




GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA

Grupo de trabajo de bases de interoperabilidad del
CTEAJE (BIS)

USO OFICIAL:



	<p>GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA</p>	<p>CTEAJE</p>
---	--	---------------

Ficha del Documento

GRUPO DE TRABAJO	Bases de Interoperabilidad y Seguridad (BIS)
NOMBRE DEL DOCUMENTO	GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA
CÓDIGO DEL DOCUMENTO	CTEAJE-GIS-707-Autenticación, Certificados y Firma electrónica v2.0
VERSIÓN	2.0

Control de Versiones del Documento

VERSIÓN	AUTOR	FECHA	DESCRIPCIÓN
V 1.0		01/06/2015	<ul style="list-style-type: none"> Versión inicial
V 1.1		30/07/2015	<ul style="list-style-type: none"> Se recogen revisiones propuestas en CTEAJE
V 1.2		10/09/2015	<ul style="list-style-type: none"> Se recogen matices de reunión de 3 de septiembre de 2015 del GT BIS
V 1.3		30/10/2015	<ul style="list-style-type: none"> Se recoge el concepto de loa (level of assurance)
V 1.4		26/11/2015	<ul style="list-style-type: none"> Se recogen sugerencias propuestas por el MINHAP y aspectos de la decisión de ejecución (ue) 2015/1506 de la comisión, de 8 de septiembre de 2015. Versión presentada y aprobada en el Pleno del CTEAJE el 02-12-2015.
V 2.0		12/12/2025	<ul style="list-style-type: none"> Se adapta el documento a la actual plantilla de documentos del CTEAJE. Se hace una revisión completa del documento para adaptarla a la referencia normativa del RDL 6/2023 y actualizar el texto a otras referencias normativas. Se modifica el ámbito de aplicación de conformidad con el artículo 27 del RDL 6/2023. Se eliminan los enlaces incluidos en los pies de página para evitar el riesgo de cambios. Se corrigen erratas y fallos ortográficos.

USO OFICIAL:

TLP: CLEAR



			<ul style="list-style-type: none"> • Se modifica el apartado 4 de plazos de adaptación. • Se eliminan las referencias a normativa de desarrollo para facilitar el mantenimiento del apartado 6. • Se añaden el apartado 10.3, 10.4 y 10.5 para incluir requisitos del artículo 27 y 25 del RDL 6/2023 respectivamente. • Se actualiza el apartado 12.1 y 12.2 de acuerdo con el EIDAS 2. • Se actualizan los apartados 13.5 y 13.6 para hacer referencia a la normativa de seguridad de aplicación. • Aprobado en Pleno de 17/12/2025
--	--	--	---

Índice

1. INTRODUCCIÓN.....	6
2. OBJETO.....	7
3. ÁMBITO DE APLICACIÓN	7
4. PLAZOS DE ADAPTACIÓN	8
5. GESTIÓN DE LA POLÍTICA DE FIRMA.....	8
6. REFERENCIAS NORMATIVAS	9
7. REFERENCIAS TÉCNICAS.....	9
8. IDENTIFICACIÓN DE LA POLÍTICA	12
9. PUBLICACIÓN DE LA GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA	14
10. SECCIÓN DE GENERACIÓN DE FIRMAS Y DE USO DE CERTIFICADOS... 15	
10.1 PAUTAS DE USO DE CERTIFICADOS EN ENTORNOS QUE NO SON DE FIRMA ELECTRÓNICA	15
10.2 FIRMA ELECTRÓNICA COMO MANIFESTACIÓN DE VOLUNTAD.....	15
10.3 SISTEMAS DE FIRMA UTILIZADOS POR JUECES, JUEZAS, MAGISTRADO Y MAGISTRADAS 16	
10.4 SISTEMAS DE FIRMA UTILIZADOS POR EL PERSONAL DE LA OFICINA JUDICIAL, DE LA OFICINA FISCAL Y DEMÁS PERSONAL AL SERVICIO DE LA ADMINISTRACIÓN DE JUSTICIA	16
10.5 SISTEMAS DE FIRMA BASADOS EN CÓDIGO SEGURO DE VERIFICACIÓN PARA LA ACTUACIÓN JUDICIAL AUTOMATIZADA.....	16
10.6 CERTIFICADOS CON IDENTIFICACIÓN POR SEUDÓNIMO	16
10.7 PAUTAS DE USO DE CERTIFICADOS EN ENTORNOS DE FIRMA ELECTRÓNICA EN PDF	16
10.8 PAUTAS DE REALIZACIÓN DE FIRMAS ELECTRÓNICAS CON VERIFICACIÓN PREVIA DE LA VALIDEZ DEL CERTIFICADO (EPES-PRE).....	18
10.9 PAUTAS DE USO DE CERTIFICADOS EN ENTORNOS DE FIRMA ELECTRÓNICA EN PKCS#7	18
10.10 PAUTAS DE REALIZACIÓN DE FIRMAS ELECTRÓNICAS DE PROCEDENCIA AJENA A LA ADMINISTRACIÓN DE JUSTICIA.....	19
10.11 PAUTAS DE GESTIÓN DE FIRMAS ELECTRÓNICAS EN SERVIDOR VINCULADAS A PERSONAS FÍSICAS IDENTIFICADAS	19
10.12 PAUTAS DE REALIZACIÓN DE FIRMAS ELECTRÓNICAS EN PDF BASADAS EN FIRMAS MANUSCRITAS, SIN USO DE CERTIFICADO	20
11. SECCIÓN DE ACEPTACIÓN DE FIRMAS ELECTRÓNICAS Y DE CERTIFICADOS	21
11.1 PRESTADORES DE SERVICIOS DE CERTIFICACIÓN ADMITIDOS	21
11.2 POLÍTICAS DE FIRMA ADMITIDAS	22

USO OFICIAL:

TLP: CLEAR



11.3	PLATAFORMAS DE VALIDACIÓN DE CERTIFICADOS ELECTRÓNICOS Y DE FIRMA ELECTRÓNICA.	22
11.4	CODIFICACIÓN COMPACTA DE FIRMAS ELECTRÓNICAS RECIBIDAS, TRAS VERIFICAR LA VALIDEZ DE SU CERTIFICADO (EPES-POST).....	23
11.5	CONSERVACIÓN A LARGO PLAZO DE FIRMAS ELECTRÓNICAS INCLUIDAS EN MECANISMOS DE CUSTODIA DE ÓRGANOS DE LA ADMINISTRACIÓN ELECTRÓNICA DE JUSTICIA	23
11.6	FIRMA ELECTRÓNICA DE DOCUMENTOS ELECTRÓNICOS PROCEDENTES DE LA DIGITALIZACIÓN DE DOCUMENTOS EN PAPEL.....	24
12.	ANEXO I. CONSIDERACIONES ADICIONALES	26
12.1	IDENTIFICACIÓN	26
12.2	AUTENTICACIÓN.....	26
12.3	ACREDITACIÓN.....	26
12.4	NIVELES DE CONFIANZA.....	27
12.5	REQUISITOS RELATIVOS AL CONJUNTO MÍNIMO DE DATOS DE IDENTIFICACIÓN DE PERSONAS FÍSICAS Y JURÍDICAS	29
13.	ANEXO II. ASPECTOS TÉCNICOS Y BUENAS PRÁCTICAS.....	30
13.1	CERTIFICADOS EN ENTORNOS WEB.....	30
13.2	DIAGRAMA SOBRE LOS NIVELES DE FIRMA ELECTRÓNICA.....	30
13.3	DIAGRAMA SOBRE LOS TIPOS DE FIRMA	31
13.4	BUENAS PRÁCTICAS EN LA REALIZACIÓN DE FIRMAS SOBRE PDF	31
13.5	ASPECTOS RELATIVOS A LA FIRMA ELECTRÓNICA EN EL PLANO DE LAS MEDIDAS DE SEGURIDAD.....	33
13.6	ASPECTOS RELATIVOS AL EMPLEO DE SELLOS DE TIEMPO EN EL PLANO DE LAS MEDIDAS DE SEGURIDAD.	33

1. INTRODUCCIÓN

En cumplimiento de establecido en el artículo 15 del Real Decreto 396/2013, de 7 de junio, por el que se regula el Comité Técnico Estatal de la Administración Judicial Electrónica (CTEAJE), corresponde a dicho órgano elaborar, desarrollar, mantener y elevar para su aprobación y difusión las Guías de Interoperabilidad y Seguridad aplicables a las tecnologías de la información y las comunicaciones en los sistemas y aplicaciones que prestan servicio a la Administración de Justicia. Estos sistemas deben ser compatibles entre sí para garantizar su comunicación e integración, de conformidad con lo dispuesto en el artículo 230.6 de la Ley Orgánica 6/1985, de 1 de julio, del Poder Judicial

Con la entrada en vigor del Real Decreto-ley 6/2023, de 19 de diciembre, que aprueba medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo, se consolida la vía telemática para la mayoría de las actuaciones procesales en los órganos jurisdiccionales, con las salvedades previstas en la norma. Esta consolidación exige regular y definir, mediante requisitos técnicos y garantías, los documentos judiciales electrónicos conforme al Esquema Judicial de Interoperabilidad y Seguridad (EJIS).

Estas guías se elaboran conforme a lo dispuesto en los Esquemas Nacionales de Interoperabilidad y de Seguridad, así como a las recomendaciones de interoperabilidad de la Unión Europea que resulten aplicables. Para su diseño se tiene en cuenta la situación tecnológica de las distintas Administraciones con competencias en medios materiales y personales de la Administración de Justicia, los servicios electrónicos e infraestructuras ya existentes, y la normativa concurrente en la materia. Todo ello con el objetivo de garantizar el adecuado cumplimiento de lo previsto en el EJIS, compuesto por el Esquema de Interoperabilidad de la Administración de Justicia (EIAJ) y en el Esquema de Seguridad de la Administración de Justicia (ESAJ).

