La Firma PKI

Ley 39/2015. Artículo 10. Sistemas de firma admitidos por las Administraciones Públicas.

1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. … se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica reconocida o cualificada y avanzada basados en certificados electrónicos reconocidos o cualificados de firma electrónica expedidos por prestadores incluidos en la «Lista de confianza de prestadores de servicios de certificación». ...

b) Sistemas de sello electrónico reconocido o cualificado y de sello electrónico avanzado basados en certificados electrónicos reconocidos o cualificados de sello …

c) Cualquier otro sistema que las Administraciones Públicas consideren válido, en los términos y condiciones que se establezcan.

PF

Nombre y Apellidos
DNI/NIE

PJ

Nombre y Apellidos
DNI/NIE
Razón social
NIF

Y sellos a PJ

Criptografía = En castellano normal, es sinónimo de cifra o de cifrado o de cifrar

Mediante la firma se logra dotar al documento de …

Autenticidad
Integridad
No repudio

Propiedades aseguradas por la firma PKI

Confidencialidad
Trazabilidad
Disponibilidad
Conservación

Propiedades aseguradas por el gestor documental o sistema de archivo

Garantías relativas al documento

Autenticidad: propiedad que puede atribuírsele como consecuencia de que puede probarse que es lo que afirma ser, que ha sido creado o enviado por la persona de la cual se afirma que lo ha creado o enviado, y que ha sido creado o enviado en el momento en que se afirma, sin que haya sufrido ningún tipo de modificación.

Integridad: propiedad o característica que indica su carácter de completo, sin alteración de ningún aspecto esencial. La integridad es un componente de la autenticidad junto a la identidad.

No repudio o irrenunciabilidad es un servicio de seguridad que permite probar la participación de las partes en una comunicación. En origen o en destino.

Confidencialidad capacidad de mantener un documento electrónico inaccesible a todos, excepto a una lista determinada de personas.

Trazabilidad: Propiedad o característica consistente en que las actuaciones de una entidad pueden ser imputadas exclusivamente a dicha entidad. En el ámbito de la gestión de documentos, proceso que facilita el seguimiento de la creación, incorporación, movimiento, uso y eventual modificación de los documentos dentro de un sistema de gestión de documentos.

Disponibilidad: indica propiedad o característica del mismo que permite que éste pueda ser consultado, localizado, recuperado, presentado o interpretado. El documento debe señalar la actividad o actuación donde se generó, proporcionar la información necesaria para la comprensión de las actuaciones que motivaron su creación y utilización, identificar el contexto marco de las actividades y las funciones de la organización y mantener los vínculos existentes con otros documentos como reflejo de una secuencia de actuaciones.

Conservación: Conjunto de procesos y operaciones dedicados a asegurar la permanencia intelectual y técnica de los documentos a lo largo del tiempo.

Autenticidad
Integridad
No repudio
Confidencialidad
Trazabilidad
Disponibilidad
Conservación

Los tipos de firma electrónica

Cualquier medio que permita acreditar la autenticidad de la expresión de la voluntad y consentimiento, así como la integridad e inalterabilidad del documento

- Prevista no desarrollada

Artículo 25 Reglamento (UE) 910/2014

Efectos jurídicos de las firmas electrónicas

1. No se denegarán efectos jurídicos ni admisibilidad como prueba en procedimientos judiciales a una firma electrónica por el mero hecho de ser una firma electrónica o porque no cumpla los requisitos de la firma electrónica cualificada. Referencia a la básica
2. Una firma electrónica cualificada tendrá un efecto jurídico equivalente al de una firma manuscrita.
3. Una firma electrónica cualificada basada en un certificado cualificado emitido en un Estado miembro será reconocida como una firma electrónica cualificada en todos los demás Estados miembros.

Los tipos de firma electrónica

Cualquier medio que permita acreditar la autenticidad de la expresión de la voluntad y consentimiento, así como la integridad e inalterabilidad del documento

- Prevista no desarrollada

Artículo 10. Sistemas de firma admitidos por las Administraciones Públicas.

