos de trabajo

Se convocaron tres grupos de trabajo iniciales, intentando combinar expertos de ambos ámbitos, en estos grupos se presentó el proyecto y una serie de elementos preliminares sobre el desarrollo del DNIe (cuestionarios guía para las reuniones), después se intercambiaron opiniones y reflexiones sobre diversas iniciativas identificadas en el uso del DNIe aplicado a la empresa, así como posibles nuevos usos y su viabilidad, elementos impulsores y frenos o inconvenientes.

De cada una de las sesiones se realizó un informe recogiendo todos los temas tratados en las mismas.

Realización de las entrevistas con los expertos.

Se realizarán un total de 9 entrevistas individuales, una entrevista por experto.

El objetivo de las mismas fue recoger la experiencia y visión profesional de personalidades con una dilatada carrera en el ámbito de la Sociedad de la Información.

De cada una de las entrevistas se realizó un informe que recogía los temas tratados.

Sesiones de Contraste.

Se realizó una sesión de contraste. Esta sesión tuvo como objetivo validar las conclusiones extraídas de los retos y oportunidades que generará el uso de DNIe.

5.1.3. Fase III. Post-prospectiva.

En esta fase se plantearon los resultados del análisis, se elaboraron las conclusiones y recomendaciones.

Los resultados quedan recogidos en un informe específico, junto con el análisis de los datos regidos y de los comportamientos observados.

Para el análisis de los datos se ha tenido en cuenta:

- Identificación de los eventos relevantes (usos y servicios que ya utilizan los ciudadanos y que pueden ser adaptados al DNIe, así como posibles nuevos usos).
- Definición de hipótesis y variables de calidad de los servicios.
- Viabilidad de los usos y aplicaciones y plazos probables para su posible implantación.
- Condicionantes.
- Consensos.
- Identificación de tendencias.

Elaboración y cierre de propuestas.

Como documento final se realizará un informe, que recoge las conclusiones extraídas del estudio.

Entrega de documentos.

Información en bruto recogida en las entrevistas con los expertos y en los grupos de trabajo y sesiones de contraste y documentos finales.

6. ANEXO II: DESCRIPCIÓN DEL DNIE

Descripción de la funcionalidad del DNIe

El Documento Nacional de Identidad (DNI), emitido por la Dirección General de la Policía (Ministerio del Interior), es el documento que acredita los datos personales que en él aparecen y la nacionalidad española de su titular.

El DNIe traslada al mundo digital las mismas certezas con las que operamos cada día en el mundo físico y que son:

- **Acreditar electrónicamente y de forma segura la identidad de la persona.**
- **Firmar digitalmente documentos electrónicos, otorgándoles una validez jurídica equivalente a la que les proporciona la firma manuscrita.**

El Documento Nacional de Identidad electrónico (DNIe)**,** cuya principal novedad es que incorpora un pequeño circuito integrado, capaz de guardar de forma segura información y de procesarla internamente.

DESCRIPCIÓN FISICA

La tarjeta soporte del DNI electrónico contiene los datos de filiación del ciudadano, los datos biométricos (modelo dactilar, foto y firma manuscrita) y los dos pares de claves RSA con sus respectivos certificados (autenticación y firma). Esta tarjeta está compuesta de 2 partes:

1. Tarjeta física del DNI electrónico.

    - La tarjeta física del DNI electrónico sigue el estándar ISO-7816-1. Está fabricada en policarbonato, que es un material que permite su uso continuado y frecuente sin sufrir deterioro, durante el tiempo de vigencia del DNI, es decir, 10 años.
    - La personalización de la tarjeta se realiza mediante la grabación en el cuerpo de la tarjeta con láser destructivo de los datos de filiación, fotografía y firma manuscrita. Este sistema de personalización garantiza la imposibilidad de manipulación de estos datos.

2. El chip del DNI electrónico, cuyas características son

    - Modelo del Chip: ST19WL34.

- Sistema operativo: DNIe v1.1
- Capacidad: de 34Kbytes Eeprom.
- Contenido del chip:

La información en el chip está distribuida en tres zonas con diferentes niveles y condiciones de acceso:

- **Zona PÚBLICA:** Accesible en lectura sin restricciones, contenido:

  Certificado CA intermedia emisora.

  Claves Diffie-Hellman.

  Certificado x509 de componente.

- **Zona PRIVADA:** Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN, contenido:

  Certificado de Firma (No Repudio).

  Certificado de Autenticación (Digital Signature).

- **Zona de Seguridad:** Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNIe.

  Datos de filiación del ciudadano (los mismos que están impresos en el soporte físico del DNI), contenidos en el soporte físico del DNI.

  Imagen de la fotografía.

  Imagen de la firma manuscrita.

- **DATOS CRIPTOGRÁFICOS:** Claves de ciudadano

  Clave RSA pública de autenticación (Digital Signature).

  Clave RSA pública de no repudio (ContentCommitment).

  Clave RSA privada de autenticación (Digital Signature).

  Clave RSA privada de firma (ContentCommitment).

  Patrón de impresión dactilar.

  Clave Pública de root CA para certificados card-verificables.

Claves Diffie-Hellman.

- **DATOS de GESTIÓN:**

  Traza de fabricación.

  Número de serie del soporte.

  El chip de la tarjeta almacena los siguientes certificados electrónicos:

- **Certificado de Componente.** Su propósito es la autenticación de la tarjeta del DNI electrónico mediante el protocolo de autenticación mutua definido en CWA 14890.

  - Permite el establecimiento de un canal cifrado y autenticado entre la tarjeta y los Drivers.
  - Este certificado no estará accesible directamente por los interfaces estándar (PKCS11 o CSP).

- **Certificado de Autenticación.** Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

  El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

  Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas.

- **Certificado de firma.** Este certificado es el que utilizaremos para la firma de documentos garantizando la integridad del Documento y el No repudio de origen. Es un certificado X509v3 estándar, que tiene activo en el Key Usage el bit de ContentCommitment (No Repudio) y que esta asociado a un par de claves pública y privada, generadas en el interior del CHIP del DNI. Es este Certificado expedido como certificado reconocido y creado en un Dispositivo Seguro de Creación de Firma, el que convierte la firma electrónica avanzada en firma electrónica reconocida, permitiendo su equiparación legal con la Firma Manuscrita (Ley 59/2003 y Directiva 1999/93/CE)

Marco legal básico

El marco legal básico sobre le DNI electrónico es el siguiente:

- Ley 59/2003, de 19 de diciembre, de Firma Electrónica.
- Ley Orgánica 15/1999, de 13 de diciembre, de Protección de los Datos.
- Real Decreto 1553/2005, de 23 de diciembre, por el que se regula documento nacional de identidad y sus certificados de firma electrónica.

FIRMA ELECTRONICA

La Firma electrónica es un sistema de acreditación que permite verificar la identidad de las personas con el mismo valor que la firma manuscrita, autentificando las comunicaciones generadas por el firmante.

Por otra parte la Ley 59/2003, de 19 de diciembre, de firma electrónica define la firma electrónica de la siguiente manera:

- (Art. 3.1) La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.

Asimismo la Ley distingue entre “firma electrónica avanzada” y “firma electrónica reconocida”:

- (Art. 3.2) La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.
- (Art. 3.3) Se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma.
- (Art. 3.4) La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.

Despliegue

La expedición del DNI electrónico comenzó en Burgos, en marzo de 2006, desarrollándose a lo largo de dos meses una experiencia piloto. Finalizada ésta, se inició su implantación en el resto del territorio nacional, que se llevará a cabo de forma gradual a lo largo de dos años, estando prevista su finalización en marzo 2008.

El DNI electrónico se puede obtener ya en las siguientes Oficinas de Expedición del DNI de la siguientes Comunidades Autónomas; A Coruña, Almería, Asturias, Ávila, Baleares, Burgos, Cádiz, Cantabria, Ceuta, Córdoba, Granada, Huelva, Huesca, Jaén, León, Lugo, Málaga, Melilla, Navarra, Ourense, Palencia, Las Palmas, Pontevedra, La Rioja, Salamanca, Segovia, Sevilla, Soria, Tenerife, Teruel, Valladolid, Zamora y Zaragoza.

Actualmente se prevé que a finales del 2007 estén expedidos alrededor de 2.500.000 DNIe y a finales del 2008 se pueda alcanzar una cifra de entre 8 y 10 millones.

7. ANEXO III: SEGURIDAD BASADA EN CERTIFICADOS

7.1. Identidades digitales

Puede definirse el concepto de *identidad* de un individuo como aquel conjunto de rasgos que le son propios y que lo caracterizan frente a los demás. Algunos de dichos rasgos son intrínsecos al individuo; otros son adquiridos con el tiempo. Por supuesto, no todos los rasgos son igualmente apreciables. Hay rasgos que son apreciables a simple vista, mientras que otros están ocultos y es necesario un conocimiento y, en ocasiones, disponer de ciertas herramientas para que puedan ser advertidos (y, consecuentemente, verificados).

