Universidad de Oviedo

Departamento de Informática

Campus de Gijón

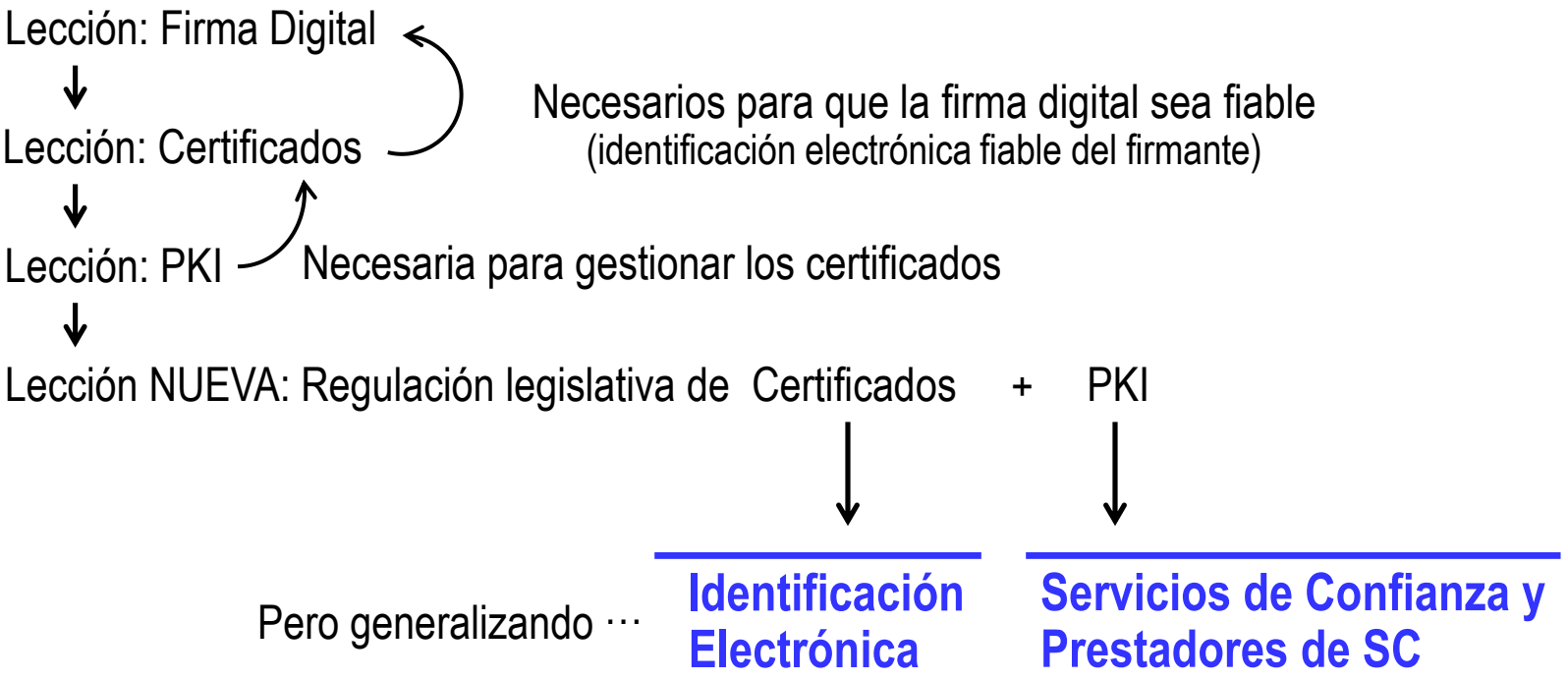
Regulación de la ID-e (certificados) y los servicios de confianza (ACs/PKIs)

Presentación

Daniel F. García

Contexto

Racionalidad de esta lección:



Se analiza la legislación sobre estos temas y …
Los estándares tecnológicos desarrollados para cumplir esa legislación

Leyes iniciales

Directiva 1999/93/CE del Parlamento Europeo y del Consejo de 13 de diciembre de 1999

por la que se establece un marco comunitario para la firma electrónica

DOCE vol.43, L13, Miércoles 19 enero 2000

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:31999L0093&from=EN

Las DIRECTIVAS **no** se aplican directamente a las naciones de la UE
Necesitan la TRANSPOSICIÓN a una ley nacional → En el caso Español:

LEY 59/2003, de 19 de diciembre, de firma electrónica (**LFE**)

BOE núm. 304 del Sábado 20 diciembre 2003

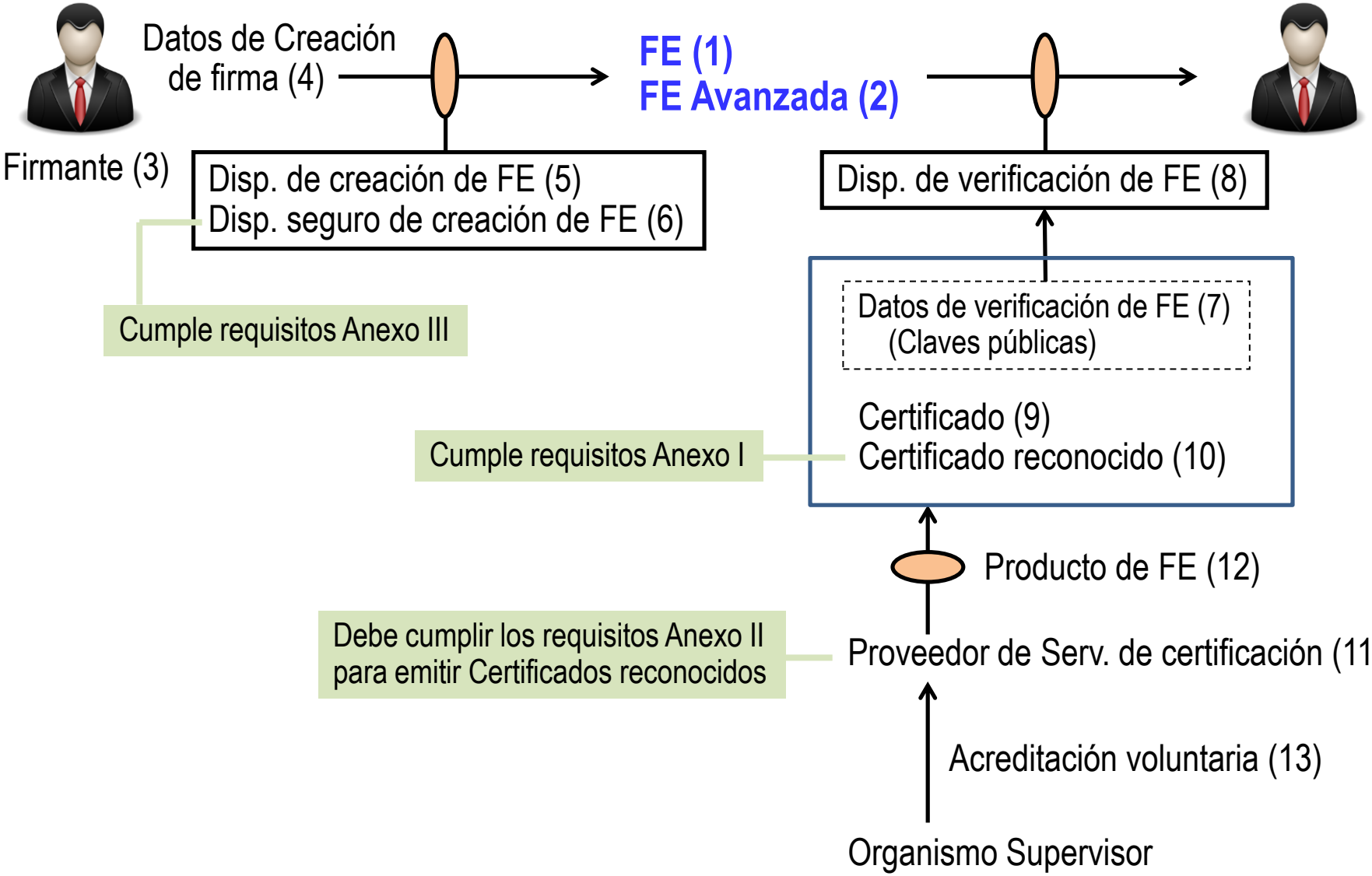
https://www.boe.es/boe/dias/2003/12/20/pdfs/A45329-45343.pdf

La Directiva 1999/93/CE …

… fue derogada por Reglamento UE 910/2014 que entró en vigor el 1-Julio-2016

Pero las tecnologías derivadas de la aplicación de la directiva siguen usándose

Directiva 1999/93 - Definiciones



Directiva 1999/93 – Consecuencias 1

Estableció 2 tipos de firmas → { Firma electrónica / Firma electrónica avanzada }

Firma electrónica

Los datos en formato electrónico
anejos a otros datos electrónicos o asociados de maneja lógica con ellos,
utilizados como medio de autenticación ← en Directiva 1999/93/CE
que utiliza el firmante para firmar ← en Reglamento UE 910/2014

Firma electrónica avanzada

La FE que cumple estos requisitos:

- **a** Estar vinculada al firmante de manera única
- **b** Permitir la identificación del firmante
- **c** Haber sido creada utilizando medios que el firmante puede mantener bajo su exclusivo control
- **d** Estar vinculada a los datos a que se refiere de modo que cualquier cambio ulterior de los mismos sea detectable

Directiva 1999/93 – Consecuencias 2

La directiva propició el establecimiento de estándares para las firmas “básicas”:

