La Iniciativa Europea para la Normalización de la Firma Electrónica (EESSI[1])

Ana Isabel González-Tablas Ferreres
Grupo de seguridad de las TI
Departamento Informática de la Universidad Carlos III de Madrid
Avda. de la Universidad 30, 28911 Leganés. Madrid. España.
E-mail: aigonzal@inf.uc3m.es

1 Introducción

Hace tres años, el 13 de diciembre de 1999, se aprobó la Directiva 1999/93/CE [CE 1999/93] del Parlamento Europeo y del Consejo, que se publicó en el Diario Oficial de las Comunidades Europeas a fecha de 19 de enero del año 2000. Esta Directiva proporciona un marco comunitario para la firma electrónica con el objetivo principal de proveerla de una validez legal equivalente a la firma manuscrita. El marco se establece mediante la identificación de los requisitos mínimos que deben cumplir los certificados digitales, los prestadores[2] de servicios de certificación (en adelante PSC), y los dispositivos de creación y verificación de firma electrónica.

Tras ello, la Comisión Europea solicitó a los organismos de normalización europeos un análisis de cuáles eran las actividades de normalización necesarias para soportar los requisitos legales establecidos en la Directiva. Este análisis ha derivado en un ambicioso programa de trabajo cuya materialización responderá a las necesidades del mercado, proporcionando las ventajas de una firma electrónica reconocida legalmente que sirva de base al desarrollo de escenarios abiertos de comercio electrónico.

Aunque ya existían varias iniciativas de normalización en esta área bajo los auspicios de organismos de normalización y foros industriales a niveles nacional, regional e internacional, aquellas iniciativas no tenían la suficiente consistencia y coherencia para obtener validez y reconocimiento entre ellas. Para remediar esta situación, el Consejo de

[1] EESSI: European Electronic Signature Standarisation Initiative

[2] Denominados proveedores en la Directiva [CE 1999/93].

Normalización Europeo ICT[3], apoyado por la Comisión Europea, lanzó una nueva iniciativa para reunir a industria, administración, expertos y otros participantes del mercado. Dicha iniciativa es la denominada Iniciativa Europea para la Normalización de la Firma Electrónica, comúnmente conocida por sus siglas: EESSI.

2 La Directiva 1999/93/CE

Sucintamente, los aspectos principales que consagra la Directiva son los siguientes:

- Reconocimiento legal de la firma electrónica.
- Neutralidad tecnológica.
- Establecimiento del libre flujo de productos y servicios de firma.
- Eliminación de autorización o licencia previa para los PSC.
- Obligación de implementar sistemas de supervisión adecuados para los PSC.
- Sistemas de acreditación voluntaria de los PSC.

La Directiva, así mismo, contiene cuatro interesantes anexos en los que se definen diversos requisitos y recomendaciones. Concretamente, estos anexos llevan por título:

- Anexo I: Requisitos de los certificados reconocidos.
- Anexo II: Requisitos de los PSC que expiden certificados reconocidos.
- Anexo III: Requisitos de los dispositivos seguros de creación de firma electrónica.
- Anexo IV: Recomendaciones para la verificación segura de firmas.

3 Misión de la EESSI

Tomando como base lo anterior, la EESSI se fijó los tres objetivos a cumplir que se presentan a continuación. El primero de ellos, analizar las necesidades de estandarización para soportar los requisitos mínimos legales establecidos en la Directiva; el segundo, evaluar los estándares disponibles e iniciativas ya existentes en los planos nacional, europeo e internacional, y finalmente, el tercero (basándose en los resultados de los dos anteriores), establecer e implementar un plan de normalización basado en la cooperación internacional.

[3] ICT (Information and Communications Technologies) Standards Board (http://www.ict.etsi.fr/)

Para cumplir estos objetivos la EESSI estableció un plan de normalización estructurado en cuatro fases:

- Fase 1 (completada en el tercer trimestre de 1999) de definición del programa de trabajo que se desarrollará en el resto de las fases.
- Fase 2 (finalizada en el segundo trimestre del 2002) de establecimiento de los requisitos esenciales para el cumplimiento de la Directiva.
- Fase 3 (de conclusión prevista a finales del 2002) de definición de los requisitos para las diferentes clases de firma electrónica.
- Fase 4 (a desarrollar en el período 2002-2003) de estudio de los requisitos adicionales a los establecidos en las fases previas.

