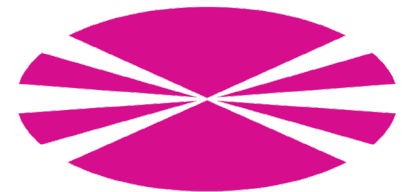


LEGISLACIÓN Y SEGURIDAD INFORMÁTICA

4. Los servicios electrónicos de
confianza: la firma electrónica




Prof. Jorge Crego
jorge.crego@udc.es



LEGISLACIÓN Y SEGURIDAD INFORMÁTICA

**4. Los servicios electrónicos de
confianza: la firma electrónica**

- 1. La nueva ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza**
 - 2. ¿Qué es una firma electrónica?**
 - 3. Efectos jurídicos de la firma electrónica**
 - 4. Los prestadores de servicios de confianza**
- 

1. La nueva ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza

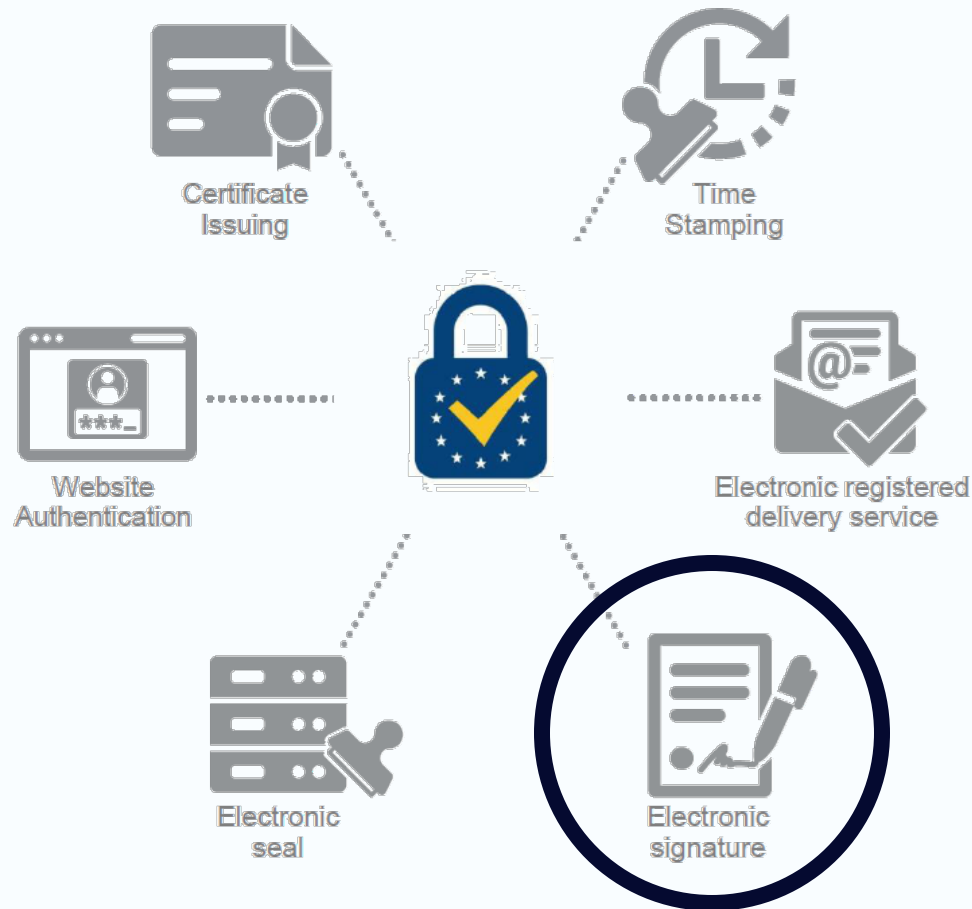


1. La nueva ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza

- Reglamento (UE) 910/2014, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior
 - Deroga: Directiva 1999/93/CE
- Ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza
 - Deroga: Ley 59/2003, de firma electrónica
 - Adapta la normativa española al Reglamento 910/2014 → solamente regula ciertos aspectos delegados a los Estados
 - ¡Cambio importante!
 - Ley 2003: firma electrónica = personas físicas + personas jurídicas
 - Ley 2020:
 - Firma electrónica = personas físicas
 - Sello electrónico = personas jurídicas



1. La nueva ley 6/2020, reguladora de determinados aspectos de los servicios electrónicos de confianza



2. ¿Qué es una firma electrónica?

William
Ephraim

William
Ephraim

William
Ephraim

William
Ephraim

William
Ephraim

2. ¿Qué es una firma electrónica?