1. Los interesados podrán firmar a través de cualquier medio que permita acreditar la autenticidad de la expresión de su voluntad y consentimiento, así como la integridad e inalterabilidad del documento.

2. En el caso de que los interesados optaran por relacionarse con las Administraciones Públicas a través de medios electrónicos, se considerarán válidos a efectos de firma:

a) Sistemas de firma electrónica cualificada y avanzada basados en certificados electrónicos cualificados de firma electrónica expedidos por prestadores incluidos en la "Lista de confianza de prestadores de servicios de certificación".

b) Sistemas de sello electrónico cualificado y de sello electrónico avanzado basados en certificados electrónicos cualificados de sello electrónico expedidos por prestador incluido en la "Lista de confianza de prestadores de servicios de certificación".

c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad

Los tipos de firma electrónica

Cualquier medio que permita acreditar la autenticidad de la expresión de la voluntad y consentimiento, así como la integridad e inalterabilidad del documento

Mediante infraestructura de clave pública (PKI) prestada por servicios de confianza

- Prevista no desarrollada

- Local con certif. software SW
- Local con dispositivo seguro de creación de firma
- Centralizada en la nube

Los tipos de firma electrónica

Cualquier medio que permita acreditar la autenticidad de la expresión de la voluntad y consentimiento, así como la integridad e inalterabilidad del documento

Mediante infraestructura de clave pública (PKI) prestada por servicios de confianza

Otros tipos de firma según la Ley 39/2015

- Prevista no desarrollada

- Local con certif. software SW
- Local con dispositivo seguro de creación de firma
- Centralizada en la nube
- Cl@ve
- Cl@ve permanente
- Código Seguro de verificación CSV

LPAC art. 10
c) Cualquier otro sistema que las Administraciones Públicas consideren válido en los términos y condiciones que se establezca, siempre que cuenten con un registro previo como usuario que permita garantizar su identidad

Los tipos de firma electrónica

Cualquier medio que permita acreditar la autenticidad de la expresión de la voluntad y consentimiento, así como la integridad e inalterabilidad del documento

Mediante infraestructura de clave pública (PKI) prestada por servicios de confianza

Otros tipos de firma según la Ley 39/2015

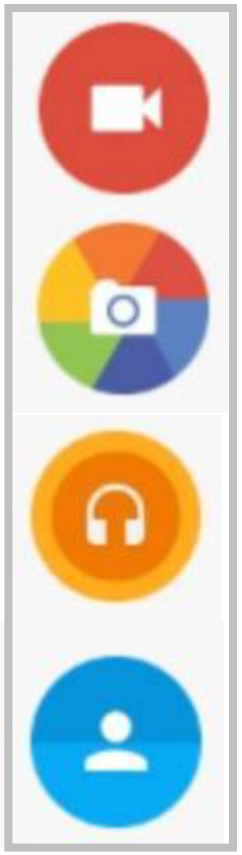
Sistemas de firma aun no regulados

- Prevista no desarrollada

- Local con certif. software SW
- Local con dispositivo seguro de creación de firma
- Centralizada en la nube
- Cl@ve
- Cl@ve permanente
- Código Seguro de verificación CSV