4 Primeros resultados de la EESSI

En julio de 1999, como resultado de la primera fase del plan de normalización, la EESSI entregó un informe final [EESSI99] que contenía una visión de los requisitos para las actividades de normalización y un detallado programa de trabajo para satisfacerlos. Se identificaron tres áreas cruciales en las actividades de normalización. La primera consideraba la especificación y desarrollo de los estándares funcionales y de calidad para los PSC. La segunda, los estándares funcionales y de calidad para los productos de creación y verificación de firmas. Y, por último, la tercera área contemplaba la identificación de los requisitos para la normalización de la interoperabilidad de la firma electrónica.

La EESSI, de momento, se ha centrado en la utilización de la tecnología de infraestructuras de clave pública para soportar la firma electrónica. Las actividades más prioritarias son las siguientes:

- Requisitos de seguridad para los productos de firma.
- Certificación o registro de conformidad de los productos y servicios de firma electrónica.
- Gestión de la seguridad y política de certificación de los PSC que expiden certificados reconocidos.
- Creación y verificación de firmas.

- Sintaxis y formatos de codificación de la firma electrónica, y aspectos técnicos de las políticas de firma.
- Elaboración de un estándar para la utilización de los certificados de clave pública X.509 como certificados reconocidos.
- Desarrollo de un protocolo para obtener la interoperabilidad con las Autoridades de Sellado de Tiempo (en adelante AST).

En el documento [EESSI99] se definen los tres tipos de firma electrónica que se considerarán para desarrollar los estándares. Estas tres clases de firma electrónica son: la "firma electrónica general" (denominada en ocasiones simplemente "firma electrónica"), la "firma electrónica reconocida" y la "firma electrónica mejorada".

Estos tipos derivan de las definiciones de "firma electrónica" y "firma electrónica avanzada" fijadas en la propia Directiva, así como también de los conceptos de "certificado reconocido" y "dispositivo seguro de creación de firma" definidos igualmente en aquella. Específicamente, las definiciones dadas en la Directiva son las que aparecen en cursiva en lo que sigue:

- Firma electrónica. Se define como: *los datos en forma electrónica anejos a otros datos electrónicos o asociados de manera lógica con ellos, utilizados como medio de autenticación* [CE 1999/93]. Tal como se interpreta en el informe final [EESSI99], dentro de esta definición se consideraría cualquier tipo de "autenticación electrónica" mientras la firma esté anexa o asociada lógicamente con los datos que se pretende autenticar. Ejemplos de firma electrónica, tal como se define en la Directiva y en este apartado, serían tanto los datos que se obtienen al utilizar sistemas de autenticación biométrica o los Códigos de Autenticación de Mensajes (MAC).
- Firma electrónica avanzada. Se define como: *la firma electrónica que cumple los requisitos siguientes: (a) estar vinculada al firmante de forma 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* [CE 1999/93].
- Certificado reconocido. Se define como: *el certificado que cumple los requisitos establecidos en el anexo I y es suministrado por un proveedor de servicios de certificación que cumple los requisitos establecidos en el anexo II* [CE 1999/93].

- Dispositivo seguro de creación de firma. Se define como aquel: *dispositivo de creación de firma que cumple con los requisitos enumerados en el anexo III* [CE 1999/93].

A partir de lo anterior, las clases de firma electrónica, ya citadas anteriormente, que se contemplan en el informe final del Equipo de Expertos de la EESSI [EESSI99] son las siguientes:

- Firma electrónica general. Se define como *la firma electrónica requerida en el artículo 5.2 de la Directiva* [EESSI99]. O, de otro modo, es la firma electrónica tal que el documento que la incorpore, por el mero hecho de *presentarse en forma electrónica, o no basarse en un certificado reconocido, o no basarse en un certificado expedido por un proveedor de servicios de certificación acreditado, o no estar creada por un dispositivo seguro de creación de firma* [CE 1999/93], no se le negarán efectos jurídicos, ni será excluida como prueba en juicio.
- Firma electrónica reconocida. Se define como aquella que *cumple los requisitos establecidos en el artículo 5.1 de la Directiva* [EESSI99], es decir, que sea *una firma electrónica avanzada, basada en un certificado reconocido, y creada por un dispositivo seguro de firma* [CE 1999/93]. La firma electrónica reconocida tendrá, respecto de los datos consignados en forma electrónica, el mismo valor jurídico que la firma manuscrita en relación con los consignados en papel, y los documentos que los incorporen serán admisibles como prueba documental en juicio.
- Firma electrónica mejorada. Se define como aquella firma electrónica bien general o bien reconocida, a la que se le aplican ciertas mejoras estandarizadas, que contrarrestan vulnerabilidades comunes reconocidas [EESSI99]. De otro modo dicho, en algunos casos y en algunas aplicaciones, se necesitará un tipo de firma que contemple requisitos técnicos adicionales a los previstos en las dos firmas anteriores, como por ejemplo un sello de tiempo. Este tipo de firma se define para recoger estos casos.