Por analogía, al conjunto de rasgos que caracterizan a un individuo en un medio electrónico se le conoce como ***Identidad Digital***. Las nuevas tecnologías imponen la necesidad de disponer de una identidad digital.

Mucha gente asume esa identidad digital como un juego, en una vertiente lúdica como son los videojuegos, o el ejercicio de las relaciones virtuales, o cuando pretenden ser una persona que no son. Es el caso de ciertas salas de charla virtual donde un hombre puede tener una identidad como mujer; o un anciano como joven; y, viceversa.

Siguiendo con la definición ofrecida más arriba, en cualquier comunicación remota, el número de rasgos no ocultos a los que se tiene acceso se hace menor. Por ejemplo, en una conversación telefónica, de una manera inconsciente, un interlocutor es capaz de determinar que la persona al otro lado del teléfono es quien dice ser, porque reconoce su voz. En una comunicación remota entre individuos a través de *Internet*, lo único que recibe una entidad de la otra son *Bytes (octetos binarios)*. Estos *Bytes* son procesados por las aplicaciones correspondientes y presentados en el formato requerido (pantalla, sonidos, ejecución de aplicaciones, textos, etc.). Cada una de las entidades debe confiar en los procesos que llevan a la generación, transmisión y presentación de esos datos.

La identidad digital no existe *a priori*, debe ser creada y ha de vincularse unívocamente al individuo, en un proceso que determinará el nivel de confianza.

Los servicios en línea para ciudadanos se están sofisticando cada vez más, gracias a la incorporación de funcionalidades que aportan una mayor interactividad; y, de forma especial, gracias a la incorporación de mecanismos para la **autenticación de la identidad electrónica**.

7.2. Proceso genérico de autenticación

Las transacciones electrónicas - ya sean entre Administraciones, entre ciudadanos o entre empresas - dependen de resolver dos tipos de cuestiones:

- obtener garantía de la identidad de las partes involucradas (¿Con quién se está, realmente, tratando?); y,
- determinar el papel, el estado, el cargo u otros atributos socio-económicos del individuo (por ejemplo, ¿Es esta persona un estudiante matriculado? ¿Es miembro de un colegio de médicos? ¿Lo es de una asociación profesional de ingeniería? ¿Está esta persona en potestad de firmar un contrato o representar a una determinada compañía?, etc.).

Sin embargo, mientras que la identidad de una persona es esencialmente una característica permanente, otros atributos como su estado, el puesto que ocupa, etc., tienden a cambiar, a menudo, de repente y de forma inesperada.

El conocimiento del papel, cargo, responsabilidades, etc. de un individuo, como fundamento de confianza y legitimidad, es esencial para muchas transacciones comerciales o administrativas. Por dicha razón, es inteligente separar los mecanismos de autenticación y autorización tanto como sea posible.

De este modo se llega a la consideración del ***proceso genérico de autenticación*** de un usuario, ante un sistema, como una secuencia de tres pasos.

Figura 1. Proceso genérico de *AUTENTICACIÓN*

En el primer paso de la secuencia el individuo procede a su **IDENTIFICACIÓN**, mediante la presentación de sus rasgos o credenciales digitales. En los entornos electrónicos, existen tecnologías muy diversas que ofrecen herramientas para generar los rasgos digitales de identidad y asociarlos a entidades/individuos (certificados digitales, tarjetas inteligentes, contraseñas dinámicas, etc).

A continuación, en un segundo paso, se produce la VERIFICACIÓN de los rasgos (credenciales), lo que permitirá determinar si un individuo es quien dice ser; esto es, se procede a ejecutar el paso de **AUTENTICACIÓN**, propiamente dicho. Por ejemplo, en el caso de la conversación telefónica (al que ya se ha hecho referencia más arriba) ese proceso de reconocimiento de la voz del individuo al otro lado de la línea, realizado inconscientemente, sería una autenticación. Cuando la persona a quien entregamos nuestro DNI nos observa buscando semejanzas con la fotografía que aparece; o compara

nuestra firma manuscrita en un documento con la que aparece en nuestra credencial, está ejecutando un proceso de autenticación visual.

Garantizar la identidad digital es un proceso complejo, especialmente cuando el medio de comunicación digital es un medio abierto, como por ejemplo Internet, donde millones de personas pueden intentar acceder al mismo tiempo a un servicio determinado.

Finalmente, el tercer paso consiste en la comprobación de que dicha identidad lleva asociados los derechos necesarios para acceder al servicio deseado. Ello provocará la **AUTORIZACIÓN**, o no, en función del nivel de privilegios que la identidad - el sujeto - en cuestión, exhiba.

Cuando la identidad de un individuo es cuestionada, es decir, sometida a un proceso de autenticación, es porque dicho individuo ha tratado de acceder a algún servicio restringido. En ese caso, tan importante como determinar que ese individuo es el titular genuino de unas determinadas credenciales, es comprobar que su identidad tiene los derechos requeridos para acceder al servicio. Este proceso que tan habitualmente se desarrolla en las aplicaciones del mundo real es, igualmente, necesario en el mundo digital.

7.3. Mecanismos de autenticación

Los diferentes mecanismos de identificación/autenticación disponibles, dotan a los sistemas de un mayor o menor grado de garantía. Este nivel de seguridad ayuda, a su vez, a clasificar los métodos de identificación, en función de su grado de "fortaleza", en los siguientes grupos (tomados de menos a más):

MÉTODO	FORTALEZA
Basado en "*lo que sé*"	-
Basado en "*lo que tengo*"	
Basado en "*lo que soy*"	+

7.3.1. Mecanismos basados en "*lo que sé*"

Como puede observarse, a la vista de la anterior tabla, los mecanismos de identificación basados en "*lo que sé*" cuentan con una mayor debilidad (o menor grado de fortaleza), desde el punto de vista de la garantía de protección que son capaces de ofrecer. Dicha debilidad estaría directamente vinculada con el problema de la custodia: aquello que alguien conoce podría, con facilidad, ser comunicado a otro (por descuido, por ejemplo);

o podría ser anotado en algún lugar indiscreto (con, *a priori*, el único y saludable fin de que sirviese de posterior recordatorio).

Estos métodos reciben esa denominación porque, en ellos, un individuo ha de identificarse, únicamente, mediante una credencial que sólo él conoce: habitualmente una palabra secreta. En la expresión clásica "santo y seña", corresponderían a la parte de la "seña".

La ventaja del método descansa en la mayor dificultad que supone "sustraer" la credencial. En principio, no es un elemento físico que se pueda robar. No obstante, y más allá de las debilidades ya apuntadas, estas *señas* memorizadas adolecen de un problema adicional: ¡se pueden olvidar!

7.3.2. Mecanismos basados en "*lo que tengo*"

En este caso, continuando con el símil del "*santo y seña*", el mecanismo corresponde a la parte del "*santo*". El individuo dispone de algo - algún elemento físico - con que identificarse o acreditarse para acceder a determinados lugares o servicios. En la vida cotidiana son innumerables los ejemplos de acreditaciones de este tipo que pueden realizarse a lo largo del día: presentar el billete recién adquirido o el abono mensual para acceder a un medio de transporte por las mañanas; mostrar la tarjeta de acceso ante los tornos de control para poder entrar en la oficina; enseñarle al acomodador la entrada para poder tomar asiento en el cine o en el teatro, por la noche; etc. Sin duda, la credencial de este tipo más habitual ha sido el **Documento Nacional de Identidad**, elemento de identificación por antonomasia que ha servido, y sirve, como "santo" acreditativo en multitud de circunstancias del día a día.

En el ámbito de los sistemas informáticos, este tipo de elementos, o dispositivos, acreditativos permiten albergar - e, incluso, generar - contraseñas (claves) más sofisticadas y complejas, y, por tanto, más difíciles de descubrir; lo que implica que, intrínsecamente, se asigne a estos mecanismos un mayor nivel de confianza que los basados únicamente en una palabra secreta que el individuo pueda conocer. Están, por ello, dotados de un mayor nivel de fortaleza.

En su contra, está la posibilidad de sustracción de que pueden ser objeto, como elementos físicos que son.

7.3.3. Mecanismos basados en "*lo que soy*"

En último lugar se tienen los que se han considerado métodos de identificación más robustos. Como su propio nombre indica están directamente relacionados con algo que describe al individuo, que define lo que es, o cómo es. En una conversación telefónica, un interlocutor identifica a otro por su voz; cuando una persona visita a un amigo, éste le abre la puerta de su casa una vez que lo ha reconocido a través de la imagen que le envía la cámara colocada en el intercomunicador de su portal, etc.