- Firma biométrica por trazo
- Biométrica otros tipos

La firma PKI asegura

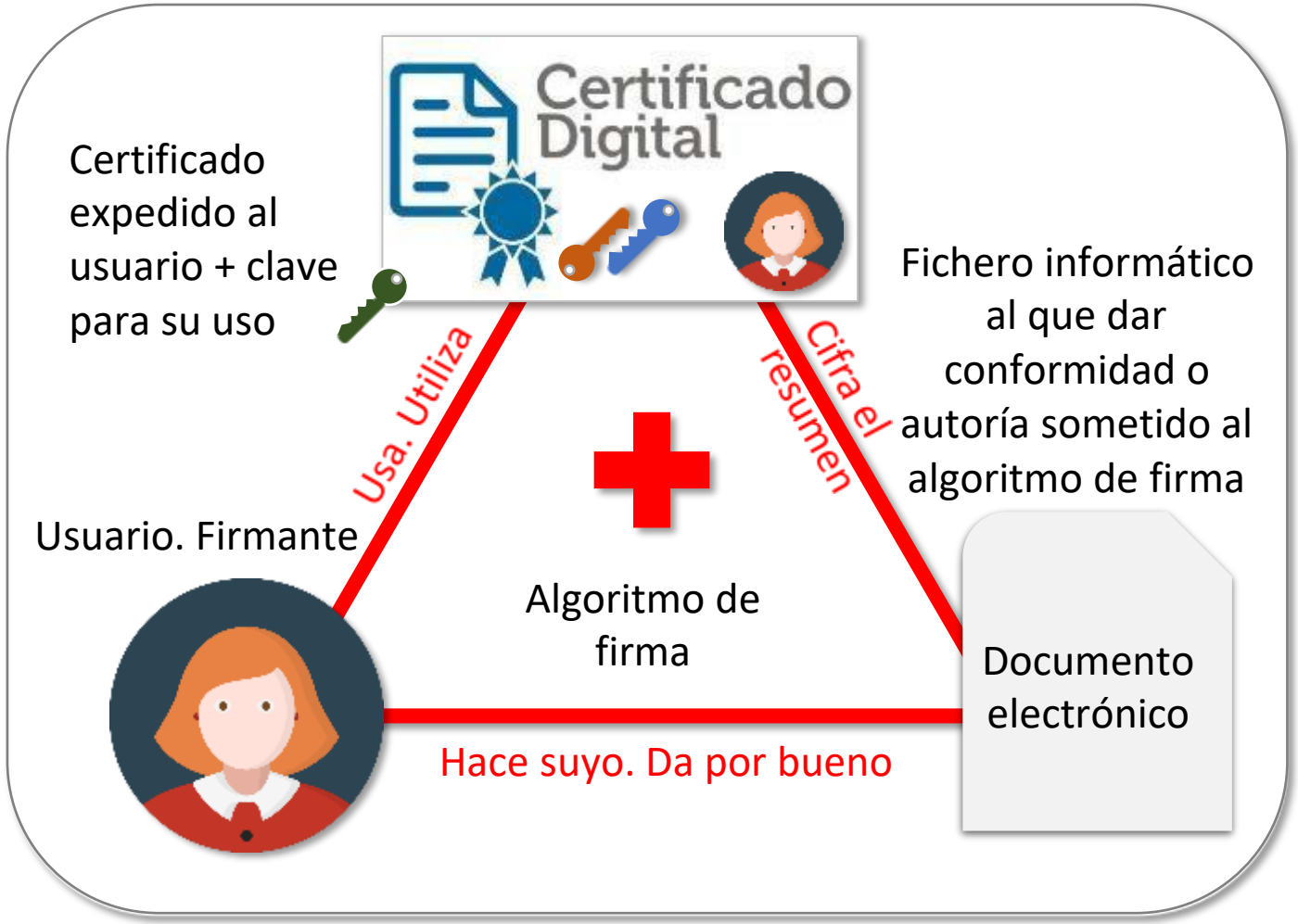


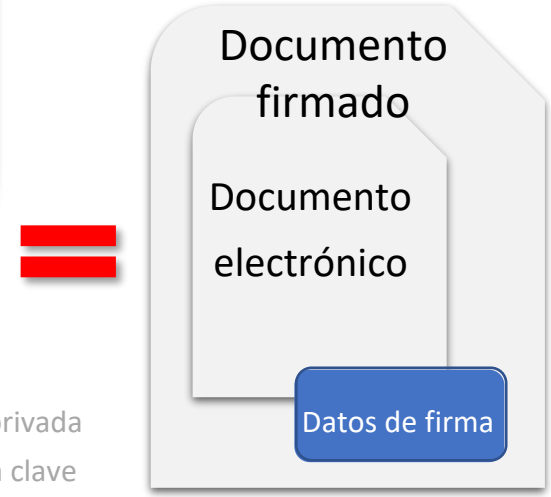
- Que la realiza quien dice ser sin identificación ante funcionario. Autenticidad.
- Que el fichero que se firma no se puede modificar sin quebrar la firma, ni por el firmante, ni por terceros. Integridad.
- Que la firma está vinculada al firmante y a ese documento, pudiéndose probar. No repudio.
- Simetría. Ningún actor es 'superior'. La confianza es cruzada.

