

Documentación no Incluida

La siguiente es una lista de formatos de firma digital y sus respectivos URL's para ser accedidos:

X.509. Sintaxis de Certificados (grupo de Normas de Directorio X.500)

Es un X.509 UIT-T (Sector de Normalización de las Telecomunicaciones de la UIT) para la PKI (Infraestructura de Clave Pública), en la criptografía, que, entre muchas otras cosas, define los formatos específicos para PKC (certificados de clave pública) y el algoritmo que comprueba un certificado ruta es válida en virtud de dar una PKI (llamado el algoritmo de ruta de certificación de validación).

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=X.509&sa=Search#949

X.520. Formatos y sintaxis de los campos (grupo de Normas de Directorio X.500)

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=X.520&sa=Search#948

X.680. | ISO/IEC 8824-1:2002), ASN1 Abstract Syntax Notation One.

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=X.680&sa=Search#1044

X.690 ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER), 1997.

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=X.690&sa=Search#1059

RFC

RFC 2459. Perfil de certificado de Internet

Esta especificación es una parte de una familia de normas para el X.509

Infraestructura de clave pública (PKI) para la Internet. Esta especificación

Es un documento independiente; implementaciones de esta norma puede

Proceder independiente de las otras partes.

Esta especificación de los perfiles de formato y la semántica de los certificados

Y las listas de revocación de certificados PKI para Internet. Procedimientos

Se describen a la transformación de la certificación caminos en la Internet

Medio ambiente. Codificación de las normas se refieren a un popular criptográficas

Algoritmos. Por último, los módulos ASN.1 se proporcionan en los apéndices

Para todas las estructuras de datos definidas o de referencia.

La especificación describe los requisitos que inspiran la

Creación de este documento, y de los supuestos que afecten a su ámbito de aplicación

En la Sección 2. La sección 3 presenta un modelo de arquitectura y

Describe su relación con la anterior IETF y la ISO / IEC / ITU Normas. En particular, la relación de este documento con la IETF PEM y especificaciones de la ISO / CEI / UIT X.509 documentos se describen.

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=RFC+2459&sa=Search#946

RFC 3739. Perfil de certificado para certificados reconocidos (cualificados)

Esta especificación es una parte de una familia de normas para la X.509 Infraestructura de Clave Pública (PKI) para la Internet. Se basa en [X.509] y [RFC 3280], que define los formatos de certificado subyacente y la semántica necesaria para una plena aplicación de esta norma.

Este perfil incluye mecanismos específicos destinados a ser utilizados con certificados cualificados.

http://www.itu.int/net/itu_search/index.aspx?cx=001276825495132238663%3Anqzm45z846q&cof=FORID%3A9&ie=UTF-8&q=RFC+3739&sa=Search#457

RFC 5126. CMS Advanced Electronic Signatures (CADES)

<http://www.imc.org/ietf-smime/mail-archive/>

TS

TS 101 456. Requisitos de política para PSC que expiden certificados reconocidos

TS 101 733. v1.5.1 December 2003 Formatos de firma electrónica

TS 101 903 v1.2.2 April 2004 Firmas Electrónicas Avanzadas en XML (XML Advanced Electronic Signatures - XAdES)

TS 101 861. Perfil de sello de tiempo

TS 101 862. v1.3.1 March 2004 Perfil de certificado reconocido

TS 102 023. Requisitos de política para Prestadores de Servicios de Sellado de fecha y hora

TS 102 042. v1.2.1 May 2005. Requisitos de política para PSC que expiden certificados de clave pública

TR 102 040 v1.3.1 March 2005 Armonización Internacional de Requisitos de política para PSC que expiden certificados

TR 102 047 v1.2.1 March 2005 Armonización Internacional de Formatos de firma electrónica

TS 102 280 March 2004 X.509 V.3 Perfil de Certificado para certificados emitidos a Personas físicas.

TR 102 272 December 2003 V 1.1.1 ANS.1 format for signature policies

Todas las anteriores se pueden bajar en la siguiente dirección:

<http://pda.etsi.org/pda/queryform.asp>

CWA

CWA 15579. e-Invoices and digital signatures

CWA 14167-1 “Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures”

CWA 14167-2 “Security of cryptographic modules”

CWA 14167-3 “ Cryptographic Module for CSP Key Generation Services – Protection Profile

CMCKG-PP

CWA 14168 “Security Requirements for Secure Signature Creation Devices” EAL4

CWA 14169 ““Security Requirements for Secure Signature Creation Devices” EAL4+”

CWA 14170 “Security Requirements for Secure Signature Creation Systems”

CWA 14171 “Procedures for Electronic Signature Verification”

CWA 14172- 1 to 8 “Conformity Assessment Guidances for Trustworthy Systems”

CWA 14890-1/2 Application Interface for smart cards used as Secure Signature Creation Devices

CWA 14365-1/2 Guide on the Use of Electronic Signatures

CWA 14355 Guidelines for the implementation of Secure Signature Creation Devices

La documentación anterior puede ser ubicada en la dirección:

http://www.cen.eu/CENORM/BusinessDomains/BusinessDomains/ISSS/cen+workshop+agreements/cwa_listing.asp

DSS

DSS Defining an XML interface to process digital signatures for Web services and other applications

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss

DSS-X Advancing digital signature services standards for XML

http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=dss-x

ISO

ISO 26300 Estandard ISO para Open Office

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=43485

ISO 29500 Estandard ISO para Microsoft Office, formato XML

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51463

ISO 32000-1 Estandard ISO para Adobe Portable Document Format (PDF)

http://www.iso.org/iso/iso_catalogue/catalogue_tc/catalogue_detail.htm?csnumber=51502

INTERACTIVA

