GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, ENERGÍA Y TURISMO

INTECO
Instituto Nacional de Tecnologías de la Comunicación

Guía sobre riesgos y buenas prácticas en autenticación online

INSTITUTO NACIONAL DE **TECNOLOGÍAS** DE LA **COMUNICACIÓN**

Edición: Noviembre 2012

La *"Guía sobre riesgos y buenas prácticas en autenticación online"* ha sido elaborada por el siguiente equipo de trabajo del Instituto Nacional de Tecnologías de la Comunicación (INTECO):

Pablo Pérez San-José (dirección)

Eduardo Álvarez Alonso (coordinación)

Susana de la Fuente Rodríguez

Cristina Gutiérrez Borge

Asimismo, ha contado con el apoyo técnico de Ignacio Alamillo (*Astrea La Infopista Jurídica*) y Ricard Martínez (Universitat de València)

El **Instituto Nacional de Tecnologías de la Comunicación (INTECO)** es una sociedad estatal adscrita al Ministerio de Industria, Energía y Turismo a través de la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información. La misión de INTECO es reforzar la ciberseguridad, la privacidad y la confianza en los servicios de la Sociedad de la Información, aportando valor a los ciudadanos, empresas, AA.PP. y al sector TIC, y coordinando esfuerzos con los organismos nacionales e internacionales que trabajan en esta materia. Su Observatorio de la Seguridad de la Información (http://observatorio.inteco.es) tiene como objetivo describir, analizar, asesorar y difundir la cultura de la seguridad, la privacidad y la e-confianza.

La realización de este documento se ha financiado dentro del proyecto SERPLAGO (*Servicios sobre plataforma cloud para procesos online de gobierno y administración electrónicos*) por la convocatoria 2011 del subprograma INNPACTO del Plan Nacional 2008-2011 del Ministerio de Economía y Competitividad, cofinanciada por los fondos FEDER de la UE.

Índice

1. Introducción

En la sociedad de la información nuestra identidad constituye un elemento valioso y merecedor de protección jurídica. A la hora de realizar una compra online, un trámite administrativo a través de Internet o al utilizar las redes sociales, por ejemplo, disponer de una identidad y poder ejercer un control real sobre sus distintos atributos constituye un elemento esencial para garantizar nuestros derechos. Más aún, a medida que la evolución de las tecnologías de la información genere nuevos productos y servicios, la gestión de la identidad en el entorno online se convertirá en un aspecto crítico y, por tanto, el proceso de autenticación de la misma será cada vez más importante.

El reconocimiento y la confirmación de la identidad de los usuarios es una de las tareas más extendidas y necesarias en la prestación de servicios y la autorización de accesos. El objetivo de estas tareas es que tanto los servicios como el acceso solamente puedan ser utilizados por los legítimos usuarios.

El desarrollo de la Sociedad de la Información y la prestación de servicios online han trasladado esta necesidad del mundo offline al mundo online. Esto se debe a que tanto los servicios web como las cuentas y perfiles en ellos tienen un titular, que es la persona autorizada para acceder a su información y actuar a través de ellos.

Ante esta situación, desde los inicios de Internet surge la necesidad de restringir los accesos y de comprobar que las personas que se comunican a través de este canal son realmente quienes dicen ser. Esta comprobación es de especial importancia en determinados casos, tales como:

- Administración electrónica. Es muy importante que cualquier tipo de relación con las Administraciones Públicas se lleve a cabo exclusivamente por parte de las personas que tienen derecho a acceder a la información y por los propios interesados o sus representantes legales. Este requerimiento es tan importante en las relaciones presenciales como en las relaciones a través de las nuevas tecnologías.

- Banca online y comercio electrónico. El acceso a cuentas bancarias y la posibilidad realizar transacciones económicas exige que solamente puedan ser llevadas a cabo por las personas con la autorización necesaria para ello. Del mismo modo, esta comprobación de la identidad de quien va a realizar estas operaciones se debe llevar a cabo también cuando el medio utilizado es Internet.

- Firma de documentos. También se debe asegurar la identidad de quien firma un documento, tanto en el caso de necesitarse comprobar la autoría de un documento como en el de la firma de documentos que supongan acuerdos vinculantes o contratos.

- Acceso a servicios o espacios web restringidos. Este es el caso de la mayor parte de usos de Internet, ya se trate del acceso a cuentas de correo electrónico, perfiles en redes sociales o cualquier otro servicio. De nuevo, este acceso debe ser autorizado únicamente a las personas que tengan permiso para ello, teniendo por tanto que comprobarse su identidad.

En estos y otros casos, al ser necesaria la comprobación de la identidad y de sus permisos, se establecen diferentes mecanismos de autenticación que permiten confirmar que la persona que trata de realizar determinadas acciones es realmente la autorizada para ello. La importancia de estos mecanismos se incrementa constantemente a medida que avanza la implantación y desarrollo de la Sociedad de la Información, ya que los ciudadanos utilizan más servicios online y almacenan más información en diferentes perfiles y cuentas en Internet.

Por ello, INTECO ha elaborado esta ***Guía sobre riesgos y buenas prácticas en autenticación online***, con el propósito de aportar información de utilidad que ayude a que estos mecanismos de identificación y verificación de la identidad en Internet se implanten correctamente y se utilicen de modo que cumplan con su función respetando los derechos de los implicados.

En ella se exponen las características y los aspectos a tener en cuenta respecto a los procesos de identificación y verificación, sus diferentes tipos en función a diversos aspectos y las implicaciones legales a considerar. Al mismo tiempo, se determinan cuáles son los principales riesgos y amenazas en relación a estos procesos y una serie de buenas prácticas y recomendaciones que ayuden a los usuarios y a los desarrolladores a evitarlos.

En todo momento se utiliza el término autenticación para así englobar dos posibilidades diferentes: la identificación (el sistema reconoce al usuario y su identidad) y la verificación (el sistema confirma que el usuario es quien dice ser). A pesar de ello, es habitual que se utilice el término identificación como sinónimo de autenticación, englobando las dos posibilidades mencionadas y refiriéndose por lo general a la verificación, ya que es el caso más habitual.

2. La autenticación online

Sin duda la autenticación es uno de los principales elementos sobre los que se asienta Internet y es una pieza indispensable para el desarrollo de los servicios de la Sociedad de la Información. Básicamente consiste en constatar que quien trata de acceder a determinada información o servicios es quien dice ser y está legitimado para ello. Los procesos de registro y autenticación garantizan la privacidad y el acceso exclusivo a determinados servicios e informaciones.

A pesar de que el registro y la autenticación son los dos momentos clave para el acceso de los usuarios a los diferentes usos y servicios online, es necesario recordar que existe otro proceso esencial, la conexión entre el dispositivo que utiliza el usuario y los servidores en los que se encuentra la información a la que quiere acceder. Por ello, es necesario conocer inicialmente cuáles son los pasos que se siguen al establecer una conexión y cómo se confirma que la conexión se lleva a cabo de un modo seguro.

2.1 LOS RASGOS DE AUTENTICACIÓN

El empleo de las tecnologías de comunicación electrónica que soportan Internet requiere de informaciones que constituyen rasgos identificadores que permiten la trazabilidad de los usuarios, es decir, el seguimiento del usuario a lo largo de diferentes pasos, registrándose todas sus acciones al tiempo que se confirma que se trata del mismo usuario, o al menos que la conexión se realiza continuamente desde el mismo dispositivo.

Así, estos elementos no solo se refieren al propio usuario, ya que al realizar conexiones en Internet es necesario tanto asegurar que el usuario que accede tiene permisos para ello como establecer una serie de líneas de comunicación señalando los dispositivos a conectar y los puntos de conexión exactos en diferentes niveles[1]:

[1] Una explicación más simple sobre el establecimiento de conexiones en Internet y su protección se encuentra en el artículo del Cuaderno de Notas "*Cortafuegos (firewalls): Qué son y para qué sirven*", disponible en: http://www.inteco.es/Seguridad/Observatorio/Articulos/UD_Cortafuegos.

- En el acceso físico del usuario, referido a dispositivos informáticos como por ejemplo un ordenador, consola o teléfono móvil, la comprobación de identidad se emplea para proteger y controlar el acceso a dicho dispositivo, a través de un identificador de usuario y otros elementos como puede ser una contraseña. Este sistema es muy similar al acceso a los servicios y aplicaciones online que se realiza posteriormente y que centra el análisis de este documento.

- En el enlace a Internet se gestiona la conexión entre el dispositivo anteriormente indicado y la red. En este paso se emplea la dirección MAC de la tarjeta de red del dispositivo como elemento de identificación. De esta forma se permite establecer medidas de seguridad como la lista de control de acceso del equipo a una red inalámbrica, prohibiendo o permitiendo la conexión de un dispositivo en concreto.

- En la capa de red de Internet, que se encarga de la comunicación de datos, la dirección IP sirve para señalar el dispositivo de origen y el dispositivo de destino de los mensajes que se intercambian a través de Internet[2], contando ambos equipos con su propia dirección IP. Esta identificación es especialmente importante no solo para la comunicación entre estos dos dispositivos, sino también frente a otros equipos y sistemas.

- En la capa de transporte de Internet, que se encarga del establecimiento de conexiones entre dispositivos para el envío y la recepción de flujos de datos entre aplicaciones, los puertos TCP/UDP complementan a la dirección IP, señalando así, además del equipo a conectar, a través de cuál de los múltiples puntos de conexión con que cuenta cada equipo se debe transmitir y/o recibir la información.

- En cuanto al funcionamiento de las aplicaciones o programas, existe una gran variedad de elementos de autenticación digitales, con niveles de seguridad apropiados para las necesidades concretas de cada servicio electrónico al que se accede. Por ejemplo, la dirección de correo electrónico de un usuario se ha convertido de forma progresiva en el principal atributo de la identidad digital que un individuo utiliza en Internet.

  Asimismo, también ha surgido un importante conjunto de mecanismos de autenticación, incluyendo contraseñas (contraseñas estáticas[3], contraseñas dinámicas o de un solo uso[4], o basadas en hardware portátil como dispositivos

[2] Los rangos de direcciones IP públicas y, por tanto, visibles en Internet, son asignados por la *Internet Assigned Numbers Authority* (IANA), un departamento de la *Internet Corporation for Assigned Names and Numbers* (ICANN), mediante un sistema global de registro.

[3] Las contraseñas estáticas son credenciales que se pueden emplear en múltiples procedimientos de autenticación. Pueden tener un periodo de vigencia transcurrido el cual se deben cambiar.

[4] Las contraseñas dinámicas o de un solo uso se generan para cada operación de autenticación, de forma que no se repiten jamás, Son, por tanto, credenciales no reutilizables.

USB[5]), certificados digitales (como los certificados X.509 de identidad[6]) e identificadores electrónicos nacionales[7], así como múltiples mecanismos biométricos.

- Finalmente, en la capa de base de datos se encuentran múltiples fichas o registros de los usuarios y sus elementos de autenticación. La gestión informatizada de los procesos exige la creación y gestión de estos registros, constituyendo verdaderas colecciones de datos de identificación que se pueden posteriormente interconectar, intercambiar y procesar para múltiples finalidades, de acuerdo con la legislación aplicable.

Existen, por tanto, múltiples atributos o informaciones que se pueden utilizar para comprobar la identidad de un usuario y de los dispositivos que utiliza.

2.2 FACTORES DE AUTENTICACIÓN

Si bien la mayor parte de los pasos o niveles expuestos se mantienen en funcionamiento e intermedian las comunicaciones sin que el usuario lo perciba, el último paso siempre es visible y habitualmente es el único considerado por los usuarios. Así, la confrontación de la información que aporta el usuario para atestiguar su identidad frente a la información almacenada en la base de datos del proveedor de servicios es el conocido como proceso de autenticación.

La autenticación consiste en la comprobación de la identidad de un usuario, generalmente un usuario que desea acceder a determinada información o servicios aunque puede afectar a acciones como la firma de un documento.

Para llevar a cabo esta autenticación y comprobar que la persona que pretende acceder a un sistema o a unos servicios, o realizar una determinada acción, es un legítimo usuario se pueden utilizar diferentes elementos que ayudan a atestiguar su identidad, también conocidos como factores de autenticación.

2.2.1 Conocimiento

El principal factor utilizado en la actualidad para comprobar que un usuario realmente es quien dice ser es demostrar que conoce determinados datos. De este modo, la mayor parte de los mecanismos de autenticación solicitan cierta información que únicamente el legítimo usuario debería conocer. Esta información puede ser muy variada, pero generalmente se reduce al uso de contraseñas.

[5] Para incrementar la seguridad, en ocasiones el generador de contraseñas se contiene en un dispositivo físico con pantalla, o bien en un dispositivo físico que se conecta al ordenador desde el que se accede al servicio.

[6] Los certificados son documentos electrónicos que permiten verificar firmas digitales generadas para acreditar la identidad de la persona que se autentica, cuyos datos constan en el propio certificado.

[7] Los identificadores electrónicos nacionales son tarjetas de identidad expedidas por la autoridad competente, en cada Estado miembro de la Unión, que permite la identificación y firma electrónica de los ciudadanos, por lo que normalmente incluyen certificados X.509. En España, el DNI electrónico es el identificador electrónico nacional.

De forma residual, y habitualmente como un mecanismo de autenticación de emergencia cuando existen problemas al utilizar los procedimientos principales, se realizan determinadas preguntas cuyas respuestas están pre-establecidas por el usuario. Así, por ejemplo, en caso de que no sea posible el uso del sistema principal, se pueden utilizar preguntas personales sobre el legítimo usuario, como cuál es el nombre de su primera mascota o el del colegio en el que estudió.

Algunos servicios permiten mecanismos de autenticación más sofisticados; por ejemplo, actualmente las redes sociales pueden corroborar la identidad de un usuario mostrándole imágenes de sus contactos para que señale quiénes son esas personas.

Debido a la necesidad de que estos conocimientos únicamente puedan ser demostrados por el legítimo usuario, algunos de estos mecanismos no se están utilizando masivamente, al tratarse de información que podría conocer una persona cercana al mismo. Es por ello que predomina claramente el uso de contraseñas.

2.2.2 Posesión

El segundo factor que se puede utilizar en los procesos de autenticación es la posesión de diferentes elementos. Si bien el más utilizado es la posesión de tarjetas inteligentes y, en particular, tarjetas criptográficas[8], no obstante, es relativamente sencillo convertir un simple dispositivo de almacenamiento (memoria USB) en una "llave"[9] utilizando ciertas aplicaciones informáticas.

De este modo, el usuario debe utilizar un dispositivo que el sistema reconocerá para acreditar su identidad. Las necesidades respecto a este sistema se centran en que el usuario se asegure de que nadie pueda acceder a dicho dispositivo. Obviamente, también es un requisito indispensable que el usuario tenga el dispositivo consigo siempre que quiera utilizar el sistema.

En España el DNI electrónico es el dispositivo de autenticación electrónica más extendido, ya que actualmente lo poseen más de 30 millones de españoles y puede ser utilizado con estos fines en diferentes servicios, especialmente en las relaciones electrónicas con las Administraciones Públicas[10].

2.2.3 Biometría

El tercer factor utilizado se centra en cómo es el usuario e incluso en cómo actúa, se trata de la biometría[11]. Estos sistemas utilizan los rasgos físicos o de comportamiento del

[8] Estas tarjetas pueden producir credenciales muy seguras, así como firmas digitales.

[9] http://bitelia.com/2012/10/unidad-usb-autenticacion

[10] Más información en INTECO (2010): *Guía para el uso seguro del DNI electrónico en Internet* http://www.inteco.es/Seguridad/Observatorio/guias/guia_DNIe

[11] Más información en INTECO (2011): *Guía sobre las tecnologías biométricas aplicadas a la seguridad:* http://www.inteco.es/Seguridad/Observatorio/guias/guia_biometria

usuario para confirmar su identidad, al considerarse que dichos rasgos son, en buena medida, únicos para cada persona e inimitables.