Definiciones eIDAS. Firma electrónica PKI

- firma electrónica, los datos en formato electrónico anejos a otros datos electrónicos o asociados de manera lógica con ellos que utiliza el firmante para firmar;
- firma electrónica avanzada, la firma electrónica que cumple los requisitos
  - estar vinculada al firmante de manera única;
  - permitir la identificación del firmante;
  - haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar, con un alto nivel de confianza, bajo su control exclusivo, y
  - estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable.
- firma electrónica cualificada, una firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firma electrónica;
- datos de creación de la firma electrónica, los datos únicos que utiliza el firmante para crear una firma electrónica;
- certificado de firma electrónica, una declaración electrónica que vincula los datos de validación de una firma con una persona física y confirma, al menos, el nombre o el seudónimo de esa persona;
- certificado cualificado de firma electrónica, un certificado de firma electrónica que ha sido expedido por un prestador cualificado de servicios de confianza y que cumple los requisitos establecidos en el anexo I de eIDAS;

Elementos necesarios en la firma electrónica





* Técnicamente los datos de firma (Clave privada del certificado y hash] están cifrados con la clave privada del certificado del firmante

La comprobación de la firma y de la integridad

Redactor. Autor.

Texto o fichero

Función Hash. Algoritmo público

HuT98NggqaDo

Clave (key) Ptivada

Función Firma Algoritmo público

Texto o fichero firmado

Firma

Pedro firma el fichero con su clave privada. El certificado utilizado se adjunta a la firma. Contiene el dato de la clave pública.

Se hace llegar el documento o fichero y su firma, a destino

Texto o fichero firmado

Firma

Receptor. Lector.
No predeterminado

Del autor. Public Key

Función Validación Algoritmo público

Servicio de confianza o tercero de confianza, emisor del certificado

Comprometido

Validado OK

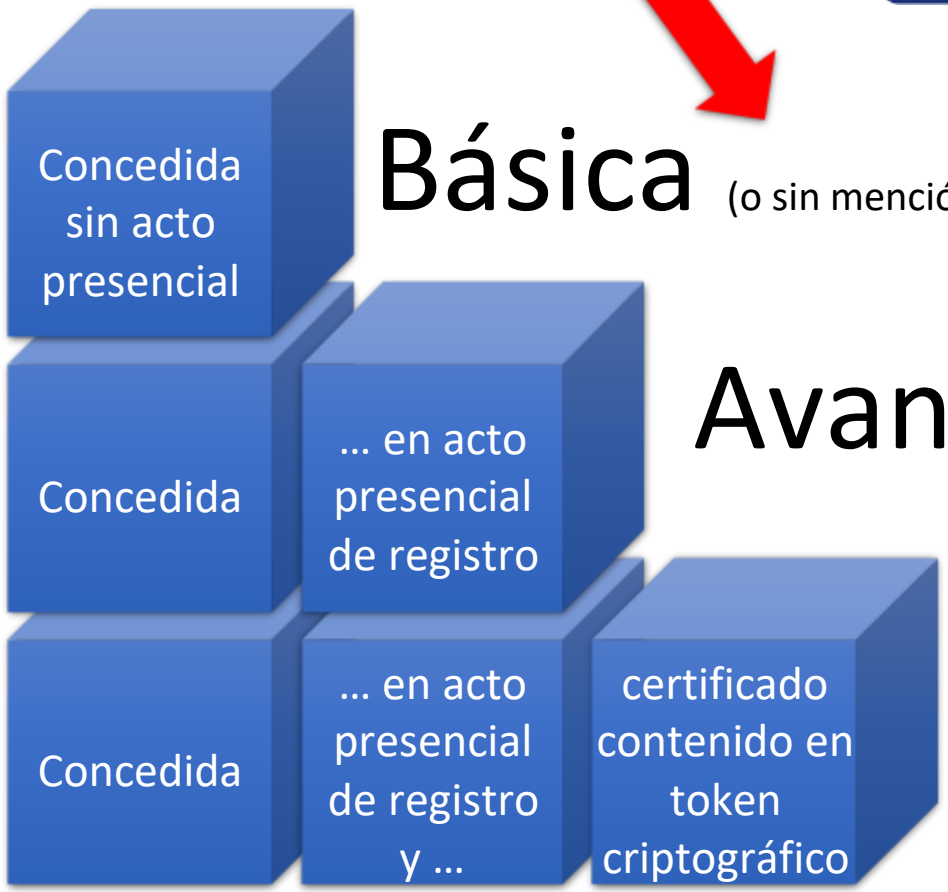
Fichero , certificado o firma comprometidos

