La firma digital

Las TIC en el comercio minorista de Aragón

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
GOBIERNO DE ARAGON
Departamento de Innovación y Nuevas Tecnologías
@dministración
UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

Índice

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

1. Presentación

Hola, me llamo Javier y soy dinamizador de Tauste.

Muchos conciudadanos que tienen sus pequeños negocios de alimentación y bebidas han participado en un curso sobre nuevas tecnologías, y estoy preparando un dossier con información sobre la firma electrónica y el certificado digital, ya que para muchos es un mundo casi desconocido el poder realizar gestiones desde su ordenador personal con estos recursos. ¿Me acompañas?

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración
UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

2. Firma electrónica

No debemos confundir la f**irma electrónica o digital y la firma digitalizada**, esta última es el resultado de pasar la firma manuscrita a través del scanner. La firma digital es el equivalente a la de puño y letra en el entorno digital y tiene el mismo valor jurídico que con la manuscrita.

Una firma digital es una identificación electrónica de una persona o entidad, creada por un algoritmo (fórmula matemática) de **cifrado** asimétrico o de clase pública que permite garantizar la identidad del firmante así como la integridad del texto o mensaje enviado.

Cifrado

El concepto de cifrado es el proceso de transformar un mensaje que originalmente está en texto claro o normal (plaintext) en un texto codificado llamado texto cifrado (ciphertext) que puede ser entendido solamente descifrándole de nuevo a texto plano. Esta operación se hace a través de una función matemática y de una contraseña especial de cifrado/descifrado llamada CLAVE. En muchos países el cifrado está regulado por leyes y normativas del gobierno.

El **objetivo de la firma digital es el mismo que el de la manuscrita**, pero así como ésta es fácil de falsificar, en el caso de la digital es imposible si no se conoce la clave privada del firmante. La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

Al estar basada en el cifrado asimétrico su principal inconveniente es su lentitud que crece con el tamaño del mensaje a enviar. Como los mensajes que se intercambian pueden tener un gran tamaño no se cifran enteros sino un resumen de los mismos. En definitiva, **la firma digital es un cifrado del mensaje-resumen utilizando la clave privada del firmante**.

El emisor y el receptor de mensajes electrónicos solamente podrán tener la confianza y seguridad que se necesitan en el tráfico comercial si se cumplen los siguientes requisitos:

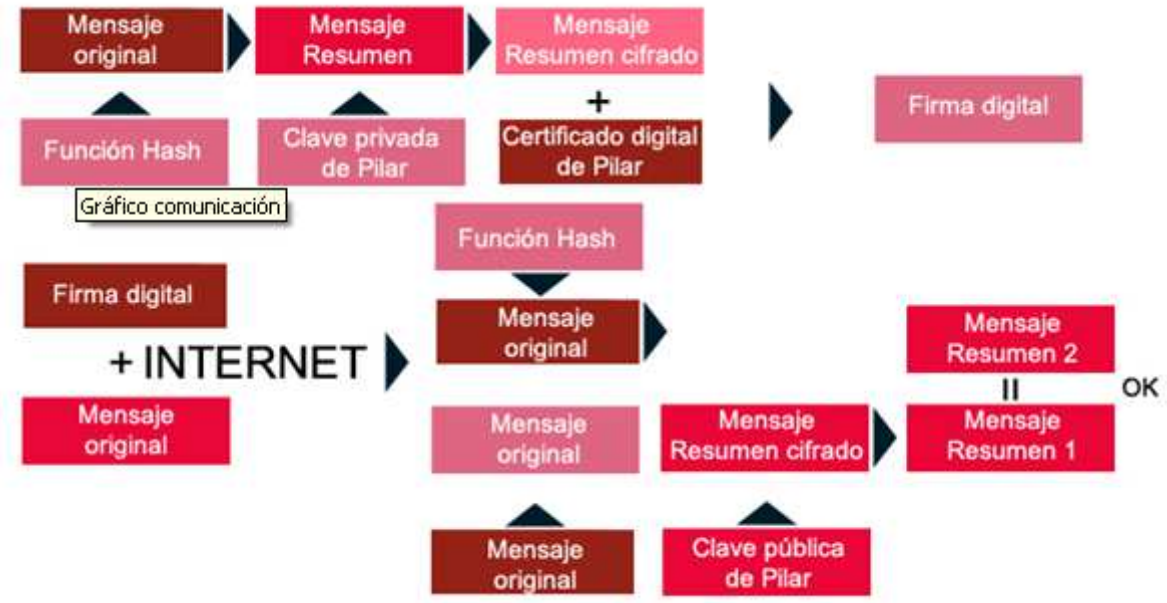
- **La autenticación**: el origen de un mensaje o documento electrónico ha de estar perfectamente identificado.
- **La integridad**: ninguna persona sin autorización puede modificar la información transmitida o almacenada.
- **No repudiación**: Ni el emisor ni el receptor pueden negar la transmisión del mensaje o el contenido del mismo.
- **La confidencialidad**: implica que el mensaje no pueda ser interceptado por terceras personas distintas del emisor o del receptor durante la transmisión del mismo.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGÓN Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) Una manera de hacer Europa