Existe gran variedad de técnicas biométricas, desde los análisis más conocidos de huella dactilar, iris o voz hasta técnicas más novedosas como el escaneo de las venas de la mano o la cadencia de la escritura en un teclado.

Debido a diferentes causas, estas técnicas de autenticación todavía son muy poco utilizadas en los procesos online, destinándose especialmente al acceso físico a instalaciones.

2.2.4 Multi-factor

Si bien los tres factores expuestos son los más habituales, es posible que se establezcan sistemas en los que se utilice una combinación de dos de ellos e incluso de los tres. Se define como autenticación basada en doble factor o multi-factor, y por lo general incluye siempre el factor conocimiento. Así, es poco habitual que un sistema de autenticación se centre en la posesión de elementos físicos o en la biometría sin incluir un sistema de contraseñas.

El uso de sistemas multi-factor aumenta considerablemente los niveles de seguridad.

2.3 PROCESO DE REGISTRO

Una vez que se ha determinado el tipo de información que se utilizará como credencial de autenticación, se debe concretar exactamente cuál será esa credencial. Esto se establece en el proceso de registro, es decir, cuando el usuario es inscrito como usuario legítimo por primera vez en el sistema. A pesar de ello, habitualmente esta determinación no es definitiva ni invariable, ya que se suele dejar abierta la posibilidad de modificación y en muchos casos es recomendable que esta modificación se realice de forma regular[12].

2.3.1 Elección de credenciales

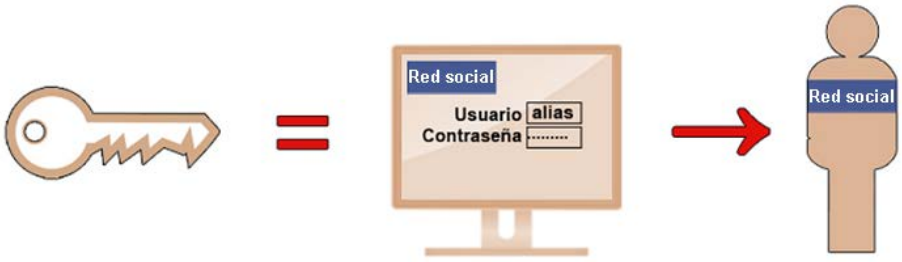
Los métodos de autenticación normalmente son decididos por el proveedor de servicios o el creador de las aplicaciones utilizadas en el proceso, pero la determinación de la información o credencial exacta puede ser llevada a cabo por diferentes actores.

Credenciales de primera parte

Las credenciales de primera parte son aquellas que el usuario se asigna a sí mismo. De este modo, la persona registrada y el proveedor de credenciales de identidad coinciden.

Esta elección se realiza libremente dentro de unas normas mínimas exigidas por el proveedor de servicios o por el administrador del sistema de autenticación.

[12] En concreto, en el caso de las credenciales consistentes en contraseñas estáticas. En algunos casos, este procedimiento de cambio de contraseña es legalmente exigible.



El más claro ejemplo de este tipo de credenciales son los nombres de usuario y contraseñas que se establecen al abrir una cuenta de correo electrónico o un perfil en redes sociales. El propio usuario decide ambos elementos con las posibles restricciones en cuanto a no poder utilizar un nombre de usuario ya existente o las exigencias de longitud y complejidad de las contraseñas para establecer unos niveles mínimos de seguridad.

Credenciales de segunda parte

Estas credenciales son aquellas que son impuestas por el proveedor de servicios o por el administrador del sistema de autenticación. En este caso, el usuario no tiene capacidad de elección.

Ejemplos de este tipo de credenciales son los dispositivos físicos de identificación, como tarjetas de coordenadas o *tokens*, que el proveedor de servicios suministre a sus clientes para su autenticación. En estos casos el usuario no cuenta con capacidad de decisión o modificación de estos dispositivos.

Si bien el nombre de usuario se puede considerar como parte de las credenciales de autenticación y éste en algunas ocasiones es impuesto al usuario según una política para su creación, en muchos de estos casos el usuario cuenta con la posibilidad de modificación de otra parte de las credenciales como son las contraseñas. En esos casos se podría tratar de una situación intermedia entre las credenciales de primera parte y de segunda parte.

Credenciales de tercera parte

Las credenciales de tercera parte son aquellas que no son determinadas por los usuarios pero tampoco por el proveedor de servicios o el administrador del sistema de autenticación que las va a utilizar. En su lugar, estas credenciales son determinadas por un proveedor de credenciales para su uso en las relaciones del usuario con otras personas y organizaciones diferentes a dicho proveedor.

Se trata de la intermediación de un tercero que otorga al usuario unas credenciales que podrá usar en otras situaciones y en relaciones en las que este proveedor de credenciales no se verá implicado directamente.

El principal ejemplo de este tipo de credenciales es el DNI electrónico, ya que se trata de un documento acreditativo establecido por un proveedor de credenciales (el Ministerio del Interior en este caso) para su utilización por parte del usuario para poder atestiguar su identidad frente a otros agentes, sean éstos particulares, empresas, organizaciones u otros organismos de las Administraciones Públicas.

2.3.2 Correspondencia entre identidad real e identidad digital

Además de la elección de las credenciales, en el proceso de registro se plantea una situación de mayor relevancia, la comprobación de que quien establece el registro es realmente quien dice ser. Es decir, un proceso de verificación previo.

Esta actuación se puede llevar a cabo de diferentes modos, pudiendo suponer cada uno un mayor o menor nivel de comprobación de esta correspondencia. A continuación se presentan algunos de los métodos de comprobación más utilizados en la actualidad.

Perfil o cuenta previamente creada

Uno de los mecanismos más utilizados es el uso de una cuenta ya creada en otros servicios online, habitualmente de correo electrónico aunque actualmente también se utilizan las cuentas o perfiles en redes sociales. De este modo, se puede enviar un enlace de comprobación a la cuenta de correo que el usuario indique y en caso de que ese enlace sea utilizado se entiende que el usuario que se registra es también el legítimo usuario de esa cuenta previa.

En estos casos no se puede considerar que se realice una comprobación de la correspondencia entre la identidad real y la identidad digital, es decir, no se está comprobando que la persona que se está registrando en el sistema sea realmente quien dice ser, sino que únicamente se están vinculando entre sí diferentes cuentas en distintos servicios.

Comprobación presencial

En este caso, en algún momento del registro es necesario que la persona que se está dando de alta en el sistema acuda a un lugar en el que se comprobará su identidad.

Ejemplo de esta forma de comprobación es la apertura de una cuenta de banca electrónica, ya que habitualmente se realiza a partir de una cuenta bancaria tradicional, siendo necesario acudir a una sucursal bancaria al menos para solicitar el acceso online y que se le entreguen en persona sus credenciales.

Utilización de certificaciones

El tercer método de comprobación de esta correspondencia es el uso de ciertas acreditaciones como el DNIe que atestiguan la identidad de una persona. De este modo, y debido a que el DNI es un documento oficial, personal e intransferible, de cuyo uso es responsable su titular, se puede llegar a realizar una comprobación efectiva sin necesidad de acudir físicamente a ningún lugar para completar el proceso de registro.

2.4 PROCESO DE AUTENTICACIÓN

Una vez que el usuario ha realizado el registro inicial en un sistema, el administrador de dicho sistema requerirá acreditar su identidad cuando quiera acceder al mismo. De este modo se evita que personas no autorizadas accedan a estos servicios o que alguien pueda hacerse pasar por un usuario legítimo suplantando su identidad. Es lo que se denomina autenticación.

La autenticación puede realizarse de dos modos distintos, la verificación y la identificación, en función de la información que tenga que aportar el usuario.

2.4.1 Verificación

Se trata del procedimiento más habitual. En él, la persona que quiere acceder al sistema debe señalar qué usuario registrado es (mediante un nombre de usuario, una cuenta de correo electrónico o el método que se determinase en el registro) y presentar sus credenciales de acceso (contraseña, elemento físico o rasgo personal). Dicho de otro modo, el usuario indica quién es y lo demuestra de la forma establecida.

Así, el sistema únicamente debe verificar que ambos elementos coinciden en sus bases de datos, es decir, que las credenciales de acceso presentadas son las mismas que se han registrado previamente para el usuario señalado.

En caso de que ambas informaciones concuerden se considerará que la persona que pretende acceder al sistema es realmente el legítimo usuario y se permitirá dicho acceso.

En caso de que no coincidan la respuesta dependerá de lo establecido por el administrador del sistema, siendo lo más habitual solicitar que se repita el intento de acceso. En caso de que la incongruencia se produzca repetidas veces, es posible que el administrador determine un bloqueo automático de la cuenta y abra una nueva posibilidad de acceso, ya sea utilizando una autenticación basada en conocimientos (al realizar preguntas cuya respuesta debería conocer únicamente el legítimo usuario) o una autenticación basada en la posesión (por ejemplo enviando un mensaje a una cuenta de correo electrónico o un número de teléfono previamente vinculados).

2.4.2 Identificación

Este segundo tipo de procedimiento es más sencillo para el usuario, pero mucho más complejo para el propio sistema al requerir mayores capacidades de computación. En él, el usuario en lugar de aportar dos tipos de informaciones solamente aporta sus credenciales. Así, el sistema es el encargado de identificar qué usuario registrado es el que se está autenticando.

Este procedimiento consiste en la comparación de las credenciales que aporta el usuario con todas las registradas en el sistema, lo cual implica mayores necesidades en la capacidad de computación del sistema y un mayor tiempo de espera para realizar la identificación.

Debido a los diversos problemas que podría acarrear este método en cuanto a las posibilidades de suplantación de identidad, es poco corriente, y en caso de ser utilizado únicamente lo sería en sistemas que basan las credenciales en la posesión de elementos físicos o en los rasgos físicos, siendo este segundo caso el que mayor seguridad aportaría.

2.4.3 Escenarios de autenticación

Del mismo modo que existen diferentes formas de determinación de credenciales y de comprobación de identidades en el registro, existen tres escenarios de autenticación online, en función del mecanismo empleado y de quién sea el agente que la lleve a cabo.

Autenticación directa

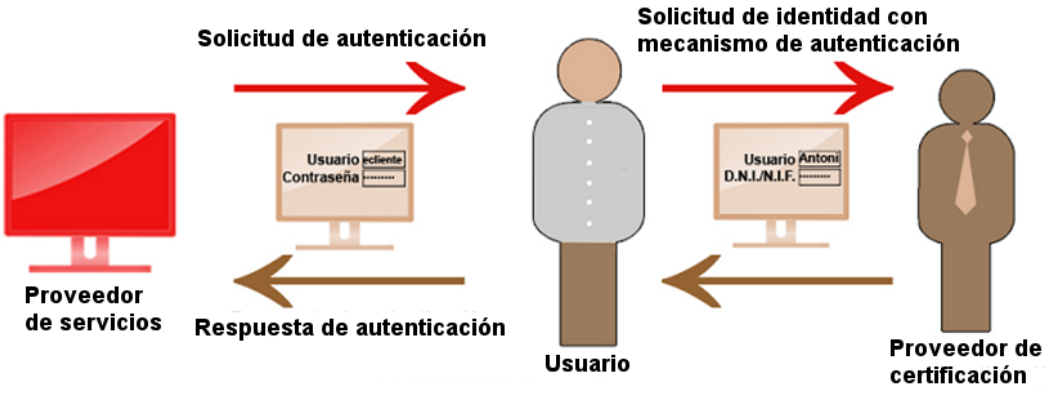
Los sistemas de autenticación directa son aquellos que se basan en la interacción entre el usuario y la organización que necesita autenticarle y suministra el mecanismo de autenticación.

Una gran parte de los sistemas de autenticación actualmente existentes se basan en el intercambio de contraseñas y otras informaciones conocidas por ambas partes

(credenciales de primera o de segunda parte), que se relacionan de forma directa. Resulta frecuente que la relación entre el usuario y el proveedor se base en este tipo de sistemas.

Autenticación certificada

Estos sistemas se basan en el empleo de certificados electrónicos de clave pública (habitualmente credenciales de tercera parte). Su principal ventaja es la posibilidad de autenticar a una persona sin necesidad de un registro presencial, dado que se puede confiar en la información de identificación del certificado, especialmente cuando la legislación aplicable establece contenidos mínimos, como es el caso del denominado certificado electrónico reconocido. Ejemplos de ello son el DNI electrónico y otros certificados de identificación como los expedidos a empresarios, trabajadores de organizaciones públicas o privadas, o a profesionales colegiados.



Cuando una persona dispone de un certificado reconocido, puede relacionarse con terceros y puede obtener de forma transparente su alta en un nuevo servicio, sin necesidad de volver a acreditar su identidad presencialmente, por lo que la confianza en el tráfico a través de Internet se incrementa.

Un certificado electrónico es un documento electrónico firmado[13] que garantiza, a las personas que lo reciben o que lo utilizan, una serie de manifestaciones contenidas en el mismo. Estas manifestaciones pueden referirse a la identidad de una persona, a la titularidad o posesión de una clave pública (y de la correspondiente clave privada), a sus autorizaciones (en forma de roles o permisos), a su capacidad de representar a otra persona física o jurídica, a su capacidad de pago, etc.

Estos certificados pueden ser emitidos tanto por organizaciones externas al usuario y al proveedor de servicios (por ejemplo el DNIe) o por este mismo proveedor (por ejemplo certificados para clientes o para miembros de una agrupación).

Existe una gran cantidad de posibles certificados, de los cuales sólo una pequeña parte ha sido regulada legalmente, con la finalidad de garantizar la identificación y la firma electrónica de las personas físicas y jurídicas y, más recientemente, de las Administraciones Públicas, sus órganos y entidades de derecho público.

Desde una perspectiva técnica, los certificados se pueden clasificar en tres grupos:

- **Los certificados de autoridad de certificación y de usuario final**. El certificado de autoridad de certificación se expide a un componente técnico de dicha autoridad, con la finalidad de establecer un modelo de confianza que permita comprobar y utilizar los certificados generados por ella (actividad que se denomina “prestación de servicios de certificación”).

  Por su parte, el certificado de usuario final se expide por una autoridad de certificación para firmar, verificar, cifrar o descifrar documentos por parte de usuarios finales del servicio (frecuentemente consumidores).

- **Los certificados de firma electrónica, de cifrado y de identidad**. El certificado de firma electrónica es un certificado de clave pública de usuario final que sirve para generar o para verificar firmas electrónicas. El certificado de cifrado es similar, pero sirve para cifrar y descifrar documentos. Por su parte, el certificado de firma electrónica y el de identificación son idénticos excepto en el uso autorizado de la clave, que en el primer caso se refiere a la actuación formalizada documentalmente, y en el segundo, únicamente la autenticación.

  Los tres se pueden combinar, de forma que un único certificado permita realizar todas estas acciones. Si además es reconocido, el prestador no podrá almacenar la clave privada que permite descifrar documentos.

[13] Por el prestador de servicios de certificación que lo expide, como garantía de seguridad y confianza en la mismo, de acuerdo con las obligaciones legales y, en su caso, convencionales que resulten aplicables.

- **Los certificados de identificación de dispositivo**. Dentro de esta categoría se incluyen todos los certificados que acreditan la identificación de un sistema, aplicación u objeto digital diferente de una persona.

  Algunos ejemplos relevantes son los certificados de sitio web, que acreditan la titularidad de una URL de Internet (incluyendo los certificados de servidor seguro con validación extendida, SSL EV) o los certificados de firma de código, que confirman la autoría de una aplicación descargada al equipo o dispositivo.

Autenticación federada

La autenticación federada es un tercer modelo de autenticación en el cual un conjunto de proveedores comparten la información de autenticación de sus usuarios y gestionan conjuntamente este proceso.