Nuevamente en el entorno tecnológico, los mecanismos de autenticación basados en "*lo que soy*", guardan una íntima relación con las técnicas biométricas informáticas. En ellas, diferentes rasgos físicos - o del comportamiento - del individuo son analizados y comparados con patrones conocidos de antemano para verificar la identidad de un determinado sujeto.

Estos mecanismos quedan dentro del grupo de los denominados métodos de autenticación "fuerte". En este caso, por tratarse de características del individuo no son algo que, *a priori*, se pueda robar o perder (uno lleva siempre su voz consigo); y no son algo que se pueda olvidar (uno tiene una determinada cadencia de tecleo, cuando se sitúa ante un teclado).

7.3.4. Mecanismos mixtos o híbridos

Muchas de las tecnologías de identificación digital son complementarias entre ellas y es importante saber cómo y cuándo es necesario combinarlas.

En este punto alcanza su máximo valor la expresión "santo y seña". Se trata de complementar las fortalezas y debilidades de los diferentes mecanismos de autenticación, empleándolos de manera conjunta.

En tales casos se habla de **autenticación** de doble-, triple- o **multi-factor**, en función del número de métodos que se combinen. De hecho, en el terreno práctico, es habitual tender a soluciones de certificación digital, basadas en tarjeta inteligente, que requieran adicionalmente, el empleo de contraseñas alfanuméricas; o aquellas otras aplicaciones más avanzadas en las que se combina el empleo de tarjetas de acceso, con verificaciones biométricas de la huella o de la geometría de la mano, por ejemplo. **El DNIe es un ejemplo de autenticación multifactor.**

7.4. Mecanismo de autenticación basado en Certificados

Los mecanismos de autenticación basados en "certificados digitales" aportan un mayor nivel de seguridad que los tradicionalmente basados en usuario y contraseña, ya que permiten, a la vez, mantener comunicaciones confidenciales y garantizar la identidad del remitente a través de los medios electrónicos.

Pueden distinguirse dos variantes, dentro de estos métodos de autenticación: aquellos que emplean algún soporte físico para albergar los certificados y los que no hacen uso de tales dispositivos. Este apartado tratará la segunda de las citadas variantes, es decir, los certificados digitales en soporte software, en los que el usuario no utiliza ningún elemento físico (tarjeta inteligente, etc.) en el momento de proceder a su identificación.

Los certificados se obtienen, previa solicitud a una "autoridad de certificación" (del inglés *Certification Authority*, CA). En el marco de la Administración española, el proceso de

solicitud del certificado digital incluye un paso que, necesariamente, ha de ser presencial. En él, el solicitante debe identificarse mediante su DNI o pasaporte, en vigor. Si la comprobación de las identidades de los solicitantes no fuese rigurosa, los certificados emitidos podrían no ser fiables.

La tecnología de certificación digital utiliza un cifrado de clave pública o cifrado asimétrico.

Este mecanismo se basa en la existencia de dos claves de cifrado: la clave pública, conocida por todos los interlocutores del dominio de comunicación; y la clave privada, cuyo conocimiento queda restringido a su legítimo propietario, quien tendrá la responsabilidad de custodiarla.

Las claves pública y privada de un usuario están relacionadas entre si, de forma tal, que si un mensaje es cifrado usando la clave pública de ese usuario, la única forma de descifrar dicho mensaje sería utilizando su clave privada, lo que constituye una garantía de confidencialidad del mensaje enviado.

A modo de ejemplo, se describe, a continuación, un procedimiento de cifrado en el que un usuario “A” se comunica con otro usuario “B” mediante el uso de un sistema de cifrado de clave pública.

- el usuario “B” solicita un certificado digital a la autoridad de certificación;
- una vez obtenido el certificado, el usuario “B” pone su clave pública en conocimiento del usuario “A”;
- a continuación, el usuario “A” cifra el mensaje con la clave pública de “B” y lo envía. A partir de este punto el mensaje estaría viajando, cifrado con la clave pública de “B”. Por lo tanto, la única forma de descifrar el mensaje sería utilizando la clave privada de “B”.
- una vez recibido el mensaje cifrado por “A”, el usuario “B” lo descifra usando su clave privada, obteniendo, finalmente, el mensaje original de “A”.

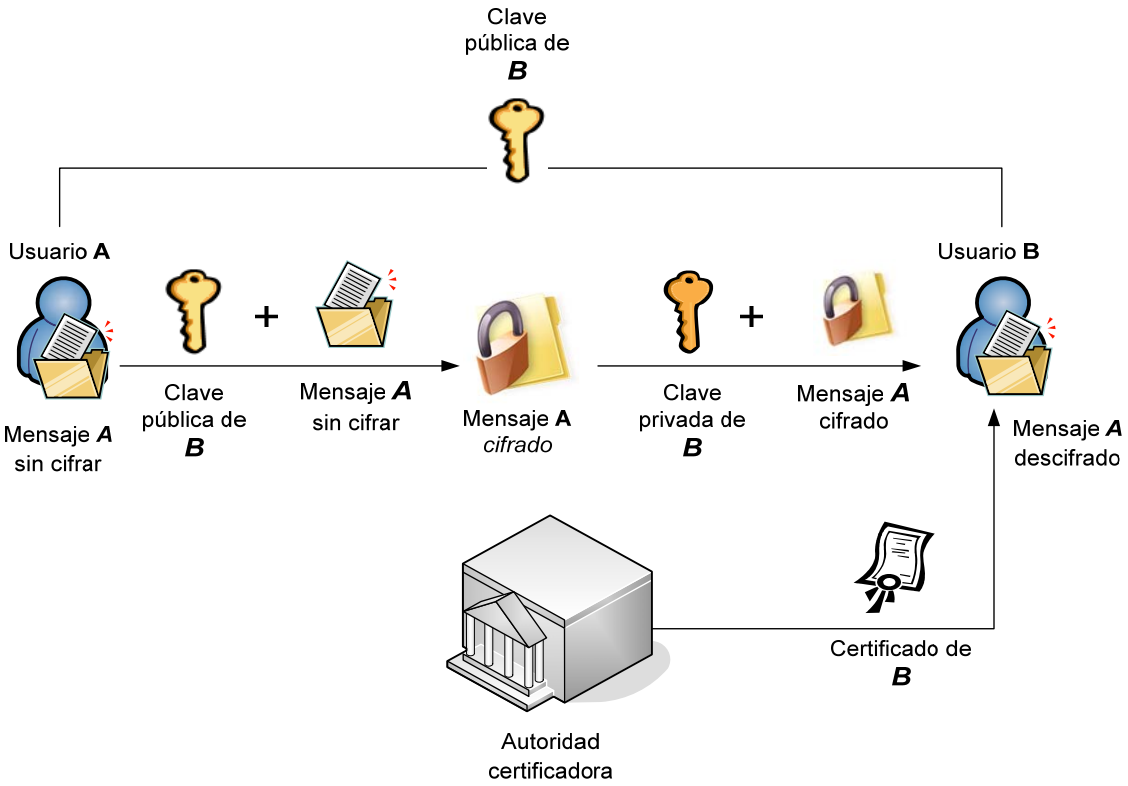


Figura 2. Proceso genérico de cifrado / descifrado en un sistema clave pública con certificado digital

Como se puede observar en la figura, no es necesario que la clave pública (del sujeto "B") viaje cifrada, debido a que si alguien (sujeto "C") lograra interceptarla, éste individuo no podría descifrar el mensaje, dado que, para ello, requeriría la clave privada de "B". Sin embargo, "C" sí podría enviar mensajes cifrados haciéndose pasar por otra persona (por ejemplo, el sujeto "A"), violando, de este modo, el principio de autenticidad.

Para evitar este problema y poder asegurar la integridad del mensaje, al mismo tiempo que se garantiza la identidad genuina del remitente, la certificación digital permite el empleo de la **firma electrónica, o firma digital**, de los mensajes. La firma electrónica permite la autenticación de un individuo de una forma inequívoca, al mismo tiempo que posibilita salvaguardar la integridad del mensaje transmitido entre las partes.

El mecanismo de firma digital consiste en aplicar una función matemática (función *hash*) al mensaje original con el fin de obtener un resumen del mismo para después cifrarlo usando la clave privada del emisor. En el posterior envío, el texto original, irá acompañado del resultado así obtenido (firma electrónica del mensaje).

