norma española

UNE-ETSI/TS 101733 V1.2.2

Febrero 2011

TÍTULO

Formatos de firma electrónica

Electronic signature formats.

CORRESPONDENCIA

Esta norma es la versión oficial, en español, de la Especificación Técnica ETSI TS 101 733 V1.2.2:2000.

OBSERVACIONES

ANTECEDENTES

Esta norma ha sido elaborada por el comité técnico AEN/CTN 133 *Telecomunicaciones* cuya Secretaría desempeña AENOR.

Editada e impresa por AENOR
Depósito legal: M 7448:2011

LAS OBSERVACIONES A ESTE DOCUMENTO HAN DE DIRIGIRSE A:
AENOR Asociación Española de Normalización y Certificación
Génova, 6
28004 MADRID-España
info@aenor.es
www.aenor.es
Tel.: 902 102 201
Fax: 913 104 032

105 Páginas

Grupo 57

ÍNDICE

Página

1 OBJETO Y CAMPO DE APLICACIÓN

Este documento define una firma electrónica que permanece válida durante largos períodos de tiempo. Esto incluye evidencia de su validez incluso si la parte signataria o verificadora intenta más tarde negar (repudiar) la validez de la firma.

Este documento especifica el uso de proveedores de servicio fiables (por ejemplo, Autoridades de fechado electrónico), y los datos que necesitan archivarse (por ejemplo, certificados cruzados y listas de revocación) para cumplir con los requisitos de las firmas electrónicas de larga duración. Una firma electrónica definida en este documento puede usarse para arbitrar en caso de disputa entre el signatario y el verificador, lo que puede ocurrir en cualquier momento, incluso años después. Este documento usa una política de firmas, referenciada por el signatario, como base para establecer la validez de una firma electrónica.

Este documento está basado en el uso de la criptografía de clave pública para producir firmas digitales, soportadas por los certificados de clave pública.

Este documento especifica también el empleo de los servicios de fechado electrónico para probar la validez de una firma largo tiempo después del periodo de vida útil normal de los elementos críticos de una firma electrónica y para soportar el no repudio. También, como opción, define el empleo de fechados electrónicos adicionales para proporcionar protección a muy largo plazo contra el compromiso de claves o la debilidad de los algoritmos.

Este documento se construye sobre normas existentes que están ampliamente adoptadas. Éstas incluyen:

- RFC 2630 [8] “Sintaxis de Mensaje Criptográfico (CMS)”;
- Recomendación X.509 de la UIT-T [1]: “Tecnología de la información. Interconexión de sistemas abiertos. El Direcorio: Marcos para autenticación”;
- RFC 2459 [6] “Certificado de infraestructura de claves públicas (PKIX) Internet X.509 [23] y perfil CRL”;
- Borrador del IETF Protocolo de fechado electrónico (TPS) (para ser publicado) (véase la bibliografía).

NOTA: Véase el capítulo 2 para una lista completa de normas para consulta.

Este documento incluye:

- formato de testigos de Firma Electrónica;
- formato de las Políticas de Firma.

Además, este documento identifica otros documentos que definen el formato para los Certificados de Clave Pública, los Certificados de Atributo, las Listas de Revocación de Certificados y los protocolos de apoyo. Incluye protocolos para usar por terceras partes de confianza para apoyar la operación de la creación y la validación de la firma electrónica, así como la gestión de los certificados usados para soportar las firmas electrónicas.

Los anexos informativos incluyen:

- un contenido estructurado de ejemplo;
- la relación entre este documento y la directiva sobre firma electrónica y las iniciativas de normalización asociadas;
- API para soportar la generación y la verificación de las firmas electrónicas;
- algoritmos criptográficos que se pueden usar;
- guía de nombres.

2 NORMAS PARA CONSULTA

Los siguientes documentos contienen cláusulas que, a través de su referencia en este texto, constituyen provisiones para este documento.

- Las referencias son específicas (identificadas por la fecha de publicación y/o el número de edición o el número de versión, etc.) o no específicas.
- Para una referencia específica no se aplican las revisiones posteriores.

- Para una referencia no específica, se aplica la última versión.

[1] Recomendación X.509 (1997) de la UIT-T | ISO/IEC 9594-8: "Tecnología de la Información. Interconexión de Sistemas Abiertos. El Directorio: Marco para autenticación".

[2] Recomendación X.208 (1998) de la UIT-T: "Especificación de la Notación de Sintáxis Abstracta Uno (ASN.1)".

[3] Recomendación X.690 (1997) de la UIT-T | ISO/IEC 8825-1: "Tecnología de la Información. Reglas de codificación ASN. 1. Especificación de las reglas de codificación básica (BER), de las reglas de codificación canónica (CER) y de las reglas de codificación distinguida (DER)".

[4] Recomendación F.1 (1998) de la UIT-T: "Disposiciones relativas a la explotación del servicio público internacional de telegramas".

[5] RFC 1777(1995): "Protocolo ligero de acceso a directorios".

[6] RFC 2459 (1999): "Certificado de infraestructura de claves públicas Internet X.509 y perfil CRL".

[7] RFC 2560 (1999): "Protocolo en línea del estado de certificado de infraestructuras de clave pública Internet X.509. OCSP".

[8] RFC 2630 (1999): "Sintaxis de Mensaje Criptográfico".

[9] RFC 2634 (1999): "Servicios de seguridad mejorada para S/MIME".

[10] ISO 7498-2 (1989): "Sistemas de procesado de la información. Interconexión de sistemas abiertos. Modelo básico de Referencia. Parte 2: Arquitectura de seguridad".

[11] ISO/IEC 13888-1 (1997): "Tecnología de la información. Técnicas de seguridad. No repudio. Parte 1: Generalidades".

[12] Recomendación X.400 (1996) de la UIT-T: "Visión de conjunto del sistema y del servicio de tratamiento de mensajes".

[13] Recomendación X.500(1997) de la UIT-T: "Tecnología de la Información. Interconexión de sistemas abiertos. El Directorio: Visión de conjunto de conceptos, modelos y servicios".

[14] Recomendación X.501 (1997) de la UIT-T: "Tecnología de la Información. Interconexión de sistemas abiertos. El Directorio: Modelos".

[15] Recomendación X.520 (1997) de la UIT-T: "Tecnología de la Información. Interconexión de sistemas abiertos. El Directorio: Tipos de atributos seleccionados".

[16] RFC 2559 (1999): "Protocolos de operación de infraestructura de claves públicas Internet X.509 – LDAPv2".

[17] RFC 2587 (1999): "Esquema LDAPv2 de infraestructura de claves públicas Internet X.509".

[18] RFC 2510 (1999): "Protolocos de gestión de certificado de infraestructura de claves públicas Internet X.509".

[19] RFC 2450 (1998): "Reglas de asignación TLA y NLA propuestas".

[20] RFC 2045 (1996): "Extensiones del correo internet multipropósito (MIME). Parte 1: Formato del cuerpo de los mensajes de internet".

[21] RFC 2078 (1997): "Generic Security Service Application Program Interface, Version 2".

[22] RFC 2511 (1999): "Internet X.509 Certificate Request Message Format".

[23] Recomendación X.509 (2000) de la UIT-T: "Tecnología de la Información. Interconexión de sistemas abiertos. El Directorio: Marcos para certificados de claves públicas y atributos".

[24] Recomendación X.680 (1997) de la UIT-T: "Tecnología de la Información. Notación de sintaxis abstracta uno (ASN.1). Especificación de la notación básica".