En la tabla siguiente se resumen las distintas clases de firma electrónica consideradas por la EESSI y sus características principales.

Clases de firma	**Firma electrónica general** (como se define en art. 5.2)	**Firma electrónica reconocida** (como se especifica en 5.1 (Anexos I, II, III))	**Firma electrónica mejorada**[4] (aplicable tanto a la firma electrónica general como a la reconocida)
Nivel de	Se le puede otorgar	Se le otorga la misma	Se complementa la

[4] Firma electrónica mejorada es la traducción de los autores de "e*nhanced electronic signature".*

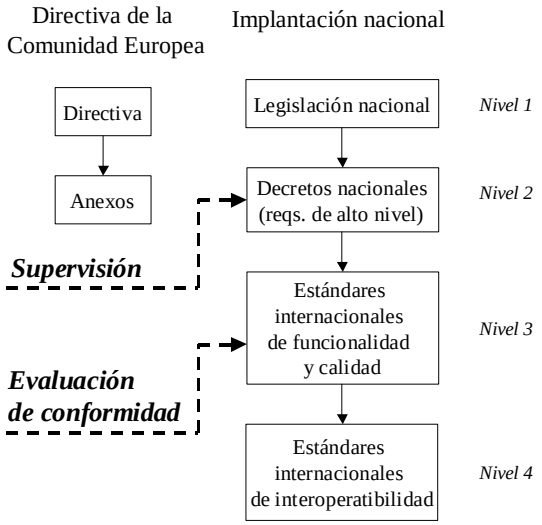
reconocimiento jurídico	eficacia jurídica (art. 5.2)	eficacia jurídica que la firma manuscrita (art. 5.1)	calidad técnica
Explicación:	Cualquier firma electrónica que no cumpla con los requisitos establecidos para las firmas electrónicas reconocidas	Cumple con los requisitos técnicos mínimos para poder equipararse jurídicamente con la firma manuscrita	Se aplican requisitos técnicos adicionales para el verificador de la firma, como sellos de tiempo, pero también para el firmante, para mejorar la seguridad técnica y obtener protección ante ciertas vulnerabilidades.

5 Marco multi-nivel para la normalización y regulación recomendado por la EESSI

En el informe final del Equipo de Expertos de la EESSI [EESSI99], se expone que la implantación en el plano comunitario de la firma electrónica requiere la combinación de un esquema legislativo y un esquema técnico normalizador. Por un lado, en un futuro existirán simultáneamente la Directiva y la legislación nacional introducida en los Estados Miembros para soportar la firma electrónica de acuerdo a la Directiva. Por otro lado, ya existen en el presente una serie de tecnologías y un conjunto de estándares técnicos que se pueden utilizar para implementar las firmas digitales. De este modo, se necesita establecer cuáles son las responsabilidades correspondientes a los cuerpos legislativos y cuáles las correspondientes a los normativos. Así mismo, también se necesita especificar de qué forma la legislación puede referenciar las normas técnicas formalmente. Por estas razones expuestas, el Equipo de Expertos de la EESSI define un marco multi-nivel para llevar a cabo la implantación adecuadamente.

La recomendación de la EESSI es minimizar la legislación de modo que ésta conserve un carácter suficientemente general. El marco básico de implementación podría proporcionarse por estándares técnicos desarrollados y soportados por la industria.

Niveles recomendados por la EESSI
para la normalización y la regulación



En el primer nivel se obtendrían especificaciones independientes tecnológicamente que contendrían requisitos legales generales correspondientes al cuerpo principal de la Directiva. Estas legislaciones estarían fuera del ámbito de responsabilidad de la EESSI.