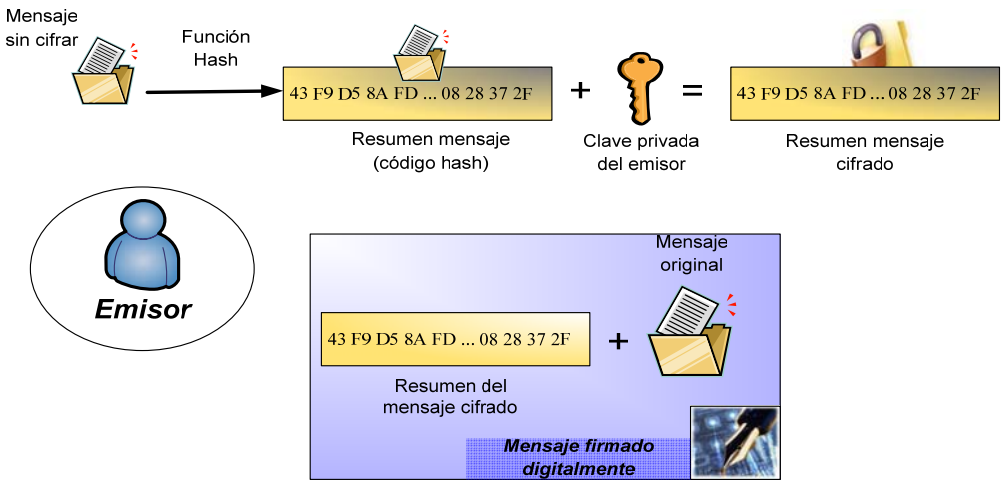


Figura 3. Proceso genérico de firmado digital de un mensaje

Cuando el receptor recibe el mensaje (firmado electrónicamente), debe emplear la clave pública del emisor para descifrar el resumen del mensaje cifrado. Paralelamente, el receptor aplica la función resumen (*hash*) sobre el mensaje recibido. Finalmente, se ha de realizar una comparación entre los dos resúmenes obtenidos (el descifrado y el calculado). Si difieren, se habrá producido una violación de la integridad o de la autenticidad del mensaje. En otras palabras, el mensaje puede haber sido modificado o el emisor no es quien debería ser. Si por el contrario, los resúmenes son iguales, el mensaje será totalmente fiable tanto en su integridad, como en la autenticidad del remitente.

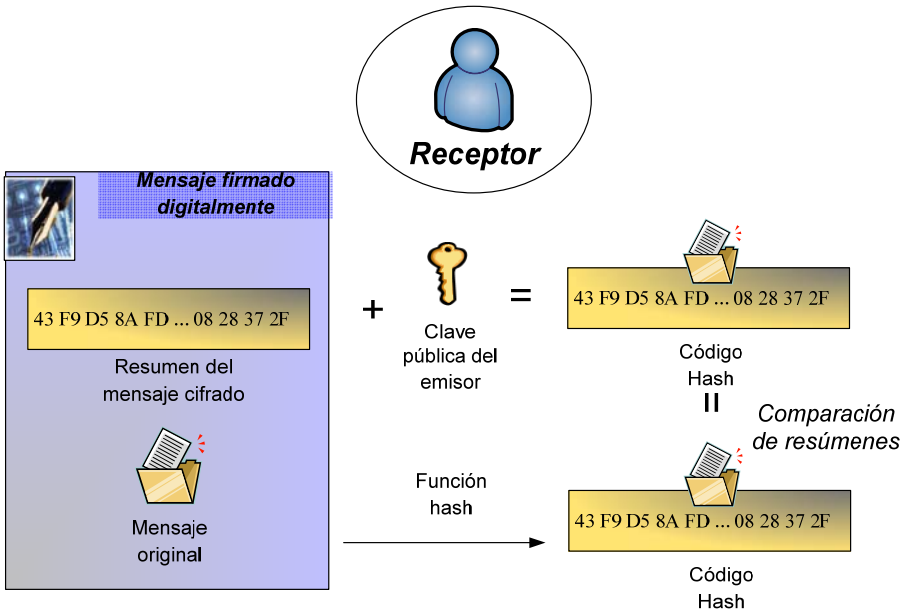


Figura 4. Proceso genérico de verificación de la firma electrónica, en la recepción de un mensaje

La utilización conjunta de los procesos de ***cifrado de clave pública*** **y** ***firma digital***, proporcionará un grado aún mayor de seguridad. En la siguiente figura se detalla el proceso completo de comunicación entre dos usuarios, o entidades, mediante el uso de la certificación digital combinada con firma digital.

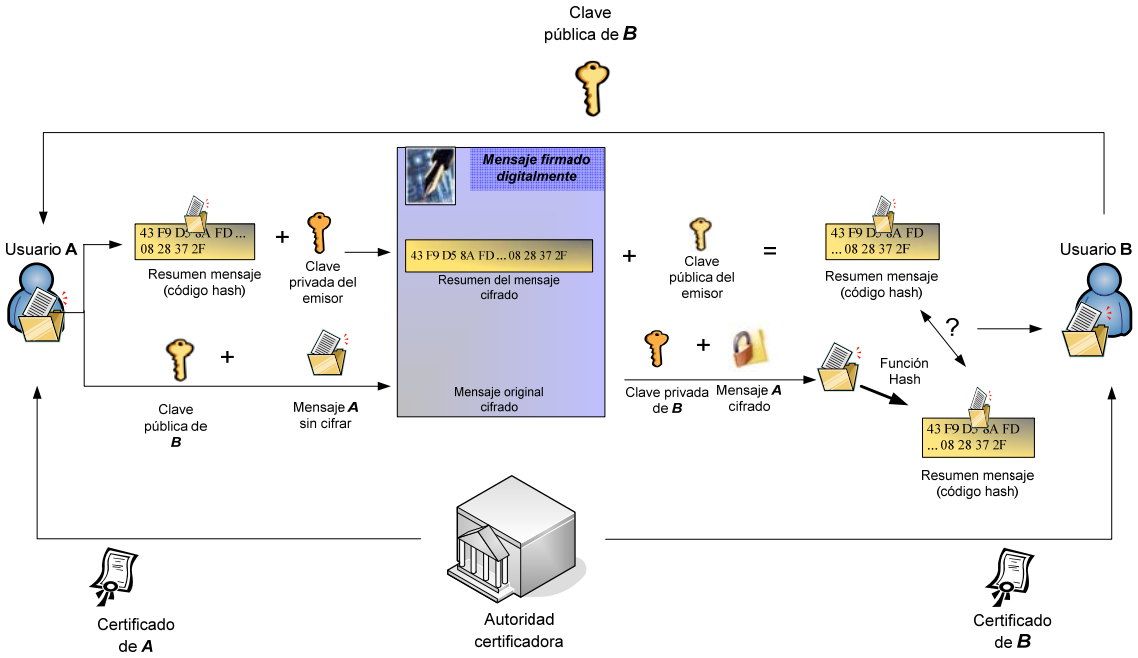


Figura 5. Proceso genérico de cifrado con clave pública y firma electrónica, basado en certificación digital

La fortaleza del método estriba en su capacidad para garantizar la conformidad con los siguientes principios:

- **Confidencialidad:** La información contendida en el mensaje ha sido cifrada y solo el receptor podrá ser capaz de descifrarla. Por lo tanto "solo" el emisor y el receptor serán capaces de ver la información que contiene el mensaje.
- **Integridad:** La información que contiene el mensaje o transacción electrónica no ha sido alterada.
- **Autenticidad (autenticación):** La información del documento y su firma se corresponden con la persona que ha firmado, tanto por parte del emisor, como por parte del receptor.
- **No repudio:** La persona que ha firmado no puede decir que no lo ha hecho.

7.4.1. Necesidad de actuaciones por parte de terceros

Uno de los elementos del mecanismo del cifrado de clave pública es la Autoridad de Certificación (del inglés *Certification Authority*, CA). Esta organización puede ser considerada como un elemento externo por lo que se detalla en este apartado.

Con el fin de desglosar y entender más en detalle las funciones y la importancia de la autoridad certificadora dentro del proceso de certificación digital, a continuación se definen las principales funciones de estos organismos.

La CA se encarga, de una manera fiable, de aceptar solicitudes de certificados de entidades, validarlas, generar certificados y mantener la información de su estado. Adicionalmente, una CA debe disponer de una *Declaración de Prácticas de Certificación* (*Certification Practice Statement* o *CPS*) que indique claramente sus políticas y prácticas relativas a la seguridad y mantenimiento de los certificados, las responsabilidades de la CA respecto a los sistemas que emplean sus certificados y las obligaciones de los subscriptores respecto de la misma.