Normativa aplicable

Firma digital



Concepto técnico

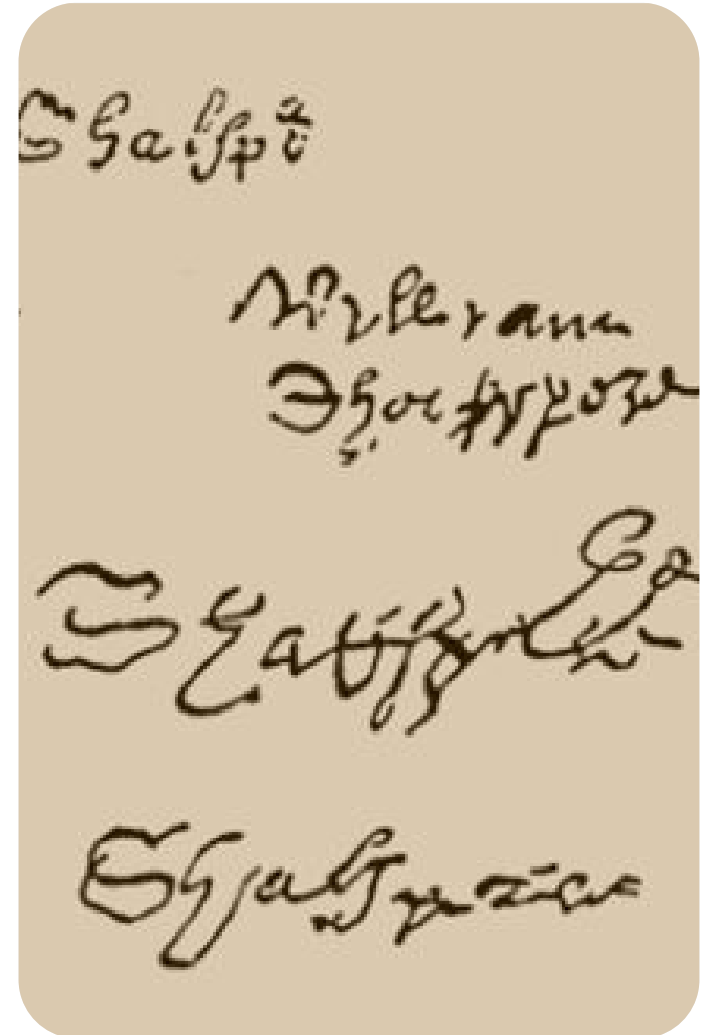
Firma electrónica



Concepto jurídico

Funciones:

- Autenticación de una persona previamente identificada
- Integridad del mensaje
- Irrefutabilidad o “no repudio”
- Confidencialidad



2. ¿Qué es una firma electrónica?

Normativa aplicable



Boost your digital transactions

By removing the need for paper to obtain a signature or seal, the solution facilitates the digitalisation of business processes, eliminating the time, costs and risks of dealing with paper formats.



Improved user experience

Shorter approval times, thanks to faster document signing processes, which leads to higher satisfaction rates.



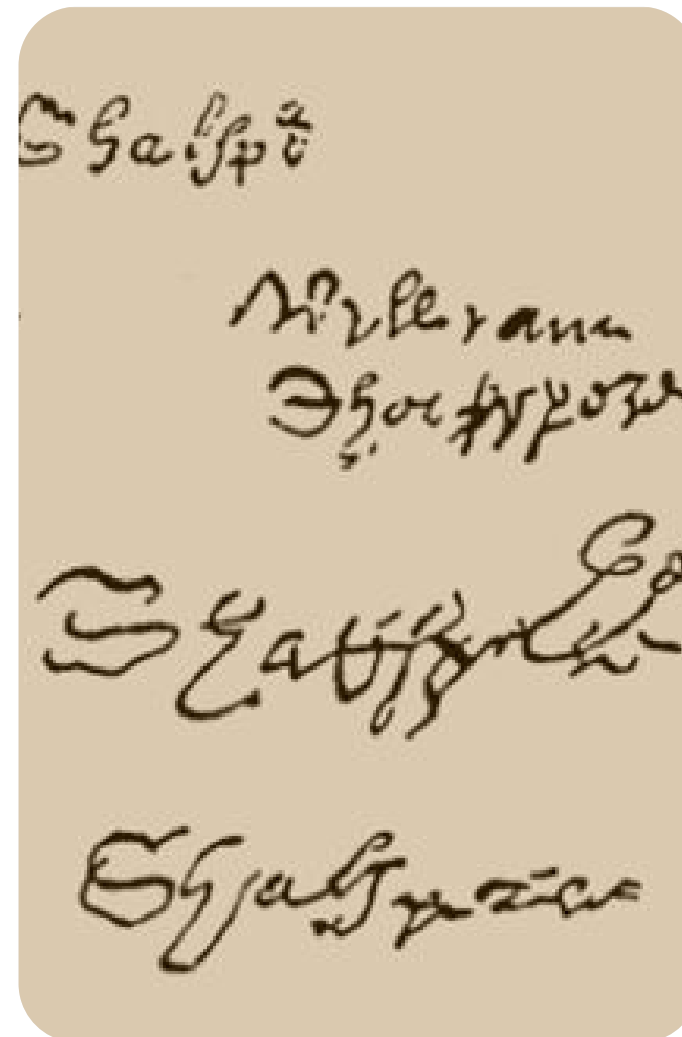
Cross-border legal assurance

eSignature is compliant with the eIDAS Regulation, meaning that it ensures the legal recognition and cross-border interoperability of the electronic signatures and seals produced by solutions based on this building block.