CMS – Cryptographic Message Syntax

XML – XML Signature – También denominada: XMLDSig, XML-DSig, XML-Sig

PDF – PDF Signature

Y los correspondientes para las firmas electrónicas avanzadas

CAdES – CMS Advanced Electronic Signature

XAdES – XML Advanced Electronic Signature

PAdES – PDF Advanced Electronic Signature

Denominación conjunta para la familia de estándares para firmas avanzadas

AdES = Advanced Electronic Signatures

https://firmaelectronica.gob.es/Home/Ciudadanos/Formatos-Firma.html

CMS

CMS == Cryptographic Message Syntax

Especificado en la RFC-5652 (Septiembre 2009) Evolución del estándar PKCS#7 (Noviembre 1993)

CMS describe la sintaxis para encapsular un único tipo de contenido, denominado ContentInfo

La sintaxis se describe en ASN.1 y se codifica en BER

Tipos de contenido encapsulados en ContentInfo →
- data (ContentInfo)
- signed-data (SignedCms)
- enveloped-data (EnvelopedCms)
- digested-data
- encrypted-data
- authenticated-data

Clases de .NET correspondientes

CMS soporta la anidación de tipos:

Un tipo signed-data se puede encapsular en un tipo enveloped-data (cifrando los datos y su firma para proporcionar confidencialidad)

Un tipo enveloped-data se puede encapsular en un tipo signed-data (firmando los datos cifrados para proporcionar integridad y autenticación)

CAdES

CAdES es un conjunto de extensiones para el tipo de contenido de CMS denominado datos firmados (signed-data) que lo hacen apropiado para las firmas electrónicas avanzadas (FEA)

La especificación CAdES es gestionada por ETSI

ETSI = European Telecommunications Standards Institute

Instituto Europeo de Normas de Telecomunicaciones https://www.etsi.org/

La especificación técnica ETSI TS 101 733

V1.2.2 (2000-12) Primera versión de la especificación

No hace referencia a CAdES y hay una versión en español: UNE-ETSI/TS 101773 v1.2.2

V1.7.4 (2008-07) ESI – CAdES == RFC-5126 (Febrero 2008)

V2.2.1 (2013-04) ESI – CAdES → Ultima versión

La especificación CAdES indica los formatos de las FEA construidas sobre CMS:

Formatos: -BES -EPES -T -C -X (varios) -A -LT

CAdES-BES

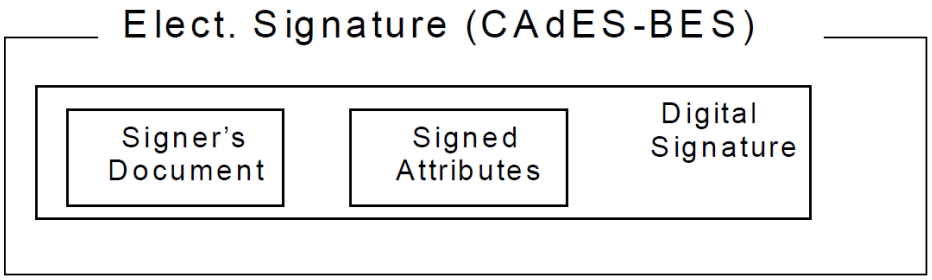
-BES = **B**asic **E**lectronic **S**ignature

La FE CAdES-BES contiene:

- Los datos de usuario firmados (*Signer's Document*)
- Atributos firmados obligatorios (*Signed Attributes*)
- Atributos firmados opcionales (*Signed Attributes*)
- Valor de la firma digital (*Digital Signature*)
- Atributos no firmados

content-type
message-digest
signing-certificate

signing-time
content-hints
signer-attributes
mime-type
etc.



CAdES-EPES

-EPES = **E**xplicit **P**olicy-Based **E**lectronic **S**ignature

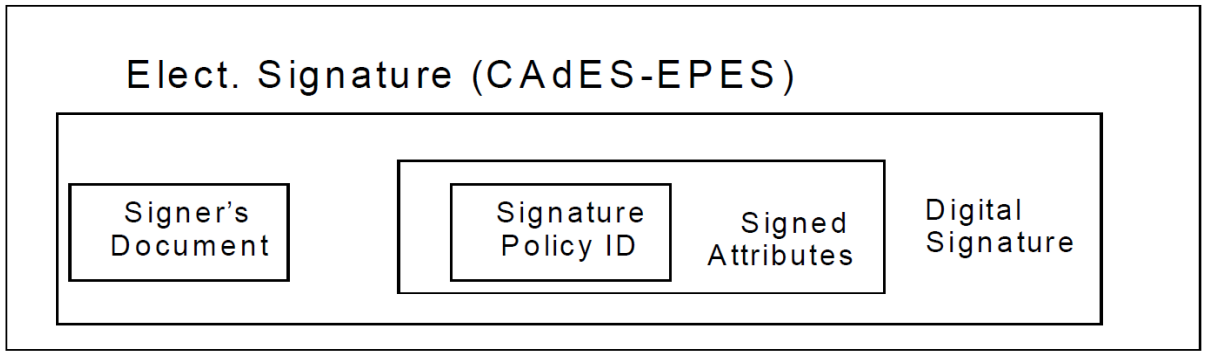
Es una FE CAdES-BES que contiene el atributo firmado SigPolicyID que indica la política de firma que será utilizada para validar la firma electrónica

Política de firma ETSI TS 101 733 V2.2.1 (2013-04) Anexo C1

Conjunto de reglas a aplicar para la creación y validación de una FE

La política debe ser legible por un humano y procesable de forma automática

ETSI TR 102 038 V1.1.1 (2002-04) ESI – XML format for signature policies

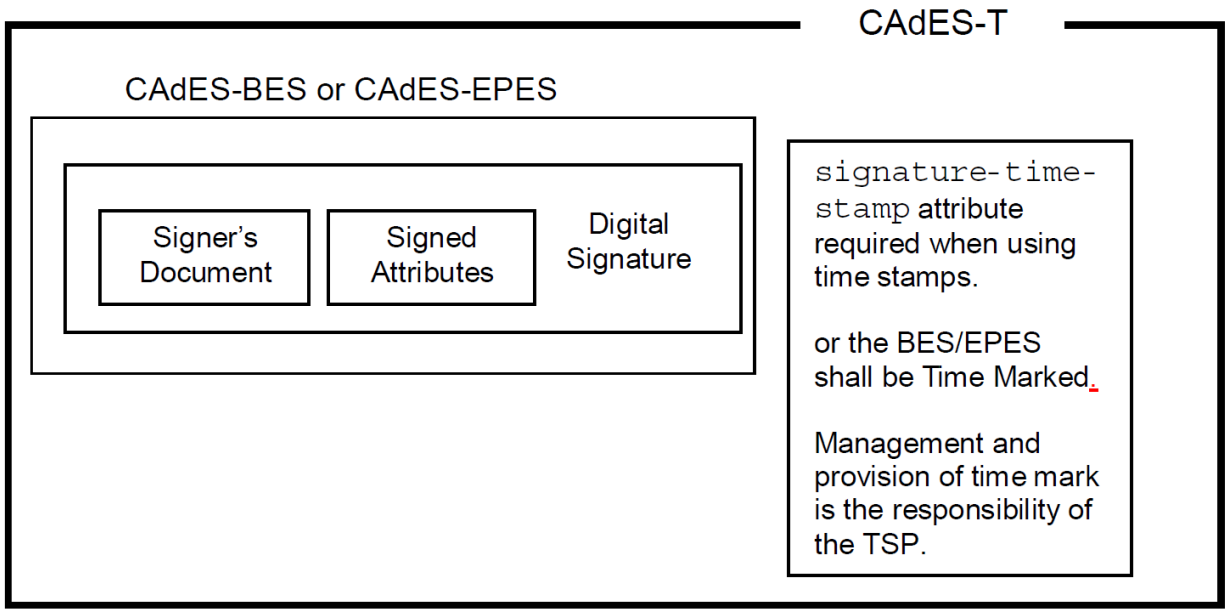


Los formatos siguientes se denominan conjuntamente "***Formats with Validation Data***" porque incluyen datos adicionales para la validación de la firma electrónica

CAdES-T

-T = with **T**ime

Es una FE CAdES-BES o CAdES-EPES a la que se añade un { Sello de tiempo (time-stamp) o Marca de tiempo (time-mark)