La gestión federada de la identidad es un conjunto de acuerdos, estándares y tecnologías que hacen que las identificaciones y las atribuciones (poderes, permisos, etc.) sean transportables entre dominios autónomos de seguridad, mediante el uso de aserciones o alegaciones de identidad.

En un entorno federado, la información de identidad es local a cada sistema, es decir, se encuentra en los equipos y servidores de cada sistema, pero puede enlazarse y emplearse de forma global, de modo que podría ser accesible para otros sistemas asociados.

En un escenario de autenticación federada, el usuario quiere acceder a un servicio electrónico de un proveedor de servicios con quien no tiene relación previa. Para ello se autentica directamente frente a su proveedor de credenciales, con el que ya ha realizado un registro previo, que le entrega un número para que el usuario lo entregue al tercero con el que no existía relación previa.

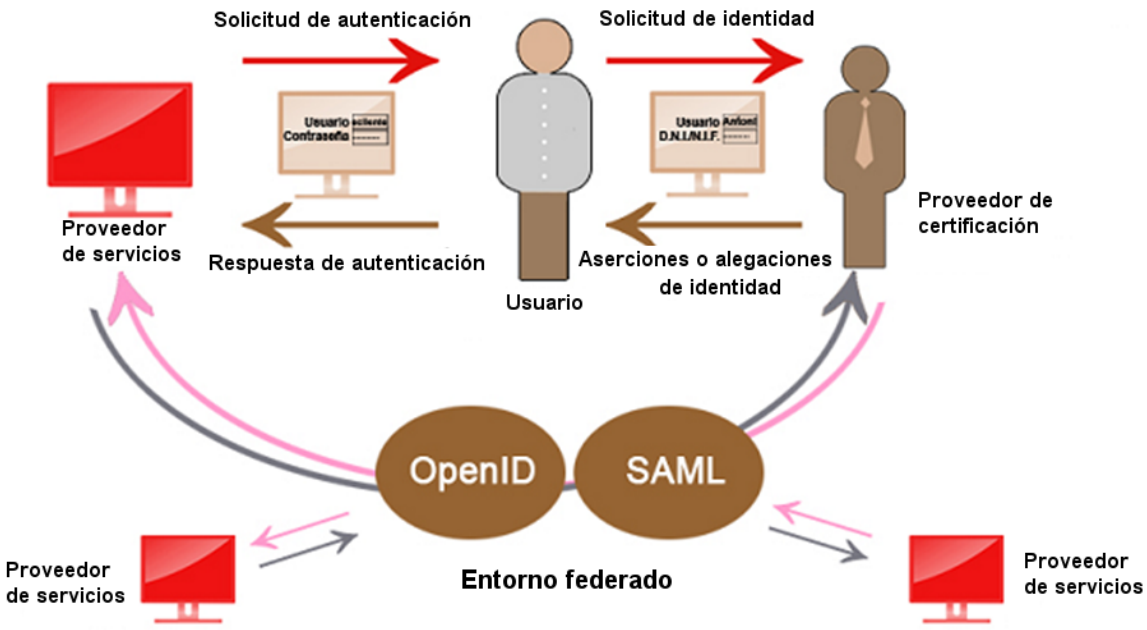
Mediante dicho número, el proveedor de servicios puede consultar al proveedor de credenciales acerca de la identidad del usuario. Finalmente, el proveedor de credenciales expide una credencial consistente en un documento electrónico[14] donde se incluyen estas informaciones sobre el usuario (la aserción).

Este mecanismo permite federar servicios de Internet en términos de identificación y autenticación, y se puede emplear para que cualquier credencial de primera o segunda parte se pueda emplear con terceros[15].

[14] Generalmente, este documento o aserción de identidad se encuentra firmado electrónicamente por el proveedor, para garantía del tercero al cual solicita acceso el usuario.

[15] Es decir, permite convertir un identificador de primera o de segunda parte en un identificador de tercera parte,

La federación de identificadores se está convirtiendo rápidamente en un elemento fundamental para lograr sistemas de autenticación en entornos ubicuos en los que el acceso a servicios e informaciones se puede realizar desde cualquier lugar y desde diferentes dispositivos. Esta tendencia está alineada con las nuevas redes y dispositivos de acceso (PDA, *Smart TV*, *tabletas*, *smartphones*, etc.) y su emplea masivamente en entornos como las redes sociales o los servicios de Cloud.



Para poder aprovechar estos mecanismos federados es necesario que los sistemas implicados utilicen determinados estándares tecnológicos y protocolos promovidos desde diferentes organismos. Entre los más destacados, podemos indicar los siguientes:

- **SAML.** Estándar de OASIS (Organization for the Advancement of Structured Information Standards) que especifica un marco de trabajo basado en XML para comunicar autenticaciones de usuario, así como atribuciones y autorizaciones, mediante manifestaciones (aserciones) de origen. Se trata de un protocolo flexible y extensible diseñado para ser empleado por otros estándares, como WS-Security, y supone la convergencia de todos ellos en una base común.

  SAML ofrece ventajas como el empleo de seudónimos y otros mecanismos de protección de datos personales, así como el uso de la firma electrónica.

  En general, los sistemas basados en alegaciones, como SAML, se emplean en la autenticación única de web (*web single sign-on*), la seguridad de servicios web y la autorización basada en atributos.

- **WS-I.** La iniciativa WS-I, acrónimo de la *Web Services Interoperability Organization*, persigue la creación de perfiles de interoperabilidad de los

servicios existentes, más que la creación de estándares nuevos. En este sentido se trabaja en la especificación de un perfil básico de seguridad (*basic security profile*), con el objeto de facilitar la seguridad de transporte de datos, de la mensajería SOAP y otros aspectos de los servicios de Internet.

- **XACML**. Protocolo que define un método para que las aplicaciones que requieran autenticaciones puedan acceder a recursos en nombre de un usuario, que previamente las ha autorizado, sin revelar su identidad. Se emplea en escenarios corporativos, para la obtención y traslado de autorizaciones.

- **OpenID.** Se trata de una iniciativa liderada por la *OpenID Foundation*, orientada a la definición de protocolos descentralizados de autenticación, el registro y el intercambio de atributos en el entorno Web.

  OpenID constituye un protocolo apropiado para la realización de operaciones de identificación digital en la Web social, debido especialmente a su elevada adopción por los prestadores de servicios de red social, comunidades virtuales, blogs y otros.

- **OAuth.** Protocolo de autorización de aplicaciones web actualmente más adoptado, por lo que promete convertirse en el estándar *de facto* para establecer la interfaz de colaboración social de proveedores de identidad (redes sociales, aplicaciones colaborativas, servicios de almacenamiento en "la nube"…), personas digitales y consumidores de identidad, en entornos tradicionales, móviles y virtuales.

3. Regulación legal de la autenticación de la identidad digital

3.1 EL RECONOCIMIENTO Y ATRIBUCIÓN DE LA IDENTIDAD

3.1.1 La atribución de signos de identidad a las personas físicas.

Desde el nacimiento y durante la posterior evolución de las personas se formalizan una serie de actos jurídicos que permiten al Estado tener constancia de su existencia, y derivar las oportunas consecuencias jurídicas, y simultáneamente ofrecer a los terceros seguridad jurídica.

Todos nuestros actos jurídicos en la práctica están ineludiblemente unidos a la declaración o prueba de nuestra identidad. Por ejemplo, para dirigirnos a cualquier administración la Ley 30/1992, de 26 de noviembre de Régimen Jurídico de las Administraciones Públicas y del Procedimiento Administrativo Común exige que la petición contenga indicación del nombre y apellidos del interesado y, en su caso, de la persona que lo represente, así como la identificación del medio preferente o del lugar que se señale a efectos de notificaciones y la firma del solicitante o acreditación de la autenticidad de su voluntad expresada por cualquier medio (art. 70). Y lo mismo sucede en el ámbito de la contratación privada.

Dos son los documentos que habitualmente se utilizan para identificar a las personas físicas en nuestro país: el Documento Nacional de Identidad y el pasaporte.

Documento Nacional de Identidad

El Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento Nacional de Identidad y sus certificados de firma electrónica, define el DNI como un documento personal e intransferible emitido por el Ministerio del Interior que goza de la protección que a los documentos públicos y oficiales otorgan las leyes (art.1). Además "*tiene suficiente valor, por sí solo, para acreditar la identidad y los datos personales de su titular que en él se consignen, así como la nacionalidad española del mismo*".

A su vez, es un documento que en su formato electrónico actual permite a los españoles, mayores de edad y que gocen de plena capacidad de obrar, la identificación electrónica, así como realizar la firma electrónica de documentos en los términos previstos en la Ley 59/2003, de 19 de diciembre, de firma electrónica.

Se trata de un documento cuya obtención es obligatoria para los mayores de catorce años residentes en España y para los de igual edad que, residiendo en el extranjero, se trasladen a España por tiempo no inferior a seis meses (art. 2). Como es lógico su expedición se vincula a la existencia real de una persona, de ahí que se requiera para su expedición presentar certificación literal de nacimiento expedida por el Registro Civil correspondiente.

El número del DNI constituye en sí mismo un identificador. Además del nombre y apellidos, y este número personal, el DNI incorpora otros datos del titular como la fecha y lugar de nacimiento, sexo, nacionalidad, domicilio, y otros elementos de identificación como son la fotografía y la firma del titular, y los caracteres OCR-B de lectura mecánica.

Pasaporte

El Real Decreto 896/2003, de 11 de julio, por el que se regula la expedición del pasaporte ordinario y se determinan sus características lo define como un documento público, personal, individual e intransferible, expedido por los órganos de la Administración General del Estado que "*acredita, fuera de España, la identidad y nacionalidad de los ciudadanos españoles salvo prueba en contrario, y, dentro del territorio nacional, las mismas circunstancias de aquellos españoles no residentes"* (art.1).

Todos los españoles tienen derecho a obtenerlo y, al igual que sucede con el DNI contiene distintos elementos que permiten establecer la identidad de su titular. Así, además de ciertos datos personales y referencias a su expedición, el pasaporte incluye como elementos de identificación: un número personal de pasaporte, el número del DNI de su titular[16], la firma digitalizada del titular, la fotografía digitalizada del titular y dos líneas de caracteres OCR en la parte inferior de la hoja de datos, para la lectura mecánica de estos.

3.1.2 Los signos de identidad de las personas jurídicas

El derecho a la identidad se vincula de modo ineludible a los derechos de la personalidad. En relación a las personas jurídicas, el artículo 35 Código Civil diferencia, por una parte, las corporaciones, asociaciones y fundaciones de interés público reconocidas por la Ley, cuya personalidad "*empieza desde el instante mismo en que, con arreglo a derecho, hubiesen quedado válidamente constituidas*"; y por otra parte, las asociaciones o sociedades de interés particular civiles, mercantiles o industriales, a las que la ley conceda personalidad propia, independiente de la de cada uno de los asociados[17].

Junto al acto de constitución de la persona jurídica a través de los procedimientos establecidos para cada caso se prevé su inscripción registral. A través del Registro Mercantil podemos obtener la información de las persona jurídica a la que se refiere el art. 22 del Código de Comercio, entre otras: los datos identificativos del empresario individual (en su caso), el nombre comercial, el rótulo de su establecimiento, la sede de

[16] En el caso de que carezca de éste, por ser residente en el extranjero o menor de 14 años, dicho número se corresponderá, respectivamente, con el de su inscripción en el Registro de Matrícula Consular, o con el del documento nacional de identidad de quien ostenta su patria potestad o tutela seguido del subradical correspondiente.

[17] En este último caso, por ejemplo los artículos 19 y 20 del Real Decreto Legislativo 1/2010, de 2 de julio, por el que se aprueba el texto refundido de la Ley de Sociedades de Capital exigen un acto unilateral en caso de sociedades unipersonales, un contrato entre dos o más personas o una suscripción pública de acciones que se formalizarán en escritura pública, que deberá inscribirse en el Registro Mercantil.

éste y de las sucursales (si las tuviere), el objeto de su empresa y la fecha de comienzo de las operaciones.

Por otra parte, las asociaciones adquieren personalidad jurídica con el acta fundacional incluyendo el derecho de asociación según el artículo 24 de la Ley Orgánica 1/2002, de 22 de marzo, reguladora del Derecho de Asociación derecho de asociación incluye el derecho a la inscripción en el Registro de Asociaciones competente.

Por tanto, y con la finalidad de ofrecer seguridad jurídica a los terceros, los Registros incluyen información relativa a determinados signos que como la denominación social o el domicilio configuran la identidad de las personas jurídicas. Parte de estos datos deben ser objeto de publicación en las páginas web de sociedades y profesionales.

3.2 LA FIRMA ELECTRÓNICA

La prueba de la identidad puede realizarse a través de los medios que proporcionan la firma electrónica y los certificados digitales. No obstante, sus funcionalidades van mucho más allá, por lo que procede exponer los elementos jurídicos básicos que permiten caracterizar a cada una de ellos.

Los términos de firma digital y firma electrónica se utilizan con frecuencia como sinónimos, pero se trata de un error puesto que están diferenciados[18].

La **firma digital**, se refiere al conjunto de técnicas de codificación y criptografía que asocian la identidad de una persona, entidad o un equipo informático al mensaje o documento firmado. Una firma digital da al destinatario seguridad de que el mensaje fue creado por el remitente (autenticidad de origen) y que no fue alterado durante la transmisión (integridad).

La **firma electrónica** es un concepto más amplio desde un punto de vista técnico ya que puede contemplar métodos no criptográficos. La normativa española se refiere a ella de forma genérica como aquel “conjunto de datos” que permiten identificar al firmante, lo que incluiría bajo este concepto tipologías ajenas a la certificación digital, como la firma autógrafa escaneada o la firma manuscrita digitalizada.

La Ley 59/2003, de 19 de diciembre, de Firma Electrónica (LFE) recoge tipos tres distintos de firma electrónica:

- La firma electrónica simple

[18] Un ejemplo de la importancia de esta distinción es el uso dado por la Comisión Europea en el desarrollo de la Directiva 1999/93/CE que establece un marco europeo común para la firma electrónica. Así, si bien comenzó empleando el término de “firma digital” en el primer borrador, finalmente acabó utilizando el término de “firma electrónica” para desligar la regulación legal de este tipo de firma de la tecnología utilizada en su implementación.

- La firma electrónica avanzada
- La firma electrónica reconocida

3.2.1 La firma electrónica simple u ordinaria

De acuerdo con el artículo 3.1 de la LFE, la "firma electrónica" se define como 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; es decir, una credencial o documento electrónico que nos identifica electrónicamente.

Esta definición, de corte general, califica como firma cualquier tecnología de identificación, con independencia de su idoneidad como instrumento de declaración volitiva dado que de lo que se trata es de identificar a una persona.

Se corresponde esta definición con la función más básica que se predica de una firma escrita, que es sencillamente indicar qué persona remite un documento. Algunos ejemplos de la misma son los identificadores y contraseñas de usuario que suministran muchas entidades, especialmente privadas, para realizar operaciones a través de las redes telemáticas; o la inclusión de la firma digitalizada en un documento, al efecto de crear la apariencia de documento firmado.

3.2.2 La firma electrónica avanzada

El artículo 3.2 de la LFE define, a continuación, la "firma electrónica avanzada" como 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 los que se refiere y que ha sido creada por medios que el firmante puede mantener bajo su exclusivo control.

Esta segunda definición, incremental en requisitos sobre la más general de simple firma electrónica, exige que la tecnología, además de identificar a la persona que remite el documento, permita imputar el documento a la persona que dispone de los mecanismos para producir la firma. Además, a diferencia de la firma manuscrita, la tecnología calificable como firma electrónica avanzada debe garantizar la integridad del documento, de modo que las modificaciones posteriores del mismo sean detectables (como sucede en el formato papel con la "tachaduras y las raspaduras").