Entre los aspectos normativos relevantes para el desarrollo del EJIS, destaca el uso de certificados electrónicos en la administración electrónica de justicia, las variantes de firma electrónica y los mecanismos de identificación, autenticación, acreditación y firma —tanto personal como automatizada— en contextos que incluyen firma electrónica, sello electrónico y securización de sedes electrónicas.

En este contexto, la política de firma y de uso de certificados en el ámbito de la Administración de Justicia es solo uno de los aspectos tratados en esta Guía.

Para acotar las variantes recomendadas en la generación de firmas y sellos electrónicos y de uso de certificados, y en la aceptación de firmas y sellos electrónicos en documentos electrónicos que se incorporan a un sistema de información empleado en el ámbito de la Administración de Justicia, se publica la presente Política de Firma Electrónica y Certificados del CTEAJE, que será de aplicación en los ámbitos de la Administración Electrónica de Justicia a los que corresponde la aplicabilidad del Real Decreto-ley 6/2023.

En su redacción se ha tenido en cuenta el Reglamento Europeo UE 910/2014, de 23 de julio, de Identificación electrónica y servicios de confianza para las transacciones electrónicas en

el mercado interior, modificado por el Reglamento (UE) 2024/1183 del Parlamento Europeo y del Consejo, de 11 de abril de 2024, y consideraciones de buenas prácticas sectoriales, así como la Política Marco de Firma Electrónica de la AGE Versión 1.9 y la normativa técnica europea en curso de desarrollo.

Aspectos relevantes contemplados en la norma son los relativos a la identificación y autenticación de los intervinientes, a la autenticidad de los documentos con técnicas como la firma electrónica y los códigos seguros de verificación, a la posibilidad de mantener conexiones cifradas con las sedes electrónicas gracias a los certificados de sede electrónica y a la actuación judicial automatizada.

2. OBJETO

1. El objeto de esta norma es servir como guía en lo relativo a la gestión de firmas electrónicas en el ámbito de la justicia, así como tomar en consideración los conceptos conexos de autenticidad de documentos electrónicos y uso de certificados en el marco de la identificación y autenticación de intervinientes cuando no se precise el uso de firma electrónica.
2. Desde un punto de vista normativo, una parte del documento define la Política de Firma de la Administración de Justicia desarrollada con el objetivo de establecer las particularidades requeridas por la Administración de Justicia.
3. La norma contempla el uso de certificados en contextos diferentes de los de la firma electrónica, así como el uso de firmas electrónicas que pueden no hacer uso de certificados.
4. La expresión descriptiva de las técnicas descritas en esta norma se traducirá en documentos técnicos normalizados que permitan su interpretación directa por sistemas automatizados, en lo que sea posible.

3. ÁMBITO DE APLICACIÓN

1. Este documento establece el marco común de autenticidad de documentos electrónicos utilizados en la Administración de Justicia en España, tanto en lo relativo a las firmas electrónicas como a los sistemas de verificación de autenticidad en línea, en el marco establecido por el Real Decreto-ley 6/2023, de 19 de diciembre.
2. Será de aplicación para los órganos competentes en la Administración de Justicia, personal de la Oficina Judicial, personal de la Oficina fiscal, demás personal al servicio de la Administración de Justicia, profesionales y ciudadanos que se relacionan con dichos órganos, para las entidades prestadoras de servicios tecnológicos utilizados en la administración de justicia y para las Administraciones con competencias en materia de justicia.
3. Cuando se establezcan comunicaciones entre órganos de las Administraciones públicas y órganos relacionados con la Administración de Justicia, y se intercambien documentos firmados electrónicamente que cumplan las políticas de firma de las Administraciones

públicas, se considerará que cumplen la política de firma de la Administración de Justicia. Los documentos firmados electrónicamente en el marco de actuaciones judiciales por los profesionales con atribuciones para ello, con arreglo a la presente política, se considerará en cuanto a su aceptación, que cumple la política de firma del órgano destinatario.

4. En relación con los documentos firmados electrónicamente, esta política se divide en dos secciones, la política de generación de firmas electrónicas en el ámbito de los órganos y profesionales de la Justicia y la de comprobación de firmas electrónicas por parte de los órganos, cuando las firmas las generan los ciudadanos, los profesionales o se generan por otros órganos del sector público o del sector privado, ajenos al ámbito de la Justicia, o por sus representantes:
 - a. En la sección de generación de firmas electrónicas se establecerán las condiciones para la generación de documentos firmados o sellados electrónicamente por el personal al servicio de la Administración de Justicia, y por los sistemas de firma electrónica o de sello electrónico automatizados utilizados en su ámbito.
 - b. En la sección de comprobación de firmas electrónicas se establecerán las condiciones para la comprobación de validez de documentos firmados electrónicamente por ciudadanos o por sus representantes, y profesionales que se relacionan con la misma, o sellados electrónicamente por empresas y organismos que se relacionan con la Administración de Justicia, o procedentes de otros órganos de la Administración de Justicia. Esta sección se define de forma que se acepten todos los certificados cualificados emitidos con arreglo a lo dispuesto en el artículo 22 del Reglamento europeo 910/2014, de 23 de julio, de Identificación electrónica y servicios de confianza para las transacciones electrónicas en el mercado interior.
5. Lo indicado en esta política es de obligado cumplimiento para las administraciones que aportan los medios materiales para la Administración de Justicia, salvo que de forma expresa se indique sobre algún aspecto su opcionalidad o su enmarcación como buena práctica.

4. PLAZOS DE ADAPTACIÓN

1. Los certificados emitidos con anterioridad a la adopción de la presente Política de Firma Electrónica seguirán siendo válidos hasta su vencimiento, en el supuesto de que lo indicado en la política afecte a la definición de los perfiles de certificados.
2. Las modificaciones futuras de la Política de Firma contarán con períodos de adaptación de al menos seis meses desde su publicación que finalizarán el 15 de enero siguiente más próximo al transcurso de dichos seis meses.

5. GESTIÓN DE LA POLÍTICA DE FIRMA

1. El mantenimiento, actualización y publicación electrónica del presente documento corresponderá al Comité técnico estatal de la Administración judicial electrónica.

- Los cambios a la política serán consensuados con las partes implicadas, así como el periodo de tiempo transitorio para la adaptación de las plataformas a la nueva política.
- El CTEAJE mantendrá, en los portales destinados a tal función, tanto la versión actualizada del presente documento como un repositorio con el historial de las versiones anteriores de la política de firma electrónica.
- En el caso de actualización del presente documento, se identificará el lugar donde un validador puede encontrar las versiones anteriores para verificar una firma electrónica anterior a la política vigente.
- El cuadro identificativo relativo a la gestión de la política es el siguiente:

Nombre del emisor de la política	CTEAJE
Dirección de Contacto	Ministerio de Presidencia, Justicia y Relaciones con las Cortes San Bernardo, 19 28015 Madrid
Correo electrónico	cteaje@mjusticia.es
Sede electrónica	https://www.administraciondejusticia.gob.es/cteaje
OID del emisor	OID 2.16.724.6.1.1.1 {joint-iso-itu-t(2) country(16) es(724) ejustice(6) cteaje(1) ejis(1) firmas(1) }
URL	https://www.administraciondejusticia.gob.es/cteaje/guias-de-interoperabilidad
Fecha de emisión	xx-xx-2025
Ámbito de aplicación	Administración de Justicia


6. REFERENCIAS NORMATIVAS

- Este documento se basa en el 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 y por el que se deroga la Directiva 1999/93/CE, y su normativa de desarrollo.
- Se ampara en lo dispuesto en el Real Decreto-ley 6/2023, de 19 de diciembre, por el que se aprueban medidas urgentes para la ejecución del Plan de Recuperación, Transformación y Resiliencia en materia de servicio público de justicia, función pública, régimen local y mecenazgo.
- Desarrolla el marco normativo de aplicación de interoperabilidad y seguridad establecido en el Esquema de Interoperabilidad de la Administración de Justicia (EIAJ) y en el Esquema de Seguridad de la Administración de Justicia (ESAJ).