En el segundo nivel se contemplarían los requisitos de alto nivel considerando el rango de tecnologías que darían soporte a las firmas electrónicas y se definirían los requisitos funcionales básicos de acuerdo a los Anexos de la Directiva. Estos decretos o regulaciones estarían a cargo del organismo de normalización nacional adecuado, y fuera del ámbito de responsabilidad de la EESSI.

En el tercer nivel del marco recomendado por la EESSI, nos encontraríamos con el conjunto de estándares de funcionalidad y calidad que definirán detalladamente para una determinada tecnología los requisitos necesarios que hagan cumplir los requisitos de alto nivel. En este nivel también se situarían los esquemas voluntarios de acreditación, también denominados de certificación, y de evaluación de la conformidad de los productos de firma.

En el cuarto nivel, se considerarían los estándares técnicos internacionales de interoperabilidad que definirán el uso específico de la tecnología para soportar la firma electrónica facilitando la interoperabilidad, primero, entre el firmante y el verificador, segundo, entre el firmante (o verificador) y el dispositivo local, y tercero, entre el firmante (o verificador) y los PSC, y cuarto, entre distintos PSC.

6 Implementación por los organismos ETSI ESI y CEN/ISSS

Los organismos de normalización europeos ETSI[5] y CEN[6] están llevando a cabo la implementación del programa de trabajo de la EESSI, respectivamente con el comité técnico ESI (Firma Electrónica e Infraestructuras[7]) y el grupo de trabajo E-SIGN dentro del ISSS (Sistema de Normalización para la Sociedad de la Información[8]), coordinándose con otros grupos de trabajo u organizaciones cuando así se requiere. El trabajo se supervisa por el Grupo Directivo de la EESSI compuesto por representantes del mercado, incluyendo industrias, prestadores de servicios, usuarios y consumidores, y administraciones públicas nacionales.

El comité técnico ETSI ESI es el principal responsable dentro de la ETSI de las infraestructuras y servicios de seguridad en las telecomunicaciones. Por ello, sus principales intereses se centran en los aspectos de interoperabilidad en las comunicaciones y transacciones, así como los aspectos más relevantes de las relaciones de confianza establecidas entre las partes.

Por su parte, el grupo CEN/ISSS se responsabiliza del trabajo de la EESSI relacionado con los estándares de funcionalidad y calidad de los productos de creación y verificación de firma, así como los relativos a los PSC.

Las áreas de trabajo identificadas y ordenadas por la EESSI por su prioridad se muestran a continuación en la siguiente tabla (se han omitido las áreas consideradas de baja prioridad).

Prioridad	Área de trabajo	Organismo responsable
Urgente	Marco para la firma electrónica reconocida	CEN-ETSI
Urgente	Especificación de los requisitos de seguridad para los sistemas fiables utilizados por los PSC que expidan certificados reconocidos	CEN
Urgente	Especificación de los requisitos de seguridad para los dispositivos físicos utilizados como dispositivos seguros de creación de firma electrónica	CEN

[5] ETSI: European Telecommunications Standards Institute

[6] CEN: Comite Europeen de Normalisation (European Committee for Standardization)

[7] ESI: Electronic Signatures and Infrastructure

[8] ISSS: Information Society Standarization System

Urgente	Uso de los certificados de clave pública X.509 como certificados reconocidos.	IETF [9]y ETSI
Urgente	Certificación/registro de conformidad de los productos y servicios de firma electrónica.	EA[10]
Alta	Gestión de la seguridad y política de certificados para los PSC que expidan certificados reconocidos.	CEN
Alta	Especificaciones y directivas para los productos de creación y verificación de firma electrónica.	CEN
Alta	Sintaxis y formatos de codificación para la firma electrónica.	ETSI
Alta	Aspectos técnicos de las políticas de firma	ETSI
Alta	Pruebas de interoperabilidad entre las normas propuestas.	Usuarios e industria
Alta	Protocolo para interoperar con las ASTs.	IETF
Media	Gestión general de la seguridad de los PSC.	CEN
Media	Gestión de la seguridad y política de certificación para los PSC que emitan sellos de tiempo fiables.	CEN
Media	Normas para los perfiles de CRLs, ARLs, respuestas de OCSPs y sellos de tiempo.	ETSI
Media	Utilización de tarjetas inteligentes para la creación de firmas electrónicas y almacenamiento de otros datos electrónicos relacionados con las PKIs.	ISO/IEC JTC1/SC17 [11]
Media	APIs para obtener independencia de la infraestructura.	Open Group [12]
Media	Definición y soporte de roles genéricos.	ICC[13]
Media	Repositorios para las políticas de firma y/o tipos de contrato.	ICC
Media	Aspectos generales de las políticas de firma.	CEN
Media	Estudios avanzados en distintas áreas.	Industria

Estas actividades se van desarrollando en las distintas fases, como se puede apreciar en las siguientes figuras junto con las entidades a las que hacen referencia.