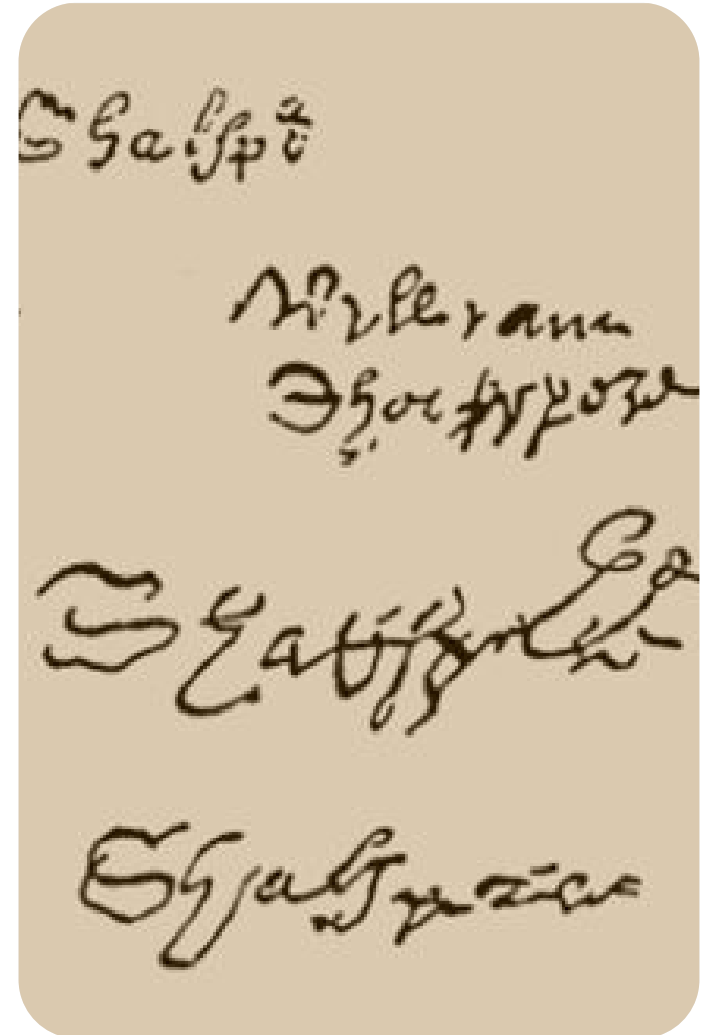
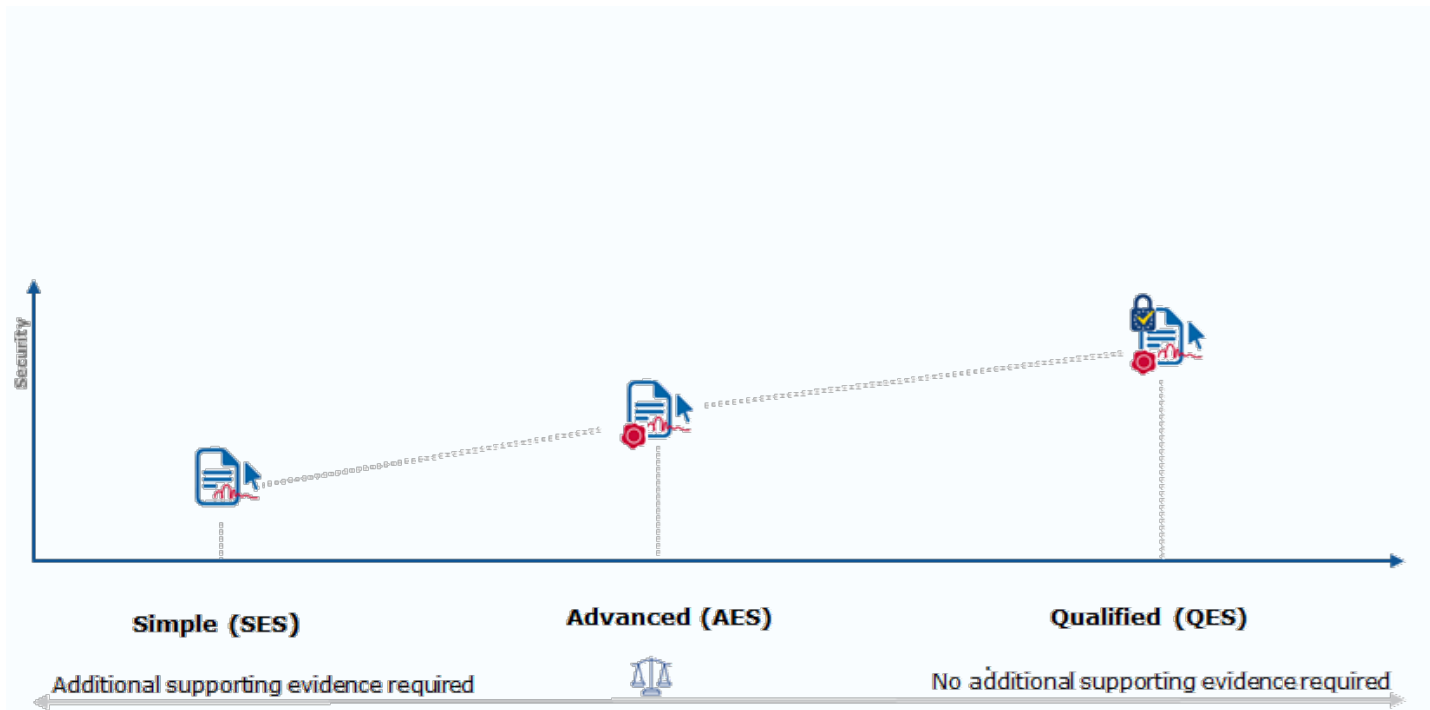
Guaranteed documents' integrity

With eSignature, you reduce risk of document duplication or alteration. The signer's identity is bound to each specific document, ensuring that signatures and seals are verified, authentic and legitimate for that document alone.