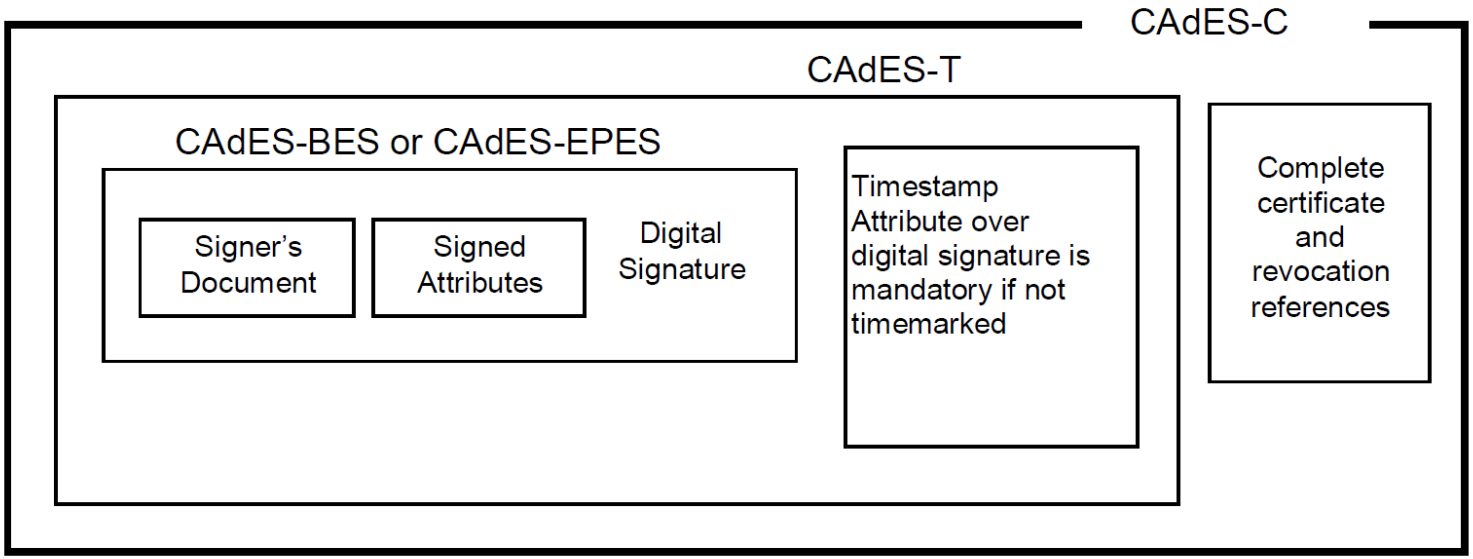


Un sello de tiempo válido, garantiza que la firma se realizó en el instante de sellado, y además NO ha sido alterada desde entonces

CAdES-C

-C = with **C**omplete Validation Data References

Es una FE CAdES-T a la que se añaden los atributos { complete-certificate-references; complete-revocation-references



Complete-certification-references

Contiene referencias a todos los certificados de la cadena de certificación

Complete-revocation-references

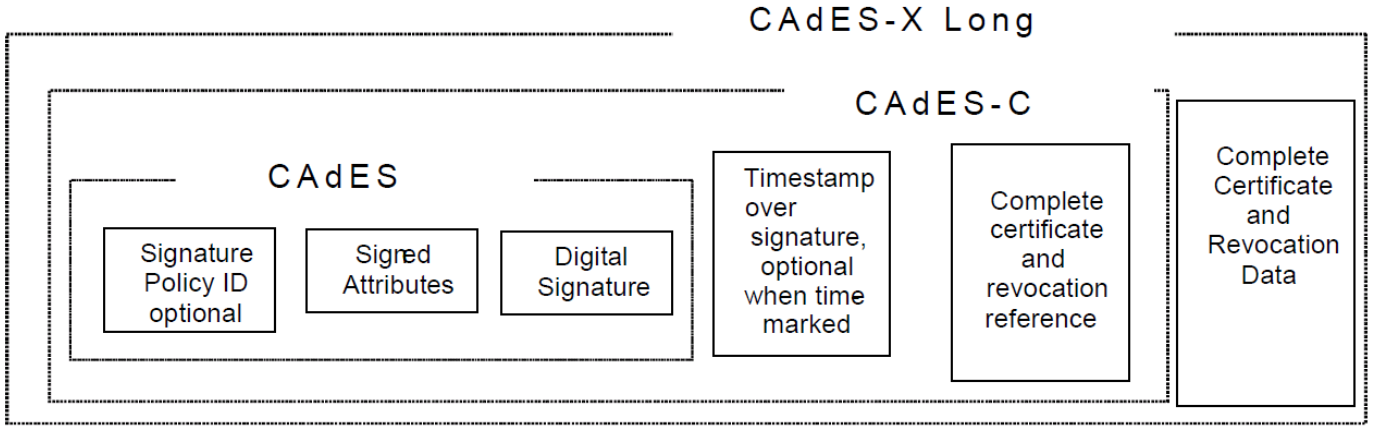
Contiene referencias a las CRLs y/o respuestas de OCSP para todos los certificados

CAdES-X

-X Long = E**X**tended **Long** Format

Es una FE CAdES-C a la que se añaden los atributos { certificate-values, revocation-values }

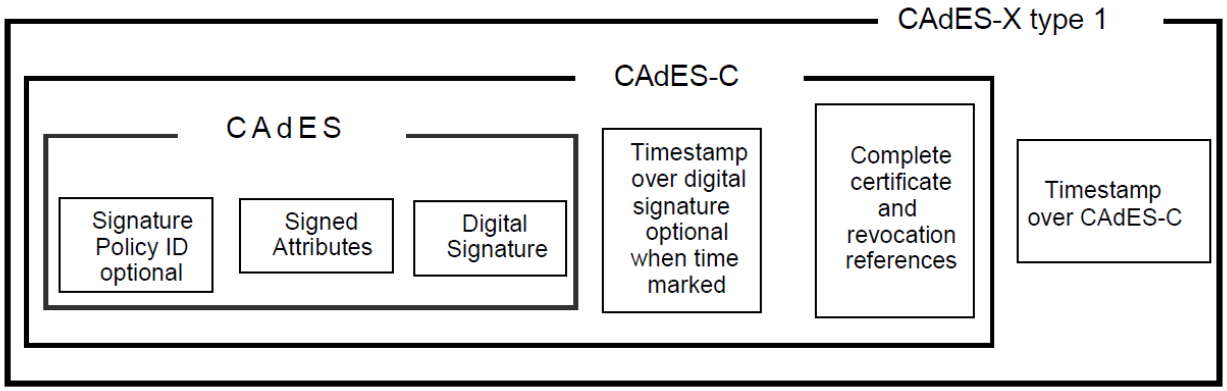
Toda la información necesaria para la verificación queda directamente incluida en la firma electrónica



CAdES-X

-X Type 1 = E**X**tended with time **Type 1**

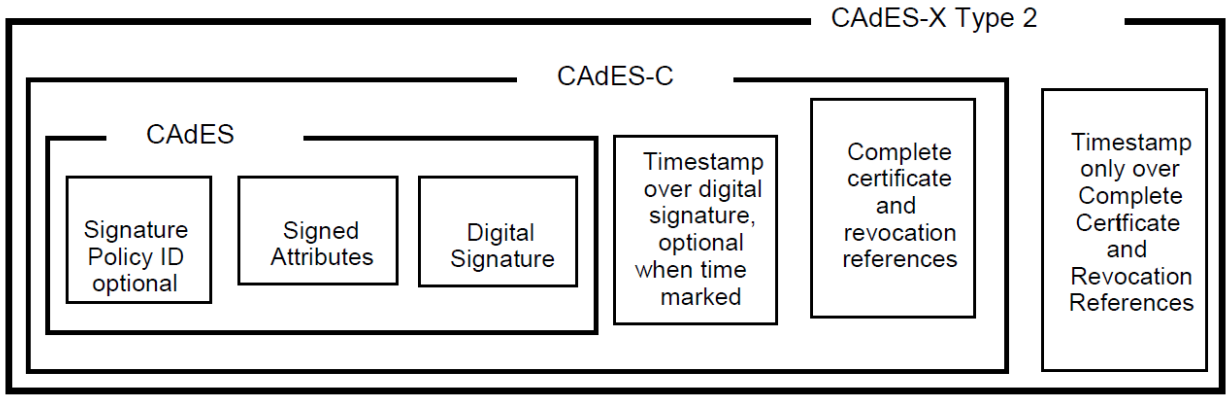
Es una FE CAdES-C a la que se añade un atributo de sello de tiempo sobre toda la firma CAdES-C



-X Type 2 = E**X**tended with time **Type 2**

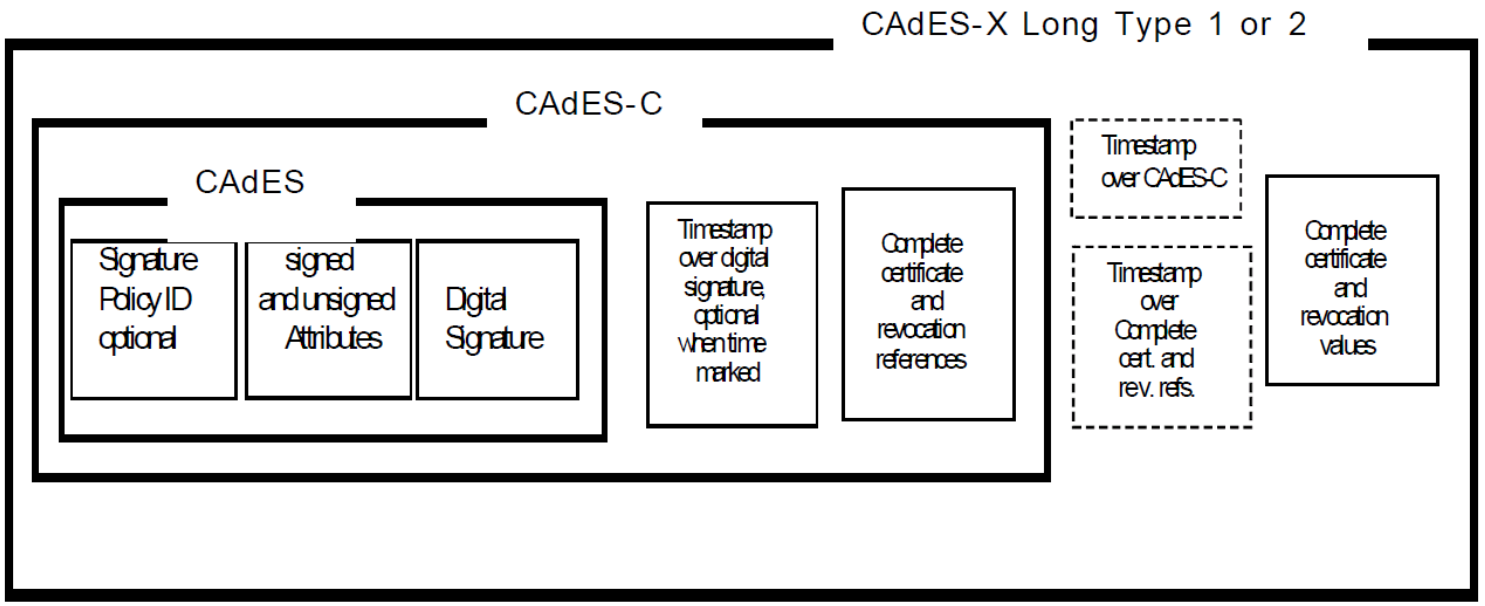
Es una FE CAdES-C a la que se añade un atributo de sello de tiempo