7. REFERENCIAS TÉCNICAS

1. Para la elaboración de esta Política se han tenido en cuenta las siguientes normas técnicas:
 - a. IETF RFC 3125 - Electronic Signature Policies.
 - b. ETSI TR 102 041 - Signature Policies Report.
 - c. ETSI TR 102 272 - Electronic Signatures and Infrastructures (ESI); ASN.1 format for signature policies.
 - d. ETSI TR 102 038 - TC Security - Electronic Signatures and Infrastructures (ESI); XML format for signature policies.
2. Además, son de aplicación las normas que se refieran a los certificados y las firmas electrónicas desarrolladas en el ámbito de ETSI y CEN, en particular, las descritas en el documento TR 119 000 - Rationalised structure for electronic signature standardisation:

Rationalized Framework (Marco racionalizado)	
TR 119 000	Rationalised structure for electronic signature standardisation
SR 019 020	Rationalised Framework of Standards for Advanced Electronic Signatures in Mobile Environment
TR 419 010	Extended rationalised stucture including IAS
TR 419 030	Rationalised structure for electronic signature standardisation - Best practices for SMEs
TR 419 040	Rationalised structure for electronic signature standardisation - Guidelines for citizens
Signature Creation and validation (Creación y validación de firma)	
TR 119 100	Business driven guidance for Signature Creation and Validation
TS 119 101	Policy and security requirements for Signature Creation and Validation
EN 119 101	Policy and security requirements for Signature Creation and Validation
EN 319 102	Procedures for Signature Creation and Validation
EN 419 103	Conformity assessment for Signature Creation and Validation
TS 119 104	General requirements on testing compliance and interoperability of Signature Creation and Validation
EN 419 111	Protection Profiles for Signature Creation and Validation Application
EN 319 122	CAAdES - CMS Advanced Electronic Signatures <ul style="list-style-type: none"> • Part 1: Core Specification • Part 2: Baseline Profile
TS 119 124	CAAdES testing conformance & interoperability
EN 319 132	XAdES - XML Advanced Electronic Signatures <ul style="list-style-type: none"> • Part 1: Core Specification • Part 2: Baseline Profile
TS 119 134	XAdES testing conformance & interoperability
EN 319 142	PAdES - PDF Advanced Electronic Signature Profiles <ul style="list-style-type: none"> • Part 1: PAdES Overview - a framework document for PAdES • Part 2: PAdES Basic - Profile based on ISO 32000-1 • Part 3: PAdES Enhanced - PAdES-BES and PAdES-EPES Profiles <ul style="list-style-type: none"> ○ Part 4: PAdES Long Term - PAdES-LTV Profile ○ Part 5: PAdES for XML Content - Profiles for XAdES signatures ○ Part 6: Visual Representations of Electronic Signatures ○ Part 7: PAdES Baseline Profile

 <p>Comité Técnico Estatal de la Administración Judicial Electrónica</p>	<p>GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA</p>	<p>CTEAJE</p>
---	--	---------------

TS 119 144	PAdES testing conformance & interoperability
TS 119 152	Architecture for Advanced electronic signatures in mobile environments
TS 119 154	Testing conformance & interoperability of AdES in mobile environments
EN 319 162	ASiC - Associated Signature Containers <ul style="list-style-type: none"> ○ Part 1: Core Specification ○ Part 2: Baseline Profile
TS 119 164	ASiC testing conformance & interoperability
EN 319 172	Signature policies
TR 119 174	Testing compliance and interoperability of signature policies
Signature Creation and Other Related Devices (Dispositivos de creación de firma y similares)	
TR 419 200	Business driven guidance for signature creation and other related devices
EN 419 203	Conformity assessment of secure devices and trustworthy systems
EN 419 211	Protection Profiles for secure signature creation devices (ex EN14169)
EN 419 212	Application interfaces for secure signature creation devices (ex EN14890)
EN 419 221	Security requirements for trustworthy systems managing certificates for electronic signatures (ex TS14167-2 to 4)
EN 419 231	Security requirements for trustworthy systems supporting time-stamping
EN 419 241	Security requirements for trustworthy systems supporting server signing (signature generation services)
EN 419 251	Protection profiles for authentication device (ex EN 16248)
EN 419 261	Security requirements for trustworthy systems managing certificates for electronic signatures (ex TS14167-1)
Cryptographic Suites (Conjuntos criptográficos)	
TR 119 300	Business driven guidance for cryptographic suites
TS 119 312	Cryptographic suites for secure electronic signatures
Trust Service Providers Supporting Electronic Signatures (Prestadores de Servicios de Confianza Digital en relación con la firma electrónica)	
TR 119 400	Business driven guidance for TSPs supporting electronic signatures
EN 319 401	General policy requirements for TSPs supporting electronic signatures
EN 319 403	Requirements for conformity assessment bodies assessing Trust Service Providers
EN 319 411	Policy and security requirements for Trust Service Providers issuing certificates <ul style="list-style-type: none"> • Part 1: Policy requirements for Certification Authorities issuing web site certificates • Part 2: Policy requirements for certification authorities issuing qualified certificates • Part 3: Policy requirements for Certification Authorities issuing public key certificates • Part 4: Policy requirements for certification authorities issuing Attribute Certificates
EN 319 412	Profiles for TSPs issuing certificates
EN 319 413	Conformity assessment for TSPs issuing certificates
EN 319 421	Policy and security requirements for TSPs providing time-stamping services
EN 319 422	Profiles for TSPs providing time-stamping services
EN 319 423	Conformity assessment for TSPs providing time-stamping services
EN 319 431	Policy and security requirements for TSPs providing signature generation services
EN 319 432	Profiles for TSPs providing signature generation services
EN 319 433	Conformity assessment for TSPs providing signature generation services
EN 319 441	Policy and security requirements for TSPs providing signature validation services
EN 319 442	Profiles for TSPs providing signature validation services
EN 319 443	Conformity assessment for TSPs providing signature validation services
Trust Application Service Providers (Prestadores de servicios de aplicaciones de confianza digital)	

USO OFICIAL:

TLP: CLEAR



TR 119 500	Business driven guidance for trust application service providers
TS 119 504	General requirements for testing compliance and interoperability of trust application service providers
EN 319 511	Policy and security requirements for registered electronic mail (REM) service providers
EN 319 512	Registered electronic mail (REM) services
EN 319 513	Conformity assessment for REM service providers
TS 119 514	Testing compliance and interoperability of REM service providers
EN 319 521	Policy and security requirements for data preservation service providers
EN 319 522	Data preservation services through signing
EN 319 523	Conformity assessment of data preservation service providers
SR 019 530	Study on standardisation requirements for e-delivery services applying e-signatures
Trust Service Status Lists Providers (Prestadores que publican listas de servicios de confianza digital)	
TR 119 600	Business driven guidance for trust service status lists providers
EN 319 601	General policy and security requirements for trust service status lists providers
EN 319 602	Trust service status lists format
EN 319 603	General requirements and guidance for conformity assessment of trust service status lists providers
TS 119 604	General requirements for testing compliance and interoperability of trust service status lists providers
EN 319 611	Policy and security requirements for trusted lists providers
EN 319 612	Trusted lists format
EN 319 613	Conformity assessment of trusted list providers
TS 119 614	Testing compliance and interoperability of trusted lists

No todas las normativas relacionadas en la tabla precedente se aplican en la gestión de firmas electrónicas y certificados. No obstante, es conveniente tenerla presentes como marco general del desarrollo de estándares relacionados con la interoperabilidad de los servicios de confianza digital de forma transfronteriza, ya que acompañarán a los desarrollos legislativos derivados de la adopción del Reglamento UE 910/2014.

8. IDENTIFICACIÓN DE LA POLÍTICA

1. Los argumentos identificables en la política de firma y certificación se estructuran mediante un modelo de codificación basado en OID (Object Identifier), descrito en la norma X.690 OSI networking and system aspects – Abstract Syntax Notation One (ASN.1).
2. Para la gestión de OID se tendrá en cuenta lo previsto en la norma ISO/IEC 9834-1:2012 - Information technology -- Procedures for the operation of object identifier registration authorities: General procedures and top arcs of the international object identifier tree, coincidente con la Recomendación X.660 de ITU.
3. Las menciones de los OID descritos en esta política sólo son obligatorias cuando la firma electrónica se realiza en formato AdES-EPES en el ámbito de la administración de Justicia, y son opcionales cuando la firma se admite en el ámbito de la administración de Justicia, procedente de un ciudadano, profesional, órgano, empresa, o institución ajena a ella.

4. El órgano responsable de la administración de OID es el CTEAJE, que determinará la estructura y significado de sus variantes. El CTEAJE recogerá las solicitudes de identificadores semánticos del resto de órganos e instituciones que colaboran en la Administración de Justicia y otorgará a la entidad o al órgano petionario valores OID de la estructura que administra, por orden de petición, o según la necesidad semántica para la que se solicita, colaborando en el mantenimiento y actualización del modelo de información asociado.
5. En lo posible, se coordinará la estructura de OID del ámbito de la justicia, con la establecida en el ámbito de la Administración General del Estado, que se identifica con el siguiente arco:
 - a. {joint-iso-itu-t(2) country(16) es(724) adm(1) mpr(3) e-Administration(1) eSignatures(1)}.
 - b. 2.16.724.1.3.1.1.
6. Cuando se realicen firmas en modalidad AdES-EPES se podrá incluir la referencia del identificador único de la versión del documento de política de firma electrónica sobre el que se ha basado su implementación, el cual determinará las condiciones que cumple la firma electrónica a la que se aplica. Solo hay dos variantes de firma AdES-EPES recomendadas, cuyos OID se indican más adelante. No se recomienda adoptar variantes AdES-EPES diferentes, al objeto de mantener simple el marco de gestión de firmas electrónicas. Si se adopta, la firma AdES-EPES, la indicación de la referencia es obligatoria cuando la firma se realice en el marco de actividad asociada a la administración de Justicia por un órgano competente o por su titular. El campo destinado para incluir la referencia será, para el formato AdES-EPES, la etiqueta SignaturePolicyIdentifier.
7. El cuadro identificador de la política es el siguiente:

Nombre del documento	Política General de Firma Electrónica
Versión	2.0
OID ² (identificador de Política)	OID 2.16.724.6.1.1.1.1.2.0 {joint-iso-itu-t(2) country(16) es(724) ejustice(6) cteaje(1) ejis(1) firmas(1) policy(1) major_version(2) minor_version(0)}
OID EPES-Pre	OID 2.16.724.6.1.1.1.2.1.0
OID EPES-Post	OID 2.16.724.6.1.1.1.3.1.0
URI de referencia de la Política	Sede electrónica del CTEAJE. https://www.administraciondejusticia.gob.es/cteaje/guias-de-interoperabilidad
Fecha de emisión	xx-xx-2025

Ámbito de aplicación	Administración de Justicia
----------------------	----------------------------

8. En este cuadro se utilizan las siguientes menciones abreviadas:

- a. joint-iso-itu-t(2) Common standardization area of ISO/IEC (International Organization for Standardization/International Electrotechnical Commission) and ITU-T (International Telecommunications Union - Telecommunication standardization sector).
- b. country(16) Joint (ITU-T and ISO/IEC) registration within a country.
- c. es(724) Within Spain, the ISO National Body and ITU Member State have agreed that Asociación Española de Normalización y Certificación (AENOR) (in English, Spanish Association for Standardization and Certification) is the Registration Authority for this country OID.
- d. ejustice(6) OID de inicio de arco para las organizaciones relacionadas con la Administración de Justicia.
- e. cteaje(1) Estructura de documentación normativa del Comité técnico estatal de la Administración judicial electrónica.
- f. ejis (1) Esquema Judicial de Interoperabilidad y Seguridad - Estructura de documentación normativa de Esquema Judicial de Interoperabilidad y Seguridad.
- g. eSignatures(1) Política de firma electrónica.
- h. Policy (1) Variante de política (1: General, 2 EPES-Pre, 3 EPES-Post, ...).
- i. major_version(1) Versión mayor.
- j. minor_version(0)} Versión menor.