3. ¿Cómo funciona?

El funcionamiento del envío de un mensaje firmado electrónicamente comprende dos procesos.

Por una parte la firma del mensaje por el remitente del mismo y por otra la verificación de la firma por el destinatario.



GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
GOBIERNO DE ARAGON
Departamento de Innovación y Nuevas Tecnologías
@dministración
UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

4. ¿Cómo se consigue?

Cualquier usuario puede conseguir una firma electrónica a través de una **Autoridad de Certificación** y garantizar su identidad a través de Internet de una forma sencilla y accesible.

Para tener una **firma electrónica** hay que seguir el **siguiente proceso**:

- Los usuarios interesados pueden obtener su firma electrónica a través de su propio ordenador deberán conectándose a la **página web de la Autoridad de Certificación correspondiente**.
- El usuario entrega su clave pública en la Autoridad de Certificación correspondiente que comprueba la identidad del usuario.
- En la oficina de acreditación el usuario debe firmar tres contratos originales y se asegurará que los datos registrados son correctos.
- Por último el usuario descargará su firma electrónica desde su propio ordenador con su par de claves, firmada por la Autoridad de Certificación.

El uso de esta firma es oficial y seguro. Es como un elemento de identificación único e intransferible como si el usuario presentara su DNI o firmara personalmente.

Autoridad de Certificación.

Puedes conocer más detalles en los siguientes enlaces:
FNMT (Fabrica Nacional de Moneda y Timbre) http:// www.fnmt.es/
ACE (Agencia de Certificación Española) http:// www.ace.es/

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

5. ¿Dónde se utiliza?

¿Donde se utiliza?

En la actualidad son muchos los usuarios que emplean la firma electrónica, como grandes compañías, pymes y ciudadanos que utilizan los certificados como medio de seguridad y herramienta para la realización de firmas electrónicas.

El certificado de la Fábrica de Moneda y Timbre y su firma electrónica asociada se están aprovechando para realizar gestiones administrativas con la **Seguridad Social**, tales como consultar el informe sobre la vida laboral o con la **Agencia Tributaria** para presentar a través de la red el Impuesto sobre la Renta de las Personas Físicas o del IVA.

En este sentido la Fábrica de Moneda y Timbre pretende mejorar y ampliar sus servicios ofreciendo otros como: sellado de tiempo, certificación de atributos, sistemas de notificación y custodia, voto electrónico, provisión de dispositivos de firma, etc.

La firma electrónica también está sirviendo para la emisión y recepción de facturas en forma automatizada y el envío a clientes en forma segura y rentable.