El sello se realiza solo sobre las referencias a certificados e información de revocación



-X Long Type 1 o 2

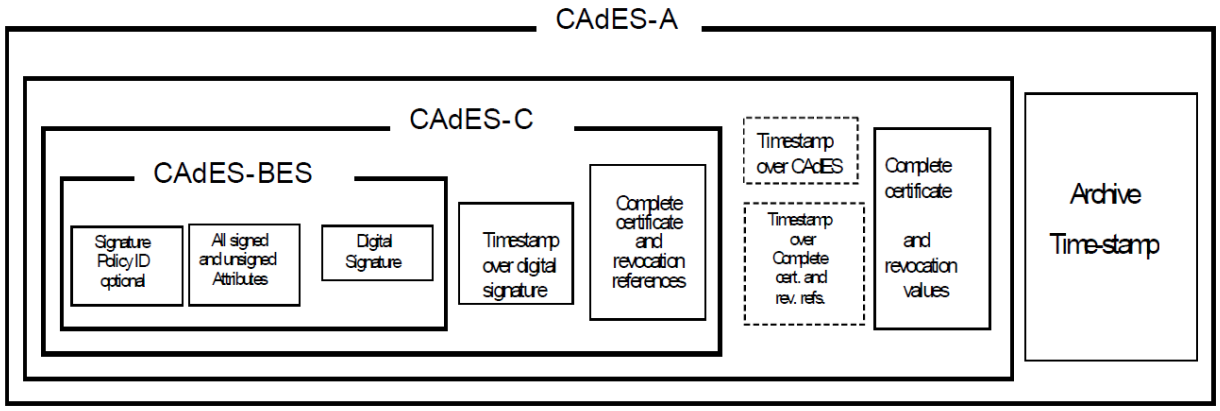
Es una FE CAdES-X Long a la que se añade un atributo de sello de tiempo Type 1 o Type 2



CAdES-A

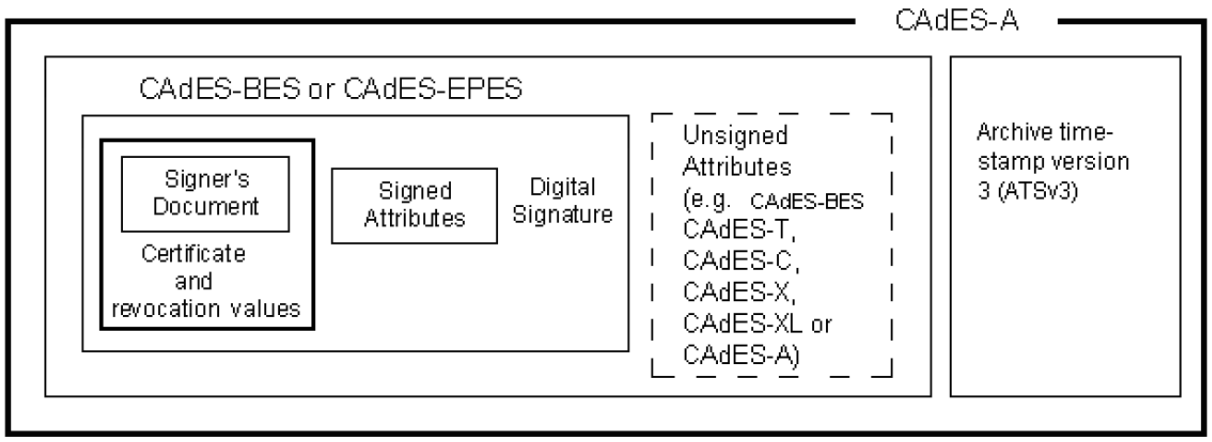
-A = **A**rchival Electronic Signature

Se añade al formato CAdES-X Long o -X Long Type 1 o 2 uno o más archive-time-stamp, ATSv2



ATSv2
obsoleto
Mantenido por compatibilidad

Se añade al formato CAdES-BES –EPES –T –C –X o –A uno o más archive-time-stamp, ATSv3

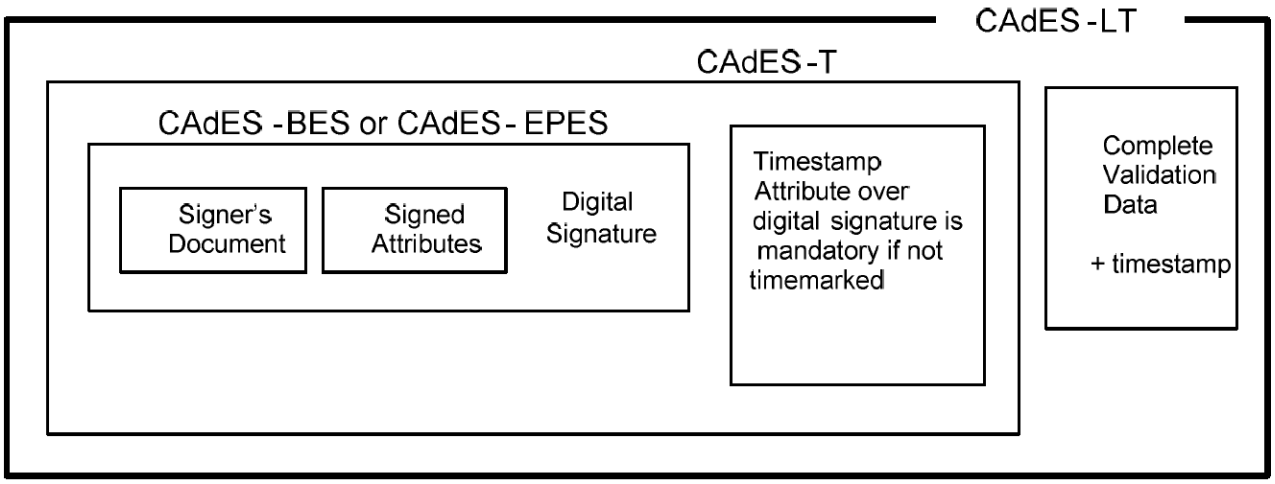


CAdES-LT

-LT = **L**ong-**T**erm Electronic Signature

Se añade a una FE con formato CAdES-T –C –X Long –X Long Type 1 o 2 ó –A
uno o mas atributos long-term-validation

long-term-validation: es una prueba de existencia (PoE, Proof of Existence) que contiene:
Time-stamp (RFC-3161) o Evidence Record (RFC-4998)
+ Certificados de CAs y TSAs y sus estados de revocación



El atributo long-term-validation proporciona la misma funcionalidad que los formatos –X y –A
Pero su implementación es más simple y permite un uso más flexible

Perfiles CAdES

Especificación Técnica ETSI TS 101 733 V2.2.1 (2013-04)

Especifica **múltiples** formatos para FEA basados en CMS

Maximizar la interoperabilidad → Usar conjuntos de opciones comunes

Perfil CAdES == Una determinada selección de opciones (atributos y sus posibles valores)

Especificación Técnica ETSI TS 103 173 V2.2.1 (2013-04)

Especifica perfiles de referencia (*baseline profiles*) para CAdES

Define 4 perfiles o niveles de conformidad incrementales →

- CAdES-**B**
- CAdES-**T**
- CAdES-**LT**
- CAdES-**LTA**

- Cada nivel usa los requisitos del nivel anterior y añade los suyos
- Cada nivel requiere la presencia de ciertos atributos CAdES adecuadamente perfilados para reducir la opcionalidad

---

El perfil CAdES-B considera los requisitos de las FE definidos en:

Decisión de la Comisión 2011/130/UE de 25 de Febrero de 2011
Requisitos mínimos para el tratamiento transfronterizo de los documentos firmados electrónicamente por las autoridades competentes

Perfiles o Niveles CAdES

Nivel CAdES-B (Basic)

Una FE CAdES que cumple el nivel –B
Es una FE CAdES–BES o –EPES que incluye unos determinados atributos

Nivel CAdES-T (with Time)

Una FE CAdES que cumple el nivel –T
Es una FE CAdES que cumple el nivel –B a la que se añade
un time-mark o time-stamp que prueba que existía en ese instante

---

IMPORTANTE: Una FE CAdES–T solo cumple el nivel –T si tiene el perfil apropiado

Ejemplo: Una firma CAdES-BES que NO cumple el nivel –B, al añadirle el time-mark
Se convierte en una firma CAdES–T
Pero no cumple el nivel –T o perfil –T

Cuidado: Se usa la misma denominación, CAdES–T para:
Una firma –BES o –EPES a la que añade un time-stamp
Una firma –B a la que se añade un time-stamp