9. PUBLICACIÓN DE LA GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA

1. La presente Guía se expresa en formato legible (PDF). La dirección en la que estarán disponibles las diferentes versiones de la presente Guía es la siguiente:

<https://www.administraciondejusticia.gob.es/cteaje/guias-de-interoperabilidad>

USO OFICIAL:

TLP: CLEAR



10. SECCIÓN DE GENERACIÓN DE FIRMAS Y DE USO DE CERTIFICADOS

10.1 Pautas de uso de certificados en entornos que no son de firma electrónica

1. Los certificados se utilizan para securizar accesos a servidores web, a través de un protocolo de comunicaciones conocido como SSL (Secure Sockets Layer) o TLS (Transport Layer Security). En este caso se reconoce este tipo de acceso porque la URL de la página web se inicia con el identificador de protocolo "https://" en vez de "http://".
2. Cuando los certificados se utilicen en servidores de web de Sedes y subsedes Electrónicas, se solicitará su expedición al Prestador de Servicios de Certificación indicando que se haga constar en un campo OU (Organizational Unit) la expresión "Sede Electrónica - Electronic Site".
3. Los certificados utilizados para cifrar las comunicaciones con las páginas de internet de sedes y subsedes judiciales electrónicas, así como con los registros judiciales electrónicos, y otras páginas web relacionadas con la Administración de Justicia deberán adquirirse a Prestadores de Servicios de Certificación incluidos en los aplicativos de navegación de páginas internet comúnmente utilizados, de forma que se garantice que no se producen mensajes de aviso de riesgo de seguridad al establecerse la comunicación cifrada. De ellos se preferirán los que cumplan lo prescrito para los certificados cualificados en el Reglamento UE 910/2014, que se incluirán en la TSL de la Unión Europea.
4. Cuando el acceso cifrado a una página web relacionada con la Administración de Justicia incluya una autenticación del usuario que accede, a través de un certificado del propio usuario, no se utilizarán en la página web aplicaciones en Java, flash u otras herramientas de programación de la propia página web que impliquen el uso de certificados adicionales de firma o autenticación.
5. Se evitará el uso de funcionalidades de firma electrónica realizadas desde las propias páginas web, bien basadas en Java, bien basadas en flash u otras herramientas de programación de la propia página web, destinadas a ser ejecutadas en el navegador. En lo posible el manejo de firmas electrónicas se realizará mediante programas y sistemas independientes que permitan realizar las firmas sobre los documentos electrónicos directamente, sin requerir el uso de un navegador, aunque se podrán adjuntar a operaciones y formularios, admitiéndose los sistemas que comprueban firmas en el lado del servidor e informan a los usuarios, bien en el momento adjuntar el fichero o bien en un momento posterior de que se ha producido un error subsanable relativo a la firma.

10.2 Firma electrónica como manifestación de voluntad

6. Se empleará la firma electrónica como un instrumento capaz de permitir la comprobación de la vinculación entre el firmante y el contenido firmado, y de establecer la presunción de que existió intención de firmar, es decir, prestación del consentimiento en el sentido que se determine por el contexto (por ejemplo, conformidad en recibir una notificación,

aunque no haya conformidad respecto al contenido de la notificación). Asimismo, la firma electrónica debe permitir detectar modificaciones del contenido firmado si se producen.

7. Un mecanismo para distinguir si el contexto de uso de certificados se lleva a cabo en relación con una firma electrónica es que el firmante sea consciente de la realización de la firma, del contenido del documento firmado y de las implicaciones de acompañar su firma al documento.
8. Siempre que el contexto de uso del certificado implique la realización de una firma, el firmante deberá poder conservar un fichero o documento electrónico en el que ha quedado plasmada, de forma que resulte evidente la realización de la firma y el contenido del documento.
9. En las firmas electrónicas automatizadas y en el uso de sellos electrónicos para la actuación automatizada, deberá quedar evidenciado en el procedimiento tecnológico que una persona con acreditación adecuada es consciente de la realización de tales firmas y consiente esa actuación automatizada.

10.3 Sistemas de firma utilizados por jueces, juezas, magistrados y magistradas

Se emplearán sistemas de firma electrónica cualificada según lo dispuesto en el Reglamento europeo UE 910/2014, de 23 de julio, y las normas técnicas publicadas en su desarrollo.

10.4 Sistemas de firma utilizados por el personal de la Oficina Judicial, de la Oficina Fiscal y demás personal al servicio de la Administración de Justicia

Se emplearán sistemas de firma electrónica cualificada y sistemas de firma electrónica avanzada basados en certificados cualificados de firma electrónica según lo dispuesto en el Reglamento europeo UE 910/2014, de 23 de julio, y las normas técnicas publicadas en su desarrollo. Los certificados serán expedidos por prestadores incluidos en la “Lista de confianza de prestadores de servicios de certificación”.

10.5 Sistemas de firma basados en código seguro de verificación para la actuación judicial automatizada

Deberán cumplir con los requisitos establecidos en el artículo 21 del 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.

10.6 Certificados con identificación por seudónimo

Cuando existan condiciones que lo hagan necesario, se podrán utilizar certificados en los que la identidad del firmante o del órgano que usa un sello electrónico se protejan mediante un seudónimo en forma de indicación significativa, datos y códigos adicionales que permitan revelar la identidad del firmante a órganos judiciales y otros órganos y personas legitimadas por parte del prestador de servicios de confianza digital que los expidió.

10.7 Pautas de uso de certificados en entornos de firma electrónica en PDF

USO OFICIAL:



1. Cuando las firmas electrónicas se generen en los ámbitos de la Administración de Justicia sobre documentos basados en formato PDF que están destinados a ser utilizados en diferentes contextos que pueden requerir su exhibición en formato electrónico o de forma impresa, se prepararán de manera que quede patente en la zona final del documento la forma de comprobar su autenticidad mediante un código seguro de verificación, para lo cual se indicará una dirección web estable (cuya denominación no se prevea que cambie por posibles reorganizaciones de los órganos bajo cuyas competencia se gestiona) en la que comprobar la validez. Esta dirección web podrá ser una correspondiente a la sede o subselección electrónica.
2. Cuando los certificados los utilicen profesionales de la Administración de Justicia, se solicitará su expedición al Prestador de Servicios de Certificación indicando que se haga constar en el campo TITLE el cargo del firmante en español y en inglés y en un campo OU (Organizational Unit) una mención del carácter oficial del certificado, como por ejemplo "Public Servant". En el caso de que se usen OIDs específicos alineados con Políticas de Firma electrónica de otras administraciones, no es preciso dejar de usarlos, siempre que los contenidos relevantes se incluyan en los campos definidos de forma estándar. Si se usan los citados OID no se puede dar por supuesto que los destinatarios de los documentos firmados electrónicamente con los certificados que los incluyen serán capaces de interpretarlos.
3. Se evitará en lo posible utilizar para la firma electrónica en PDF sistemas que dependan del uso de entornos Flash y Java en navegadores web. Serán preferibles entornos de firma electrónica que se ejecuten en servidor, o el uso de programas específicos de firma en PDF, que no requieran usar un navegador e incluso no requieran usar internet (salvo para lo que se indica más adelante en relación con el sellado de tiempo y la consulta OCSP). Como excepción, se admiten las modalidades de firma en Java en entornos de ejecución controlados desplegados por las propias administraciones, tales como portafirmas y otros, en los que existe infraestructura de soporte técnico para los usuarios a los que se destina este tipo de aplicaciones y es posible determinar que el usuario cuenta con la configuración adecuada para su ejecución, sin que este perciba una complejidad excesiva.
4. Siempre que sea posible se preservará el principio de "Apariencia de buena firma". Para ello se incluirá en las firmas electrónicas basadas en PDF una información gráfica correspondiente a la firma manuscrita de la persona que suscribe el documento, y, de ser considerado conveniente por el uso al que se destina el documento, otra información gráfica relacionada con el órgano bajo cuyo auspicio se expidió el documento, como por ejemplo la digitalización de un sello de caucho, un escudo o un logotipo. Esta información gráfica se vinculará a la firma electrónica basada en el uso de certificados, utilizada para suscribir el documento por el firmante.
5. En aplicación del mismo principio, para firmas electrónicas basadas en PDF se recomienda usar certificados emitidos por prestadores de servicios de certificación incluidos en la lista de confianza AATL de Adobe (que además cumplan lo prescrito para

los certificados cualificados en el Reglamento UE 910/2014, que se incluirán en la TSL de la Unión Europea).