2. ¿Qué es una firma electrónica?

Tipos de firma electrónica



2. ¿Qué es una firma electrónica?

Tipos de firma electrónica

Firma electrónica (simple)

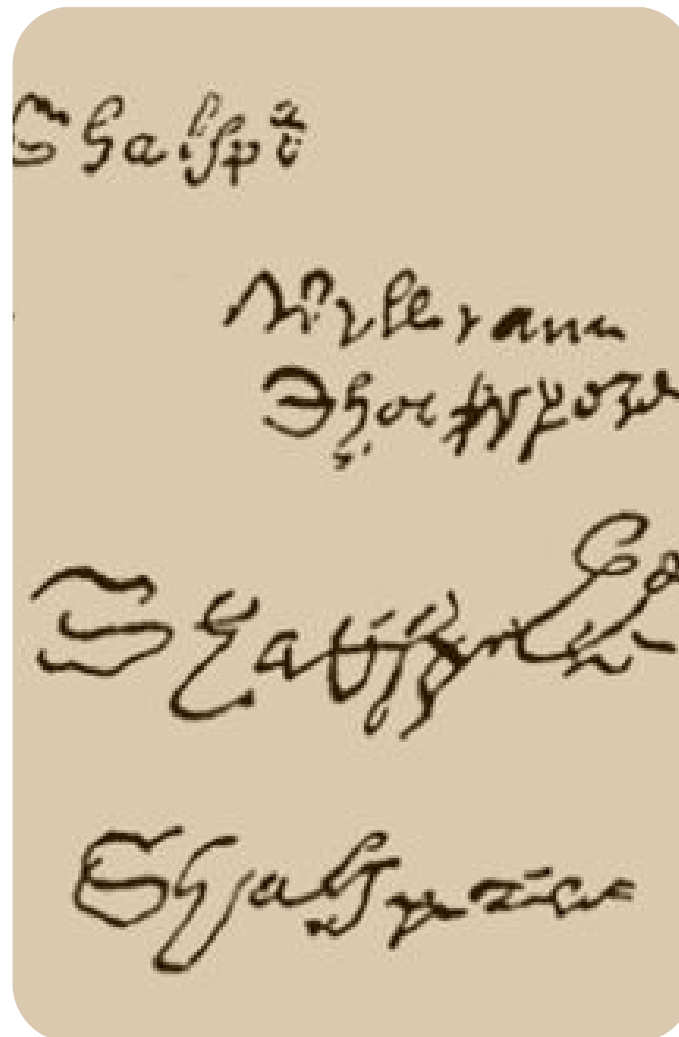
“Los datos en formato electrónico anejos a otros datos electrónico o asociados de manera lógica con ellos que utiliza el firmante para firmar” (art. 3.10 ReIDAS)

Revise y acepte nuestros Términos y condiciones

☐ Sí, he leído y acepto el acuerdo.

Usted declara que es administrador de esta Cuenta y que está autorizado para actuar en nombre del propietario de la misma y que cumplirá con los términos del presente Acuerdo.

CREAR CUENTA



2. ¿Qué es una firma electrónica?

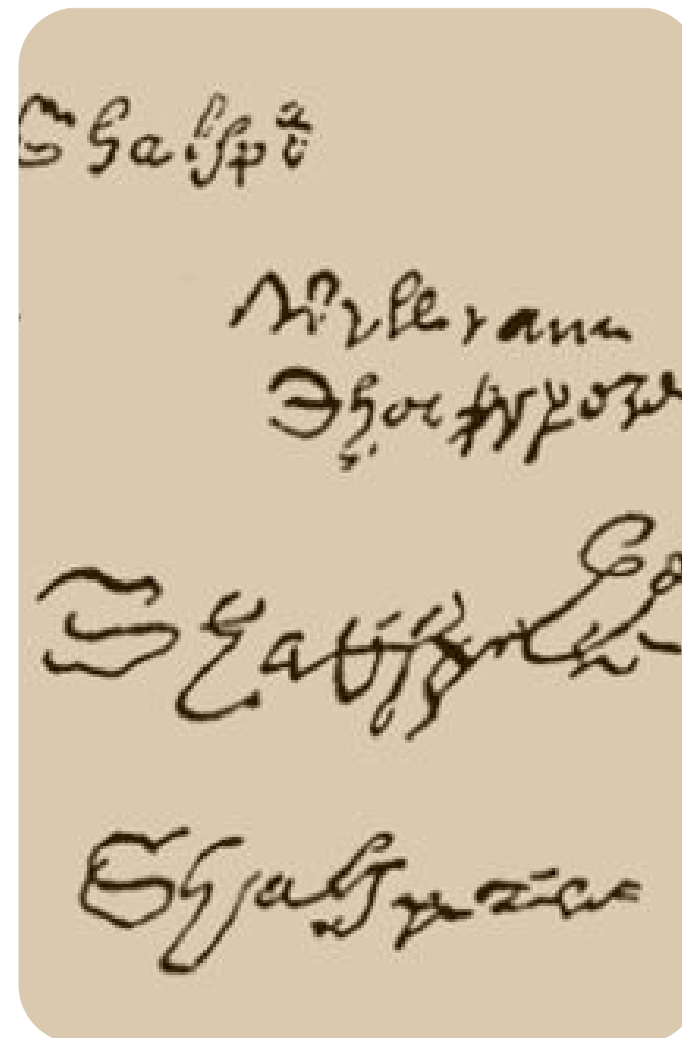
Tipos de firma electrónica

Firma electrónica avanzada

“La firma electrónica que cumple con los requisitos contemplados en el artículo 26” (art. 3.11 ReIDAS)

El art. 26 ReIDAS establece cuatro 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
- Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable



2. ¿Qué es una firma electrónica?

