

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.

EXTRACTO DEL DOCUMENTO UNE-ETSI/TS 101733 V1.2.2

ÍNDICE

	Página
DERECHOS DE PROPIEDAD INTELECTUAL	8
PRÓLOGO	8
INTRODUCCIÓN	9
1 OBJETO Y CAMPO DE APLICACIÓN	9
2 NORMAS PARA CONSULTA	10
3 DEFINICIONES Y ABREVIATURAS	11
3.1 Definiciones	11
3.2 Abreviaturas	12
4 DESCRIPCIÓN GENERAL	13
4.1 Partes principales	13
4.2 Firmas electrónicas y datos de validación	14
4.3 Tipos de datos de validación.....	15
4.4 Tipos extendidos de datos de validación.....	17
4.5 Datos de validación de archivo.....	19
4.6 Arbitraje.....	19
4.7 Proceso de validación	20
4.8 Ejemplo de secuencia de validación	20
4.9 Características opcionales adicionales de una ES.....	25
5 DESCRIPCIÓN GENERAL	25
5.1 La política de firma	25
5.2 Información firmada.....	26
5.3 Componentes de una firma electrónica	26
5.3.1 Referencia a la Política de firma	26
5.3.2 Indicación del tipo de compromiso	27
5.3.3 Identificador del certificado del signatario	27
5.3.4 Atributos de Cargo.....	28
5.3.4.1 Cargo alegado	28
5.3.4.2 Cargo certificado	29
5.3.5 Localización del signatario	29
5.3.6 Momento de la firma.....	29
5.3.7 Formato del Contenido	30
5.4 Componentes de los Datos de Validación.....	30
5.4.1 Información del Estado de Revocación	30
5.4.2 Información CRL	30
5.4.3 Información OCSP	31
5.4.4 Camino de la certificación	31
5.4.5 Fechado electrónico para una firma de larga validez	31
5.4.6 Fechado electrónico para la larga validez de las firmas antes de que se comprometan las claves de la CA	32
5.4.6.1 Fechado electrónico de la ES con Datos de Validación Completa.....	33
5.4.6.2 Certificados de fechado electrónico y referencias de la información de revocación.....	33
5.4.7 Fechado electrónico para larga duración de la firma	34
5.4.8 Referencia a datos adicionales.....	34
5.4.9 Fechado electrónico para el reconocimiento mutuo	34
5.4.10 Compromiso de clave TSA	35
5.5 Firmas múltiples.....	35
6 POLÍTICA DE FIRMA Y POLÍTICA DE VALIDACIÓN DE FIRMA	35
6.1 Identificación de la política de firma	37
6.2 Información general de la política de firma	37

6.3	Tipos de compromisos reconocidos.....	38
6.4	Reglas para el Uso de Autoridades de certificación	38
6.4.1	Puntos de confianza.....	38
6.4.2	Trayecto de certificación.....	39
6.5	Reglas de revocación	39
6.6	Reglas para el uso de cargos.....	40
6.6.1	Valores de atributo.....	40
6.6.2	Puntos de confianza para los Atributos certificados	40
6.6.3	Trayecto de certificación para los atributos certificados	40
6.7	Reglas para el uso de fechado electrónico y de temporización	40
6.7.1	Puntos de confianza y trayectos de certificado	40
6.7.2	Nombres de autoridad de fechado electrónico.....	41
6.7.3	Restricciones de temporización. Periodo de cautela.....	41
6.7.4	Restricciones de temporización. Retardo del fechado electrónico	41
6.8	Reglas que se han de seguir para los datos de verificación.....	41
6.9	Reglas para restricciones de algoritmo y longitudes de clave.....	41
6.10	Otras reglas de política de firma	41
6.11	Protección de la política de firma.....	42
7	IDENTIFICADORES Y CARGOS	42
7.1	Formatos de nombre del signatario	42
7.2	Formatos de nombre TSP.....	42
7.3	Cargos y atributos del signatario	42
8	ESTRUCTURA DE DATOS DE UNA FIRMA ELECTRÓNICA	43
8.1	Sintaxis general.....	43
8.2	Tipo del contenido de los datos.....	43
8.3	Tipo del contenido de los datos firmados	43
8.4	Tipo SignedData	43
8.5	Tipo EncapsulatedContentInfo	43
8.6	Tipo SignerInfo.....	44
8.6.1	Proceso de cálculo de la elaboración del mensaje.....	44
8.6.2	Proceso de generación de la firma del mensaje.....	44
8.6.3	Proceso de verificación de la firma del mensaje	44
8.7	Atributos CMS presentes obligatorios importados	44
8.7.1	Tipo de contenido	44
8.7.2	Elaboración del mensaje	44
8.7.3	Momento de la firma.....	44
8.8	Atributos de certificado de firma alternativos.....	45
8.8.1	Definición de atributo de certificado de firma ESS.....	45
8.8.2	Definición del atributo de otro certificado de firma.....	45
8.9	Atributos obligatorios adicionales.....	46
8.9.1	Identificador de la política de firma	46
8.10	Atributos CMS importados opcionales.....	47
8.10.1	Firma de refrendo	47
8.11	Atributos ESS importados opcionales	47
8.11.1	Atributo de referencia del contenido firmado.....	47
8.11.2	Atributo identificador del contenido	48
8.11.3	Atributo de indicación del contenido.....	48
8.12	Atributos opcionales adicionales	48
8.12.1	Atributo de indicación del tipo de compromiso	48
8.12.2	Localización del signatario	50
8.12.3	Atributos de signatario	50
8.12.4	Fecha electrónico del contenido	51
8.13	Soporte para firmas múltiples.....	51
8.13.1	Firmas independientes	51
8.13.2	Firmas incorporadas	51