La definición se corresponde con las funciones tradicionales de la firma manuscrita, de modo que la firma avanzada resulta idónea para que las personas físicas procedan a utilizar dicha tecnología. El ejemplo más habitual de tecnología de firma electrónica avanzada es la firma digital basada en criptografía asimétrica.

Base ahora decir que una de las principales funciones de la LFE, es apuntalar jurídicamente la asunción según la cual el mecanismo tecnológico de la firma digital

puede actuar "como si fuera" la firma manuscrita de una persona, mediante el concepto –tecnológicamente neutral– de la firma electrónica (avanzada o reconocida).

3.2.3 La firma electrónica reconocida

Finalmente, la LFE contiene una tercera definición de firma electrónica, en su artículo 3.3, en virtud del que se considera "firma electrónica reconocida" a la firma electrónica avanzada basada en un certificado reconocido y que ha sido producida mediante un dispositivo seguro de creación de firma electrónica, categoría cuyo "reconocimiento" se refiere a una presunción de idoneidad que la cualifica especialmente como equivalente a la firma manuscrita, y sin que ello implique la discriminación de los restante tipos de firma electrónica.

Se trata, de nuevo, de una definición incremental en cuanto a los requisitos, que exige que la tecnología de firma electrónica reconocida sea especialmente idónea y adecuada para que una persona física, de hecho típicamente un ciudadano o profesional usuario de servicios privados y públicos, se identifique y firme.

3.2.4 Otros tipos de firma electrónica

No obstante, además de las contempladas en la LFE, podemos citar otros tipos de firma en función de cómo las clasifiquemos:

Según su formato:

- **Fechada** *(Timestamp)*, ya que incorpora un sello de tiempo (AdES-T).
- **Validada** *(complete y Extended):* añade referencias para comprobar las firmas (AdES-C); o bien que además añade el sello de tiempo a las referencias añadidas en la anterior (AdES-X).
- **Longeva** *(Extended long-term)*, incluye certificados e información de revocación actual para su comprobación a largo plazo *(*AdES-X-L).

Según su ubicación física:

- **Explícita** (*Detached)*. La firma se genera como un fichero independiente del fichero firmado. Cualquier fichero se puede firmar de esta forma. Hay varias aplicaciones para generar este tipo de firma.
- **Implícita o incrustada** (*Attached)*. La firma va incluida en el documento que va firmado. Es posible si la aplicación que crea el fichero de datos lo permite.

Según su jerarquía:

Cuando un documento debe ser firmado por varios, pueden presentarse dos tipos de firmas en función del caso concreto:

- **Jerárquicas** (*Countersing*). Cuando un documento debe firmarse en orden. Una firma verifica o firma las anteriores.

- **Paralela o cofirma** (*CoSign)*. Todas las firmas firman los datos. No hay orden, solo importan el número de firmas totales.

Según el lenguaje empleado

Cuando se genera una firma digital podemos utilizar dos lenguajes distintos, generando dos formatos distintos:

- **CAdES**: CMS (*Cryptografic Message Syntax*) *Advanced Electronic Signature.*

- **XaDES:** XML (*Extensible Markup Language*) *Advanced Electronic Signature.*

3.2.5 Los efectos jurídicos de la firma electrónica

Principio de validez general de la firma electrónica

Toda firma electrónica, con independencia de su calificación como “ordinaria”, “avanzada” o “reconocida”, es igualmente firma en la medida en que sirve al objetivo de imputar el contenido del documento a la persona que lo autoriza. En consecuencia, el artículo 3.9 de la LFE indica que no se negarán efectos jurídicos a una firma electrónica que no reúna los requisitos de firma electrónica reconocida, en relación a los datos a los que esté asociada, por el mero hecho de presentarse en forma electrónica.

Así pues, la diferencia real entre una simple firma electrónica, una firma electrónica avanzada o una firma electrónica reconocida no reside en su admisibilidad jurídica, ni en su potencial eficacia, sino en el conjunto de requisitos necesarios para lograr dichos efectos.

Por tanto, aunque sobre la firma reconocida recae una presunción legal que la equipara a la firma manuscrita, una firma simple puede cumplir perfectamente con su función aunque puedan ser necesarios elementos adicionales, como su obtención previa en el mundo físico ante una responsable de la empresa o administración.

Eficacia de la firma electrónica

La LFE regula los efectos de la firma electrónica doblemente:

- Por una parte, el artículo 3.4 de la LFE determina que 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;

esto es, que la firma electrónica que cumple estos requisitos se "reconoce" legalmente como equivalente a la firma manuscrita.

- Por otra parte, el artículo 3.9 de la LFE establece que no se negarán efectos jurídicos a la firma electrónica que no reúna los requisitos de la firma electrónica reconocida, en relación a los datos a los que esté asociada por el mero hecho de presentarse en forma electrónica. Es decir, toda firma puede potencialmente recibir efectos jurídicos, no pudiendo ser ninguna tecnología discriminada por ser electrónica.

Esta concepción doble se traduce en los dos principios generales descriptivos de la eficacia de la firma electrónica: el principio de no discriminación, de acuerdo con el cual la parte a quien interesa la eficacia de una firma electrónica tiene derecho a que se practique una prueba suficiente, que determine si la firma era suficientemente fiable como para imputar el acto a la persona que la produjo; y el principio de equivalencia funcional, que no elimina la necesidad de esta prueba, pero la reduce considerablemente, mediante la presunción de la especial idoneidad de la tecnología para actuar como la firma de la persona.

Los efectos, por tanto, se condicionan siempre y en todo caso a la prueba de la autenticidad de la firma, demostrada la cual la firma producirá su efecto típico, que es el de permitir la imputación del documento firmado a la persona.

La prueba judicial de la firma electrónica

Es precisamente esta prueba de la autenticidad de la firma electrónica la que se debe practicar en caso de repudio o rechazo del documento por parte del demandado. Se trata de lo mismo que sucede en el caso de la firma manuscrita, que en caso de conflicto se sustancia mediante una prueba pericial caligráfica.

Al efecto, la LFE determina un tratamiento específico de la prueba de la autenticidad de la firma electrónica, en los casos de la firma avanzada y de la firma reconocida (no así de la firma ordinaria).

En virtud del artículo 3.8 de la LFE, en caso de impugnarse la autenticidad de la firma electrónica reconocida con la que se hayan firmado los datos incorporados al documento electrónico, se procederá a comprobar que: se trata de una firma electrónica avanzada basada en un certificado reconocido, que cumple todos los requisitos y condiciones establecidos en esta Ley para este tipo de certificados y que la firma se ha generado mediante un dispositivo seguro de creación de firma electrónica.

La obligación de realizar las citadas comprobaciones corresponde a quien presente el documento electrónico firmado con firma electrónica reconocida.

Si dichas comprobaciones obtienen un resultado positivo, se asume la autenticidad de la firma electrónica reconocida con la que se ha firmado dicho documento electrónico, teniendo que hacerse cargo de las costas, gastos y derechos que origine la comprobación quien hubiese formulado la impugnación. E incluso, si a juicio del tribunal la impugnación hubiese sido temeraria, podrá imponerle además una multa de entre 120 y 600 euros.

El mismo artículo 3.8 de la LFE dice que si se impugna la autenticidad de la firma electrónica avanzada, se deberá asumir lo dispuesto por el artículo 326.2 de la LEC, que permite el empleo de cualquier medio de prueba que resulte útil y pertinente.

Más allá de esta aparente doble regulación, en ambos casos el tratamiento probatorio es el mismo, en caso de conflicto, ya que se debe acudir a una prueba pericial informática, que en su caso podrá simplificarse mediante la aportación, por parte de quien proceda (prestadores de servicios de seguridad o de certificación de la firma electrónica, o fabricantes de la tecnología y de certificados de acreditación) que los servicios y los productos empleados cumplen los requisitos de seguridad aplicables al caso concreto.

En el caso de la firma electrónica reconocida, el contenido de la prueba se encuentra determinado por la LFE (verificación de que el algoritmo de firma empleado corresponde a un sistema de firma electrónica reconocida, verificación de la condición del dispositivo empleado como seguro, verificación de las prácticas del prestador del servicio que emiten el certificado como reconocido).

Sin embargo, en el caso de la firma avanzada no se establece criterio ninguno, dado que en aplicación del principio de neutralidad tecnológica, cualquier tecnología puede ser calificada como firma electrónica avanzada, haga uso o no de certificados o dispositivos de firma, y por tanto difícilmente puede prever el legislador cómo se debe demostrar que una tecnología concreta no ha sufrido un problema de seguridad que la invalide como firma electrónica avanzada.

Esta segunda solución también es aplicable a la firma electrónica simple u ordinaria, como resulta habitual en los tribunales.

3.3 LOS CERTIFICADOS DIGITALES

En relación con la identidad, los certificados previstos en la Ley de firma electrónica se pueden clasificar según diversos criterios:

- Certificados ordinarios o certificados reconocidos.
- Certificados de personas físicas, de personas jurídicas o de entidades sin personalidad jurídica propia.

- Certificados para actuar en nombre propio o por representación.
- Certificados individuales o certificados corporativos.
- El DNI electrónico.

3.3.1 Certificado ordinario o reconocido

El **certificado ordinario** es, de acuerdo con el artículo 6 de la Ley 59/2003, de 19 de diciembre, de firma electrónica (LFE), "*un documento firmado electrónicamente por un prestador de servicios de certificación que vincula unos datos de verificación de firma a un firmante y confirma su identidad".* Se denomina "ordinario" para diferenciarlo del certificado "reconocido".

Los **certificados reconocidos** son, de acuerdo con el artículo 11.1 LFE, "*los certificados electrónicos emitidos por un prestador de servicios de certificación que cumple los requisitos establecidos en esta Ley en cuanto a la comprobación de la identidad y el resto de circunstancias de los solicitantes, y a la fiabilidad y las garantías de los servicios de certificación que prestan".*

Todos los certificados ordinarios y reconocidos son, de acuerdo con estas definiciones legales, certificados de clave pública[19].

El certificado reconocido es una pieza fundamental para la firma electrónica reconocida, y por este motivo se regula su contenido y los procedimientos y las garantías para emitirlo. Por su menor importancia, la regulación del certificado ordinario es también menor: no se regula el contenido, y sólo se establecen unas obligaciones comunes – típicamente informativas y de publicación de información – a todos los prestadores que expiden certificados.

En concreto, el certificado reconocido deberá contener, de acuerdo con el artículo 11.2 LFE, lo siguiente:

- La indicación de que el certificado se expide como reconocido.
- El código identificativo único del certificado.
- La identificación del prestador de servicios de certificación que expide el certificado y su domicilio.

[19] La normativa española – al igual que la Directiva europea – deja fuera del concepto legal de certificado (ordinario o reconocido) a cualquier certificado de clave pública que no sea de persona o que no sea de identidad o de firma electrónica, como es el de cifrado o el de componente técnico.

- La firma electrónica avanzada del prestador de servicios de certificación que expide el certificado.

- La identificación del firmante, en el caso de personas físicas, por su nombre y apellidos y por el número de documento nacional de identidad o mediante un seudónimo que conste como tal de manera inequívoca y, en el caso de personas jurídicas, por su denominación o razón social y su código de identificación fiscal.

- Los datos de verificación de firma que correspondan a los datos de creación de firma que se encuentren bajo el control del firmante.

- El inicio y finalización del período de validez del certificado.

- Los límites de uso del certificado, si se establecen.

- Los límites del valor de las transacciones para las que puede utilizarse el certificado, si se establecen.

De acuerdo con el artículo 11.3 LFE, los certificados reconocidos podrán contener cualquier otra circunstancia o atributo específico del firmante en caso que sea significativo, según la finalidad propia del certificado y siempre que lo solicite el firmante.

3.3.2 Certificado de persona física, de persona jurídica o de entidad sin personalidad jurídica

El **certificado de persona física** es el que se expide a un usuario individual, que se denomina suscriptor del certificado, que será el firmante (en certificados de clave pública de firma) o el que descifre los documentos protegidos con su clave pública (en certificados de cifrado).

El **certificado de persona jurídica** no se recoge en la Directiva 99/93/CE, ni se define en la Ley 59/2003. Sin embargo, a partir del artículo 7 de la LFE es posible describirlo como el que permite imputar la autoría de los documentos directamente a la persona jurídica (apartado 4), siempre que estos documentos hayan sido firmados dentro de una relación con las Administraciones Públicas o dentro del giro o tráfico ordinario de la persona jurídica (apartado 3).

El certificado de persona jurídica se expide con la intervención necesaria de una persona física, porque es necesario que lo solicite, en nombre de la persona jurídica, su administrador, representante legal o voluntario con poder suficiente a estos efectos que se denomina "custodio"[20].

[20] El custodio de un certificado de persona jurídica es la persona física solicitante de un certificado de persona jurídica, que dispone de un dispositivo de firma electrónica y que, por tanto, lo utiliza para producir firmas electrónicas.

No obstante, las aplicaciones del certificado de persona jurídica tienen más que ver con la producción de documentos originales imputables a la entidad que con la firma escrita del representante legal o voluntario de la persona jurídica. Esta posibilidad obliga a replantear la necesidad de la representación en la relación electrónica entre las personas jurídicas y las Administraciones Públicas, ya que legalmente es la persona jurídica la que directamente actúa.

Además, el certificado de persona jurídica no podrá afectar al régimen de representación orgánica o voluntaria regulado por la legislación civil o mercantil aplicable a cada persona jurídica, previsión que genera bastantes problemas jurídicos para delimitar qué actos podrían eventualmente quedar excluidos de la "firma de persona jurídica" en la relación electrónica con la Administración.

Así pues, se debe interpretar que esta previsión legal señala que precisamente en la actuación electrónica de la persona jurídica mediante su firma electrónica no existe representación, por ser innecesaria y que, por tanto, a dicha actuación no se le deben aplicar las normas sobre la representación. De este modo, cuando una norma administrativa señale que, por ejemplo, determinado documento debe ser firmado por la empresa o su representante, será posible que actúe directamente la empresa con su firma de persona jurídica o que actúe un representante mediante un certificado de persona física, en este segundo caso acreditando su representación de forma suficiente.

La regulación del certificado de persona jurídica no se aplica ni a los certificados de las entidades de certificación de firma electrónica ni a los certificados emitidos a las Administraciones Públicas, que se regirán por su normativa específica (en el caso de éstas últimas, la ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los servicios públicos (Ley 11/2007) y sus correspondientes reglamentos de desarrollo).

Los **certificados de entidad sin personalidad jurídica** se encuentran regulados en la disposición adicional tercera de la Ley 59/2003, de firma electrónica, que establece que "*podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica a que se refiere el artículo 33 de la Ley General Tributaria a los solos efectos de su utilización en el ámbito tributario, en los términos que establezca el Ministro de Hacienda*", previsión que ha sido modificada para abrir la posibilidad de uso no tributario de dichos certificados. Actualmente, la emisión de certificados para entidades sin personalidad jurídica se regula por Orden EHA/3256/2004, de 30 de septiembre, por la que se establecen los términos

---

El custodio es un administrador, representante legal o voluntario de la persona jurídica, con poderes suficientes para solicitar el certificado de persona jurídica (no, en cambio, para los actos realizados con el certificado, que se imputan a la persona jurídica por efecto de la ley, sin necesidad de poder).

El custodio ha de utilizar el certificado de la persona jurídica dentro de sus límites. En otro caso, el responsable de los actos podría ser el custodio, a título personal.

Por este motivo, el custodio dispone del derecho (y del deber) de revocación del certificado. Adicionalmente, hay que decir que las circunstancias que afecten al custodio afectarán a la vida del certificado de persona jurídica.

en los que podrán expedirse certificados electrónicos a las entidades sin personalidad jurídica.

Dicha Orden aplica a las entidades sin personalidad jurídica normas análogas a las aplicables para los certificados de personas jurídicas, aunque con especialidades. En particular respecto al procedimiento de registro, con la finalidad de asegurar que sólo un representante legal o voluntario de la entidad sin personalidad, que actuará como custodio, recibe el certificado.