Las labores de una CA son:

- **Admisión de solicitudes**. Un usuario rellena un formulario y lo envía a la CA solicitando un certificado. La generación de las claves pública y privada es responsabilidad del usuario o de un sistema asociado a la CA.
- **Autentificación del sujeto**. Antes de firmar la información proporcionada por el sujeto, la CA debe verificar su identidad. Dependiendo del nivel de seguridad deseado y el tipo de certificado se deberán tomar las medidas oportunas para la validación.
- **Generación de certificados**. Después de recibir una solicitud y validar los datos la CA genera el certificado correspondiente y lo firma con su clave privada. Posteriormente lo manda al subscriptor y, opcionalmente, lo envía a un almacén de certificados para su distribución.
- **Distribución de certificados**. La entidad certificadora puede proporcionar un servicio de distribución de certificados para que las aplicaciones tengan acceso y puedan obtener los certificados de sus subscriptores. Los métodos de distribución pueden ser: correo electrónico, servicios de directorio como el X.500 o el LDAP, etc.
- **Anulación de certificados**. Al igual que sucede con las solicitudes de certificados, la CA debe validar el origen y autenticidad de una solicitud de anulación. La CA debe mantener información sobre una anulación durante todo el tiempo de validez del certificado original.
- **Almacenes de datos**. Hoy en día existe una noción formal de *almacén* donde se guardan los certificados y la información de las anulaciones. La designación oficial de una base de datos como almacén tiene por objeto señalar que el trabajo con los certificados es fiable y de confianza.

Cuando una CA emite un certificado digital, lo hace con un periodo máximo de validez que oscila entre tres y cinco años. El objetivo de este periodo de caducidad es obligar a la renovación del certificado para adaptarlo a los cambios tecnológicos. Así se disminuye el riesgo de que el certificado quede comprometido por un avance tecnológico. La fecha de caducidad viene indicada en el propio certificado digital.

Sin embargo, existen otras situaciones que pueden invalidar el certificado digital aún cuando no ha caducado, de manera inesperada:

- El usuario del certificado cree que su clave pública ha sido robada.
- Desaparece la condición por la que el certificado fue expedido. Por ejemplo, el cambio de apoderado de una entidad jurídica.
- El certificado contiene información errónea o información que ha cambiado. Por ejemplo, una errata en los apellidos.
- Una orden judicial.
- Etc.

Por tanto, debe existir algún mecanismo para comprobar la validez de un certificado antes de su caducidad. Las CRL son uno de estos mecanismos.

Una CRL es una lista de números de serie de certificados digitales revocados por una autoridad de certificación concreta. Dicha lista está firmada digitalmente por la propia autoridad de certificación.

Cuando un tercero desea comprobar la validez de un certificado debe descargar una CRL actualizada desde los servidores de la misma autoridad de certificación que emitió el certificado en cuestión. A continuación comprueba la autenticidad de la lista gracias a la firma digital de la autoridad de certificación. Después debe comprobar que el número de serie del certificado cuestionado está en la lista. En caso afirmativo, no se debe aceptar el certificado como válido.

Estrictamente hablando, no es necesario descargar una CRL cada vez que se verifica un certificado. Solamente es necesario cuando no se dispone de la CRL de una entidad de certificación concreta, y cuando dicha lista tiene una cierta antigüedad que aconseja su renovación.

7.5. Mecanismo de autenticación basado en Certificados en soporte Hardware

La autenticación mediante el uso de certificados digitales en soporte hardware puede considerarse como una “evolución” del mecanismo visto en el apartado anterior, relativo a autenticación mediante certificados en soporte software. La diferencia, obviamente, en este caso, reside en el empleo de dispositivos seguros para el almacenamiento de las credenciales electrónicas: principalmente, *tokens* y tarjetas inteligentes. Estos elementos se convierten en algo que el usuario “posee” y que utiliza en el momento de su identificación. Por este motivo, la seguridad en este mecanismo se eleva de una forma considerable respecto a los métodos vistos anteriormente, ya que, tanto la clave pública, como la clave privada, se generan y almacenan en el interior de estos dispositivos, de una forma segura.

Actualmente, los elementos más usados para la autenticación en soporte hardware son las tarjetas inteligentes. De ellas tratará, principalmente, este capítulo.

Existen diferentes tipos de tarjetas inteligentes, en virtud de las características o funcionalidades que ofrezca la circuitería que incorporan en su interior. De este modo, se tienen:

- **Tarjetas de memoria** que únicamente actúan como contenedoras de ficheros; pero que no albergan aplicaciones ejecutables. Se emplean, generalmente, en aplicaciones de identificación y control de acceso sin altos requisitos de seguridad.
- **Tarjetas micro-procesadas** o tarjetas con microprocesador que presentan una estructura interna análoga a la de un ordenador (procesador, memoria volátil, memoria persistente). Almacenan ficheros y aplicaciones y suelen emplearse para identificación y pago como monederos electrónicos.
- **Tarjetas criptográficas**. Son tarjetas micro-procesadas avanzadas, que incorporan módulos *hardware* de propósito específico para la ejecución de algoritmos de cifra y firma digital. En estas tarjetas se almacenan, de forma segura, los certificados digitales (y las claves privadas) de los usuarios. Permiten firmar documentos o autenticarse sin que las credenciales del usuario salgan de la tarjeta. El procesador de la propia tarjeta es el que realiza la firma.

Estas tarjetas contienen una placa de circuito impreso en la que se distinguen:

  - **CPU** (*Central Processing Unit*): el procesador de la tarjeta. Pueden tener opcionalmente módulos hardware (coprocesador) para operaciones criptográficas.
  - **ROM** (*Read-Only Memory*): memoria interna en la que se incrusta el sistema operativo de la tarjeta, las rutinas del protocolo de comunicaciones y los algoritmos de seguridad de alto nivel, por *software*. Esta memoria, como su propio nombre indica, no se puede reescribir y se inicializa durante el proceso de fabricación.
  - **EEPROM**: memoria de almacenamiento (equivalente al disco duro en un ordenador personal) en el que está grabado el sistema de ficheros, los datos usados por las aplicaciones, claves de seguridad y las propias aplicaciones que se ejecutan en la tarjeta. El acceso a esta memoria está protegido, a distintos niveles, por el sistema operativo de la tarjeta.
  - **RAM** (*Random Access Memory*): memoria volátil, de trabajo, del procesador.

- Las tarjetas criptográficas mantienen el material criptográfico, sensible, siempre en su interior y protegen su uso mediante un control de acceso. Para utilizar la tarjeta el usuario debe disponer de un número de identificación personal, que sólo él conocerá.
- La tarjeta criptográfica contiene la clave privada, en su interior. Esta clave se genera en la propia tarjeta y es protegida mediante algoritmos de cifrado, de modo que nadie puede acceder a ella.

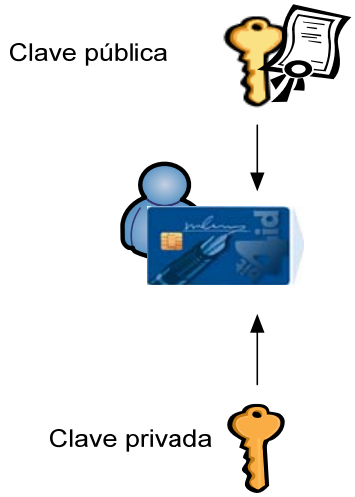


Figura 6. Tarjeta criptográfica

El mecanismo de cifrado para el intercambio de mensajes con soporte *hardware* se diferencia del mecanismo con soporte *software* en que, en este caso, el cifrado y descifrado de los mensajes se realiza a través de la tarjeta criptográfica. Por este motivo, para proteger el intercambio de información entre la tarjeta y los sistemas que interactúan con ella, se deberá de crear un canal de comunicación seguro que proteja la información. El establecimiento de este canal seguro se realiza mediante el intercambio de certificados entre la tarjeta y el sistema.