9	DATOS DE VALIDACIÓN	51
9.1	Firma electrónica con fechado electrónico.....	52
9.1.1	Definición del atributo de fechado electrónico de la firma	52
9.2	Datos de validación completa	53
9.2.1	Definición del atributo de las referencias de certificado completo.....	53
9.2.2	Definición de atributo de referencias de revocación completa	54
9.3	Datos de validación extendida	55
9.3.1	Definición del atributo de valores de certificado	55
9.3.2	Definición del atributo de valores de revocación	55
9.3.3	Definición del atributo de fechado electrónico de la ES-C.....	56
9.3.4	Definición de atributo de certificados con fechado electrónico y CRL.....	56
9.4	Datos de validación de archivo.....	56
9.4.1	Definición del atributo de fechado electrónico de archivo.....	57
10	OTRAS ESTRUCTURAS DE DATOS NORMALIZADAS	57
10.1	Formato del certificado de clave pública.....	57
10.2	Formato de lista de revocación de certificado.....	58
10.3	Formato de respuesta OCSP	58
10.4	Formato de testigo de fechado electrónico	58
10.5	Formatos de nombre y de atributos.....	58
10.6	Certificado de atributo.....	58
11	ESPECIFICACIÓN DE LA POLÍTICA DE FIRMA.....	58
11.1	Estructura ASN.1 global.....	59
11.2	Política de validación de firma	59
11.3	Reglas comunes.....	60
11.4	Reglas de compromiso.....	60
11.5	Reglas de signatario y de verificador.....	61
11.5.1	Reglas del signatario	61
11.5.2	Reglas del verificador.....	62
11.6	Requisito de Certificado y de revocación	62
11.6.1	Requisitos de certificado	62
11.6.2	Requisitos de revocación.....	63
11.7	Condiciones de confianza del certificado de firma	64
11.8	Condiciones de confianza del fechado electrónico.....	64
11.9	Condiciones de confianza de atributo.....	65
11.10	Restricciones de algoritmo.....	66
11.11	Extensiones de la política de firma.....	66
12	PROTOCOLOS DE DATOS PARA INTEROPERAR CON LOS TSP	66
12.1	Protocolos operacionales.....	66
12.1.1	Recuperación del certificado	67
12.1.2	Recuperación de la CRL.....	67
12.1.3	Estado del certificado en línea.....	67
12.1.4	Fechado electrónico.....	67
12.2	Protocolos de gestión	67
12.2.1	Petición de certificado.....	67
12.2.2	Distribución del certificado al signatario	67
12.2.3	Petición para revocación de certificado.....	67
13	CONSIDERACIONES DE SEGURIDAD	67
13.1	Protección de la clave privada.....	67
13.2	Elección de los algoritmos.....	68
14	REQUISITOS DE CONFORMIDAD	68
14.1	Signatario	68
14.2	Verificador que usa fechado electrónico	68
14.3	Verificador que usa registros de seguridad.....	69
14.4	Política de firma	69

ANEXO A (Normativo) DEFINICIONES ASN.1.....	70
A.1 Definiciones del formato de firma usando la sintaxis ASN.1 según la Recomendación X.208 (1988).....	70
A.2 Definiciones de políticas de firma usando la sintaxis ASN.1 según la Recomendación X.208 (1988).....	75
A.3 Definiciones del formato de firma usando la sintaxis ASN.1 según la Recomendación X.680 (1997).....	78
A.4 Definiciones de política de firma usando la sintaxis ASN.1 según la Recomendación X.680 (1997).....	83
ANEXO B (Informativo) EJEMPLO DE CONTENIDOS ESTRUCTURADOS Y MIME	88
B.1 Descripción general	88
B.2 Información de cabecera.....	88
B.3 Codificación del contenido.....	89
B.4 Contenido multiparte	89
B.5 S/MIME.....	90
ANEXO C (Informativo) RELACIONES ENTRE LA DIRECTIVA EUROPEA Y LA EESSI .	92
C.1 Introducción.....	92
C.2 Firmas electrónicas y la Directiva.....	92
C.3 Formatos de firma electrónica del ETSI y la Directiva.....	92
C.4 Normas EESSI y Clases de firma electrónica	93
C.4.1 Estructura de la normalización EESSI.....	93
C.4.2 Clases de firmas electrónicas	93
C.4.3 Clases EESSI y el formato de firma electrónica del ETSI	93
ANEXO D (Informativo) API PARA LA GENERACIÓN Y PARA LA VERIFICACIÓN DE LOS TESTIGOS DE FIRMAS ELECTRÓNICAS	94
D.1 Estructura de los datos.....	94
D.2 IDUP-GSS-API definidas por el IEFT.....	95
D.3 Interfaces de seguridad CORBA definidas por el OMG.....	96
ANEXO E (Informativo) ALGORITMOS CRIPTOGRÁFICOS	97
E.1 Algoritmos de elaboración	97
E.1.1 SHA-1	97
E.1.2 MD5	97
E.1.3 General	97
E.2 Algoritmos de firma digital	98
E.2.1 DSA.....	98
E.2.2 RSA.....	98
E.2.3 General	98
ANEXO F (Informativo) GUÍA SOBRE LOS NOMBRES.....	100
F.1 Asignación de nombres	100
F.2 Facilitación de acceso a la información de registro	100
F.3 Esquemas de nombres.....	101
F.3.1 Esquemas de nombres para ciudadanos individuales	101
F.3.2 Esquemas de nombres para los empleados de una organización	101
BIBLIOGRAFÍA.....	102
HISTORIA.....	105

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 Directorio: 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): "Protocolos 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".