Texto o fichero OK

El receptor puede validar la integridad, mediante el has que vuelve a calcular y la identidad de firmante no revocada.

Tipos de firma PKI y validez según certificados.

De menos
a más robustez



Básica (o sin mención calificadora)

No existen certificados de este tipo

Avanzada

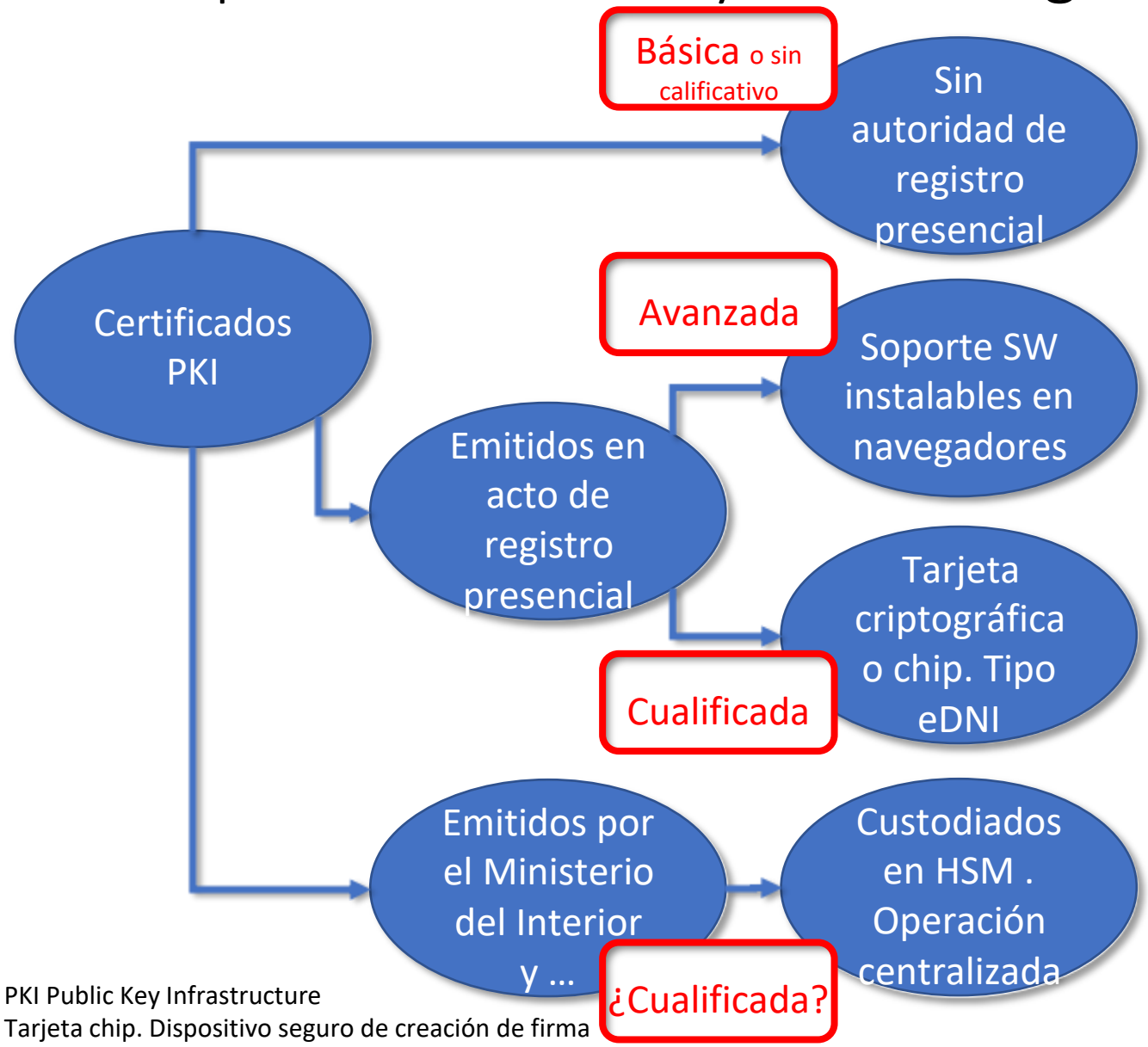
Certificado de tipo SW

Cualificada

Con certificado en dispositivo seguro de creación de firma (token o chip).

Certificado HW

Tipos de firma PKI y validez según certificados.



Técnicamente es un certificado, pero no asegura la identidad ya que al no haberse expedido en acto de registro ha podido emitirse 'para otro'

Se instala, se exporta, se importa en otros dispositivos, se duplica

Emitido en tarjeta chip entregada al titular. No puede copiarse. Las operaciones criptográficas de firma se realizan en su interior

Emitido por la DGP previa identificación fuerte + pregunta por datos que solo conoce el usuario. Custodiado de forma centralizada. Usado 'en la nube'

PKI Public Key Infrastructure
Tarjeta chip. Dispositivo seguro de creación de firma
HSM Hardware Security Module o Módulo de Seguridad Hardware, que tiene la consideración de dispositivo seguro de creación de firma