Tipos de firma electrónica

Firma electrónica cualificada

“La firma electrónica avanzada que se crea mediante un dispositivo cualificado de creación de firmas electrónicas y que se basa en un certificado cualificado de firmas electrónicas” (art. 3.12 ReIDAS)



Firma electrónica avanzada + Certificado cualificado + Dispositivo cualificado



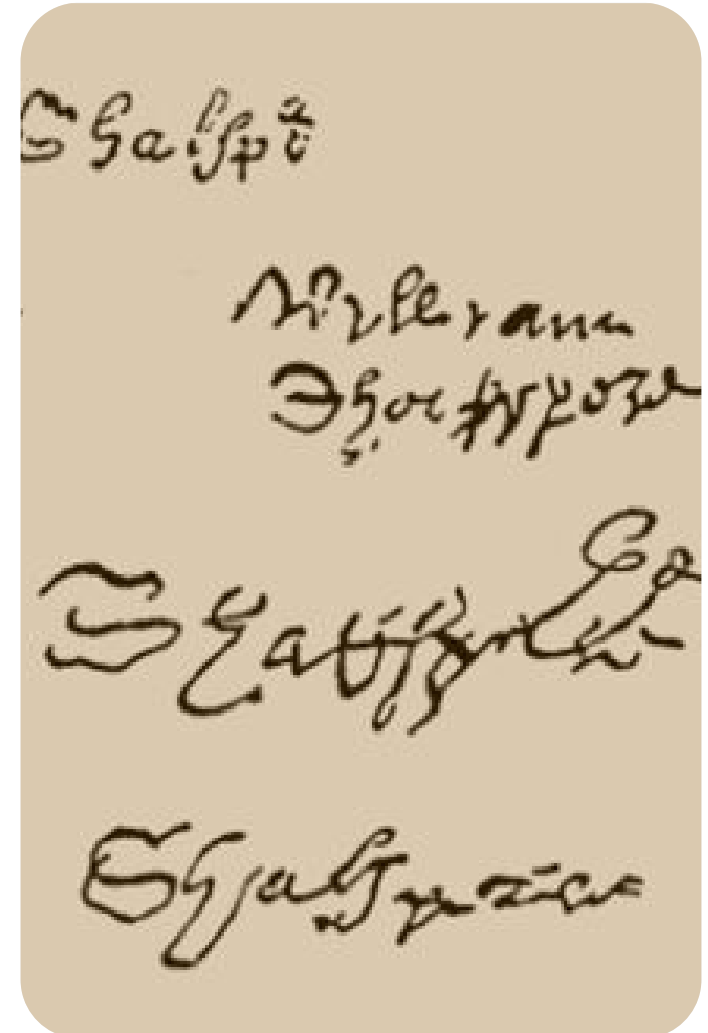
Anexo I

Datos sobre el prestador cualificado, datos sobre el firmante, datos de validación de la firma correspondientes a los datos de creación, período de validez, etc.