GOBIERNO DE ESPAÑA
MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO
GOBIERNO DE ARAGON
Departamento de Innovación y Nuevas Tecnologías
@dministración
UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

6. Certificados digitales

Según la ley un certificado digital o electrónico, también conocido como ISDM digital, es un **documento firmado electrónicamente por un Prestador de Servicios de Certificación o Autoridad de Certificación** que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Adicionalmente, además de la clave pública y la identidad de su propietario, un certificado digital puede contener otros atributos para, por ejemplo, concretar el ámbito de utilización de la clave pública, las fechas de inicio y fin de la validez del certificado, etc.

Los certificados suelen tener una **cierta duración y una vez vencida pueden ser renovados**. También pueden ser revocados en ciertos casos como cuando la clave privada deja de ser secreta.

Saber más

Autoridad de Certificación

La Autoridad de Certificación o Prestador de Servicios de Certificación, es una entidad pública o privada encargada de la gestión de certificados digitales. Se le considera como una tercera parte de confianza por los dos elementos implicados firmante y propietario/receptor del certificado.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON · Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

7. Características

Un Certificado Digital se caracteriza por ser el eje de la seguridad en las redes abiertas y servir como prueba de identidad electrónica.

Seguridad

Sirven para que datos confidenciales, como referencias de tarjetas de crédito o información personal, transiten de forma segura por redes abiertas. Así los compradores pueden estar seguros de que un website es legítimo.

Prueba

El certificado digital es fiable porque contiene a una tercera parte de confianza llamada Autoridad de Certificación (CA), que acredita que la información es auténtica y añade su firma en el certificado antes de expedirlo.

Gracias a estas **características** nos posibilita lo siguiente:

- Prescindir de las contraseñas o los números PIN tan fáciles de olvidar.
- Los usuarios pueden utilizarlos para añadir firmas electrónicas.
- Los destinatarios pueden comprobar la autenticidad del correo electrónico confidencial.
- Se puede acceder a los bancos y comercios online, así como a cualquier red de uso privada.

La calidad de **autenticación y seguridad** de la información que contienen los certificados **dependen del tipo o clase de certificado que se expida**.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración
UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

8. Tipos de Certificado

Tipos de Certificado

Actualmente el formato (estándar) que se ha extendido casi para todas las aplicaciones, este es el llamado X.509. Su principal ventaja es que con el mínimo necesario de información se pueden realizar muchas transacciones, principalmente comerciales y financieras.

Entre los **tipos de certificados** que existen podemos citar:

Tipos	Características
Certificado personal	Es el empleado por ciudadanos, de forma particular, para enviar mensajes haciendo uso de la firma electrónica.
Certificado de cargo	Es el utilizado por funcionarios públicos para firmar electrónicamente, cuando estén autorizados por su cargo.
Certificado profesional	Se emplea por usuarios habituales de los Registros.
Certificado de representante jurídico de una empresa	Puede verificar on line de la vigencia del certificado así como la del cargo de representante, permitiéndole firmar de acuerdo con las facultades del mismo en la empresa.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

9. ¿Cómo se obtiene?

El proceso de obtención del Certificado Digital consta de:

- **Solicitar el certificado**. El sistema pedirá el NIF al usuario y le preguntará si tiene confianza en la CA para obtener el certificado. Entonces generará el par de claves pública y privada y se le devolverá un código de solicitud con el que deberá acudir a una Oficina de Acreditación.

- **Acreditarse en una oficina**. El usuario se presentará en la oficina acreditadora de cualquiera de los organismos que utilizan este tipo certificado para acreditar su identidad. Deberá aportar el documento acreditativo de su identidad (DNI O o pasaporte) y el Código de Solicitud que la CA le asignó en el paso anterior. Una vez identificado, se le pedirá que firme el modelo de solicitud así como sus condiciones de utilización, por triplicado.

- **Descargar el certificado**. Realizar una nueva conexión a la web de la Descarga de su Certificado de Usuario para descargar su certificado e instalarlo en su navegador.