Perfiles o Niveles CAdES (2)

Nivel CAdES-LT (Long-Term)

Una FE CAdES que cumple el nivel –LT
Es una FE CAdES que cumple el nivel –T a la que se añade
SOLO UN atributo long-term-validation que contiene:

Un sello de tiempo y
Los certificados y sus estados de revocación
(usados para validar la firma y los sellos de tiempo)

IMPORTANTE: Una FE CAdES que cumple el nivel –LT es en definitiva una firma CAdES–LT que cumple un determinado perfil

Pero … Una firma CAdES–LT se puede construir basándola en:

–T –C –X Long –X Long Type 1 o 2 –A

Estas NO SIRVEN para cumplir el nivel –LT

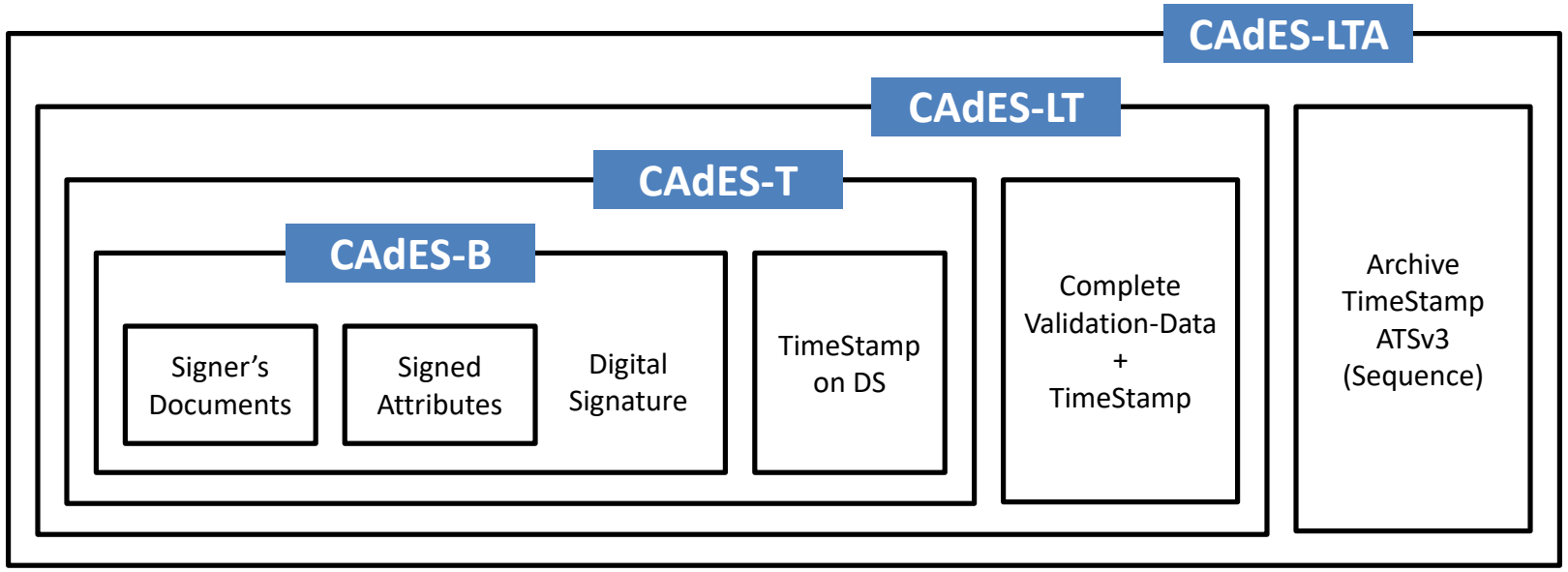
Además, pueden tener VARIOS atributos long-term-validation

Perfiles o Niveles CAdES (3)

Nivel CAdES-LTA (Long-Term-Archival)

Una FE CAdES que cumple el nivel –LTA
Es una FE CAdES que cumple el nivel–LT a la que se añaden
UNO o MAS atributos archive-time-stamp-v3

Resumen de Anidación de los Niveles

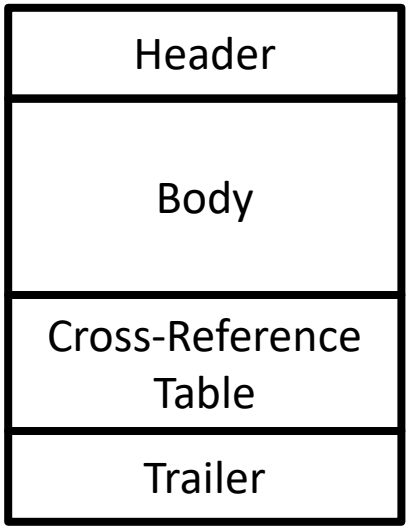


PDF (Portable Document Format)

Formato de fichero usado para contener:
un **documento** (texto, fuentes, gráficos, audio, video, etc.)
una descripción de su **estructura** (layout) y
la información necesaria para su **visualización**

Versión PDF	Año	Versión Acrobat	
1.0	1993	1.0	
1.6	2005	7.0	
1.7	2006	8.0	← ISO 32000-1 Publicado en Julio-2008
2.0	2017	2.0	← ISO 32000-2 Publicado en Julio-2017

Estructura de un fichero PDF



Texto indicando la versión Ej.: %PDF-1.7

Secuencia de “objetos indirectos” etiquetados que constituyen el contenido del documento

Información que permite el acceso aleatorio a objetos indirectos
No hay que leer todo el fichero para acceder a un objeto

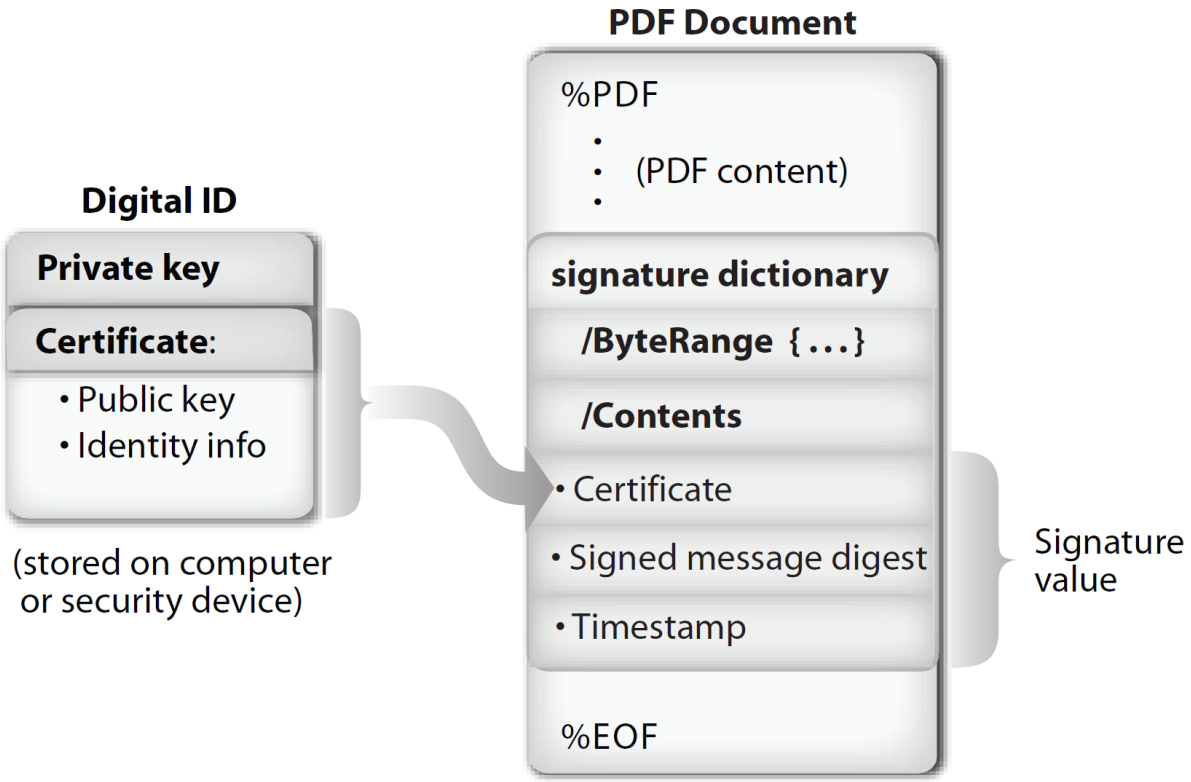
Permite el acceso rápido a la Cross-Reference Table

Firmas digitales en PDF (1)

Las firmas se **incrustan** en el propio fichero PDF

Cada firma incrustada en un PDF se asocia con un manejador (*signature handler*)

El certificado del firmante se incrusta en el PDF + Info adicional (imagen de la firma, sello de tiempo)



Firmas digitales en PDF (2)