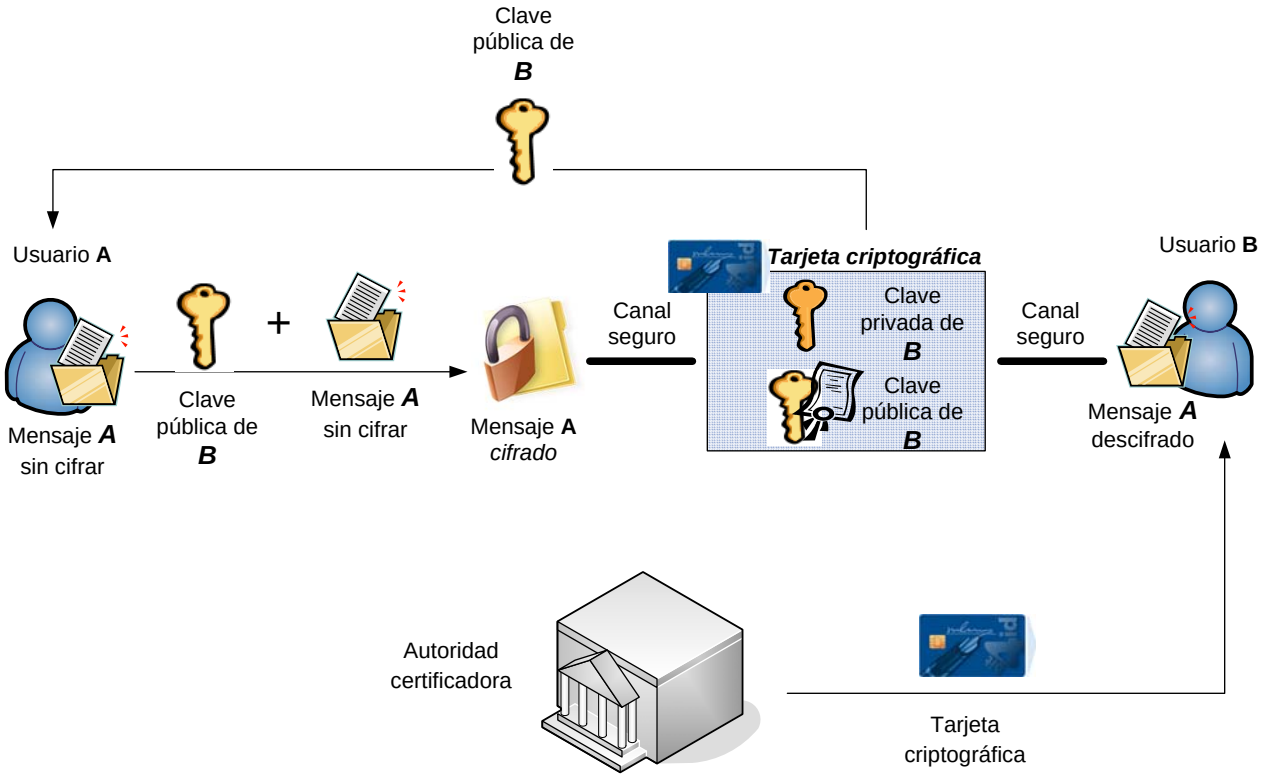


Figura 7. Proceso de cifrado mediante "tarjeta criptográfica"

Como puede apreciarse en la figura, el proceso de cifrado de mensajes no varía mucho con respecto al mecanismo anterior. Una de las novedades que aporta este nuevo sistema es que, en este caso, la Autoridad Certificadora entrega el certificado digital y la clave privada en una tarjeta criptográfica.

La firma digital mediante el uso de la certificación por *hardware* implica que el proceso de cifrado o firma del mensaje es enteramente realizado por, en este caso, la tarjeta criptográfica.

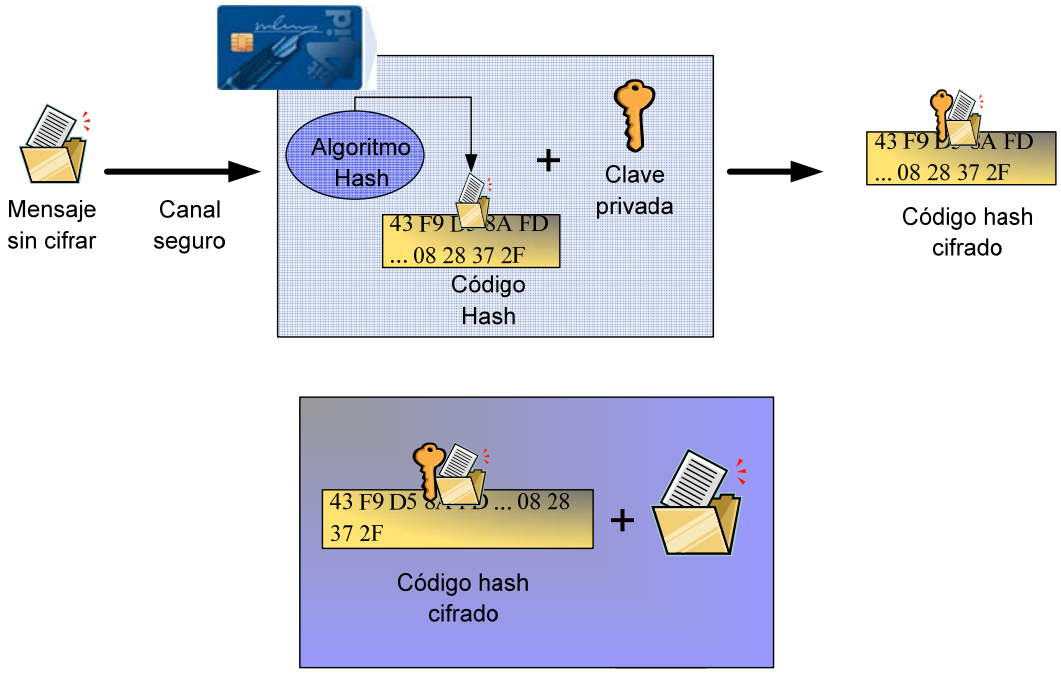


Figura 8. Firma digital mediante la "tarjeta criptográfica"

7.6. DNI electrónico

Entre los métodos de autenticación mediante certificación digital soportada en *hardware*, merece especial mención el DNI electrónico (DNIe). El DNI electrónico es una tarjeta criptográfica que, a parte de identificar al ciudadano, ofrece a éste la posibilidad de interactuar con los nuevos servicios de la Sociedad de la Información, de una forma cómoda y segura a través los medios electrónicos.

Para realizar transacciones seguras a través dichos medios el DNIe utiliza la certificación digital que incluye la firma digital de los mensajes.

Desde el punto de vista técnico, la información contenida en el chip del DNIe está distribuida en tres zonas con diferentes niveles y condiciones de acceso:

- *Zona pública*: Accesible en lectura sin restricciones, contenido:
  - Certificado CA intermedia emisora.
  - Claves Diffie-Hellman.
  - Certificado x.509 de componente.

- *Zona privada*: Accesible en lectura por el ciudadano, mediante la utilización de la Clave Personal de Acceso o PIN, contenido:
  - Certificado de Firma (Firma-e).
  - Certificado de Autenticación (No repudio).
- *Zona de seguridad:* Accesible en lectura por el ciudadano, en los Puntos de Actualización del DNIe .
  - Datos de filiación del ciudadano (los mismos que están impresos en el soporte físico del DNI), contenidos en el soporte físico del DNI.
  - Imagen de la fotografía.
  - Imagen de la firma manuscrita.
  - La plantilla biométrica de la impresión dactilar.

Desde una óptica funcional, el DNIe ofrece, actualmente, dos prestaciones básicas: identificación y firma electrónica; siendo sus ámbitos de aplicación, entre otros y a modo de ejemplo, los que se citan a continuación:

- Realización de compras **firmadas** a través de Internet.
- Ejecución completa de **trámites** con las Administraciones Públicas a cualquier hora y sin tener que desplazarse ni hacer colas.
- Realización de **transacciones seguras** con entidades financieras.
- Acceso físico a edificios.
- Utilización de **forma segura nuestro ordenador personal**.
- Participación en una conversación por Internet con la certeza de que nuestro interlocutor es quien dice ser.

El logro de estas funcionalidades se apoya en los elementos que incluye la tarjeta del DNIe , entre los que cabe citar, de manera destacada, los *certificados digitales* que se encuentran dentro de la "zona privada" y que solo podrán ser accedidos mediante el uso de un código personal (PIN) conocido por el usuario. Se trata del Certificado de Autenticación y el Certificado de Firma.

- *Certificado de Autenticación.* Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación asegura que la comunicación electrónica se realiza con el interlocutor legítimo (la persona es quien dice ser). El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.

- El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).
- *Certificado de Firma.* Este certificado permitirá firmar - con firma-e reconocida, según *Ley 59/2003, de 19 de diciembre, de firma electrónica* - acciones y asumir compromisos, de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él. El certificado de firma es del tipo X.509 v3 estándar; tiene activo en el *Key Usage* el bit de *ContentCommitment* (No Repudio); y está asociado a un par de claves (pública y privada), generadas en el interior del chip del DNIe.

Otro elemento a destacar en la seguridad del DNI digital es la identificación de los usuarios mediante datos biométricos. La tarjeta DNIe permite realizar una identificación biométrica en los puntos de acceso que estén preparados para ello. En el proceso de autenticación, el usuario coloca el dedo en el dispositivo lector de huellas, introduce el DNIe y posteriormente se procede a la evaluación de correspondencia entre la huella presentada y la que se encuentra almacenada digitalmente en el interior del chip. Si esta comprobación resulta positiva, el usuario será correctamente identificado. Esta funcionalidad está actualmente restringida a su uso en los centros de emisión del DNIe, no estando disponible fuera del entorno de la DGP.