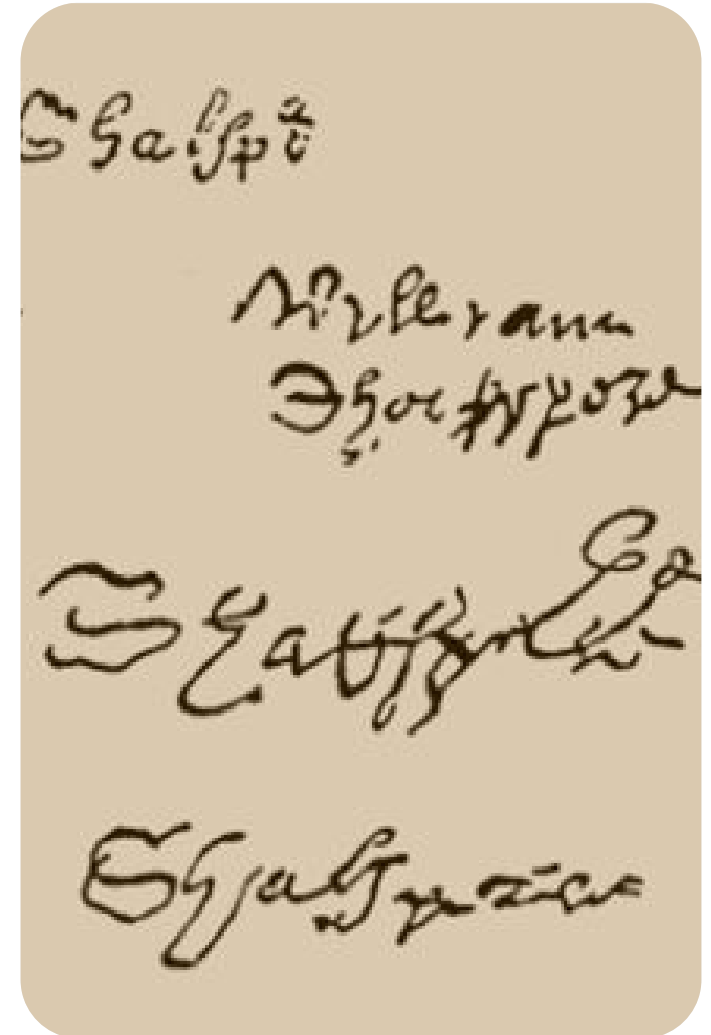
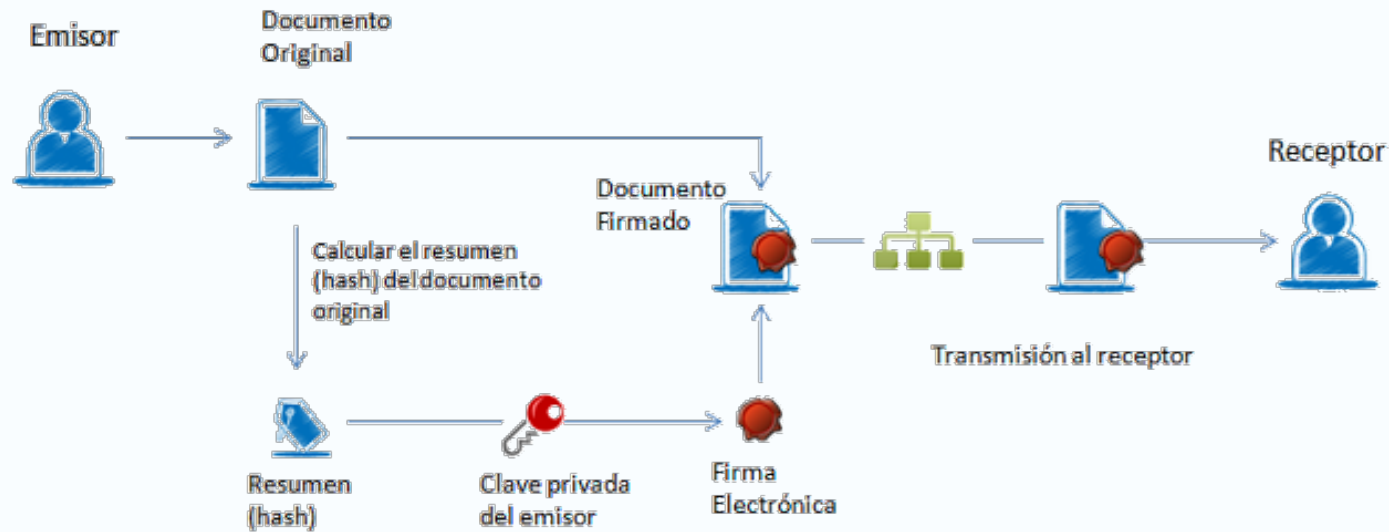


Anexo II

Datos de creación confidenciales, singulares, protegidos contra falsificación, deducción y utilización por terceros



2. ¿Qué es una firma electrónica?



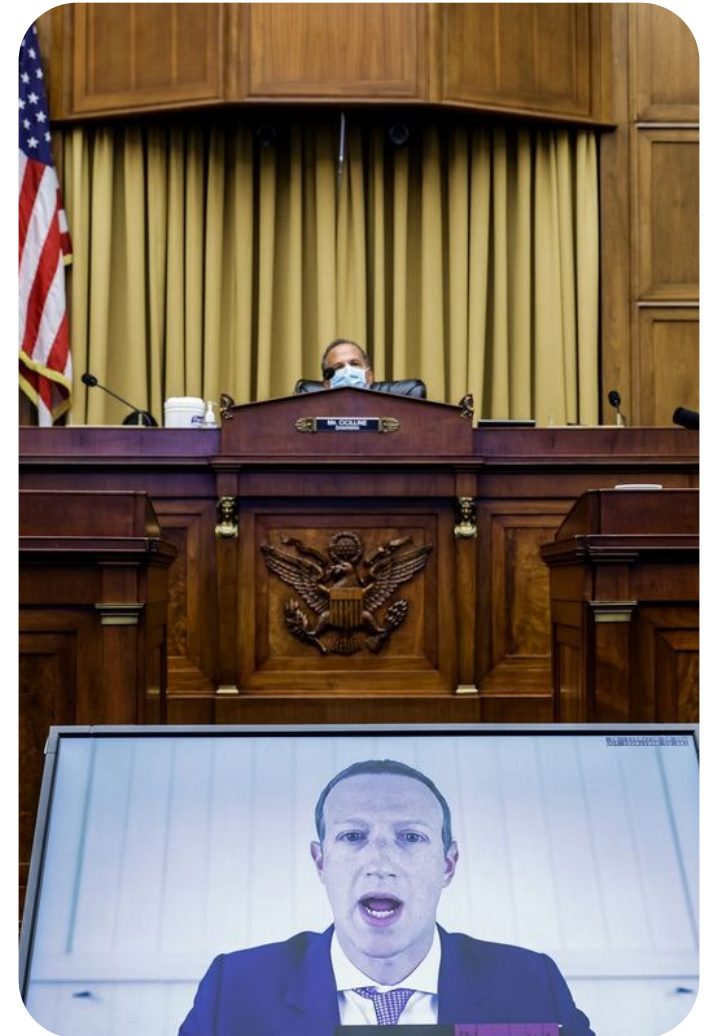
3. Efectos jurídicos de la firma electrónica