Generación de la firma

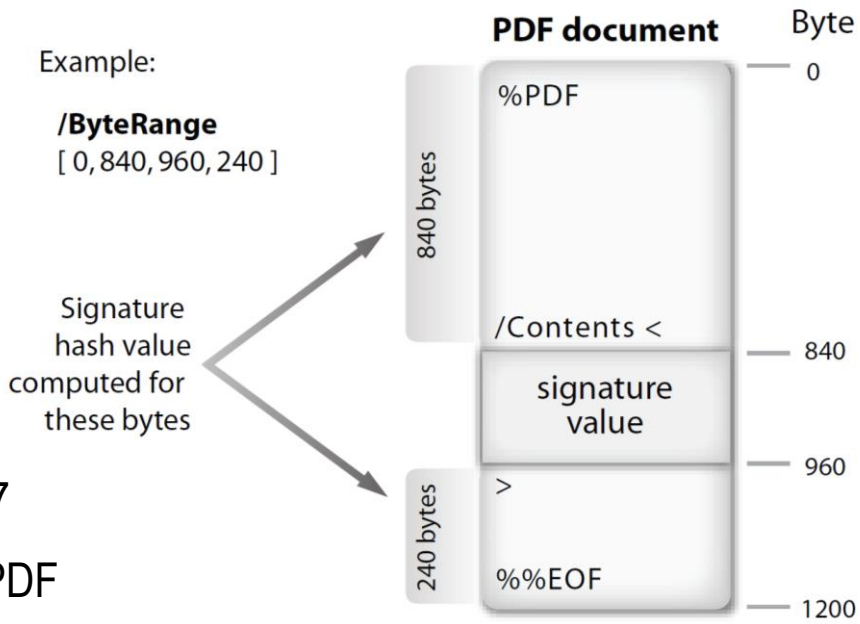
Reservar espacio suficiente para incrustar la firma en medio del fichero PDF

Definir en /ByteRange las dos partes del fichero
Excluir la zona reservada para la firma

Calcular el hash de todo el fichero PDF
Excluyendo la zona de firma

Cifrar el hash con la clave privada del firmante
Crear un objeto firma que se codifica en PKCS#7

Escribir el objeto codificado en el /Contents del PDF



Validación de la firma

El validador recupera el certificado del firmante del PDF y busca el certificado del emisor del cert.

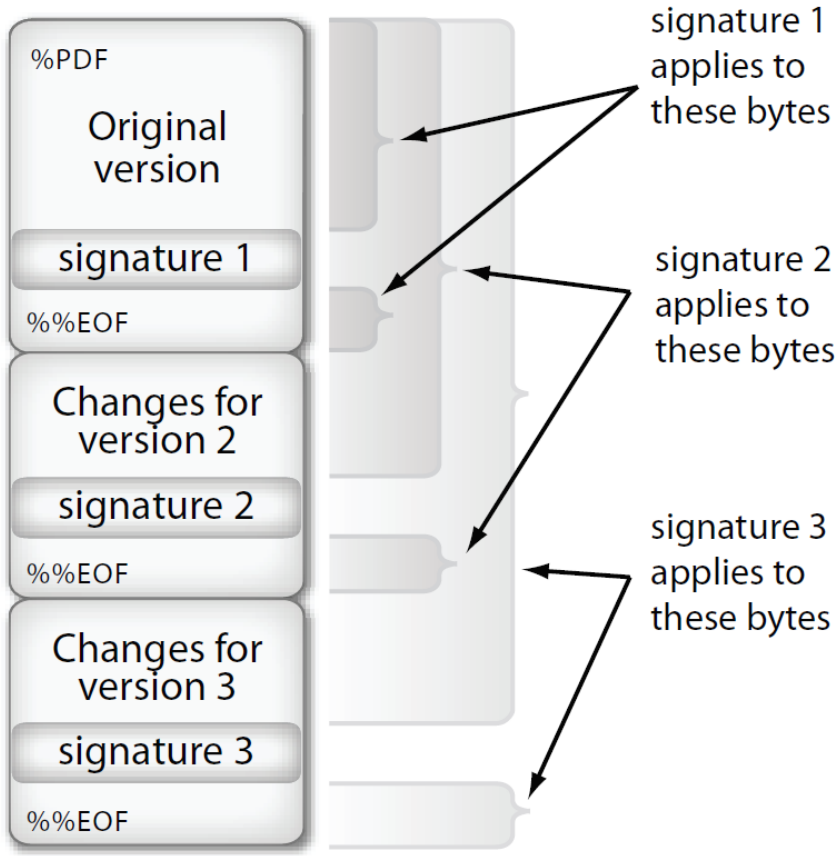
1) Calcula el hash del PDF excluyendo la firma

2) Descifra el hash de la firma usando la clave pública del certificado del firmante

3) Compara el hash calculado con el hash descifrado → SI coinciden la firma es válida

Firmas digitales en PDF (3)

El estándar PDF soporta la firma múltiple de un documento usando su tecnología de **Actualización Incremental** (*Incremental Updates*)



La AI consiste en:
Mantener la versión previa del fichero inalterada
Y guardar todos los cambios de la nueva versión al final de la versión previa

Permite añadir una nueva firma a un PDF
SIN modificar datos cubiertos por la firma previa

PAdES: PDF Advanced Electronic Signature 1

PAdES es un conjunto de restricciones y extensiones al estándar ISO 32000-1 que lo hacen adecuado para la Firma Electrónica Avanzada (FA)

PAdES cumple los requisitos de la Directiva 1999/93/EC de FEA de la UE
Que han sido integrados y ampliados en el Reglamento UE 910/2014

El estándar PAdES es gestionado por la ETSI y tiene 6 partes:

ETSI TS 102 778 →

Part-1	v1.1.1	(2009-07)	PAdES Overview
Part-2	v1.2.1	(2009-07)	PAdES Basic
Part-3	v1.2.1	(2010-07)	PAdES Enhanced
Part-4	v1.1.2	(2009-12)	PAdES Long Term
Part-5	v1.1.2	(2009-12)	PAdES for XML Content
Part-6	v1.1.1	(2010-07)	Visual representation of ES

Perfil PAdES Basic

Indica como incluir en un PDF un firma codificada en CMS / PKCS#7 v1.5 (RFC 1215)

Proporciona soporte para firmas en serie

Opcionalmente permite incluir timestamps, certificados, infoRevocación, …

PAdES: PDF Advanced Electronic Signature 2

Perfil PAdES Enhanced

Los perfiles PAdES-BES o -EPES indican como incluir en un PDF un firma CAdES-BES o -EPES

Perfil PAdES Long-Term

El perfil PAdES-LTV permite añadir a los formatos –CMS –BES y –EPES múltiples veces:

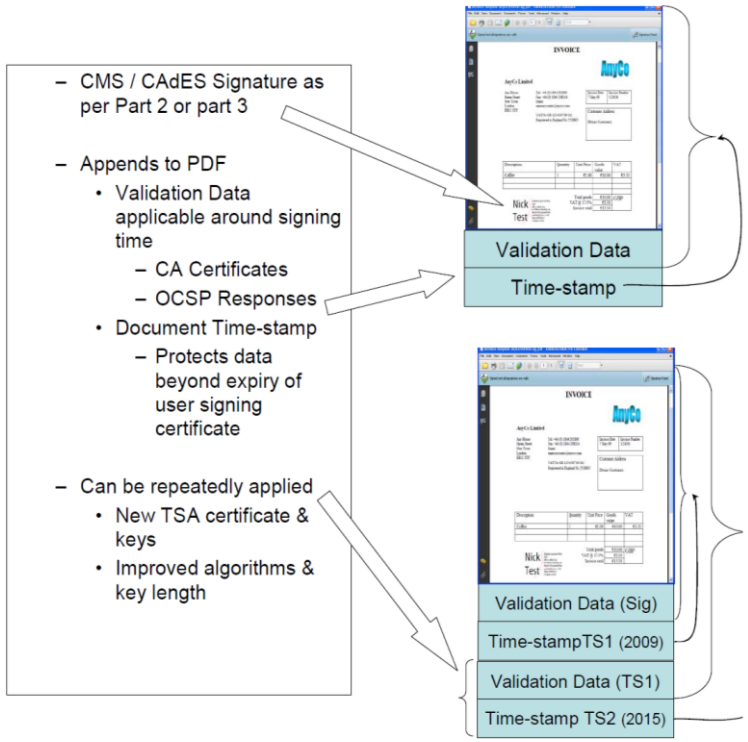
- Datos de validación
- Sello de tiempo

Perfil PAdES for XML Content

Especifica los requisitos de los formatos XAdES básicos usados para firmar documentos XML que son integrados en contenedores PDF

Además incluye requisitos para la integración de XFA forms firmados en contenedores PDF

XFA : Extensión de XML para soportar formularios Web



Leyes actuales 1

Reglamento UE 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 y por la que se **deroga la Directiva 1999/93/CE**

DOCE vol.57, L 257, Jueves 28 agosto 2014

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32014R0910&from=ES

Los REGLAMENTOS se aplican directamente a los estados de la UE

El desarrollo europeo del Reglamento 910/2014 se hace mediante { Decisiones de Ejecución / Reglamentos de Ejecución

Ejemplo de leyes que desarrollan el Reglamento 910/2014 (hay varias)

Reglamento de Ejecución (UE) 2015/1502 de la Comisión de 8 de septiembre de 2015

sobre la fijación de especificaciones y procedimientos técnicos mínimos para los niveles de seguridad de medios de identificación electrónica con arreglo a lo dispuesto en el artículo 8, apartado 3, del Reglamento (UE) 910/2014