3.3.3 Certificado para actuar en nombre propio o por representación

El certificado de firma puede servir para actuar en nombre propio o en representación de una persona, como determina el artículo 6.2 de la Ley 59/2003.

Aunque el caso más habitual en estos momentos es el certificado para actuar en nombre propio, cada vez serán más importantes los certificados que incorporen la representación de un tercero, que, de acuerdo con el artículo 11.3 de la Ley 59/2003, deberán declarar que su finalidad específica es, además de la identificación de las personas que los reciben, la de actuar por representación: se trata, pues, de un certificado específico, de representante.

El artículo 11.4 de la Ley determina que el certificado reconocido de representante deberá incluir una indicación del documento público que acredite de forma fehaciente las facultades del firmante (que es suscriptor del certificado individual, y del poseedor de claves del certificado corporativo) para actuar en nombre de la persona o entidad a la que representa y, cuando sea obligatoria la inscripción, de los datos del registro público, de conformidad con el apartado segundo del artículo 13 de la Ley.

En términos prácticos, un certificado de representación que no incorpore límites de actuación estará manifestando que el representante puede hacer cualquier acto en nombre de su representado, bien por tratarse de un representante legal (orgánico, en el caso de las personas jurídicas representadas), bien por tratarse de un representante voluntario con apoderamiento general.

3.3.4 Certificado individual o corporativo

El certificado personal puede ser **individual**, cuando lo solicita una persona física o jurídica para su uso en nombre propio o por cuenta de tercero, sin indicar una relación de vinculación con otra persona, como trabajador o similar.

Este es el modelo de certificado en que se construye el régimen de relaciones jurídicas de la Directiva 99/93/CE o de la Ley 59/2003, y se corresponde con la prestación de servicios al consumidor.

Aunque no aparece citado expresamente, el certificado personal también puede ser corporativo, cuando indica una relación de vinculación de esta naturaleza con otra persona, que se puede incluir si lo justifica la finalidad específica del certificado (artículo 11.3 de la Ley 59/2003).

Habitualmente el **certificado corporativo** nace de una relación laboral o de una relación orgánica de pertenencia a una corporación pública o privada, y se diferencia del certificado individual en que la suscriptora del certificado será la corporación, mientras que la persona signataria que lo recibe será considerado como poseedor de la clave de firma, debidamente autorizado para utilizarla de acuerdo con sus facultades, permisos y privilegios indicados en el certificado.

3.4 EL DNI ELECTRÓNICO: UN CASO ESPECIAL

La instauración del DNI electrónico ha sido uno de los objetivos del Gobierno de España, manifestado desde el *Plan Info XXI*. Con el DNIe se pretende dotar a los ciudadanos de una tarjeta de identificación que recoja los datos básico identificativos del individuo. Al mismo tiempo, se configura como un mecanismo generador de firmas de obligatoria aceptación por todos los sujetos del tráfico jurídico, en la línea del programa de identificación electrónica fomentado por la Unión Europea, identificado bajo la línea de "gestión interoperable de la identidad electrónica"[21].

El DNI electrónico, además de constituir un medio seguro y fiable de acreditación de la identidad personal en el ámbito físico, añade la funcionalidad de su utilización como medio de identificación fehaciente en el ámbito digital: mediante su uso en dispositivos electrónicos, a través de Internet y en redes de comunicaciones privadas.

De esta forma, los dos certificados electrónicos que incorpora el DNI electrónico (de autenticación del ciudadano y de firma digital) que resultan voluntarios, sirven para autenticar la identidad personal de su titular y para permitir la firma electrónica de documentos por parte del firmante.

El DNI electrónico incluye un chip que permite identificarse a través de cualquier sistema de comunicaciones electrónicas, siempre que se requiera o se necesite para una operación telemática, así como realizar operaciones con garantía de autenticación biométrica basada en huella dactilar.

Los certificados de identidad y firma electrónica son emitidos, con carácter exclusivo, por el Estado, para lo cual se ha constituido una Autoridad de Certificación electrónica propia,

[21] La LFE fija el marco normativo básico del DNIe remitiéndose a la normativa específica en cuanto a las particularidades de su régimen jurídico. De acuerdo con la definición incluida en el artículo 15.1 LFE, "el documento nacional de identidad electrónico es el documento nacional de identidad que acredita electrónicamente la identidad personal de su titular y permite la firma electrónica de documentos".

personalizada en el Ministerio del Interior a través de la Dirección General de la Policía Nacional. Al respecto, el artículo 16.1 LFE establece que *"los órganos competentes del Ministerio del Interior para la expedición del documento nacional de identidad electrónico cumplirán las obligaciones que la presente Ley impone a los prestadores de servicios de certificación que expidan certificados reconocidos con excepción de la relativa a la constitución de la garantía a la que se refiere el apartado 2 del artículo 20".*

Adicionalmente, el artículo 16.2 del propio texto legal determina que "*la Administración General del Estado empleará, en la medida de lo posible, sistemas que garanticen la compatibilidad de los instrumentos de firma electrónica incluidos en el documento nacional de identidad electrónico con los distintos dispositivos y productos de firma electrónica generalmente aceptados*". Es importante que la Administración General del Estado realice este esfuerzo ya que, en relación a la utilización y los efectos jurídicos que se derivan del DNI electrónico, el artículo 15.2 LFE establece que "*todas las personas físicas o jurídicas, públicas o privadas, reconocerán la eficacia del documento nacional de identidad electrónico para acreditar la identidad y los demás datos personales del titular que consten en el mismo, y para acreditar la identidad del firmante y la integridad de los documentos firmados con los dispositivos de firma electrónica en él incluidos".*

El DNI electrónico incorpora, al igual que el DNI tradicional, la identificación de la persona física y los demás datos personales del firmante que consten en el mismo. Sin embargo, a diferencia de los certificados expedidos a los ciudadanos por las administraciones públicas, no incorpora ninguna otra circunstancia o atributo específico del firmante, como por ejemplo, su número de la tarjeta sanitaria, su condición de titular de un cargo público, su pertenencia a un colegio profesional o su titulación, etc.

Esta circunstancia va a permitir que coexistan junto al DNI electrónico otros certificados electrónicos que incorporan este tipo de atributos. Por ejemplo, cualquiera de los certificados electrónicos que expidan las Administraciones Públicas, los colegios profesionales, los registradores y notarios y cualquier otro prestador de servicios de certificación público o privado. Dichos certificados no serán discriminados de forma arbitraria en su uso en las relaciones electrónicas con la Administración, para lo cual resulta esencial el derecho al uso de los sistemas de firma electrónica avanzada diferentes del DNI electrónico reconocido en el artículo 6.2.h) Ley 11/2007, y desarrollado posteriormente en los artículos 13.2.b), 15 y 21 del propio texto.

La distribución del DNI electrónico ha ayudado a la implantación de la firma electrónica y ha permitido que se conozca y se fomente su utilización. Además, ha contribuido a que se produzca una mayor introducción en el mercado de aplicaciones que requieran de esta tecnología.

El desarrollo reglamentario del DNI electrónico se ha realizado por el Real Decreto 1553/2005, de 23 de diciembre, por el que se regula la expedición del Documento

Nacional de Identidad y sus certificados de firma electrónica. Hay que destacar que, frente a la vigencia del Documento Nacional de Identidad, los certificados electrónicos reconocidos incorporados al mismo tendrán un período de vigencia de treinta meses (artículo 12 del Real Decreto).

Un DNI dura normalmente diez años, lo que significa que se deben producir tres renovaciones ordinarias de los certificados en su interior, siempre que no haya incidencias que exijan la previa revocación de los mismos (y su reemisión posterior, sobre la misma tarjeta).

Esta circunstancia resulta importante, ya que, aunque inicialmente un DNI electrónico sea emitido con los dos certificados en su interior, es necesario que el ciudadano renueve de forma regular sus certificados o, en caso contrario, no podrá hacer uso de dichas funcionalidades. Las renovaciones que deben realizarse en las Comisarías de Policía, empleando los equipamientos dispuestos al efecto.

3.5 LA IDENTIFICACIÓN DIGITAL FRENTE A LA ADMINISTRACIÓN

La Ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos define cómo se identificarán todos los sujetos que participan en el procedimiento administrativo.

En primer lugar, se parte de la admisión de los sistemas de firma electrónica conforme a la Ley 59/2003, y en particular:

- Los sistemas de firma electrónica incorporados al Documento Nacional de Identidad, para personas físicas.
- Sistemas de firma electrónica avanzada, incluyendo los basados en certificado electrónico reconocido, admitidos por las Administraciones Públicas.
- Otros sistemas de firma electrónica, como la utilización de claves concertadas en un registro previo como usuario, la aportación de información conocida por ambas partes u otros sistemas no criptográficos, en los términos y condiciones que en cada caso se determinen.

Adicionalmente el art. 15.3 permite utilizar los certificados electrónicos expedidos a Entidades sin personalidad jurídica, previstos en la Ley 59/2003. Por tanto, caben todas las modalidades de firma electrónica, incluida la simple, aunque en este caso se exige la identificación previa del usuario y la concertación de claves. Por ejemplo, con métodos como el sistema utilizado por la AEAT para la tramitación del impuesto del IRPF.

El mismo precepto fijas las condiciones de uso de estos dispositivos por la propia Administración.

La Ley también regula los sistemas para la identificación electrónica de las Administraciones Públicas y para la autenticación de los documentos electrónicos que produzcan:

- Sistemas de firma electrónica basados en la utilización de certificados de dispositivo seguro o medio equivalente que permita identificar la sede electrónica y el establecimiento con ella de comunicaciones seguras.
- Sistemas de firma electrónica para la actuación administrativa automatizada.
- Firma electrónica del personal al servicio de las Administraciones Públicas.
- Intercambio electrónico de datos en entornos cerrados de comunicación, conforme a lo específicamente acordado entre las partes.

En cuanto a los funcionarios, pueden utilizar firmas electrónicas provistas por la propia Administración que puedan identificar de forma conjunta al titular del puesto de trabajo o cargo y a la Administración u órgano en la que presta sus servicios, o la firma electrónica basada en el Documento Nacional de Identidad.

4. Riesgos para la seguridad y la privacidad

4.1 PRINCIPALES ERRORES

En el proceso de autenticación pueden concurrir diferentes riesgos o problemas en relación a la seguridad, siendo los principales la asignación incorrecta de identidad, sea esta provocada (suplantación) o por error, y el no reconocimiento de la identidad de una persona, es decir, los conocidos como falsos positivos y los falsos negativos.

A pesar de ser los dos casos más habituales, es necesario señalar que los posibles riesgos pueden deberse a otras circunstancias, especialmente en relación a la gestión de los diferentes aspectos relacionados con la autenticación.

4.1.1 Falsos negativos

Un falso negativo en un proceso de autenticación supone que a un usuario legítimo no se le reconoce como tal, negándosele el acceso al sistema. Si bien en principio las consecuencias de este error se limitan a esa denegación de acceso, esto puede tener otras consecuencias en caso de que la denegación de acceso sea permanente.

Por ejemplo, puede perderse información importante si el acceso es denegado permanentemente y solamente está alojada en ese servicio. Por otro lado, si la cuenta o el servicio al que se desea acceder se utiliza para gestionar dinero, podrían producirse pérdidas económicas.

4.1.2 Falsos positivos

El otro tipo de error que puede darse en el proceso de autenticación es el falso positivo, es decir, la aceptación como usuario legítimo a uno que no lo es, por lo que se le permite el acceso a un sistema y una información que no debería tener. En el caso de la firma digital, se estaría afirmando una autoría falsa.

Esta situación puede generar diferentes problemas, como el robo de información, la suplantación de identidad o casos de fraude online.

4.2 RIESGOS EN LOS PROCESOS DE AUTENTICACIÓN

Los diferentes riesgos para la seguridad y la privacidad relacionados con los procesos de autenticación son muy diversos, pudiendo ser consecuencia de los falsos positivos, los falsos negativos o deberse a otros aspectos relacionados con el diseño y la gestión de los procesos de autenticación.

4.2.1 Ausencia o déficit de medidas de seguridad

En esta categoría se engloban diferentes aspectos que, en su mayoría, pueden ser solventados por quien diseña el sistema de verificación. Se trata en todo caso de medidas preventivas que ayudan a mantener elevados niveles de seguridad. Entre los posibles problemas en este conjunto destacan:

- **Credenciales poco robustas.** Es posible que las credenciales definidas para permitir o denegar el acceso a un servicio online no alcancen unos mínimos exigibles de seguridad. En el caso de las contraseñas estos niveles se pueden valorar en función de su complejidad y su extensión.

- **Posibilidad de ataques de fuerza bruta**. Actualmente es posible automatizar el intento de acceso a un servicio, probando cientos de credenciales por segundo hasta conseguir la opción acertada y con ella el acceso. En caso de que el sistema no cuente con un mecanismo de bloqueo del acceso ante la reiteración de errores podría facilitarse este tipo de ataques.

- **Robo de credenciales.** Las credenciales que permiten la autenticación de cada usuario suelen ser almacenadas en los sistemas del administrador. Por ello, es de especial importancia que el acceso a dichos sistemas cuente con altas medidas de seguridad, de modo que nadie pueda acceder a dichas credenciales.

- **Ausencia de medidas de protección en la comunicación.** Otro de los aspectos a tener en cuenta es que la transmisión de las credenciales desde el dispositivo del usuario hasta los equipos del proveedor se realice con medidas de seguridad que no permitan a terceros acceder a ellas. El ejemplo más claro es el cifrado de estas comunicaciones.

4.2.2 Deterioro, modificación involuntaria y olvido de credenciales.

En este grupo pueden incluirse diferentes situaciones en las que las credenciales establecidas dejan de ser válidas o no pueden utilizarse.

El ejemplo más básico es el olvido de las contraseñas, pero también pueden ocurrir otros incidentes como los daños en los tokens o tarjetas de acceso. En el caso de la biometría pueden darse modificaciones físicas como, por ejemplo, lesiones que dificulten la lectura de las huellas dactilares o el uso de lentes de contacto que dificulten es escaneo del iris.

4.2.3 Ausencia o inefectividad de sistemas secundarios.

Ya sea por el bloqueo del sistema principal o por no poderse utilizar las credenciales, suele ser necesario establecer un sistema secundario de autenticación (ej: pregunta de seguridad). Este sistema secundario debe de ser tan robusto como el sistema principal, ya que en caso contrario posibilitaría un acceso sencillo a usuarios no autorizados.

La inexistencia de estos sistemas secundarios puede impedir la autenticación de usuarios legítimos, mientras que la falta de seguridad en ellos puede permitir falsos positivos.

4.2.4 Errores en el registro inicial

El registro inicial es un momento crítico para los futuros procesos de autenticación, por ello cualquier error en él puede acarrear problemas posteriormente. De especial

importancia en el registro es la determinación de las credenciales de autenticación, por lo que ese aspecto debe tratarse con especial cautela.

Una de las medidas más básicas para asegurar que no existen problemas en la selección de credenciales es pedir que se introduzcan dos veces, para así poder confirmarlas por partida doble. En caso de que ambas muestras sean diferentes se informa de la existencia de un error y el proceso no se da por concluido.

4.2.5 Errores en la autenticación

Del mismo modo que se pueden producir errores en el registro, éstos pueden ocurrir en el mismo momento de la autenticación. Generalmente suele tratarse de lapsus al introducir los identificadores de usuario o las credenciales. También puede tratarse de averías o ausencia de los elementos necesarios para introducir la información necesaria (teclados, lectores de tarjetas inteligentes, sensores y escáneres biométricos, etc.).

4.2.6 Ausencia de un proceso de confirmación ante la modificación de credenciales y otros cambios sustanciales

Una vez que se permite que un usuario sin autorización acceda a un sistema, es posible que trate de realizar cambios como la modificación de las credenciales de acceso. De este modo, los usuarios legítimos no podrían acceder y su cuenta, perfil o registro de usuario quedaría secuestrado. Más aún, entre estas posibles modificaciones estar la propia eliminación de la cuenta o perfil de usuario.