- Es de aplicación lo señalado en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015 en relación con los formatos de las firmas electrónicas y de los sellos electrónicos, y en particular, en las firmas de los ficheros PDF lo indicado en la norma técnica ETSI TS 103172.

10.8 Pautas de realización de firmas electrónicas con verificación previa de la validez del certificado (EPES-Pre)

- Una forma compacta de realizar firmas electrónicas, especialmente en entornos automatizados consiste en comprobar que el certificado que se va a utilizar en la firma no está revocado antes de proceder al proceso técnico de la firma.
- En estos casos, procede identificar dicha política en la propia firma electrónica, de forma que, si una entidad debe comprobar la validez de la firma y detecta en ella la identificación de política, no sea preciso realizar otros procesos como la obtención de sellos de tiempo adicionales y comprobaciones OCSP que serían necesarios si se optara por promover la firma AdES-EPES a AdES-XL.
- La identificación de política para esta comprobación previa de validez de certificado antes de firmar (destinada a firmas de nivel EPES) es:

```
{joint-iso-itu-t(2) country(16) es(724) ejustice(6) cetaje(1) eSignatures(1) EPES-
Policy(2) Major_Version(1) Minor_Version(0)}
```

- Las firmas electrónicas realizadas en este contexto se circunscriben a firmas XAdES y firmas CAdES.
- Esta modalidad compacta de codificación de firmas de validez implícita se usa preferentemente en entornos del propio órgano, si no se prevé que los documentos firmados electrónicamente tengan que surtir efecto fuera de él, para lo que serán preferibles las modalidades AdES-XL.

10.9 Pautas de uso de certificados en entornos de firma electrónica en PKCS#7

- Cuando las firmas electrónicas se generen en los ámbitos de la Administración de Justicia en formato PKCS#7 o versiones avanzadas CAdES se utilizarán las versiones "detached".
- En particular puede ser el caso de tipos de documentos multimedia, tales como las grabaciones de video o audio en las salas de vistas.
- Los sistemas de comprobación de firmas electrónicas específicos de los contextos en los que se use en formato PKCS#7 o sus versiones avanzadas CAdES, permitirán la consulta de los datos del certificado asociado a la clave con la que se generó la firma, información sobre el momento en que se realizó la firma y datos de comprobación de validez del certificado en dicho momento. Además, aportarán información de metadatos del

documento firmado como, por ejemplo, nombre y ubicación del fichero, tipo de fichero, tamaño, duración de la grabación, codificación y procedimiento judicial al que se asocia.

- Es de aplicación lo señalado en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015 en relación con los formatos de las firmas electrónicas y de los sellos electrónicos, y en particular, en las firmas de tipo CMS lo indicado en la norma técnica ETSI TS 103173.
- Serán admisibles variantes "detached" de firmas XAdES para este propósito. Es de aplicación lo señalado en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015 en relación con los formatos de las firmas electrónicas y de los sellos electrónicos, y en particular, en las firmas de tipo XML lo indicado en la norma técnica ETSI TS 103171.

10.10 Pautas de realización de firmas electrónicas de procedencia ajena a la Administración de Justicia

- Las firmas electrónicas procedentes de ámbitos que no sean de la Administración de Justicia, podrán ser firmas avanzadas¹ de cualquier tipo de entre los previstos en las normas ETSI TS 101 733 (CAAdES), ETSI TS 101 903 (XAdES) y ETSI TS 102 778 (PAdES) o las versiones actualizadas de estas normas. En todo caso serán admisibles las que cumplan lo previsto en la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015 en relación con los formatos de las firmas electrónicas y de los sellos electrónicos.
- Las aplicaciones informáticas basadas en servidor en el ámbito de la Administración de Justicia recopilarán todas las evidencias electrónicas necesarias para convertir las firmas electrónicas recibidas en sus variantes completas CAAdES-XL, XAdES-XL o PAdES-LTV según corresponda, en caso de que las citadas evidencias no formen ya parte de la firma. Alternativamente podrán utilizar firmas compactas AdES-EPES (Post) según se indica en el apartado 11.4.
- Una vez incluidas las firmas en el sistema informático de gestión judicial, que empleará técnicas de gestión de integridad, tales como "hashes encadenados", o sellos de tiempo sobre grupos de referencias de documentos no será preciso el resellado temporal individualizado de firmas electrónicas conducentes a las modalidades AdES-A de dichas firmas.

10.11 Pautas de gestión de firmas electrónicas en servidor vinculadas a personas físicas identificadas

- Se admite la creación de firmas electrónicas a distancia en un entorno de creación de firma electrónica gestionado en servidor en nombre del firmante.
- Esta posibilidad se reserva, en base al citado Reglamento UE 910/2014 a los Prestadores de Servicios de Confianza Digital.

¹ Ver tipos y niveles de firmas electrónicas en el Anexo

3. Los prestadores que ofrezcan servicios de firma electrónica a distancia deben aplicar procedimientos de seguridad de la gestión y administrativos específicos y utilizar sistemas y productos fiables, incluidos canales de comunicación electrónica seguros para garantizar que el entorno de creación de firmas electrónicas es fiable y se utiliza bajo el control exclusivo del firmante. En el caso de una firma electrónica cualificada creada mediante un dispositivo de creación de firmas electrónicas a distancia, se aplicarán los requisitos aplicables a los prestadores cualificados de servicios de confianza contemplados en dicho Reglamento.
4. Las administraciones con competencias en provisión de medios para la Administración de Justicia podrán adoptar prácticas equivalentes a las citadas para lo que podrán designar uno o más prestadores para llevarlas a cabo o realizarlas con sus medios cumpliendo con las auditorías y otros requisitos exigibles a los Prestadores de Servicios de Confianza Digital.

10.12 Pautas de realización de firmas electrónicas en PDF basadas en firmas manuscritas, sin uso de certificado

1. En el caso de que se empleen firmas electrónicas avanzadas no basadas en certificado, sino en la vinculación a los documentos electrónicos de firmas manuscritas captadas con técnicas biométricas se respetarán los siguientes criterios:
 - a. El proceso de creación de las firmas manuscritas digitalizadas implicará el cifrado de la información biométrica asociada a la realización del trazo de la firma sobre un dispositivo idóneo y su incorporación al propio documento. El cifrado se apoyará sobre una clave pública gestionada por el software de codificación de firmas, asociada con una clave privada custodiada por un notario o un Prestador de Servicios de Confianza Digital.
 - b. En caso de controversia sobre la firma, debe ser posible su cotejo para lo que se podrá recurrir al notario o Prestador de Servicios de Confianza Digital supervisado por el órgano designado (Secretaría de Estado de Telecomunicaciones y para la Sociedad de la Información, adscrita al Ministerio de Industria, Energía y Turismo), que custodia la clave privada, que colaborarán para el descifrado de la información biométrica del documento, lo que podrá utilizar un perito calígrafo para comparar la firma con otras indubitadas del mismo autor.
 - c. La posibilidad de extraer la información dinámica estará disponible sin coste en el Prestador a disposición de los firmantes y terceros con interés legítimo.
 - d. La firma y el contenido del documento se vincularán de forma indisoluble, de forma que esta vinculación pueda ser comprobada por quien acceda al documento.
 - e. La imagen estática de la firma será visible en el documento PDF.

- f. El software de análisis pericial que permita comparar una firma controvertida con otras indubitadas estará disponible sin coste en un tercero depositario a disposición de los firmantes y terceros con interés legítimo.
- g. Las firmas electrónicas de este tipo pueden ir reforzadas con sellos de tiempo o firmas o sellos automatizados.
- h. Se preferirán los sistemas que estén respaldados por sellos de calidad que el fabricante o distribuidor haya obtenido tras superar una auditoría de una entidad auditora especializada en sistemas de firma manuscrita digitalizada avanzada.
- i. Se garantizará el cumplimiento de la normativa vigente en materia de protección de datos personales.

11. SECCIÓN DE ACEPTACIÓN DE FIRMAS ELECTRÓNICAS Y DE CERTIFICADOS

11.1 Prestadores de servicios de certificación admitidos

1. Serán válidos los certificados expedidos por Prestadores de Servicios de Confianza Digital supervisados según el marco definido por el Reglamento Europeo (UE) 910/2014.
2. En dicho contexto, se admitirán los prestadores que se incluyan en listas TSL conformes con la norma TS 102 231² administradas por los órganos de supervisión de Prestadores de Servicios Confianza Digital (PSDC) de los países miembros de la Unión Europea según se establezca en la TSL colectiva de la UE, tanto PDF como XML. Se considerará válida la versión XML en caso de existir discrepancias entre ellas.
3. Serán válidos los certificados expedidos por PSDC (Prestadores de Servicios de Confianza Digital) incluidos en listas TSL de otros países, incluso aunque no sean miembros de la Unión Europea, que cuenten con un órgano de supervisión de los servicios de certificación y que se comuniquen al CTEAJE. El CTEAJE podrá solicitar documentación complementaria que permita acreditar un nivel de supervisión equivalente al que se sigue en España. El CTEAJE dará publicidad en su sede electrónica a las listas TSL de los países que hayan comunicado la existencia de sus listas, dando prioridad a los países con los cuales España tenga firmados convenios de cooperación en materia de Justicia.
4. Los PSDC deberán cumplir con lo previsto por los organismos de normalización en relación con los estándares y normas técnicas aplicables, especialmente respecto a los requisitos técnicos y operacionales que posibilitan la expedición de certificados cualificados. Cuando emitan certificados de personal al servicio de la Administración de Justicia, o para los sistemas de firma electrónica o de sello electrónico automatizados, podrán incluir en los campos de unidad organizativa, la información necesaria para identificar adecuadamente al ente u órgano titular del sello, de conformidad con el Real