[9] IETF: Internet Engineering Task Force

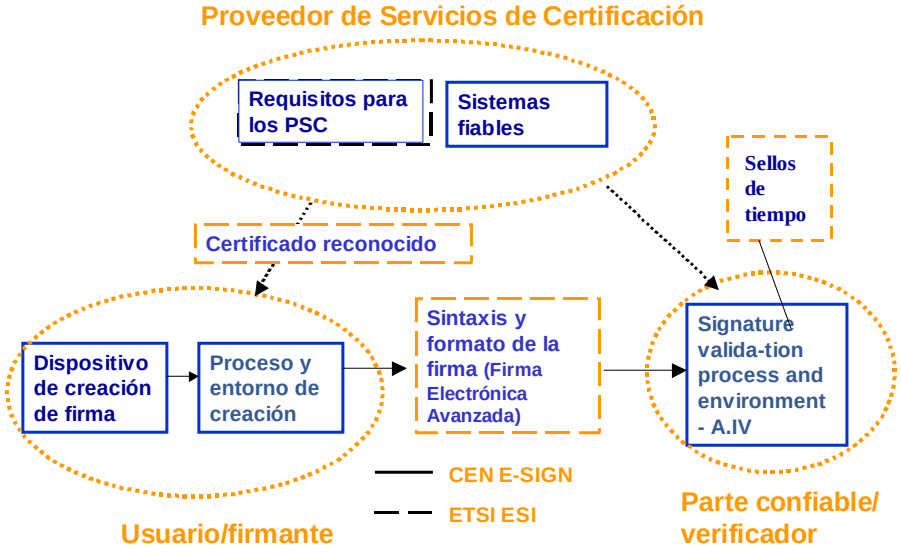
[10] EA: European Co-operation for Accreditation

[11] ISO/IEC JTC1/SC17: International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1/ Subcommittee 17

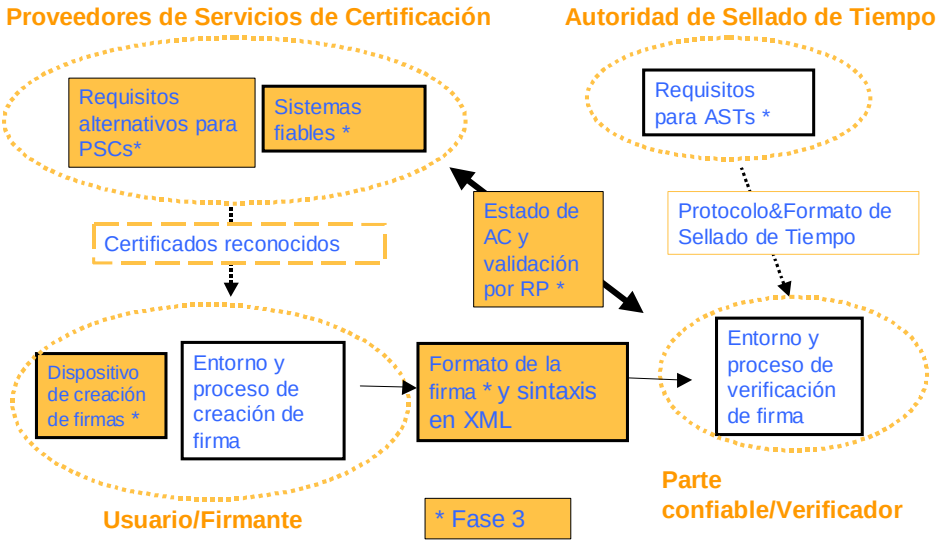
[12] Open Group: http://www.opengroup.org

[13] ICC: International Chamber of Commerce

Fase 2 de los estándares de la EESSI



Fase 3 (2001-2002)



Las nuevas actividades que se planifican para llevar a cabo en el período 2002-2003, correspondiente a la cuarta fase, consideran los siguientes aspectos:

- Mantenimiento de las especificaciones publicadas.
- Armonización de la emisión de información del estado de las AST.
- Internacionalización de las políticas de certificación.
- Estándares técnicos para las políticas de firma.