Por ello, suele ser recomendable que este tipo de modificaciones cuenten con unos requisitos que vayan más allá que la mera presentación de las credenciales de acceso, por ejemplo la confirmación a través de otra cuenta o servicio previamente vinculado pero independiente.

4.2.7 Vulneraciones de la normativa sobre protección de datos personales

La elección del modelo de autenticación y de la cantidad de información que se solicita al usuario, pueden tener consecuencias de diversa índole e incluso plantear una vulneración de la normativa sobre la protección de datos personales. Esto se debe en gran medida a la necesidad de informar debidamente al usuario sobre la información que se va a utilizar y los usos que se le van a dar, además de una serie de obligaciones en el almacenamiento y tratamiento de estas informaciones.

Otro de los posibles problemas relacionados con la protección de datos y la privacidad en los procesos de autenticación es que el administrador desvele más información de la que realmente es estrictamente necesaria. Un ejemplo de esta situación es la información que se puede proporcionar al señalar a un usuario que intenta abrir una cuenta con una dirección de correo electrónico que ya existe una cuenta asociada a dicha dirección o que no existe ninguna. La mera comunicación de esta información vía correo electrónico

eliminaría en buena medida este riesgo, ya que solamente sería visible para quien pueda acceder a dicha cuenta.

4.2.8 Robo o pérdida de datos personales

Cuando una persona no autorizada accede al sistema y a la información contenida en él, se compromete la confidencialidad de la información. Una de sus posibles consecuencias más evidentes en estos casos es la pérdida de privacidad.

Otro riesgo derivado del error en la autorización es la pérdida de la propia información, ya que los datos podrían ser eliminados, impidiéndose así que los usuarios legítimos accedieran a ella (problema de disponibilidad de la información).

Este riesgo es de especial relevancia tanto en ámbitos empresariales, donde la pérdida de confidencialidad de la información puede poner en riesgo la viabilidad y el futuro de una empresa, como en las plataformas de redes sociales, ya que en ellas suele alojarse mucha información personal.

4.2.9 Suplantación de identidad

El mero acceso a un sistema por parte de una persona no autorizada haciéndose pasar por un usuario legítimo podría considerarse en sí una suplantación de identidad, pero esta suplantación puede ir más allá si el intruso actúa de modo que sus acciones parezcan ser realizadas por el usuario legítimo.

Si bien este acceso a los servicios y cuentas de otra persona es una de las principales formas de suplantación de identidad, ésta puede darse de otros modos, esencialmente registrando una cuenta, perfil o usuario en nombre de otra persona. De este modo, la persona suplantada podría incluso desconocer tal suplantación.

Debe tenerse en cuenta que las víctimas de una suplantación no tienen porqué ser únicamente particulares o personas físicas, sino que también se puede suplantar la identidad de una entidad u organización, por ejemplo mediante ataques de *defacing* a una página web, o de suplantación de la identidad del servidor web, como en envenenamiento DNS o el *pharming*.

Varias son las consecuencias más evidentes de una situación de suplantación de identidad:

- **Fraude**: La suplantación de identidad puede tener como objetivo el fraude económico, por ejemplo en caso de que se suplante a una empresa u organización que preste unos servicios a cambio de contraprestaciones económicas. En este caso el usurpador puede llegar a recibir los ingresos que efectúan usuarios sin ofrecer a cambio los servicios anunciados.

- **Comisión de delitos:** El extremo más grave de la suplantación de identidad es la comisión de delitos, de modo que el suplantador podría quebrantar la ley de tal forma que parezca que quien lo hace es la persona suplantada. Este extremo es más grave si cabe cuando la suplantación se lleva a cabo utilizando información biométrica, ya que se trata de una información muy difícil de simular y por tanto de reprobar en un proceso judicial.

- **Daños en la imagen pública:** Los efectos de que una persona suplante la identidad de otra pueden ser varios, pero claramente pueden producirse daños a su imagen pública. En muchas ocasiones la apropiación de una identidad se vincula con acosos cuyo objetivo es provocar un daño a la persona suplantada. En estos casos la suplantación es un primer paso instrumental a una conducta más compleja que puede adoptar múltiples manifestaciones. Por ejemplo, el suplantador puede adoptar conductas escandalosas, manifestar opiniones socialmente inaceptables, interactuar con los contactos de la víctima de modo agresivo, etc. Todas estas conductas suelen perseguir el objetivo de ofrecer una falsa imagen pública del suplantado con el objetivo de atacar su reputación.

5. Buenas prácticas para administradores

Las entidades que gestionan sistemas de autenticación tienen la responsabilidad de establecer un modelo técnico, organizativo y jurídico respetuoso con los derechos de las personas implicadas para establecer una relación de confianza, así como de implementar las medidas de seguridad suficientes para proteger adecuadamente la información personales de sus usuarios.

Para ello, a continuación se señala una serie de buenas prácticas y recomendaciones referidas a la autenticación de la identidad que deberían ser tenidas en cuenta por parte de los gestores y desarrolladores de sistemas de autenticación.

5.1 ELECCIÓN ADECUADA DEL TIPO DE CREDENCIAL

Desde una perspectiva de seguridad, la determinación del tipo de información que va a ser utilizada para la autenticación es un primer paso esencial, ya que en buena medida limitará los riesgos. Así, el uso de sistemas de doble factor siempre que sea posible aumenta considerablemente los niveles de seguridad frente a posibles accesos no autorizados o falsos positivos.

Si bien es cierto que los sistemas de autenticación basados en la biometría son altamente fiables, es necesario recordar que, además de implicar mayores necesidades en cuanto a recursos computacionales, los datos biométricos pueden considerarse datos de carácter personal de especial protección, por lo que su uso conlleva una serie de obligaciones legales superiores a las derivadas de la utilización de dispositivos físicos o contraseñas.

En esta elección se debe considerar a su vez los diferentes tipos de dispositivos desde los que se va a tratar de acceder al sistema, ya que es posible que no en todos los casos sea factible la utilización de diferentes elementos físicos para la autenticación. A este respecto se debe señalar el constante desarrollo de nuevas soluciones para facilitar la utilización de los diferentes elementos a través de diferentes medios. Como ejemplo de ello puede nombrarse el proyecto DNIe Droid, desarrollado por INTECO para permitir la utilización del DNI electrónico en smartphones que cuenten con el sistema operativo Android[22].

5.2 PREVENCIÓN FRENTE A ATAQUES DE FUERZA BRUTA

Ante la posibilidad de que un atacante trate de acceder a un sistema probando diferentes credenciales, es recomendable establecer un sistema de bloqueo que impida cualquier acceso tras registrarse determinado número de intentos fallidos. Este límite debe permitir que el usuario acceda pese a haber cometido algún error al tratar de acceder, por ello el bloqueo generalmente no se produce hasta un quinto intento fallido.

[22] http://www.inteco.es/pressRoom/Prensa/Actualidad_INTECO/DNIe_Droid

Tras llevarse a cabo este bloqueo se deben habilitar sistemas secundarios de autenticación, ya sea para el acceso o para la redefinición de nuevas credenciales.

Como alternativa al bloqueo, ya que éste convierte al legítimo usuario en la víctima al no poder acceder a sus servicios o perfiles, o de forma complementaria se puede considerar la incorporación de sistemas como los conocidos como captchas, que exigen una comprobación de que quien trata de autenticarse es un humano, no un sistema informático que pueda automatizar los ataques de fuerza bruta. Estos sistemas pueden consistir en descifrar una palabra o contraseña que se presenta distorsionando sus caracteres o exigir la respuesta de una pregunta como por ejemplo una suma.

5.3 SISTEMAS SECUNDARIOS SEGUROS

Es necesario que se implanten sistemas secundarios que posibiliten el acceso en caso de que el sistema principal no pueda utilizarse por cualquier motivo. Estos sistemas secundarios pueden llegar incluso a un tercer nivel en caso de que el sistema secundario establecido no pueda ser útil. Ejemplo de ello es la posibilidad de que el sistema secundario establecido consista en el envío de unas nuevas credenciales, o de un acceso para redefinirlas, a una cuenta de correo, pudiendo el usuario haber cancelado dicha dirección o perdido su control.

Los sistemas secundarios de autenticación deben contar con el mismo nivel de seguridad que se exige en el mecanismo principal, ya que en caso de requerir menores exigencias podrían convertirse en una puerta abierta de cara a posibles suplantaciones.

Uno de los sistemas secundarios más utilizados es formular una pregunta que el usuario ha determinado con anterioridad junto a su respuesta. En muchos casos se sugieren algunas preguntas que realmente no pueden considerarse seguras al poder ser respondidas por cualquier persona que conozca mínimamente al usuario, de modo que podría llegar a suplantar su identidad y acceder a su perfil o cuenta sin su consentimiento. Ejemplo de estas preguntas de seguridad son el nombre de algún familiar, de una mascota, de su primer colegio o de su película favorita.

Tampoco puede considerarse seguro un sistema de autenticación secundario en el que se utilice a otros usuarios como garantes de una identidad, ya que se facilitaría un ataque mediante ingeniería social para acceder a un determinado servicio. Un ejemplo de ello sería un servicio online que para restablecer una contraseña en caso de olvido pida que se señalen determinados usuarios que se consideren contactos de confianza para que verifiquen la identidad de quien quiere restablecer la contraseña. Este sistema facilitaría accesos indebidos ya que delega en otros usuarios la autenticación, sean estos contactos reales o creados para establecer un ataque mediante ingeniería social.

5.4 REQUISITO DE VERIFICACIÓN DE IDENTIDAD REAL

En muchos casos, en el registro inicial no se comprueba realmente la identidad de la persona que realiza este primer paso, sino que solamente se verifica el control sobre alguna cuenta de correo electrónico o de otro servicio online. Esta práctica permite que cualquier persona realice el registro sin que se compruebe su identidad y por tanto pudiendo hacerse pasar por otra persona. Este déficit de comprobación es de especial importancia en determinados ámbitos.

Para evitar posibles problemas es recomendable incluir en el registro inicial el requisito de la verificación de la identidad real. Esta verificación puede llevarse a cabo directamente, exigiendo una verificación presencial, o indirectamente, mediante terceros de confianza que atestigüen esta identidad a través de certificados digitales o del DNI electrónico.

Por ejemplo, en la apertura de una cuenta corriente de banca online se debe exigir el empleo de un sistema de identidad cuyo expedidor garantice que ha procedido a la verificación de la identidad real.

Asimismo, siempre es recomendable emplear sistemas de identidad digital de sedes web que garanticen la comprobación de la identidad real del titular de la citada sede web, como por ejemplo en el caso de certificados SSL/TLS con Validación Extendida.

5.5 ESTABLECER UNA BUENA POLÍTICA DE ELECCIÓN DE IDENTIFICADORES DE USUARIO

Al igual que la elección de las credenciales y/o contraseñas, es necesaria una correcta política de elección de identificadores de usuario. En referencia a este aspecto, es necesario considerar la posibilidad de elección por parte del usuario.

De este modo, se puede permitir la utilización de seudónimos o nombre elegidos por los usuarios para así posibilitar un mayor grado de privacidad, esto se debe a que el uso del nombre del usuario o su dirección de correo electrónico, por ejemplo, posibilitarían el reconocimiento de los usuarios por pate de otros, no siendo necesario en muchos casos.

En otros casos en cambio sería altamente recomendable que el identificador de usuario permita identificar claramente a la persona interesada. En estos casos puede utilizarse el DNI electrónico o simplemente el número del mismo.

5.6 EXIGIR CIERTA COMPLEJIDAD DE LAS CREDENCIALES

Es importante que las credenciales cuenten con unos niveles de complejidad adecuados para no poder ser descifrados rápidamente. Esta práctica se enfoca especialmente al uso de contraseñas para verificar una identidad.

De este modo, la elección de contraseñas debe incluir unas condiciones de complejidad como pueden ser una longitud mínima y la inclusión de mayúsculas, minúsculas, números y símbolos.

Del mismo modo, es recomendable impedir el uso de combinaciones demasiado sencillas, comunes o fáciles de adivinar (por ejemplo: password, contraseña, qwerty, 123456, abc123).

Por otro lado, debe recomendarse a los usuarios finales que eviten que las contraseñas sean o incluyan datos personales. Esta recomendación puede llegar a convertirse en una prohibición en algunos casos, como por ejemplo en lo que respecta al uso de los mismos datos que se han aportado en el registro (nombre, fecha de nacimiento, número de teléfono, etc.).

Por otro lado, los gestores de los sistemas deben promover, e incluso exigir, la renovación de las contraseñas cada cierto tiempo.

5.7 COMPROBACIÓN DE CREDENCIALES EN EL REGISTRO

En el registro deben establecerse claramente las informaciones que se utilizarán para posteriores accesos y autenticaciones. Por ello se debe prestar especial atención al comprobar que el usuario no comete errores que le puedan impedir el acceso en el futuro.

Un ejemplo de esta situación es teclear erróneamente una contraseña en el proceso de registro. Esta situación puede evitarse exigiendo que la misma sea tecleada dos veces y comprobando que concuerda, además de avisar al usuario en caso de que el teclado mantenga activa alguna función como la escritura en mayúsculas.

5.8 ESTABLECER MEDIDAS DE SEGURIDAD ANTE CAMBIOS DE CREDENCIALES Y OTRAS MODIFICACIONES DE CALADO

Es necesario que determinados cambios en la configuración de usuario, como por ejemplo la modificación de credenciales o la eliminación de la cuenta o perfil, se produzcan tras comprobarse nuevamente la identidad del usuario.

Dicha comprobación debería realizarse mediante un sistema diferente al empleado para el acceso, de modo que en caso de que un atacante pudiera superar el sistema de autenticación inicial no pueda impedir al legítimo usuario el acceso.

5.9 IMPLICACIÓN DE TERCEROS

La implicación de otros agentes en el proceso de autenticación debe llevarse a cabo con especial cautela, ya que puede llegar a permitirse que estos terceros conozcan determinados datos de identificación.

La autenticación federada es un claro ejemplo en el que la autenticación se lleva a cabo contando con más agentes implicados que el propio usuario y el proveedor de servicios. Este tipo de autenticación es recomendable siempre que el agente verificador o autenticador presente garantías en referencia al respeto de la privacidad de los usuarios.

En cualquier caso, el acceso a la información de identificación se debe limitar a terceros que tengan una posición justificada y fiable en cada caso.

5.10 ALMACENAMIENTO SEGURO

La información de autenticación es almacenada en los sistemas del agente encargado del proceso de autenticación para así poder utilizarla al comprobar la concordancia de ésta con la aportada por los usuarios del servicio. Esto obliga a que dicho almacenamiento cuente con altas medidas de seguridad para que nadie pueda acceder a ella sin autorización.

Estas medidas deben impedir que nadie pueda acceder a las credenciales del resto de usuarios, pero deben establecer también qué personas o perfiles de usuario dentro la organización prestadora de servicios pueden acceder a ellas. Es decir, en la definición de roles y responsabilidades de la organización se debe delimitar el acceso a las credenciales de los usuarios clientes.

En cualquier caso, siempre es aconsejable que la información almacenada esté cifrada, de modo que incluso en caso de que alguien pudiera superar las diferentes medidas de seguridad, éste no pudiera acceder a las credenciales.

Es necesario tener en cuenta a su vez el lugar donde se localizan los servidores en los que se almacenará la información de autenticación, debido especialmente a las diferentes legislaciones aplicables en cada país respecto a los sistemas de seguridad y la protección de datos personales.