3. Efectos jurídicos de la firma electrónica

Reconocimiento y declaración de voluntad

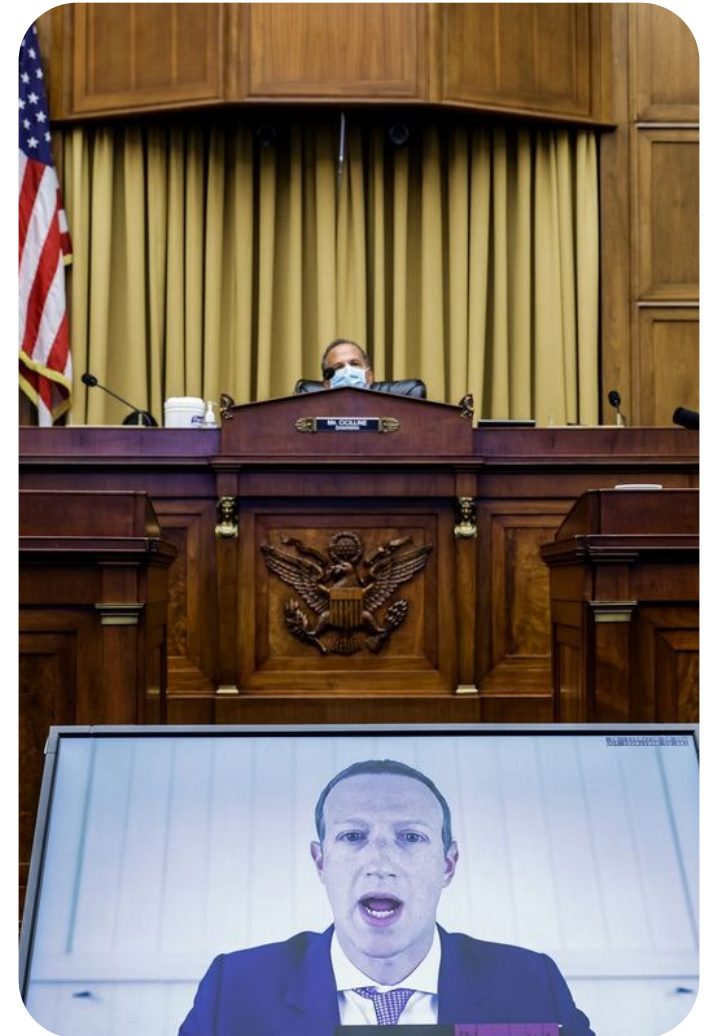
- El art. 25 ReIDAS regula el reconocimiento de las firmas electrónica:
 - Firmas electrónicas cualificadas = firma manuscrita
 - Firmas electrónicas no cualificadas → no se les denegarán efectos jurídicos ni admisibilidad como prueba en juicio
 - Las firmas electrónicas cualificadas basadas en un certificado cualificado emitido en un Estado miembro se reconocerán como firma electrónica cualificada en todos los demás
- La firma electrónica implica una declaración de voluntad → expresa consentimiento del firmante



3. Efectos jurídicos de la firma electrónica

La firma electrónica como prueba

- Si firma electrónica cualificada = firma manuscrita → firma electrónica certifica la validez de un documento en juicio
- La LSEC modifica la LEC en lo referente a la impugnación de firmas electrónicas (art. 326 LEC):
 - Firma electrónica no cualificada → cabe solicitar cotejo pericial
 - Firma electrónica cualificada → presunción de veracidad, si figura en la lista de confianza de prestadores y servicios cualificados
 - Si aun así se impugna: carga de la comprobación en quien lo impugne, costas, gastos y derechos si el resultado es negativo, multa si la impugnación es temeraria