- Verificación de interoperabilidad de implementaciones de prueba del estándar XAdES en septiembre del 2003.
- Requisitos de la políticas de los PSC que expiden certificados de atributos.
- Propiedades técnicas de la firma electrónica avanzada.
- Requisitos de interoperabilidad de las tarjetas inteligentes para ser utilizadas como dispositivos seguros de creación de firma.
- Evaluación de la conformidad de los dispositivos seguros de creación de firma que soporten firmas electrónicas generales o no reconocidas.
- Emisión de información del estado de los certificados a partes confiables.

El trabajo realizado en las fases llevadas a cabo hasta ahora ha derivado en la publicación de diversas especificaciones e informes técnicos por parte de la ETSI ESI, así como diversos CWA[14] (Acuerdos de Grupos de Trabajo CEN) por parte del CEN/ISSS, que están disponibles públicamente en [CEN/ISSS] y [ETSI ESI].

7 Perspectivas europeas e internacionales

La Comisión ha evaluado los documentos publicados por la EESSI en la segunda fase, para ver si cumplen con los requisitos expuestos en la Directiva. Como resultado de esta evaluación, se ha propuesto una Decisión que considera la aprobación de estas especificaciones como Estándares Generalmente Reconocidos. Esta propuesta fue discutida y ampliamente apoyada en la reunión de los Estados Miembros celebrada en julio de 2002. Así, se prevé la publicación en el Diario Oficial de la Comunidad Europea de un conjunto de referencias a los documentos de la EESSI para que así pueda establecerse el marco técnico adecuado que permita la implantación plena de la Directiva.

En el marco supracomunitario, se está trabajando principalmente en tres áreas. La primera es el reconocimiento de la conformidad de los requisitos de dispositivos seguros de creación de firma según un CC-MRA[15], y se pretende realizar el mismo trabajo para los sistemas fiables. La segunda área contempla el reconocimiento mutuo de políticas de certificación, evaluando la posible trasposición de los requisitos desarrollados por la ETSI-EESSI y los de la infraestructura de clave pública federal de Estados Unidos. Por

[14] CWAs: *CEN Workshop Agreements*

[15] CC-MRA: *Common Criteria – Mutual Recognition Arrangement*

último, se pretende realizar un gran esfuerzo en la armonización de los estándares de interoperabilidad.

Referencias

[CEN/ISSS] Página Web de CEN/ISSS. http://www.cenorm.be/isss/Workshop/e-sign/Default.htm

[CE 1999/93] 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. http://europa.eu.int/information_society/eeurope/action_plan/pdf/esignatures_es.pdf

[EESSI] Página Web de EESSI. http://www.ict.etsi.fr/eessi/EESSI-homepage.htm

[EESSI99] EESSI 1999. Final Report of the EESSI Expert Team. 20th July 1999. http://www.ict.etsi.fr/eessi/Documents/Final-Report.pdf

[ETSI ESI] Página Web de ETSI ESI. http://portal.etsi.org/esi/el-sign.asp

Acrónimos

AST	Autoridades de Sellado de Tiempo
CC-MRA	Common Criteria – Mutual Recognition Arrangement
CEN	Comite Europeen de Normalisation (European Committee for Standardization)
CWA	CEN Workshop Agreements
EA	European Co-operation for Accreditation (European community bodies)
EESSI	European Electronic Signature Standardisation Initiative
ESI	Electronic Signatures and Infrastructure
ETSI	European Telecommunications Standards Institute
ICC	International Chamber of Commerce
ICT	Information and Communications Technologies
IETF	Internet Engineering Task Force
ISO/IEC JTC1/SC17	International Organization for Standardization/International Electrotechnical Commission Joint Technical Committee 1/ Subcommittee 17
ISSS	Information Society Standardization System
MAC	Message Authentication Code
PKI	Public Key Infrastructure
PSC	Proveedores de Servicios de Certificación
XAdES	XML Advanced Electronic Signatures