5.11 TRANSMISIÓN CIFRADA

El intercambio de información entre los dispositivos de los usuarios y los equipos en los que se aloja el sistema, y especialmente el intercambio de credenciales, debe realizarse de modo que nadie ajeno a este intercambio pueda conocer esta información. Para ello, se aconseja que esta información se cifre, de modo que en caso de que alguien pueda acceder a las credenciales enviadas no sea capaz de interpretarlas.

Esta buena práctica es de especial relevancia en el desarrollo de aplicaciones y servicios para dispositivos móviles, ya que utilizan tecnologías inalámbricas y por tanto sus transmisiones son más fáciles de interceptar. Se han detectado numerosos casos en los que la información se transmite en texto plano, plenamente legible para cualquiera, poniendo así en riesgo la privacidad de estas credenciales.

5.12 NO APORTAR MÁS INFORMACIÓN DE LA DEBIDA SOBRE LOS USUARIOS

La actuación de los prestadores de servicios y de los agentes encargados de la autenticación debe tener entre sus premisas la conservación de la privacidad de los usuarios, por lo que no deben aportar información acerca de ellos salvo en casos totalmente imprescindibles.

Por ejemplo, es habitual que al tratar de realizar un nuevo registro en el que se utilice información ya registrada se avise de esta situación, por ejemplo informando de que la dirección de correo electrónico que se intenta utilizar para registrarse en un servicio ya ha sido utilizada para registrarse anteriormente. Está práctica aporta más información de la que debería sobre los usuarios del sistema, ya que en el caso de ciertos datos que podrían identificar a una persona, por ejemplo su dirección de correo electrónico, pondrían en evidencia que dicha persona se ha registrado en el servicio.

Esta situación se puede evitar, por ejemplo, realizando dicha notificación mediante un correo electrónico, de modo que solamente pudiera conocer este aviso el usuario con acceso a esa cuenta de correo.

Del mismo modo que no se debería informar sobre si una información ya ha sido registrada, tampoco se debería informar en caso de que no lo estuviera. En este caso la situación inadecuada podría ocurrir tanto en el proceso de registro como en el proceso de autenticación.

5.13 REQUISITOS LEGALES

Al gestionar los sistemas de autenticación se debe tener en cuenta que tanto la información utilizada en el proceso de autenticación como la información que se protege mediante este mecanismo, e incluso los servicios a los que se da acceso, pueden contar con determinados requisitos legales.

De este modo, es necesario valorar en cada caso cuáles son las implicaciones legales a las que se debe hacer frente, pudiendo en muchos casos ser necesario replantear determinados aspectos del proceso de autenticación diseñado.

Un claro ejemplo de estas situaciones es el uso de determinadas informaciones biométricas que, al poder llegar a señalar aspectos sobre la salud o el origen étnico, podrían necesitar un tratamiento especial para poder cumplir los requisitos establecidos por la Ley Orgánica de Protección de Datos de Carácter Personal (LOPD).

Las mismas consideraciones se deben tener en cuenta en el proceso de registro, ya que determinados servicios, por ejemplo la banca electrónica, cuentan con sus propios requisitos legales en lo que respecta a la identificación de los usuarios.

5.14 SERVICIO MULTIPLATAFORMA E INTEROPERABILIDAD

Debido a la variedad de dispositivos de acceso (pc, tableta, smartphone, etc.) y de sistemas operativos (Microsoft Windows, Mac OS, Android, iOS, etc.) que los usuarios pueden emplear, es necesario que al implementar un sistema de autenticación online se tenga en cuenta esta situación para que el sistema sea accesible por diferentes medios.

A su vez, las posibilidades de interacción y las diferentes alternativas que se pueden presentar, tanto en el presente como en el futuro, hacen que sea recomendable que en el desarrollo de estos sistemas se tenga en cuenta los modelos y requisitos de interoperabilidad y se valore su implementación. De este modo los sistemas podrán ser modificados o migrados en el futuro, adaptándose a las nuevas tecnologías, sin mayores inconvenientes.

5.15 AUTENTICACIÓN BASADA EN CERTIFICADOS

La utilización de certificados implica mayores niveles de seguridad, por lo que es recomendable su implementación. En estos casos, y debido a la intermediación de otros agentes, se debe tener en cuenta una serie de aspectos para poder preservar estos altos niveles de seguridad:

- Es recomendable establecer políticas de identidad y firma electrónica que definan en qué certificados se puede confiar para cada uso o transacción concretos. Para las Administraciones Públicas, la aprobación de esta política es obligatoria en virtud de lo establecido en el artículo 18 del Real Decreto 4/2010, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad.

- Se debe gestionar adecuadamente la confianza en los prestadores de servicios de certificación que expiden los certificados. Una buena práctica es desactivar, en todas las aplicaciones, la confianza automática en los certificados raíz de los prestadores no conocidos. Es una buena forma de evitar posibles compromisos de seguridad, especialmente en el caso de la autenticación SSL/TLS. A su vez se pueden emplear las Listas de Confianza de Prestadores que publican las Autoridades competentes para la supervisión de esta actividad.

- Es necesario establecer procedimientos de validación de los certificados de identidad, empleando los mecanismos establecidos por cada prestador. Debe tener siempre mayor prioridad la verificación con métodos en línea, como OCSP, frente a métodos con desfase temporal.

- Se debe conectar, siempre que sea posible, con sitios que empleen certificados SSL/TLS con EV, y aplicar configuraciones apropiadas de algoritmos de seguridad y gestión de la confianza en los proveedores de certificados digitales.

6. Experiencias de éxito

En este capítulo se presentan diferentes iniciativas relacionadas con la autenticación merecedoras de ser reseñadas en las que se han utilizado varios elementos y técnicas ya señaladas.

6.1 VERIFICACIÓN DE IDENTIDAD EN EL ACCESO A SERVICIOS DE OPERADOR MÓVIL VIRTUAL (tuenti.com)

Una experiencia que ha sabido aprovechar los diferentes sistemas de identificación digital en las redes sociales es la desarrollada por la red social Tuenti, para implementar la verificación de la identidad de las personas que acceden a su servicio de operador móvil virtual “Tu”.

Debido al requisito legal de identificar a las personas que adquieren tarjetas de telefonía móvil de prepago, y a la insuficiente calidad de los identificadores de primera parte de la red social Tuenti, la compañía ha apostado por el empleo del DNI electrónico en el procedimiento de registro.

El empleo de un nivel de identificación superior para la activación de la SIM virtual, constituye una estrategia absolutamente válida para prestar este servicio sin la necesidad de redes de atención al cliente o procedimientos administrativos basados en documentación en papel posteriormente digitalizada.

6.2 INTEROPERABILIDAD DE IDENTIFICADORES NACIONALES EUROPEOS (STORK)

STORK –acrónimo de *Secure idenTity acrOss boRders linKed* – es un proyecto europeo que tiene como objetivo desarrollar una plataforma europea de identificación electrónica de interoperabilidad. Permitirá a los ciudadanos establecer nuevas relaciones electrónicas trasnacionales, con tan sólo presentar su identificación electrónica nacional.

El papel de la plataforma consiste en actuar como intermediario de identificación en la relación entre un usuario y un proveedor de servicios online. Mientras que el proveedor puede solicitar diversos datos, el primero siempre controla los datos que se envían. Este enfoque centrado en el usuario se ha tomado en línea con los requisitos legales de los Estados miembro, que obligan a adoptar medidas concretas para garantizar que los derechos fundamentales de los ciudadanos, tales como la intimidad, sean respetados.

STORK es, sin duda, una de las más completas propuestas de carácter práctico sobre la interoperabilidad de las identificaciones nacionales, extensible a otros tipos de identificación.

6.3 FIRMA Y AUTENTICACIÓN CON DNIE ELECTRÓNICO EN SMARTPHONES Y TABLETAS ANDROID: DNIe DROID (INTECO)

DNIe Droid es un proyecto de I+D+i desarrollado por INTECO que permite realizar operaciones de firma y de autenticación con el DNI electrónico desde un terminal que utilice el sistema operativo Android (la plataforma para dispositivos móviles más utilizada en España actualmente) para acceder a servicios online que requieran el uso del DNI electrónico para comprobar la identidad del usuario.

Dicho desarrollo ha sido certificado conforme a la norma *Common Criteria*, con un nivel de garantía EAL1. INTECO ha adaptado este controlador a la tecnología Android, a partir de su versión 3.1, para facilitar la comunicación entre el controlador y el lector de tarjetas inteligentes vía USB. Esto se hace por medio de un lector de tarjetas inteligentes USB estándar (debe ser compatible con CCID, que es lo habitual), generalmente a través de la conexión micro USB del terminal.

INTECO ha creado una aplicación práctica basada en el código de DNIe Droid y que permite la interacción física entre el dispositivo móvil y los servicios. El software permite mostrar los datos personales del usuario extraídos de su DNIe, consultar los puntos del permiso de conducir en la DGT y el historial de vida laboral en el INSS.

Una vez se libere el código fuente del driver en el que se basa, los desarrolladores podrán crear multitud de aplicaciones que usen el DNIe: importarán en las mismas el código, reutilizándolo y así cualquier programa en Android que requiera el acceso con DNIe podrá utilizar el DNIe Droid de INTECO. También es posible la publicación de la aplicación DNIe Droid para que todas las aplicaciones que necesiten hacer uso del DNI electrónico puedan utilizarla, facilitando así la integración de las funcionalidades de autenticación y firma electrónica en las aplicaciones de terceros.

Aunque los ciudadanos puedan utilizar la aplicación creada por INTECO con los tres servicios citados, el objetivo último de este proyecto es que los desarrolladores aprovechen esta innovación para crear software basado en el uso del DNI electrónico, dinamizando de este modo la industria y beneficiando a los ciudadanos.

El proyecto se ha desarrollado sobre la base del Controlador Java para el DNIe puesto en marcha por el Ministerio de Hacienda y Administraciones Públicas, en colaboración con INTECO y Red.es.

6.4 IDENTIFICACIÓN EN LA e-CIENCIA (RedIRIS.es)

RedIRIS es la red académica y de investigación española, que dirige sus esfuerzos a proporcionar servicios avanzados de comunicaciones a la comunidad científica y universitaria en España. Esta red ofrece un sistema de interconexión entre los servicios de identificación de las instituciones afiliadas y proveedores de servicio, a nivel nacional e

internacional. El servicio se basa en tecnologías de federación de identificaciones, de manera que:

- Los usuarios se identifican en los servidores locales de la institución, utilizando el procedimiento de identificación definido por la misma y sin que las credenciales sean expuestas fuera del dominio local.

- Cada institución aplica de manera autónoma los mecanismos de control que considere necesarios para ofrecer a sus usuarios la posibilidad de decidir sobre la información personal susceptible de ser transmitida.

- Los proveedores de servicio aplican de manera autónoma los mecanismos de control de acceso a los recursos que tienen bajo su control.

Algunos de los consumidores de identificaciones federadas a través de este servicio incluyen prestadores de servicios externalizados, incluso en *cloud computing,* más de un centenar de bibliotecas en línea y múltiples herramientas colaborativas.

6.5 PARTICIPACIÓN POLÍTICA BASADA EN IDENTIFICACIÓN DIGITAL (MiFirma.com)

MiFirma es una asociación sin ánimo de lucro que ha creado un portal web donde se ofrece soporte a la realización de iniciativas legislativas populares a través de Internet, una posibilidad prevista en la Ley Orgánica 3/1984, de 26 de marzo, reguladora de la iniciativa legislativa popular, en su redacción del 2006, pero que hasta la fecha no se había implantado con éxito.

En esta y otras modalidades de participación ciudadana a través de Internet, la acreditación de la identidad resulta un elemento clave. En especial, la disponibilidad de un amplio número de certificados digitales permite ya proceder a la captura de las quinientas mil firmas requeridas por la norma, con menores costes en forma electrónica que en soporte papel. El sistema ha sido confirmado como válido por la Junta Electoral Central y constituye un excelente ejemplo de incremento de la calidad democrática de la sociedad con base en la identidad digital.

Asimismo, en otros escenarios de participación menos exigentes, la tecnología subyacente a MiFirma.com también permite el empleo de identidades basadas en perfiles de red social, gracias a la integración con OpenID.

6.6 IDENTIFICACIÓN BIOMÉTRICA PARA LA GESTIÓN DE AYUDAS PÚBLICAS (Gobierno de Polonia)

Se trata de un proyecto de gestión de ayudas públicas otorgadas por el Gobierno de Polonia a través de cajeros automáticos, autenticando a los ciudadanos mediante el reconocimiento de la estructura de las venas de los dedos y un PIN. Mensualmente un

total de 2.000 personas hacen uso de la tecnología en cada una de las 65 sucursales en la que está instalada.

El objetivo es la gestión de las ayudas gubernamentales de forma segura, cómoda y automatizada. En un principio solamente se consideró la gestión de las prestaciones por desempleo pero actualmente su uso se ha ampliado a otras ayudas.

Con el uso de esta tecnología se pretende mejorar la eficiencia de la gestión de las ayudas gubernamentales. Hoy en día, si no se usa el sistema biométrico, el beneficiario entrega un documento de identificación en una oficina bancaria, el cual se debe comprobar, y se rellenan una serie de formularios. Este proceso se demora considerablemente en el tiempo. Esto suele conllevar la creación de largas colas de espera para poder acceder a las ayudas, provocando el descontento de los ciudadanos.

Sin embargo, utilizando el sistema implantado, el usuario puede acudir a un cajero automático a la hora que le resulte más conveniente para obtener la ayuda. Esta comodidad es beneficiosa tanto para la entidad bancaria, aliviando sus oficinas de clientes pudiendo ofrecer un mejor servicio, como para el usuario, que no necesita acudir en horario de apertura de oficinas.

7. Recomendaciones para los usuarios

En gran medida, los riesgos existentes en los procesos de autenticación pueden mitigarse mediante el diseño seguro de las aplicaciones y servicios web. Sin embargo, estas medidas pocas veces pueden ser adoptadas por los particulares.

No obstante, es posible señalar diferentes **pautas** dirigidas a los **usuarios finales para su autoprotección.** De este modo el usuario podrá comprender la importancia de sus actos de cara a preservar los necesarios niveles de seguridad en los sistemas a los que accede.

7.1 UTILIZAR CONTRASEÑAS ROBUSTAS

Al margen de cuáles sean los requisitos mínimos de seguridad establecidos en el sistema, el usuario final debe ser consciente de que las credenciales deben ser complejas para poder cumplir su función, que no es otra que permitir la autenticación únicamente al legítimo usuario.

Por ello, y especialmente en el uso de contraseñas, debe seguirse una serie de pautas[23]:

- Longitud mínima de 8 caracteres, incluyendo mayúsculas, minúsculas, números y símbolos o caracteres especiales. Estas medidas dificultan en buena medida los ataques de fuerza bruta.

- No utilizar contraseñas o combinaciones fáciles de adivinar ni palabras completas, ya que mediante ataques en los que se utilicen diccionarios sería posible descifrarlas (por ejemplo: password, contraseña, qwerty. 123456, abc123).

- Evitar que las contraseñas sean, o incluyan, datos personales (por ejemplo nombres o fechas de nacimiento).

7.2 NO COMPARTIR NI PONER AL ALCANCE DE OTROS LAS CREDENCIALES

El usuario, además de ser el principal afectado en caso de incidentes que permitan a otros acceder a sus servicios, es el principal responsable de mantener a salvo sus credenciales. Por ello, es de gran importancia que estas credenciales no estén disponibles para otras personas, especialmente en el uso dispositivos físicos (por ejemplo tarjetas de identificación) y contraseñas.

Así, una tarjeta de identificación permanentemente conectada a un equipo o un *post-it* con la contraseña anotada pegado a la pantalla son prácticas que inutilizan los sistemas de autenticación al estar las credenciales al alcance de cualquiera.

[23] El artículo Gestión de Contraseñas, publicado como parte de los Cuadernos de notas del Observatorio de Seguridad de la Información del INTECO, disponible en http://www.inteco.es/Seguridad/Observatorio/Articulos/Gestion_contrasenas contiene recomendaciones para crear y gestionar correctamente las contraseñas.