² O la norma que la sustituya, como la ETSI TS 119 612

Decreto-ley 6/2023. Los prestadores de servicios de certificación, de conformidad con lo descrito en su Declaración de Prácticas de Certificación, deberán:

- Aplicar los estándares relativos a políticas y prácticas de certificación y generación de certificados electrónicos; estado de los certificados; dispositivos cualificados de creación de firma; programas controladores; dispositivos criptográficos; interfaces de programación; tarjetas criptográficas; conservación de documentación relativa a los certificados y servicios; y límites de los certificados, conforme a lo establecido en el Reglamento UE 910/2014 y en la normativa técnica desplegada en el marco de su desarrollo. Incluir dentro de los certificados la información relativa a las direcciones de Internet donde se ofrecen servicios de validación del propio certificado sin coste alguno. Estos servicios de consulta de validez de certificados se basarán en información actualizada y no en mecanismos de consulta de listas de revocación que pudieran requerir tener en cuenta un "período de gracia" desde el momento de la firma hasta el momento en que se puede tener la certeza de que el certificado no estaba revocado.
- Opcionalmente pueden contener, además, la dirección electrónica de otro servicio de comprobación de validez que otorgue acceso a la lista de certificados revocados y no caducados del mismo tipo que el cuestionado, igualmente sin coste alguno.
- Cumplir lo previsto en los apartados 2.2 y 4.2 de la Decisión de Ejecución (UE) 2015/1506 de la Comisión, de 8 de septiembre de 2015.

11.2 Políticas de firma admitidas

- Las oficinas judiciales receptoras de documentos electrónicos, documentos administrativos electrónicos y documentos judiciales electrónicos permitirán la validación de firmas electrónicas que incluyan referencias a otras políticas de firma, cuando no contradigan la política general relativa a la aceptación de firmas electrónicas.
- En términos generales, no se prevén restricciones en cuanto a la aceptación de documentos firmados electrónicamente, sea cual sea la política de firma con la que se generaron.
- En el caso de que las firmas que no incorporen evidencias electrónicas del momento de generación de la firma (timestamping) y de la comprobación de la validez del certificado tras ese momento, podrá ser el órgano aceptante el que transforme la firma electrónica recibida en la variante extendida que incluye dicha información, para dar lugar a variantes de tipo AdES-XL o PAdES-LTV, incorporando el sello de tiempo y la información de validación. También podrá generar firmas compactas EPES (Post) según se indica en el apartado 11.4.

11.3 Plataformas de validación de certificados electrónicos y de firma electrónica.

USO OFICIAL:



1. Los certificados podrán ser validados mediante plataformas de validación de certificados electrónicos y de firma electrónica, que proporcionarán servicios de confianza a las aplicaciones usuarias o consumidoras de los servicios de certificación y firma, proporcionando servicios de validación de los certificados y firmas generadas y admitidas en diversos ámbitos de las Administraciones con competencias en materia de justicia.
2. Estas plataformas incorporarán las listas de confianza de los certificados interoperables entre las distintas Administraciones nacionales y europeas según el esquema operativo de gestión correspondiente de la lista de confianza (TSL), de acuerdo con en el artículo 22 del Reglamento UE 910/2014, de 23 de julio.
3. Los servicios de consulta de validez de certificados se basarán en información actualizada en tiempo real y no en mecanismos de consulta de listas de revocación que pudieran requerir tener en cuenta un "período de gracia" desde el momento de la firma hasta el momento en que se puede tener la certeza de que el certificado no estaba revocado.

11.4 Codificación compacta de firmas electrónicas recibidas, tras verificar la validez de su certificado (EPES-Post)

1. Cabe la posibilidad de usar una forma compacta de codificar firmas electrónicas recibidas, tras comprobar que el certificado utilizado en la firma es válido y no está revocado, que es correcta la verificación de la jerarquía de certificación y que el certificado raíz de la jerarquía que lo emitió se incluye en la lista TSL.
2. En estos casos, se puede utilizar la variante compacta AdES-EPES gestionada por la propia entidad receptora del documento firmado electrónicamente, que lleva a cabo las comprobaciones citadas.
3. La identificación de política para esta comprobación de validez de certificado tras la recepción de la firma (destinada a firmas de nivel EPES) es:

```
{joint-iso-itu-t(2) country(16) es(724) ejustice (6) cetaje(1) eSignatures(1) EPES-
Policy(3) Major_Version(1) Minor_Version(0)}
```

4. Las firmas electrónicas realizadas en este contexto se circunscriben a firmas XAdES y firmas CAdES.
5. Esta modalidad compacta de codificación de firmas de validez implícita se usa en entornos del propio órgano que la custodia, si no se prevé que los documentos firmados electrónicamente tengan que surtir efecto fuera de él, para lo que serán preferibles las modalidades AdES-XL.

11.5 Conservación a largo plazo de firmas electrónicas incluidas en mecanismos de custodia de órganos de la Administración Electrónica de Justicia

1. Las firmas electrónicas de los documentos judiciales electrónicos, siempre que hayan sido transformadas a las variantes extendidas que incluyen la información del momento de la realización y de la validez del certificado utilizado en dicho momento, para dar lugar a

variantes de tipo AdES-XL o PAdES-LTV, una vez que se encuentren custodiados en un sistema de información empleado en el ámbito de la Administración de Justicia gozarán de la presunción de su validez, incluso cuando haya transcurrido el período de validez de cada certificado o de los certificados de las autoridades de certificación que los emitieron. Para la obtención de firmas de variantes AdES-XL o PAdES-LTV, no será preciso tener en cuenta el "Período de gracia"³ ya que los PSDC garantizarán que el servicio de consulta de certificados revocados ofrece la información actualizada en tiempo real.

- Esta presunción de validez de las firmas electrónicas a largo plazo en tanto que custodiadas en el sistema de gestión procesal, se aplicará también a las variantes compactas AdES-EPES que hayan sido creadas en el marco de las políticas EPES-Pre y EPES-Post citadas, por el propio organismo que las custodia.
- Cuando se utilicen modalidades compactas de codificación de firmas electrónicas para su archivo que afecten solo a la entidad que las gestiona, se recogerán sus especificaciones en la Política Documental de la entidad, de forma que quede garantizada y documentada la posibilidad de comprobar la autenticidad de los documentos electrónicos custodiados a largo plazo.
- Cuando los documentos judiciales electrónicos incluyan un Código Seguro de Verificación, su autenticidad podrá cotejarse en la sede o subsede judicial electrónica del órgano que lo expidió, en virtud de las medidas de seguridad empleadas para su custodia. Al acceder, en la sede o subsede judicial electrónica, al documento referenciado por el Código Seguro de Verificación, se obtendrá el documento judicial electrónico que incluirá, en su caso, las firmas electrónicas que correspondan. Los documentos judiciales electrónicos que se impriman serán válidos en su forma impresa siempre que puedan cotejarse de la manera indicada.
- La posibilidad de cotejar los documentos se garantizará al menos por 5 años tras el archivo de las actuaciones y, en el caso de las sentencias, por 15 años desde que sean firmes. Estos plazos no serán de aplicación cuando una norma procesal establezca otra cosa.

11.6 Firma electrónica de documentos electrónicos procedentes de la digitalización de documentos en papel

- Cuando una Administración pública, un profesional de la justicia o un ciudadano (que haya optado voluntariamente a relacionarse por medios electrónicos con la Administración de justicia) aporte en un procedimiento documentos electrónicos procedentes de la digitalización de documentos en papel, convertidos a formato PDF, plasmará en ellos su firma electrónica con indicación del momento de la firma y de la validez del certificado utilizado y se responsabilizará de su autenticidad y de que la versión digital es una imagen fiel del documento original. Deberá presentar el documento original cuando sea requerido si se apreciara cualquier impedimento respecto a la valoración de lo indicado en el documento que no pueda deducirse del propio documento digitalizado. En particular, la

³ Concepto descrito en diversas normas técnicas, por ejemplo, en la RFC 5126 <https://tools.ietf.org/html/rfc5126>

aportación del original podrá ser requerida cuando sea preciso realizar valoraciones periciales documentoscópicas.

2. Las oficinas judiciales y el resto de los órganos relacionados con la Administración de Justicia podrán proceder a la digitalización certificada de documentos presentados y conservados en papel que tengan el carácter de original. Los documentos así digitalizados tendrán la consideración de copias auténticas y surtirán el efecto del original, con su misma validez y eficacia, de acuerdo con lo establecido en el artículo 40 del Real Decreto ley 6/2023. Una vez dichos documentos se incluyan bajo la custodia del sistema procesal, será posible proceder a la destrucción de los originales o a su devolución a quien los aportó. Se recomienda un período de guarda de 60 días para gestionar posibles eventualidades de digitalización de páginas dobles.

12. ANEXO I. CONSIDERACIONES ADICIONALES

Aunque el presente documento, en tanto que política de firma electrónica, se ciñe a indicar la forma de realizarla y comprobarla, los conceptos conexos de identificación, autenticación y acreditación son relevantes, en particular tras la nueva regulación: el Reglamento europeo UE nº 910/2014, por lo que conviene tenerlos presentes en el marco de la política.

Por otro lado, al desplegar sistemas informáticos que planteen la generación de firmas electrónicas o la comprobación de firmas, conviene valorar si el uso de la firma electrónica es la técnica más adecuada para el procedimiento, o si es preferible utilizar otra técnica que permite la autenticación del interviniente.