DOCE vol.58, L 235, Miércoles 9 septiembre 2015

https://eur-lex.europa.eu/legal-content/ES/TXT/PDF/?uri=CELEX:32015R1502&from=ES

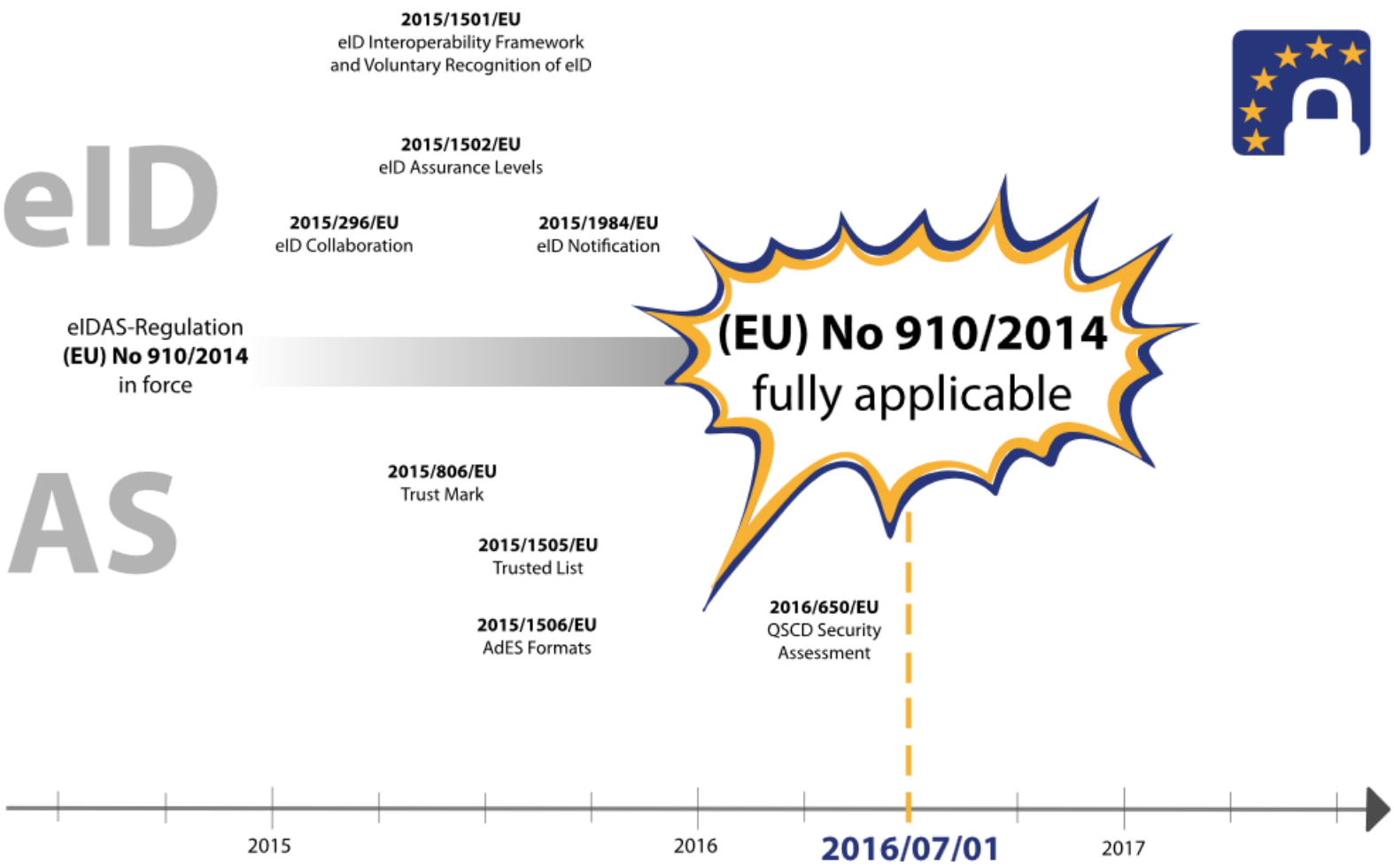
Ley 6/2020, de 11 de noviembre, de regulación de los servicios electrónicos de confianza

BOE núm. 258 del jueves 12 noviembre 2020

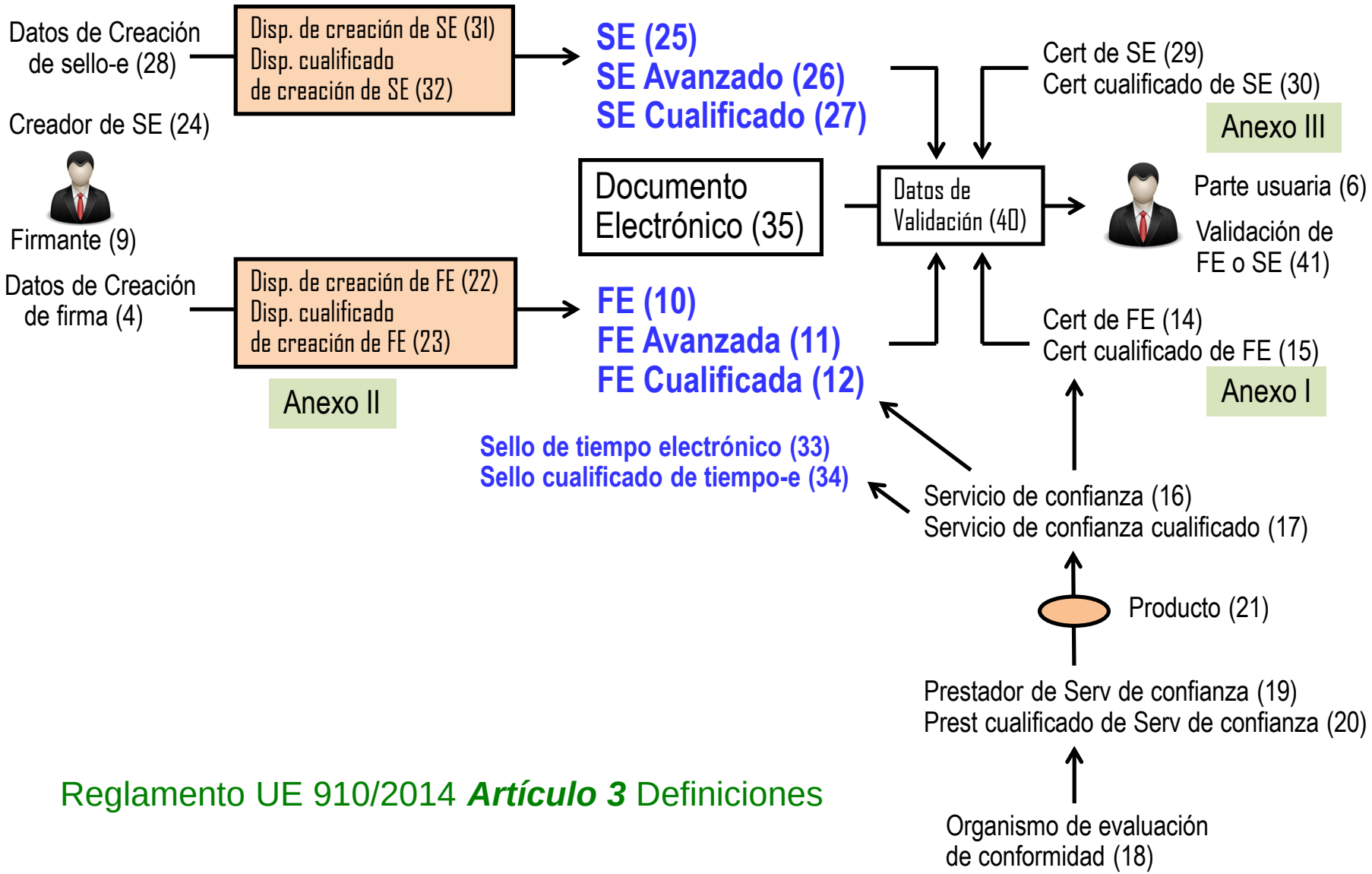
https://www.boe.es/boe/dias/2020/11/12/pdfs/BOE-A-2020-14046.pdf

Leyes actuales 2

eIDAS == **e**lectronic **ID**entification **A**nd **S**ignature



Reglamento 910/2014 - Definiciones



Reglamento UE 910/2014 ***Artículo 3*** Definiciones

Reglamento 910/2014 – Firmas y Sellos

Un sello electrónico (SE) es equivalente a una firma electrónica (FE)

La diferencia es que …

FE → La crea una persona física, denominada “firmante” (Definición 9)

SE → Lo crea una persona jurídica, denominada “creador de un sello” (Definición 24)

Sellos electrónicos importantes: los creados para y utilizados por las administraciones públicas

https://sede.minetur.gob.es/es-ES/firmaelectronica/Paginas/sellos-electronicos.aspx

Reglamento 910/2014 – 3 tipos de firma electrónica

Art 3 Def 10) 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

Art 3 Def 11) Firma electrónica avanzada

La firma electrónica que cumple los requisitos del artículo 26:

a) Estar vinculada el firmante de manera única

b) Permitir la identificación del firmante

c) Haber sido creada utilizando datos de creación de la firma electrónica que el firmante puede utilizar con un alto grado de confianza y bajo su control exclusivo

d) Estar vinculada con los datos firmados por la misma de modo tal que cualquier modificación ulterior de los mismos sea detectable

Esta definición de FEA coincide exactamente con la de la Directiva 1999/93/CE Art 2 Def 2