Tipos de firma, según

1. Proceso de expedición

2. Según el certificado expedido

3. Relación de firma y fichero

4. El formato técnico

Tipos de firma, según sistema de expedición

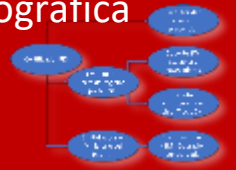
Proceso de expedición 1

- Sin personación en registro al ser expedido
- En soporte SW utilizable en navegadores
- En soporte chip o tarjeta criptográfica
- Residiendo en un HSM

Tipos de firma, según a quien se le expide

1 Proceso de expedición

- Sin personación en registro al ser expedido
- En soporte SW utilizable en navegadores
- En soporte chip o tarjeta criptográfica
- Residiendo en un HSM



2 Según el certificado expedido

- Persona física, de presentante
- Empleado público
- Con seudónimo
- Servidor. Sede electrónica. Sello
- Servidor túnel SSL
- Firma de código informático

PF, PJ, fuerzas del orden, funcionarios, representantes, …

Tipos de firma, según encapsulado

1 Proceso de expedición

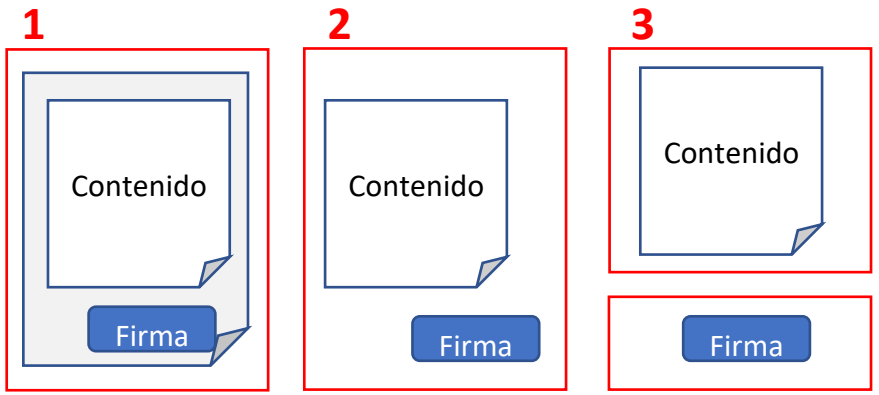
- Sin personación en registro al ser expedido
- En soporte SW utilizable en navegadores
- En soporte chip o tarjeta criptográfica
- Residiendo en un HSM