Por ello, se incluyen las siguientes definiciones conexas:

12.1 Identificación

1. Se consideran «datos de identificación de la persona», el conjunto de datos que se emite de conformidad con el Derecho de la Unión o nacional y permite establecer la identidad de una persona física o jurídica, o de una persona física que representa a otra persona física o a una persona jurídica.
2. Se considera «identificación electrónica», el proceso consistente en utilizar los datos de identificación de la persona en formato electrónico que representan de manera única a una persona física o jurídica o a una persona física que representa a otra persona física o a una persona jurídica.
3. Se consideran «medios de identificación electrónica», la unidad material y/o inmaterial que contiene los datos de identificación de la persona y que se utiliza para la autenticación en servicios en línea o, cuando proceda, en servicios fuera de línea.

12.2 Autenticación

1. Se considera «autenticación», proceso electrónico que permite la confirmación de la identificación electrónica de una persona física o jurídica, o la confirmación del origen y la integridad de datos en formato electrónico. Consecuentemente, un proceso de autenticación permite tener certeza de que la identificación electrónica asociada se corresponde con la de su titular.
2. Los sistemas de autenticación de una persona podrán establecerse utilizando preferentemente combinaciones de 2 o más factores de autenticación de entre los siguientes: "algo que se tiene", "algo que se sabe", o "algo que se es". Serán preferibles los que dificulten su cesión y los que permitan el acceso en marcos de tiempo efímeros de modo que exijan nuevas gestiones de identificación, para actuaciones posteriores a una dada.

12.3 Acreditación

1. Se considera «acreditación» al proceso electrónico que establece el nivel de privilegio con que cuenta una persona física o jurídica, o a una persona física que representa a una

persona jurídica, ya identificada y autenticada para acceder a determinada información o a realizar determinadas actuaciones, en función de restricciones específicas de cada procedimiento. Se establecerá, para cada persona identificada con acceso a los sistemas, su perfil de acceso, el cual determinará la información a la que puede acceder y las funciones y actuaciones que tiene a su disposición, así como las que le están restringidas.

12.4 Niveles de confianza

Cuando se utilicen sistemas de firma remota que se activen tras un proceso de identificación y autenticación del titular del certificado se tendrán en cuenta los niveles de garantía de la identificación (LoA - Levels of Assurance, por su denominación en inglés) definidos en la norma ISO / IEC 29115: 2013.

El nivel de garantía (Level of Assurance LoA) al que hace mención esta Norma Internacional se refiere a la confianza que merecen los procesos, las actividades de gestión y tecnologías utilizados para establecer y gestionar de forma efectiva la identidad de una entidad para su uso en las transacciones de autenticación.

La Norma Internacional ISO / IEC 29115: 2013 ofrece una guía fundamental para la gestión de la garantía de la autenticación de entidad en un contexto dado. En particular, se centra en los:

- Cuatro niveles de garantía de la autenticación de la entidad.
- Criterios y directrices para el logro de cada uno de los cuatro niveles de garantía de la autenticación de la entidad.
- Orientación para la correspondencia de otros sistemas de garantía de autenticación a los cuatro niveles de garantía especificados.
- Orientación para el intercambio de los resultados de autenticación que se basa en los cuatro niveles de garantía.
- Orientación en cuanto a los controles que se deben utilizar para mitigar las amenazas relativas a la autenticación.

Utilizando los cuatro niveles especificados de garantía (LoAs), el documento presenta las pautas relativas a las tecnologías de control, los procesos y las actividades de gestión, así como los criterios de garantía que se deben utilizar para mitigar las amenazas relativas a la autenticación con el fin de poner en práctica los cuatro niveles de garantía.

También proporciona una idea sobre la forma en que se corresponden otros sistemas de garantía de autenticación con los cuatro niveles especificados en la norma y orienta sobre la forma de intercambiar resultados de una transacción de autenticación. Por último, esta Norma Internacional proporciona orientación informativa relativa a la protección de la información de identificación personal asociado con el proceso de autenticación.

La norma ISO / IEC 29115: 2013 ayuda a lograr:

- Establecimiento el servicio.

USO OFICIAL:



- Cumplimiento Legal y Contractual.
- Disposiciones financieras.
- Gestión de la seguridad de la información y de auditoría.
- Componentes de servicios externos.
- Métricas de capacidades operativas.

La norma se destina principalmente a proveedores de servicios de credenciales (CSP- Credential Service Providers) y a quienes tengan interés en sus servicios, por ejemplo, las partes que confían, asesores y auditores de esos servicios.

Los niveles son los siguientes:

1. LoA 1 – Garantía Baja – Low – Little or no confidence in the asserted identity.
2. LoA 2 – Garantía Media – Medium – Some confidence in the asserted identity.
3. LoA 3 – Garantía Alta– High – High confidence in the asserted identity.
4. LoA 4 – Garantía Muy alta – Very high – Very high confidence in the asserted identity.

El impacto de los errores de autenticación será mínimo, moderado, sustancial o alto según el LoA requerido.

Estos niveles pueden encajarse en los 4 niveles definidos en el proyecto Stork (Secure idenTity acrOss boRders linKed) con la denominación QAA (Quality Authentication Assurance).

STORK QAA level	Description
1	No or minimal assurance
2	Low assurance
3	Substantial assurance
4	High assurance

Los niveles de aseguramiento 2 a 4 de la norma ISO / IEC 29115: 2013 y de Stork se alinean con los niveles Bajo, Sustancial y Alto definidos en el 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) no 910/2014 del Parlamento Europeo y del Consejo, relativo a la identificación electrónica y los servicios de confianza para las transacciones electrónicas en el mercado interior.

Volviendo a la posibilidad de gestionar sistemas de firma remota, se recomienda que en ellos se utilicen Niveles de garantía LoA Sustancial o Alto. Será habitual que se escale entre un

USO OFICIAL: TLP: CLEAR



nivel de aseguramiento LoA a otro añadiendo técnicas de autenticación. Por ejemplo, un usuario autenticado con un sistema basado en datos usuario/password, (LoA bajo) puede optar a firmar un documento electrónico a partir de que el sistema refuerza el control de autenticación enviándole un valor por SMS a su móvil (pasando a LoA substancial) o haciendo uso de un sistema complementario de autenticación biométrica disponible en su ordenador o teléfono móvil (pasando a LoA alto).

En otros contextos, para acceder a una notificación puede ser suficiente una técnica de LoA bajo sin requerir firma electrónica (que por el hecho de usar un certificado se consideraría equivalente a un LoA alto).

A pesar de que habitualmente se utilizarán sistemas que tengan un nivel de garantía LoA bajo, substancial o alto según se indica en la normativa derivada del Reglamento europeo UE 910/2014 (equivalentes a los niveles 2 a 4 de la norma ISO / IEC 29115: 2013) en ciertas circunstancias será aceptable admitir sistemas que no requieran ofrecer garantías sobre la identidad, es decir, que la mera alegación de identidad (LoA 1) es suficiente para realizar la gestión electrónica solicitada. Por ejemplo, en la admisión de solicitudes por los ciudadanos que solo tenga sentido que se inicien por el interesado.

12.5 Requisitos relativos al conjunto mínimo de datos de identificación de personas físicas y jurídicas

En relación con la interoperabilidad transfronteriza se señala que los requisitos relativos al conjunto mínimo de datos de identificación de la persona que representen de manera exclusiva a una persona física o jurídica, a que se refiere el artículo 11 del Reglamento de Ejecución (UE) 2015/1501 de la Comisión de 8 de septiembre de 2015 se describen en el ANEXO del citado Reglamento de Ejecución.

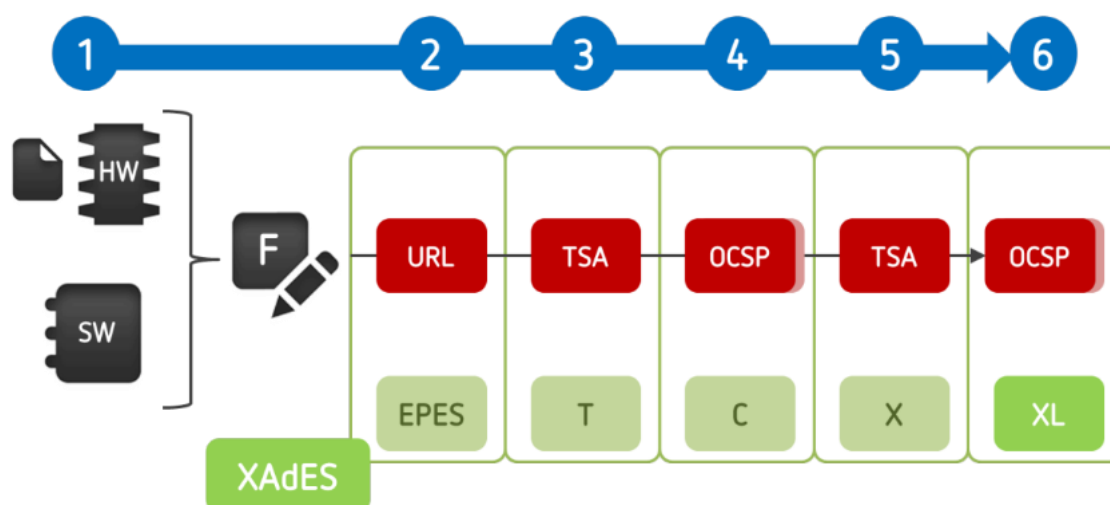
13. ANEXO II. ASPECTOS TÉCNICOS Y BUENAS PRÁCTICAS

13.1 Certificados en entornos web

1. En las remisiones de documentos a través de sedes electrónicas (páginas web) se preferirá la autenticación SSL sobre la realización de firmas electrónicas mediante applets java salvo que se considere que el documento firmado conservado por el sistema y por el usuario se adapta mejor al objetivo de gestión.
2. Para acceder a notificaciones, se recomienda autenticar mediante SSL-Cliente y recoger las evidencias de "HTTP header fields" y del enlace clickado, y que se genere el acta (o recibo) de acceso a la notificación en el lado servidor con firma-e del órgano.