Por otro lado, para solicitar el DNIe, el ciudadano se ha de presentar en las dependencias del Cuerpo Nacional de Policía donde se realizarán todos los trámites que conllevan la creación de un nuevo DNIe de forma transparente para el usuario. La Dirección General de la Policía y de la Guardia Civil (Ministerio de Interior) actúa como Autoridad de Certificación (AC), mientras que la Autoridad de Registro está constituida por todas las oficinas de expedición del DNIe.

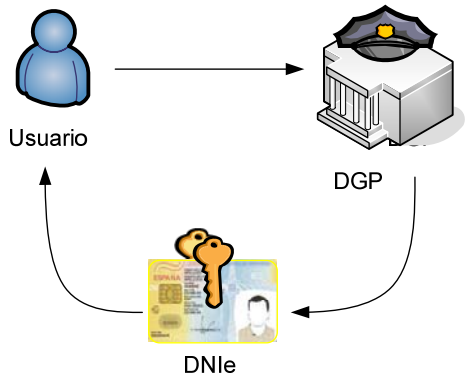


Figura 9. Solicitud del DNIe

En la Infraestructura de Clave Pública adoptada para el DNI electrónico, se ha optado por asignar las funciones de Autoridad de Validación a entidades diferentes de la Autoridad de Certificación, a fin de aislar la comprobación de la vigencia de un certificado electrónico de los datos de identidad de su titular. Actualmente están disponibles como Centros de Validación, el MAP para la Administración Pública y FNMT para el resto, estando previsto que el Ministerio de Industria / Red.es se convierta en el tercer validador del DNIe.

Así, la Autoridad de Certificación (Ministerio del Interior – Dirección General de la Policía y la Guardia Civil) no tiene, en modo alguno, acceso a los datos de las transacciones que se realicen con los certificados que ella emite y las Autoridades de Validación no tiene acceso a la identidad de los titulares de los certificados electrónico que maneja, reforzando – aún más, si cabe - la fiabilidad del sistema.

Por otro lado los certificados electrónicos reconocidos incorporados al DNIe tendrán un periodo de vigencia de treinta meses, siempre que este periodo no supere el del soporte físico, en cuyo caso, la fecha de caducidad del certificado vendrá determinada por la del soporte.

La verificación de las revocaciones es obligatoria para cada uso de los certificados de identidad pública. El procedimiento ordinario de comprobación de la validez de un certificado será la consulta a los Prestadores de Servicios de Validación, los cuales, mediante el protocolo OCSP, indicarán el estado del certificado.

A continuación se incluye un extracto del documento **Guia_de_referencia_basica_v1.0.pdf** que se puede descargar desde la página www.dnielectronico.es y que resume la funcionalidad del DNIe:

Descripción funcional del DNI electrónico:

- *Nuevas capacidades. Identificación.*
  - *El DNI electrónico, además de la capacidad de identificación física de su titular, posee la capacidad de identificación en medios telemáticos y de firmar electrónicamente como si de una forma manuscrita se tratase. De esta forma garantiza que la personalidad del firmante no es suplantada.*
  - *Asimismo la firma electrónica permite proteger la información enviada a través de un medio telemático.*

- *Firma electrónica.*
  - *La firma electrónica es el conjunto de datos en forma electrónica, consignados junto a otros o asociados con ellos, que pueden ser utilizados como medio de identificación del firmante.*
  - *La firma electrónica permite que tanto el receptor como el emisor de un contenido puedan identificarse mutuamente con la certeza de que son ellos los que están interactuando, evita que terceras personas intercepten esos contenidos y que los mismos puedan ser alterados, así como que alguna de las partes pueda "repudiar" la información que recibió de la otra y que inicialmente fue aceptada.*
  - *La firma electrónica avanzada es la firma electrónica que permite identificar al firmante y detectar cualquier cambio ulterior de los datos firmados, que está vinculada al firmante de manera única y a los datos a que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.*
  - *A su vez, se considera firma electrónica reconocida la firma electrónica avanzada basada en un certificado reconocido y generada mediante un dispositivo seguro de creación de firma. La firma electrónica reconocida tendrá respecto de los datos consignados en forma electrónica el mismo valor que la firma manuscrita en relación con los consignados en papel.*

- *Certificados electrónicos. Una breve descripción.*
  - *Son los documentos expedidos por los prestadores de servicios de certificación que relacionan las herramientas de firma electrónica que tiene cada usuario con su identidad, dándole a conocer como firmante en el ámbito telemático.*

El DNI electrónico contiene la siguiente información:

- *Certificados X509v3 de ciudadano (autenticación y firma) y claves privadas asociadas, que se generarán e insertarán durante el proceso de expedición del DNIe:*
  - *Cerificado de autenticación*

    El Ciudadano podrá, a través de su Certificado de Autenticación, certificar su identidad frente a terceros, demostrando la posesión y el acceso a la clave privada asociada a dicho certificado y que acredita su identidad.
  - *Cerificado de firma electrónica reconocida*

    Permitirá realizar y firmar acciones y asumir compromisos de forma electrónica, pudiéndose comprobar la integridad de los documentos firmados por el ciudadano haciendo uso de los instrumentos de firma incluidos en él.

Vida útil. Al hablar de vida útil se deben contemplar dos aspectos:

- *En primer lugar, la validez del DNI electrónico no varía según el DNI actual, manteniéndose los mismos periodos que actualmente (Artículo 6. Validez, RD 1553/2005, de 23 de diciembre), es decir:*
  - *Cinco años, cuando el titular no haya cumplido los treinta al momento de la expedición o renovación*
  - *Diez años, cuando el titular haya cumplido los treinta y no haya alcanzado los setenta.*
  - *Permanente cuando el titular haya cumplido los setenta años.*
- *En segundo lugar está la validez de los certificados contenidos en el chip de la tarjeta del DNI electrónico que tendrán un período de vigencia de treinta meses. (Artículo 12. Validez de los certificados electrónicos, RD 1553/2005, de 23 de diciembre)*

Uso del DNI electrónico *(Fuente www.dnielectronico.es)*

Tal y como recoge la Declaración de Prácticas de Certificación del DNI electrónico, los certificados electrónicos podrán utilizarse:

- *Como medio de Autenticación de la Identidad.*

  El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá, a través de su certificado, acreditar su identidad frente a cualquiera, ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.
- *Como medio de firma electrónica de documentos.*

Mediante la utilización del Certificado de Firma (nonRepudition), el receptor de un mensaje firmado electrónicamente puede verificar la autenticidad de esa firma, pudiendo de esta forma demostrar la identidad del firmante sin que éste pueda repudiarlo.

- *Como medio de certificación de Integridad de un documento.*

  Permite comprobar que el documento no ha sido modificado por ningún agente externo a la comunicación. La garantía de la integridad del documento se lleva a cabo mediante la utilización de funciones resumen (hash), utilizadas en combinación con la firma electrónica. Esto esquema permite comprobar si un mensaje firmado ha sido alterado posteriormente a su envío.

Para tal fin, utilizando la clave privada del ciudadano, se firma un resumen del documento, de forma tal que cualquier alteración posterior del documento dará lugar a una alteración del resumen.

El Certificado de Identidad Pública español (DNI electrónico) contribuirá, necesariamente a la existencia de empresas prestadoras de servicios de valor añadido ya que el DNI electrónico no facilitara en ningún caso los denominados "sobres" (sistemas de cifrado, sellos de tiempo, etc.)

De la misma forma favorecerá la aparición de iniciativas privadas que presten servicios de certificación a los ciudadanos. Esto se conseguirá en base a reconoce al DNI electrónico como medio suficiente para acreditar, la identidad y los demás datos personales de los interesados, pudiendo ser utilizado como medio de identificación para la realización de un registro fuerte que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

Escenario

Imaginemos la siguiente situación: un ciudadano establece una comunicación a través de Internet con un organismo de la Administración Pública (o una Entidad Privada) que ofrece un servicio telemático para que el ciudadano cumplimente un trámite administrativo que requiere su consentimiento explicito para la realización.

Este escenario plantea el uso de los dos tipos de certificados electrónicos por parte del ciudadano:

- ***Certificado de Autenticación**: Tiene como finalidad garantizar electrónicamente la identidad del ciudadano al realizar una transacción telemática. El Certificado de Autenticación (Digital Signature) asegura que la comunicación electrónica se realiza con la persona que dice que es. El titular podrá a través de su certificado acreditar su identidad frente a cualquiera ya que se encuentra en posesión del certificado de identidad y de la clave privada asociada al mismo.*
- *El uso de este certificado no está habilitado en operaciones que requieran no repudio de origen, por tanto los terceros aceptantes y los prestadores de servicios no tendrán*

garantía del compromiso del titular del DNI con el contenido firmado. Su uso principal será para generar mensajes de autenticación (confirmación de la identidad) y de acceso seguro a sistemas informáticos (mediante establecimiento de canales privados y confidenciales con los prestadores de servicio).