Copia de seguridad del certificado. Es muy importante hacer una copia de seguridad del certificado digital.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

10. Ventajas e inconvenientes

Los usuarios que dispongan de firma electrónica pueden consultar **datos de carácter personal**, **realizar trámites u otras gestiones o acceder a diferentes servicios**. Estas gestiones no pueden realizarse mediante correo electrónico, ya que al tratarse de un sistema sin firma electrónica no ofrece el nivel de seguridad necesario para consultar y modificar datos desde Internet.

Se pueden realizar trámites y gestiones ante la un Organismo y obtener una respuesta inmediata sin tener que desplazarse físicamente.

Supone unos ahorros significativos por eliminación de costos por papel, mensajería, implantación rápida sin necesidad de reprogramar las aplicaciones actuales y sin importar la plataforma de hardware o aplicativa.

Además hay que añadir los siguientes aspectos:

- Proporciona el máximo grado de **confidencialidad y seguridad** en Internet.
- Identifica a las partes que se conectan a través de la red.
- Tiene una gran **trascendencia en el campo de la gestión de los derechos de autor**.
- Se identifica a la persona que envía un mensaje, así como se garantiza la **integridad del contenido** del mismo.

Como hemos visto son muchas las ventajas pero también hay que contar con los problemas que aparecen cuando una herramienta depende de las **medidas de seguridad que adopten los usuarios**.

Por este motivo, el principal inconveniente es que la seguridad depende del usuario. La clave privada no sería tal si la conocieran otras personas.

Actualmente es utilizada generalmente por grandes o medianas empresas y en menor proporción por los ciudadanos.

Cuando la firma electrónica está en una tarjeta criptográfica conocer la clave es prácticamente imposible pero cuando se encuentra en un fichero se puede duplicar o encontrar el password o contraseña que da acceso a la clave.

Los **precios de los certificados varían mucho de las distintas Autoridades de Certificación que los emitan** ya que están sometidos a las condiciones del mercado. Según los precios las facilidades de los certificados son diferentes.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa

11. Despedida

Ya hemos finalizado, espero que esta información os sea de utilidad. Recuerda que podrás ahorrarte mucho tiempo realizando trámites con la firma electrónica y los certificados digitales y tendrás más tiempo para dedicar a tu empresa.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA
PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER)
Una manera de hacer Europa

12. Resumen

En esta píldora hemos visto la Firma electrónica y el Certificado digital.

Recuerda que objetivo de la **firma digital es el mismo que el de la manuscrita**, pero así como ésta es fácil de falsificar, en el caso de la digital es imposible si no se conoce la clave privada del firmante. La firma digital permite al receptor de un mensaje verificar la autenticidad del origen de la información así como verificar que dicha información no ha sido modificada desde su generación.

El certificado digital es un **documento firmado electrónicamente por un Prestador de Servicios de Certificación o Autoridad de Certificación** que vincula unos datos de verificación de firma a un firmante y confirma su identidad.

Ambos recursos facilitan numerosas acciones con Organismos públicos, además con la firma digital nuestro campo en Internet se amplía.

Y no olvides las ventajas de utilizar ambas:

- Proporciona el máximo grado de **confidencialidad y seguridad** en Internet.
- Identifica a las partes que se conectan a través de la red.
- Tiene una gran **trascendencia en el campo de la gestión de los derechos de autor**.

Se identifica a la persona que envía un mensaje, así como se garantiza la **integridad del contenido** del mismo.

¡Enhorabuena! Has finalizado con éxito.

GOBIERNO DE ESPAÑA · MINISTERIO DE INDUSTRIA, TURISMO Y COMERCIO · GOBIERNO DE ARAGON Departamento de Innovación y Nuevas Tecnologías · @dministración · UNIÓN EUROPEA · PROYECTO COFINANCIADO POR EL FONDO EUROPEO DE DESARROLLO REGIONAL (FEDER) · Una manera de hacer Europa