13.2 Diagrama sobre los niveles de firma electrónica

1. Según se añade información sobre políticas o se incluyen evidencias electrónicas como sellos de tiempo e informaciones firmadas relativas a la validez de los certificados que respaldan las firmas electrónicas (basadas en ficheros CRL o respuestas OCSP) se añaden campos a la firma electrónica, según el esquema siguiente:

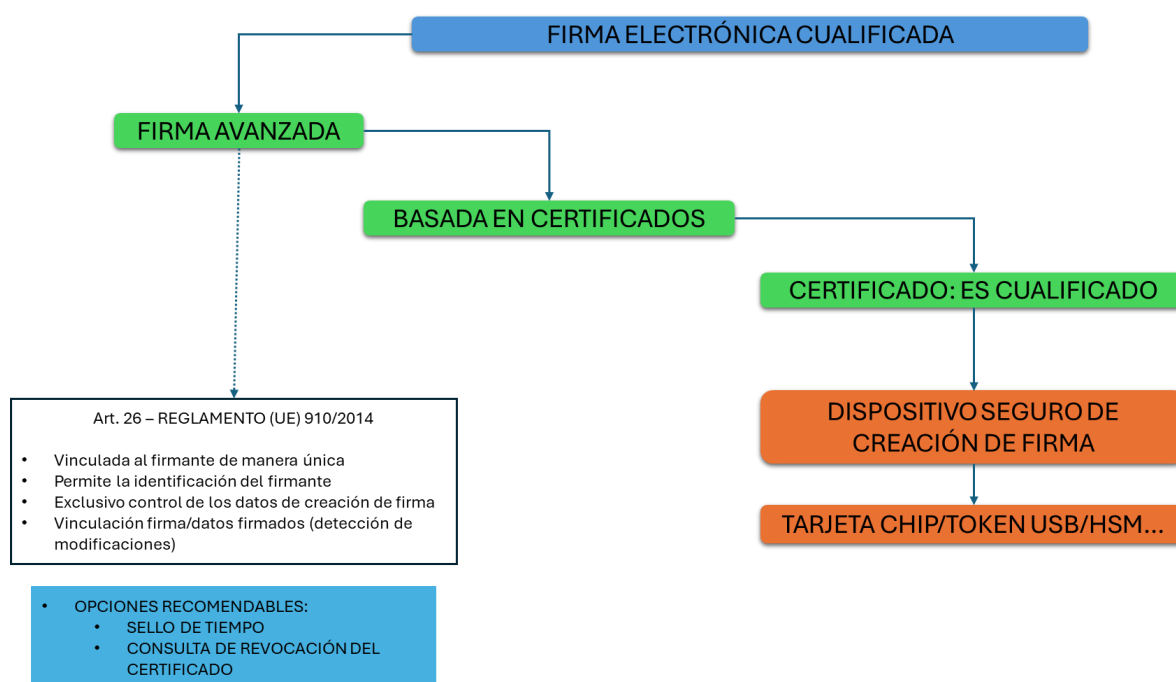


La interpretación de este diagrama es la siguiente: En función del contexto, las firmas (F) se pueden realizar en base a claves custodiadas en un dispositivo electrónico (hardware, HW) o en un fichero del ordenador que ejecuta la firma (software, SW). La firma (F) vincula al firmante (que custodia la clave en HW o SW) con el documento. A la firma (que incluye el certificado del firmante) se le pueden añadir capas con extensiones. La capa EPES (Explicit Policy Electronic Signature) añade la "URL" (dirección web) en la que se identifica y describe la política de firma. La capa T (Timestamping) añade un sello de tiempo proporcionado por una "TSA" (timestamping Authority). La capa C (complete) añade información sobre donde radican los datos de verificación de la validez (certificados, respuestas "OCSP" y listas de revocación "CRL"). La capa X (extended) añade un sello de tiempo a las referencias introducidas por XAdES-C y la capa X-L (extended long-term), añade la respuesta "OCSP"

del emisor del certificado usado en la firma en el que queda constancia de que no está revocado para permitir la verificación en el futuro. Existe otra capa más (A) pero no se considera relevante a los efectos de esta descripción.

Estos tipos de firma se especifican en las normas EN 319 122, EN 319 132, EN 319 142.

13.3 Diagrama sobre los tipos de firma




13.4 Buenas prácticas en la realización de firmas sobre PDF

- Siempre que sea posible se preservará el principio de "Apariencia de buena firma". Para ello se incluirá en las firmas electrónicas basadas en PDF una información gráfica correspondiente a la firma manuscrita de la persona que suscribe el documento, y, de ser considerado conveniente por el uso al que se destina el documento, otra información gráfica relacionada con el órgano bajo cuyo auspicio se expidió el documento, como por ejemplo la digitalización de un sello de caucho, un escudo o un logotipo. Esta información gráfica se vinculará a la firma electrónica basada en el uso de certificados, utilizada para suscribir el documento por el firmante.
- Las firmas electrónicas realizadas en este contexto en documentos PDF deberán realizarse tomando en consideración las siguientes peculiaridades:

- a. Tarjeta chip: Siempre que sea posible se utilizarán para la firma electrónica certificados soportados en tarjeta chip⁴ (para cumplir el requisito de “dispositivo seguro de creación de firmas que la normativa impone a las firmas electrónicas para ser consideradas cualificadas o reconocidas). El DNI electrónico cumple este requisito. En contextos de firma en servidor el concepto equivalente es el de HSM (Hardware Security Module).
- b. Prestador de confianza: Frecuentemente los profesionales tendrán que usar los certificados puestos a su disposición por el organismo del que dependen o por su colegio profesional, por lo que ha de presuponerse que son de confianza. Sin embargo, ciertas herramientas de visualización de ficheros PDF relevantes incluyen una relación de Prestadores de Servicios de Certificación cuya confianza ha sido verificada por el fabricante del software. Cuando la firma se realiza con un certificado emitido por uno de estos PSC, ciertas herramientas de visualización de ficheros PDF relevantes muestran un distintivo verde indicando esta confianza, que no se muestra en otros casos. Por ese motivo, cuando sea posible elegir el Prestador de Servicios de certificación (PSC) será preferible hacerlo entre los reseñados por las herramientas citadas, entre las que cabe destacar Adobe Reader.
- c. Sellado de tiempo: No siendo un requisito derivado directamente de la normativa es muy recomendable configurar la herramienta de firma electrónica para que incluya en las firmas PDF la información del momento en el que se lleva a cabo la firma (incluyendo un servidor de “time stamping” o sellado de tiempo).
- d. Consulta de Revocación: Permite responder a la pregunta ¿cómo conoce el destinatario que la firma se realizó con un certificado no revocado? Siempre que sea posible se configurará la herramienta de firma electrónica para que incluya en las firmas PDF la información de que el certificado usado en la firma electrónica era válido y no revocado (para ello, el certificado utilizado debe incluir cierta información internamente, por lo que se recomienda evitar usar certificados que no la tengan, lo que depende del Prestador de Servicios de Certificación que lo expide). Para ver la información que contiene un certificado puede ser conveniente “exportarlo”.
- e. Firma manuscrita: Se puede mantener la apariencia de la firma manuscrita, configurando la herramienta para que incluya un gráfico al codificar la firma electrónica. Este gráfico podría obtenerse digitalizando una firma manuscrita realizada en papel. Aunque esta apariencia facilita la percepción de la firma del documento para los menos versados, no debe olvidarse que la verdadera firma es la realizada con el respaldo del certificado electrónico y la clave privada asociada.
- f. Rol del firmante y razón de firma: Se recomienda usar cuando sea posible los campos de firma “rol del firmante” y “razón de firma”. En ellos se indicará las

⁴ Además de las tarjetas chip (también denominadas tarjetas inteligentes), se consideran dispositivos seguros de creación de firma electrónica, los denominados “Token” de firma y los HSM (“Hardware Security Module”)

	<p>GUÍA DE INTEROPERABILIDAD Y SEGURIDAD DE AUTENTICACIÓN, CERTIFICADOS Y FIRMA ELECTRÓNICA DEL COMITÉ TÉCNICO ESTATAL DE LA ADMINISTRACIÓN JUDICIAL ELECTRÓNICA</p>	<p>CTEAJE</p>
---	--	---------------

atribuciones de firmante (o su representación) y el sentido que hay que dar a la firma como "aceptación" "suscripción del contenido" "conocimiento de lo firmado" o "tramitación", "certificación", "testimonio" por citar ejemplos.

13.5 Aspectos relativos a la firma electrónica en el plano de las medidas de seguridad.

Los sistemas de firma electrónica deberán cumplir con los requisitos establecidos en el Esquema Nacional de Seguridad, en función del nivel de seguridad requerido, con las particularidades que prevea el Esquema de Seguridad para la Administración de Justicia.

13.6 Aspectos relativos al empleo de sellos de tiempo en el plano de las medidas de seguridad.

Los sellos de tiempo deberán cumplir con los requisitos establecidos en el Esquema Nacional de Seguridad, en función del nivel de seguridad requerido, con las particularidades que prevea el Esquema de Seguridad para la Administración de Justicia.

USO OFICIAL:

TLP: CLEAR