2 Según el certificado expedido

- Persona física, de presentante
- Empleado público
- Con Pseudónimo
- Servidor. Sede electrónica. Sello
- Servidor túnel SSL
- Firma de código informático

3 Relación de firma y fichero

- Dettached (CMS y XMLdsig). Separada fichero
- Enveloping (CMS y XMLdsig). La firma contiene el documento
- Enveloped (XMLdsig y Pdf). La firma está incluida en el documento. Attached.



Attached
Anexada

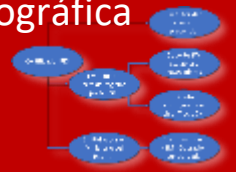
Enveloppe
Sobre

Dettached
Externa

Tipos de firma, según formato técnico

1 Proceso de expedición

- Sin personación en registro al ser expedido
- En soporte SW utilizable en navegadores
- En soporte chip o tarjeta criptográfica
- Residiendo en un HSM



2 Según el certificado expedido

- Persona física, de presentante
- Empleado público
- Con Pseudónimo
- Servidor. Sede electrónica. Sello
- Servidor túnel SSL
- Firma de código informático

3 Relación de firma y fichero

- Detached (CMS y XMLdsig). Separada fichero
- Enveloping (CMS y XMLdsig). La firma contiene el documento
- Enveloped (XMLdsig y Pdf). La firma está incluida en el documento. Attached.

4 El formato técnico

- CMS (Crytografic Message Syntax) PKCS#7
- XML Signature y variantes Advanced
- Para Pdf (PAdES)

Ejemplo de firma XML ‘dettached’

```
<Signature Id=""MiFirmaDetached"" xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
        <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-
                    c14n-20010315"></CanonicalizationMethod>
        <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-
                sha1"></SignatureMethod>
        <Referente URI="http://www.ejemplo.org/midocumento.html">
                <Transforms>
                    <Transform Algorithm="http://www.w3.org/TR/2001/REC-
                        xml-c14n-20010315#WithComments"></Transform>
                </Transforms>
                <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"></DigestMethod>
                <DigestValue>vo7Aa…fwJ8=</DigestValue>
        </Reference>
    </SignedInfo>
    <SignatureValue>BwUwA…2OLtBQ=</SignatureValue>
    <KeyInfo>
        <X509Data>
            <X509Certificate>MIIB9jCC…wZgyg=</X509Certificate>
        </X509Data>
        <KeyValue>
            <RSAKeyValue>
                <Modulus>Pkkl…TP7U=</Modulus>
                <Exponent>AQAB</Exponent>
            </RSAKeyValue>
        </KeyValue>
    </KeyInfo>
</Signature>
```

XMP = eXtended Markup Language. Lenguaje de marcas (etiquetas y valores) extendido