7.3 UTILIZAR DIFERENTES CONTRASEÑAS PARA CADA SERVICIO

En el uso de contraseñas, el tipo de credenciales más extendido, es importante no utilizar la misma para todos los servicios, siendo recomendable que para cada servicio se elija una contraseña distinta.

De este modo, en caso de que la privacidad de alguna de ellas fuera comprometida, solamente se vería afectado uno de los múltiples servicios online, no perdiendo el control de los demás.

7.4 MODIFICAR LAS CONTRASEÑAS REGULARMENTE

Para evitar posibles problemas, es recomendable cambiar las contraseñas utilizadas con cierta regularidad. Esta práctica permite que, en caso de que las contraseñas hayan sido expuestas, dejen de ser útiles para quien las haya conocido.

A esta indicación se debe añadir la necesidad de modificar, siempre que sea posible, las contraseñas que se establezcan por defecto.

7.5 CONFIGURAR ADECUADAMENTE LAS OPCIONES DE SEGURIDAD

En la mayoría de los casos, los sistemas de autenticación cuentan con diversas opciones de seguridad que deben ser configuradas por los usuarios. Es de especial importancia activar estas opciones y configurarlas de modo que puedan cumplir con su labor. Por ejemplo, es positivo establecer la necesidad de una segunda credencial en caso de accesos atípicos (por ejemplo desde dispositivos no utilizados anteriormente) o activar la autenticación de doble factor o de dos pasos en determinados servicios (por ejemplo el envío de parte de las credenciales a través del teléfono móvil en el acceso a la banca electrónica).

A su vez, otras opciones deben utilizarse de modo que no faciliten el acceso de intrusos. Por ejemplo, en caso de existir una alternativa que permita al sistema aportar algún indicio de la contraseña si es olvidada, éste debe ayudar a recordarla, pero no ser suficientemente evidente como para facilitar el acceso a otras personas.

Esta correcta configuración de las diferentes opciones de seguridad debe llevarse a cabo tanto en el acceso principal como los sistemas secundarios, ya que un acceso secundario inseguro o abierto a otras personas inutiliza todas las medidas de seguridad existentes en el método de acceso principal.

7.6 CONTACTAR CON EL ADMINISTRADOR EN CASO DE INCIDENTE

Siempre que se detecte algún problema en la autenticación, tanto si dificulta como si impide el acceso, es recomendable ponerse en contacto con el administrador del sistema. De este modo podrán solucionarse los inconvenientes y prevenir futuros problemas.

Esta recomendación es plenamente válida en caso de detectar alguna intrusión o sospechar que otra persona ha podido acceder a un espacio restringido.

7.7 GESTIÓN SEGURA DE CERTIFICADOS

En primer lugar, es necesario adquirir siempre certificados de prestadores confiables y que hayan comunicado el inicio de su actividad al supervisor, que en España es la Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, y que publica el listado de estos prestadores en su sede electrónica[24]. Además, en ciertos, casos se recomienda adquirir certificados reconocidos, y cuando sea posible, con seudónimo[25].

Por otro lado, también es recomendable proteger adecuadamente los datos de activación de nuestra clave privada de identidad o firma, no cederla ni copiarla.

Finalmente, es necesario emplear dispositivos seguros para la creación de firma electrónica, como el DNI electrónico, aunque pueda suponer más costes o ralentizar el uso. Es muy conveniente proteger nuestra clave privada de identidad y firma electrónica frente a cualquier intento de robo o suplantación[26].

7.8 USAR EL DNI ELECTRÓNICO PARA FIRMAR Y PARA TRÁMITES

El DNI electrónico es una herramienta muy útil a la hora de autenticarse para acceder a servicios online o para firmar documentos. Su fortaleza reside en que cuenta con unos certificados digitales de seguridad y para su uso se necesita una contraseña que únicamente puede ser establecida por el titular del mismo, ya que para ello se deben utilizar las huellas dactilares.

[24] Disponible en la dirección https://www11.mityc.es/prestadores/busquedaPrestadores.jsp.

[25] Por ejemplo, certificados de persona física vinculada a una empresa, con seudónimo de la persona física e identificación plena de la empresa, que se utilizan para la facturación electrónica.

[26] Cuando las claves privadas de los certificados se encuentran almacenadas en software, su seguridad depende de la calidad de dicho software. En el pasado, diversas plataformas se han visto atacadas por malware capaz de obtener dicha clave privada, "robando" el certificado.

8. Conclusiones

Las nuevas tecnologías han abierto un amplio abanico de oportunidades en la prestación de servicios e incluso en las relaciones que los ciudadanos pueden establecer. Este desarrollo y la mayor implantación de la Sociedad de la Información ponen de manifiesto una de las necesidades más importantes a las que se enfrentan las TIC, la comprobación de la identidad de los usuarios o autenticación.

La autenticación hasta ahora era especialmente importante en el acceso a servicios e informaciones a las que solamente algunos usuarios deberían poder acceder. Pero actualmente está cobrando relevancia, y en el futuro se verá reforzada, la necesidad de integrar y corroborar la firma digital, de modo que se pueda utilizar esta firma como evidencia de la autoría y aprobación de diferentes documentos y acciones. Así, mediante esta firma se puede desde afirmar la autoría de un documento hasta declarar el consentimiento en una transacción económica.

Además, la mayor implantación y profundización en la Sociedad de la Información y el uso de Internet, junto a las actuales y futuras tendencias como el almacenamiento de información y prestación de servicios en la nube o la Administración electrónica, remarcan la importancia de la seguridad en la autenticación, de modo que se permita el acceso únicamente a los usuarios legítimos.

Ante este nuevo escenario, la respuesta de los desarrolladores y administradores de sistemas de autenticación ha sido la búsqueda de nuevas formas de autenticación que permitan llevar a cabo este proceso de una forma más segura y sin que esto suponga un inconveniente en la experiencia de los usuarios al utilizar servicios online.

A su vez, el proceso de registro está experimentando una evolución en la que se mejora la seguridad e incluso se comienza a sustituir por una autenticación externa, en la que existen unos agentes de confianza que intermedian en la relación con los usuarios.

En cuanto a los estándares tecnológicos, la tendencia actual trae consigo el desarrollo y mayor securización de los certificados digitales y las aserciones, manteniendo en buena medida al usuario al margen de este proceso y de sus complejidades. Esta mayor relevancia de los desarrolladores y administradores frente al usuario se entiende claramente al ser aquellos quienes establecen las normas y las condiciones bajo las que se llevarán a cabo los procesos de autenticación y ser también quienes mayores conocimientos tienen sobre seguridad y sobre los posibles riesgos.

De entre los diferentes aspectos en que los desarrolladores y administradores de los sistemas de autenticación deben tener en cuenta se pueden considerar de vital importancia:

- Establecer requisitos en la elección de credenciales que aseguren altos niveles de protección contra el acceso por parte de intrusos. De especial importancia es la robustez y complejidad de las credenciales.

- Verificar la identidad real durante el registro siempre que sea posible. Si bien las actuales tendencias dificultan que se realice una comprobación física, ciertos elementos como el DNI electrónico pueden suplir estos inconvenientes.

- Mantener los mismos niveles de seguridad de los sistemas principales de autenticación en los sistemas secundarios. Un sistema secundario poco robusto inutiliza todas las medidas de seguridad que se implementen en los sistemas principales. Por ello es necesario que la misma preocupación y cuidado por la seguridad que se aplique en las principales puertas de acceso se aplique en esas puertas traseras.

- Almacenar y transmitir la información de forma segura. El cifrado de la información transmitida y almacenada es de especial importancia en este caso.

- Utilizar certificados digitales y promover el uso de la firma electrónica.

- Aprovechar la existencia del DNI electrónico como elemento de seguridad para la autenticación.

A pesar de todos estos desarrollos y mejoras en los aspectos técnicos y de administración, el papel del usuario no es menor, y éste debe ser consciente de la gran importancia que tiene su actitud y las medidas de seguridad que ponga en práctica. Así, de entre las diferentes medidas de seguridad que los usuarios deben tener en cuenta destacan:

- Usar contraseñas robustas, reemplazarlas con cierta regularidad y no utilizar las mismas para diferentes servicios.

- Mantener las credenciales, tanto contraseñas como dispositivos de seguridad, fuera del conocimiento y alcance de otras personas.

- Activar y configurar correctamente las diferentes opciones de seguridad, tanto en los sistemas principales de acceso como en los secundarios (por ejemplo preguntas de seguridad), de modo que no sean fácilmente accesibles o adivinables por otras personas.

- Primar las opciones de configuración que impongan una autenticación realizada en varios pasos o con varios factores, por ejemplo posesión de un dispositivo y conocimiento de una contraseña.

- Utilizar certificados digitales y especialmente el DNI electrónico como elementos de identificación y firma electrónica en las relaciones online.

Estas recomendaciones son de especial relevancia, ya que posibilitarán un refuerzo de las medidas de seguridad que los administradores y desarrolladores de sistemas de autenticación.

Las Administraciones Públicas por su parte, se encuentran inmersas en un proceso de concienciación y orientación en esto aspectos, tratando de preservar la seguridad en la autenticación y la interoperabilidad de estos sistemas. Esta interoperabilidad tiene como finalidad que las informaciones utilizadas puedan ser usadas por diferentes agentes, asegurando así su compatibilidad. La interoperabilidad no solo se trata de llevar a cabo a nivel nacional, sino que implica también a nivel europeo.

En este sentido, destacan actuaciones como el desarrollo de instrumentos de identidad nacional como el DNIe, o el proyecto STORK, orientado a garantizar que, además, pueda emplearse en el resto de la Unión Europea.

A su vez, estos esfuerzos se encuentran en un constante evolución y reorientación, como bien muestra el desarrollo de la aplicación DNIe Droid con la finalidad de que el ámbito de uso del DNI electrónico no se limite a los equipos informáticos ya habituales sino que se pueda adaptar a los dispositivos con mayor tendencia de uso, como son actualmente los smartphones.

9. Glosario

Ataque de fuerza bruta

Ataque mediante el cual se intenta acceder a un sistema utilizando todas las combinaciones posibles para formar una credencial o contraseña. La tecnología actual permite generar y probar cientos de contraseñas por minuto para conseguir el acceso a un sistema.

Autenticación

Proceso mediante el cual se comprueba la identidad de una persona. Puede tratarse de una identificación en caso de que el sistema reconozca al usuario directamente, o de una verificación si el usuario señala inicialmente su identidad y el sistema se limita a comprobar la veracidad del modo establecido.

Certificado digital

Documento mediante el cual una autoridad de certificación garantiza la identidad del poseedor de determinada clave pública, siempre que se encuentre en conjunción con una clave privada que solamente dicho poseedor conoce.

De este modo se utiliza un tercero de confianza (la autoridad de certificación) para que un usuario se identifique ante él y así obtenga un certificado digital y un par de claves (pública y privada) que servirán como instrumentos de autenticación e identificación.

Clave privada y clave pública

Claves que conforman un sistema de autenticación basado en certificados digitales mediante el cual se puede tanto firmar como cifrar un documento. Cada par de claves es adjudicado únicamente a una persona, por ello este sistema funciona mediante la conjunción de ambos elementos.

Para la firma se utiliza la clave privada (clave solamente conocida por el usuario), de modo que cualquier persona pueda comprobar su autoría mediante el uso de la clave pública, al alcance de todos mediante la autoridad de certificación que ha expedido el certificado digital al que está asociada. Por otro lado, para cifrar un archivo se utiliza la clave pública, de modo que solamente quien conozca la clave privada podría descifrar dicho archivo.

En el caso de la autenticación el proceso es similar al del cifrado, ya que el sistema de autenticación conoce la clave pública mientras que el usuario debe aportar la clave privada para corroborar la correspondencia.

Credencial

Elemento utilizado para atestiguar una identidad. Puede ser, por ejemplo, una contraseña, la respuesta a una pregunta, un elemento físico como una tarjeta criptográfica o un rasgo físico o de comportamiento. Se puede considerar parte de las credenciales a los identificadores de usuarios (nombres de usuario por ejemplo).

Falso positivo

Error de un sistema de autenticación que confirma positivamente la identidad de una persona debiendo realmente rechazarla. Esta situación permite a una persona no autorizada el acceso a un servicio o información para quien no debería estar disponible. En caso de ocurrir en un proceso de firma electrónica se estaría validando una autoría de forma errónea.

Falso negativo

En este caso el error cometido por el sistema de autenticación consiste en no reconocer positivamente a un usuario legítimo. Como consecuencia, el usuario no puede acceder al servicio o la información deseada o no puede realizar su firma electrónica.

Firma digital

La firma digital es un método criptográfico que asocia la identidad de una persona o de un equipo informático al mensaje o documento. En función del tipo de firma, puede, además, asegurar la integridad del documento o mensaje, de modo que la firma digital atestigüe que el documento o programa en cuestión no sólo ha sido creado por una persona u organización, sino que no ha sido objeto de modificaciones por parte de otros.

Firma electrónica

La firma electrónica es el término utilizado por la normativa española. No obstante, desde un punto de vista técnico tiene un alcance más amplio que el de la firma digital, ya que también contempla métodos no criptográficos (por ejemplo, engloba supuestos como la firma manuscrita digitalizada o la firma manuscrita escaneada).

Ingeniería social

Método de ataque que centra sus esfuerzos en engañar al usuario en lugar de en la explotación de vulnerabilidades técnicas en el software. Estos ataques generalmente son un simple medio para un objetivo posterior, usualmente obtener acceso a determinada información o sistemas.

Puede consistir en diversas formas de contacto (llamadas telefónicas, comunicaciones online, encuentros personales, etc.) con el objetivo de que el usuario o víctima realice una

determinada acción, desde desvelar una contraseña o ser agregado como contacto en una red social hasta informar sobre las herramientas y programas que utiliza.

IP

Una dirección formada por una serie de números que identifica a un equipo de forma unívoca dentro de una red.

MAC

Es un valor que los fabricantes asignan a cada componente de una red, y que los identifica de manera unívoca. Tienen dirección MAC las tarjetas de red, los routers, los USB wifi y todos los dispositivos que puedan tener una IP.

Puertos TCP/UDP

Estos puertos son los puntos de conexión con los que cuentan los diferentes dispositivos y complementan la dirección IP. De este modo, al realizarse una conexión entre dos dispositivos, la dirección IP señala el dispositivo y los puertos TCP/UDP indican los puntos que van a utilizarse para realizar dicha conexión. Así, esta combinación de IP y número de puerto permanece invariable durante la comunicación de modo que se pueda corroborar que dicha comunicación se realiza entre los dos mismos dispositivos y sin interrupciones o modificaciones.

Reciben su nombre (TCP y UDP) de los protocolos utilizados, *Transmission Control Protocol* (Protocolo de Control de Transmisión), orientado a la conexión bidireccional, y User Datagram Protocol (Protocolo de Datagramas de Usuario) no enfocado a la bidireccionalidad.

Registro

Proceso mediante el cual un usuario se inscribe por primera vez en un sistema. En este proceso se determinan, entre otros aspectos, los métodos utilizados para acceder al sistema y la información que se debe presentar para poder ser autenticado.

Síguenos a través de:

http://observatorio.inteco.es

Perfil Facebook ObservaINTECO
http://www.facebook/ObservaINTECO

Perfil Twitter ObservaINTECO
http://www.twitter.com/ObservaINTECO

Perfil Scribd ObservaINTECO
http://www.scribd.com/ObservaINTECO

Canal Youtube ObservaINTECO
http://www.youtube.com/ObservaINTECO

Blog del Observatorio de la Seguridad de la Información:
http://www.inteco.es/blogs/BlogSeguridad

Envíanos tus consultas y comentarios a:

observatorio@inteco.es

INTECO

Instituto Nacional
de Tecnologías
de la Comunicación

www.inteco.es