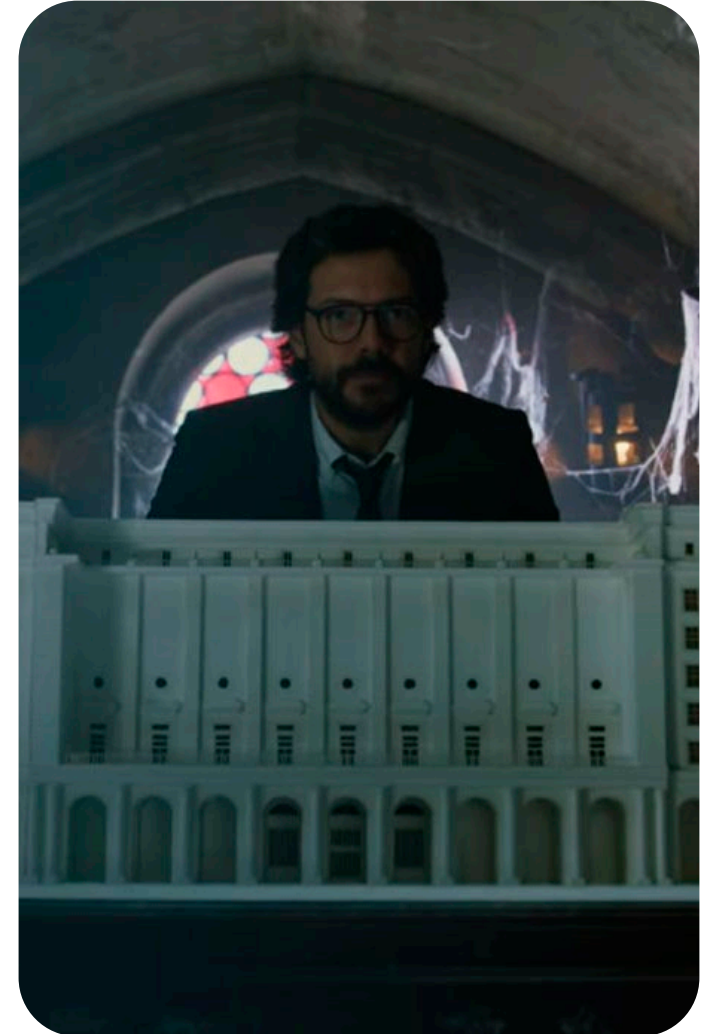
4. Los prestadores de servicios de confianza



4. Los prestadores de servicios de confianza

Definición y obligaciones

- “Persona física o jurídica que presta uno o más servicios de confianza, bien como prestador cualificado o como prestador no cualificado” (art. 3.19 ReIDUS)
- Obligaciones
 - Art. 19 ReIDAS:
 - Medidas técnicas y organizativas de gestión de riesgos
 - Notificar al organismo de supervisión sin demora cualquier violación de seguridad o pérdida de integridad
 - Art. 9 LSEC
 - Publicar información veraz y acorde con la legislación
 - No almacenar ni copiar los datos de creación, salvo gestión en nombre del titular
 - Servicio de consulta sobre el estado de validez o revocación de los certificados, de acceso público
 - Protección de los datos recogidos en el certificado electrónico
 - Constatar identidad cuando se empleen pseudónimos + revelar identidad ante solicitud judicial o de autoridad pública (art. 8 LSEC)
 - Informar a la AEPD si existe una violación de seguridad que comprometa datos personales (art. 19.2 ReIDAS)
- Prestadores cualificados: presta uno o varios servicios de confianza cualificados y el organismo de supervisión le ha concedido la cualificación
 - Obligaciones adicionales (art. 9.3 LSEC). Ej.: seguro de responsabilidad civil de 1,5M€, + 500.000€ por servicio adicional que preste
 - Verificación inicial por parte del organismo de supervisión (art. 21 ReIDAS) e inclusión en la [lista de confianza](#) (art. 22 ReIDAS)
 - Auditorías periódicas (art. 20 ReIDAS)



4. Los prestadores de servicios de confianza

Lista de confianza

Search a trust service by



Type of service

Search by type of trust service (e.g. time-stamping, certificate for e-signature) and country



























Name of trust service

Search based on the name of a trust service



Signed file

Find the trust service that issued the signing certificate(s) contained in a file

 Austria Issue date 2021-01-08	...	 Belgium Issue date 2020-12-15	...	 Bulgaria Issue date 2020-12-21	...
 Croatia Issue date 2020-12-22	...	 Cyprus Issue date 2021-01-05	...	 Czech Republic Issue date 2020-11-30	...
 Denmark Issue date 2020-12-17	...	 Estonia Issue date 2020-12-04	...	 Finland Issue date 2020-07-29	...
 France Issue date 2021-01-06	...	 Germany Issue date 2021-01-04	...	 Greece Issue date 2020-12-14	...
 Hungary Issue date 2021-01-08	...	 Iceland Issue date 2020-09-24	...	 Ireland Issue date 2020-07-17	...
 Italy Issue date 2021-01-11	...	 Latvia Issue date 2020-07-21	...	 Liechtenstein Issue date 2020-12-09	...
 Lithuania Issue date 2020-11-27	...	 Luxembourg Issue date 2020-11-02	...	 Malta Issue date 2020-11-20	...
 Netherlands Issue date 2020-12-16	...	 Norway Issue date 2021-01-06	...	 Poland Issue date 2020-10-27	...



4. Los prestadores de servicios de confianza

Responsabilidad

- Asumen toda la responsabilidad frente a terceros por la actuación de aquellos en que deleguen algunas funciones (art. 10 LSEC)
 - Ej.: actuaciones de comprobación de identidad para expedir certificado cualificado
- Limitación de responsabilidad frente a la persona a la que ha prestado sus servicios o terceros de buena fe si esa persona, entre otros (art. 11 LSEC):
 - No proporcionó al prestador información veraz, completa y exacta, cuando su inexactitud no haya podido ser detectada
 - Falta de comunicación de modificación de circunstancias relacionadas con el servicio
 - Negligencia en la conservación de los datos de creación del servicio, en el aseguramiento de su confidencialidad y protección de acceso o revelación de estos
 - No solicitar la suspensión o revocación en caso de duda sobre la confidencialidad
 - Uso de datos más allá del período de validez
 - Uso negligente por parte del destinatario
 - Inexactitud de datos, si estos han sido acreditados por un documento público u oficial