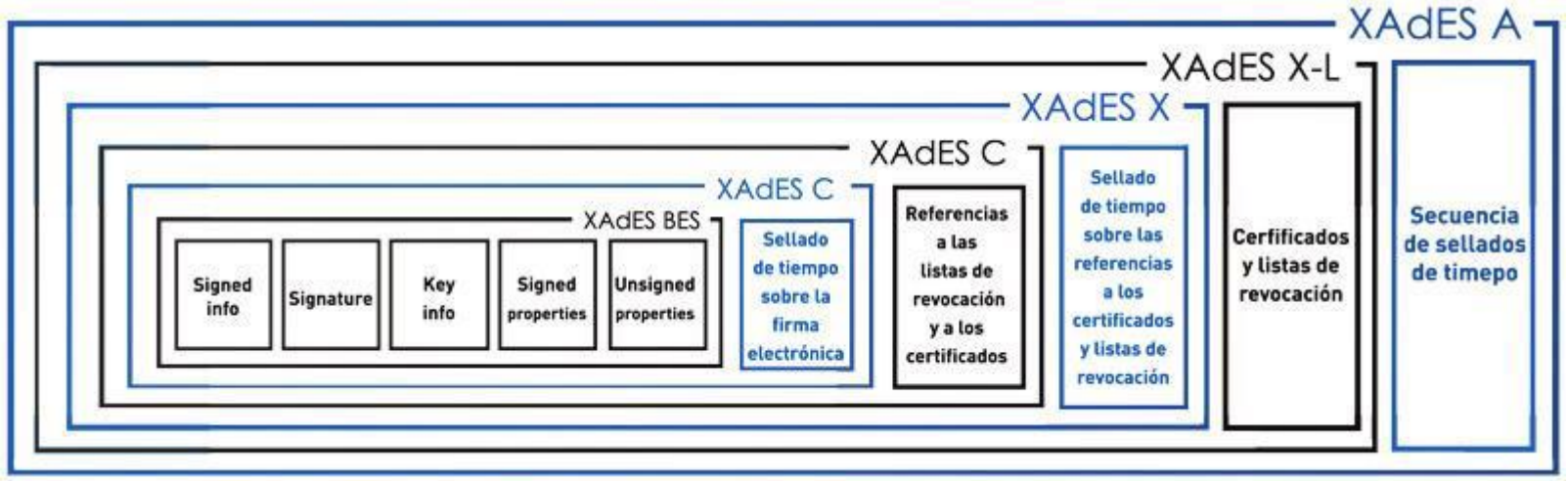
Formato de firma XAdES de firma y variantes

CMS (Crytografic Message Syntax) PKCS#7

XML Signature y variantes Advanced

Para Pdf (PAdES)

Firma Longeva LTV



XML Advanced Electronic Signatures (Firma electrónica avanzada de XML). Define una serie de extensiones a la norma XML-DSig que garantizan una firma electrónica avanzada. Llega hasta la longeva o de archivo (XadES A)

Referencias normativas

- **Reglamento (UE) nº 910/2014** del Parlamento Europeo y del Consejo, de 23 de julio de 2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior. https://www.boe.es/buscar/doc.php?id=DOUE-L-2014-81822
- **Ley 6/2020**, de 11 de noviembre, reguladora de determinados aspectos de los servicios electrónicos de confianza. www.boe.es/buscar/act.php?id=BOE-A-2020-14046
- **Ley 39/2015**, de 1 de octubre, del Procedimiento Administrativo Común de las Administraciones Públicas. www.boe.es/buscar/act.php?id=BOE-A-2015-10565
- Ley 40/2015, de 1 de octubre, de Régimen Jurídico del Sector Público. www.boe.es/buscar/act.php?id=BOE-A-2015-10566
- **Real Decreto 311/2022**, de 3 de mayo, por el que se regula el Esquema Nacional de Seguridad. **ENS**. https://www.boe.es/diario_boe/txt.php?id=BOE-A-2022-7191
- **Real Decreto 4/2010**, de 8 de enero, por el que se regula el Esquema Nacional de Interoperabilidad en el ámbito de la Administración Electrónica. **ENI** www.boe.es/buscar/act.php?id=BOE-A-2010-1331
- **Real Decreto 203/2021**, de 30 de marzo, por el que se aprueba el Reglamento de actuación y funcionamiento del sector público por medios electrónicos. www.boe.es/buscar/act.php?id=BOE-A-2021-5032

Normativa relevante relativa a la firma

Normativa técnica de organismos internacionales

+

Guía de aplicación de la Norma Técnica de Interoperabilidad de Política de firma y sello electrónicos y de certificados de la administración publicada por resolución de 27 de octubre de 2016, de la Secretaría de Estado de Administraciones Públicas, por la que se aprueba la Norma Técnica de Interoperabilidad de Política de Firma y Sello Electrónicos y de Certificados de la Administración.