Este certificado puede ser utilizado también como medio de identificación para la realización de un registro que permita la expedición de certificados reconocidos por parte de entidades privadas, sin verse estas obligadas a realizar una fuerte inversión en el despliegue y mantenimiento de una infraestructura de registro.

- *Certificado de Firma (nonRepudiation), cuyo fin es permitir al ciudadano firmar tramites o documentos. Este certificado (certificado cualificado según ETSI y las RFC3039, RFC3739) permite sustituir la firma manuscrita por la electrónica en las relaciones del ciudadano con terceros (Ley 59/2003, de firma electrónica, artículos 3.4 y 15.2).*

Descripción de Uso

Asumiendo que:

- *El ciudadano dispone de un DNI con capacidades electrónicas (criptográficas).*
- *Está conectando al servicio telemático de forma remota a través de Internet.*
- *Dispone de una instalación local con un lector de tarjetas inteligentes compatible (PC/SC).*
- *Cuenta con el CSP o el PKCS#11 del DNI electrónico. (librerías criptográficas del DNIe).*

a) Establecimiento de conexión privada con Organismo Público o Entidad Privada.

El siguiente esquema de comunicaciones establece el protocolo a seguir para el establecimiento de un canal privado y autenticado entre el ciudadano y el Organismo Público o Entidad Privada. El canal establecido queda autenticado en ambos extremos por el uso de certificados que garantizan la identidad de las partes:

1. *El Ciudadano hace una petición de conexión segura autenticada.*
2. *El Organismo Público (o Entidad Privada) crea un mensaje autenticado y lo envía al ciudadano.*
3. *El Ciudadano verifica la validez del certificado de servidor ofrecido.*
4. *Se genera la clave de sesión y cifrado de la misma con la clave pública del El Organismo Público (o Entidad Privada).*
5. *Se construye el mensaje de intercambio de claves.*

6. *El Ciudadano introduce el DNI electrónico en el lector, introduce su clave de acceso personal (PIN) para el acceso al certificado electrónico de Autenticación y, con éste certificado, valida el mensaje de intercambio de claves.*
7. *Se establece el canal privado.*
8. *El Organismo Público (o Entidad Privada) verifica el mensaje de establecimiento de sesión.*
9. *El Organismo Público (o Entidad Privada) comprueba en la Autoridad de Validación el estado validez del Certificado de Autenticación del Ciudadano.*
10. *Se establece un canal seguro, se cierra túnel SSL.*

Tal y como queda reflejado en el esquema anterior, el proceso de autenticación entre ambas partes para el establecimiento de un canal seguro requiere del uso de:

- *Certificado de Organismo Público (o Entidad Privada): Este certificado asociado al servidor del Organismo o Entidad garantiza que el ciudadano se esta conectando a dicho organismo y no a otro. El certificado utilizado por el Organismo o Entidad no es en ningún caso emitido por la DGP o el Ministerio del Interior, la veracidad de este certificado deberá ser garantizada por una Autoridad de Certificación diferente de la DGP y sujeta a la Ley de Firma Electrónica 59/2003 en el marco de obligaciones aplicables a los prestadores de servicios de certificación.*
- *Certificado de autenticación del ciudadano. El ciudadano para autenticarse frente al Organismo (o Entidad Privada) dispone de un certificado con capacidad de autenticación. De esta forma el Organismo (o Entidad Privada) podrá determinar la identidad del ciudadano para ofrecerle un servicio personalizado. La veracidad de este certificado vendrá determinada por la Dirección General de la Policía.*

Las partes implicadas para el establecimiento del canal privado son:

- ***DNI electrónico:** Dispositivo de firma y autenticación segura en posesión del ciudadano emitido por la Institución del DNI, que contendrá:*
  - *Conjunto de claves privadas al ciudadano.*
  - *Conjunto de certificados del ciudadano.*
  - *Elementos de seguridad para garantizar la integridad del documento frente a posibles alteraciones.*
- ***Ciudadano:** Persona física titular del DNI electrónico.*
- ***Organismo Público** (o Entidad Privada): Proveedor de servicios.*
- ***Autoridad de Validación:** Servicio informativo del estado de validez de los certificados del ciudadano.*

Usabilidad

El protocolo descrito en el esquema corresponde al establecimiento de una sesión SSL (Secure Socket Layer). La elección de este mecanismo viene determinada por que prácticamente el 100% de los servidores y clientes utilizados disponen de esta capacidad.

Este protocolo permite el establecimiento de canales privados con los proveedores de servicios, organismos públicos u otros. Si bien, existen dos tipos de canales:

- ***Autenticación Servidor:** En esta modalidad, sólo el servidor requiere tener un certificado por lo que la identidad del cliente, el ciudadano en nuestro caso, será anónima.*
- ***Autenticación Servidor-Cliente:** Requiere que tanto el proveedor de servicios se autentique frente al cliente (ciudadano), como que el cliente se autentique frente al servidor. (**Este es el ideal recomendado**)*

La diferencia real en cuanto a usabilidad estriba principalmente en que si el proveedor de servicios, puede determinar con garantía la identidad del ciudadano estará en disposición de ofrecerle información personalizada.

La utilización del certificado de Autenticación del DNI electrónico garantiza la identidad del ciudadano, y podrá ser utilizado por los proveedores de servicios para establecer reglas de acceso a la información en base a la identidad del mismo.

b) Firma de Trámites Administrativos con DNI electrónico.

El siguiente esquema establece el protocolo a seguir para la firma de formularios electrónicos, mediante el uso del DNI electrónico, cumpliendo con la normativa sujeta al uso de certificados cualificados:

1. *El Organismo Público (o Entidad Privada) envía el formulario para el trámite administrativo.*
2. *El Ciudadano cumplimenta el formulario y lo envía.*
3. *El Organismo Público (o Entidad Privada) reconstruye el formulario en formato texto y lo reenvía nuevamente al ciudadano.*
4. *El Ciudadano verifica que el trámite administrativo se corresponde exactamente con el cumplimentado.*
5. *Se solicita al ciudadano la firma electrónica del formulario.*
6. *El Ciudadano introduce su clave de acceso personal (PIN) para el acceso al certificado de Firma (nonRepudiation).*
7. *El DNI electrónico firma electrónicamente el formulario.*
8. *El Ciudadano envía formulario firmado al El Organismo Público (o Entidad Privada).*

9. *El Organismo Público (o Entidad Privada) verifica validez de la firma, para comprobar integridad formulario.*
10. *El Organismo Público (o Entidad Privada) comprueba en la Autoridad de Validación estado validez certificado de Firma (nonRepudiation) del ciudadano.*
11. *Si es correcto, continuar el procedimiento…*

Conviene recordar que para llevar a cabo un proceso de firma electrónica debemos disponer de una aplicación informática que nos permita realizar esta funcionalidad.

Hay dos alternativas tecnológicas para disponer de la funcionalidad de firma electrónica:

- *La funcionalidad de firma electrónica se logra a través de una aplicación informática previamente instalada en nuestro equipo.*
- *La funcionalidad de firma electrónica está incluida en el proceso general del prestador de servicios telemáticos, por lo que no es necesario descargar e instalar ninguna aplicación de firma electrónica.*

Confirmación por parte del organismo de la correcta recepción del trámite.

El trámite administrativo se completa con la entrega por parte del Organismo receptor del formulario firmado con acuse de recibo. Aunque este trámite es ajeno al DNI electrónico, parece necesario que el prestador del servicio ofrezca garantía al ciudadano de la correcta realización del trámite efectuado. Dentro de unas buenas prácticas el prestador de servicios deberá proporcionar al ciudadano un recibo indicando que su trámite ha sido aceptado.

El siguiente esquema muestra el protocolo a seguir entre las diferentes partes:

12. *El Organismo Público (o Entidad Privada) confecciona el recibo para el trámite cumplimentado por el ciudadano.*
13. *El Organismo Público (o Entidad Privada) firma el recibo.*
14. *El recibo es firmado y sellado por una Tercera parte de confianza, denominada Autoridad de Sellos de Tiempo (que garantiza el instante exacto en el que un trámite fue aceptado por el prestador de servicios, y debe ser evidentemente una entidad externa a dicho prestador y reconocida en el ámbito de la legislación española).*
15. *Se envía al Ciudadano el recibo firmado y sellado.*

(Fuente www.dnielectronico.es)