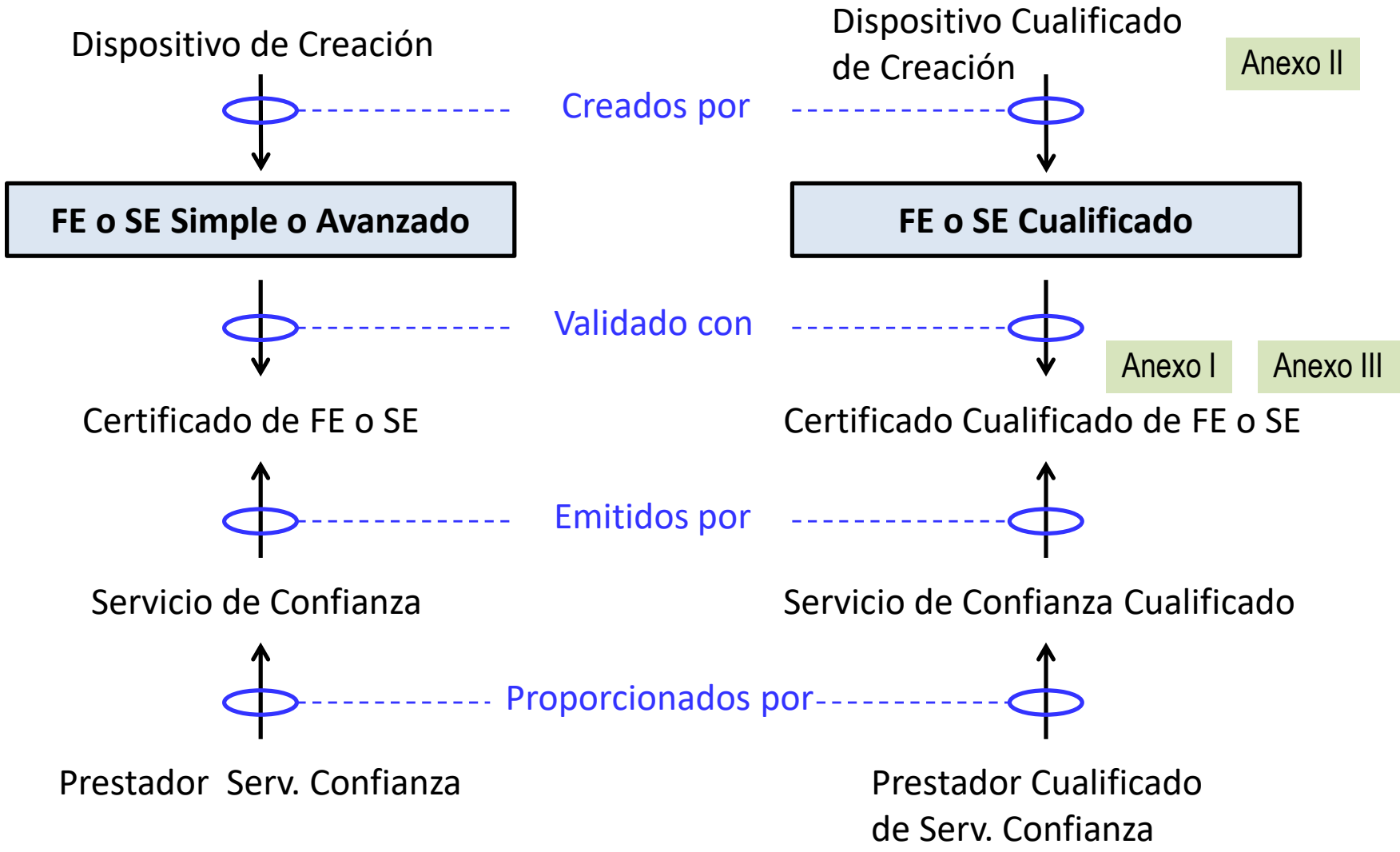
Art 3 Def 12) Firma electrónica cualificada

Una firma electrónica avanzada que:

(1) se crea mediante un dispositivo cualificado de creación de firmas electrónicas y

(2) que se basa en un certificado cualificado de firma electrónica

El tipo Cualificado afecta a varios elementos



Elementos cualificados

Dispositivo cualificado de Creación Reglamento UE 910/2014 Anexo II

Requisitos razonables para los datos de creación de la FE (claves privadas)

- Garantizar su confidencialidad
- No se pueden deducir
- Se pueden proteger por el firmante

Requisito mas extraño

SOLO un Prestador Cualificado de SC podrá crear y gestionar una copia de seguridad de los datos de creación de la FE

Certificados cualificados de FE o SE Reglamento UE 910/2014 Anexos I y III

Requisitos estándares e iguales para FE y SE

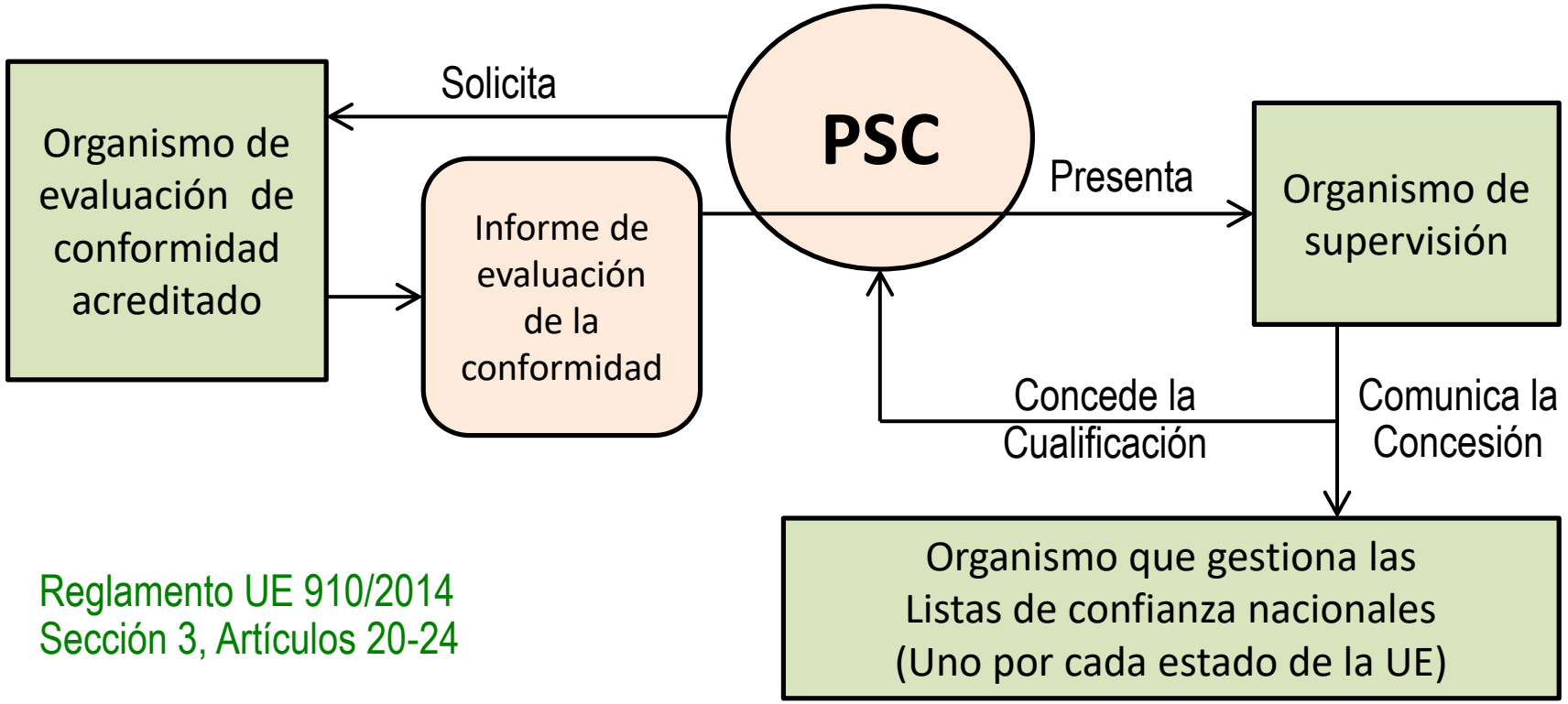
Req. h) El cert contiene la localización en la que está disponible el cert del emisor (PSC)

El servicio debe ser gratuito

Req. i) El cert contiene la localización de los servicios para consultar el estado de validez

Servicios de Confianza Cualificados

Un PSC (Prestador de Servicios de Confianza) para iniciar un servicio de confianza cualificado debe hacer:



Reglamento UE 910/2014
Sección 3, Artículos 20-24

Organismo de supervisión y gestión de listas en España:
Ministerio de Asuntos Económicos y Transformación Digital

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/NormasTecnicas.aspx

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

Servicios de Confianza Cualificados

Un **PSC** puede comenzar la prestación de Servicios de Confianza Cualificados después de que la cualificación haya sido publicada en las listas de confianza (**TSL** == **T**rust-Services **S**tatus **L**ist)

En España la **TSL** la publica el Ministerio en dos formatos:

HR (**Human Readable**) == Legible por personas – Formato PDF

MP (**Machine Processable**) == Procesable por máquinas – Formato XML

La TSL se elabora siguiendo la norma ETSI TS 119 612

https://avancedigital.mineco.gob.es/es-es/Servicios/FirmaElectronica/Paginas/Prestadores.aspx

Un **PCSC** puede usar la etiqueta de confianza UE (Reglamento de Ejecución 2015/806) →

EU Trust Mark for Qualified Trust Services

Un **PCSC** es auditado cada 24 meses

Requisitos a cumplir por un PCSC: Prestador Cualificado de Servicios de Confianza (Art. 24)

Son 5, cada uno con múltiples condiciones

Interesantes:

Req 3 → El PCSC tiene 24h para revocar un cert cualificado tras recibir la solicitud de revocación

Req 4 → El PCSC debe proporcionar información sobre validez/revocación de un cert cualificado a cualquier parte usuaria de forma **GRATUITA**