Contents

Práctica 4: Firma electrónica

Objetivos

- Ser capaz de firmar documentos con validez legal
- Ser capaz comprobar la firma de documentos

Enunciado

Se trata de que el estudiante sea capaz de generar documentos firmados electrónicamente. La ley 59/2003, de 19 de diciembre, de firma electrónica (B.O.E. 20.11.2003), regula el uso de la firma electrónica. La ley 11/2007, de 22 de junio, de acceso electrónico de los ciudadanos a los Servicios Públicos, reconoce el derecho de los ciudadanos a relacionarse con las Administraciones Públicas por medios electrónicos.

Existen distintos formatos que posibilitan que una firma electrónica pueda ser verificada a largo plazo (de forma indefinida) con plenas garantías jurídicas: AdES-T, AdES–C, AdES X.

En esta práctica se trata de diferenciar entre: la firma electrónica básica, la firma electrónica avanzada, la firma electrónica reconocida. Encontrar la definición y descripción de cada una. De describir los distintos formatos de firma electrónica avanzada (AdES: Advanced Electronic Signature), entre ellos AdES-BES (Basic), AdES-T (timestamp) y AdES-C (complete). Por último trabajar con alguna aplicación para generarlas y/o verificarlas.

Hacer un estudio comparativo de las siguientes alternativas:

- Xolido (http://www.xolido.com/)

- Autofirma (https://firmaelectronica.gob.es/Home/Descargas.html)

Referencias:

- AdES: Firma electrónica avanzada. (Advanced Electronic Signature) http://www.cert.fnmt.es/content/pages_std/docs/Firmas_longevas.pdf
- Publicación del Minusterio de Industria Turismo y Comercio. https://www.mincotur.gob.es/Publicaciones/Publicacionesperiodicas/EconomiaIndustrial/RevistaEcono

XolidoSign

Software que, entre otras funcionalidades, permite comprobar firmas con independencia del certificado electrónico empleado.

Aplicación de Escritorio

MANUAL de XolidoSign

VALIDe

Servicio de validación y demostrador de firma electrónica dependiente el Ministerio de Presidencia del Gobierno de España. Página on-line de validación de:

- Certificados electrónicos
- Sedes electrónicas
- Firmas

Analizar la potencialidad de esta herramientas respecto a la validez legal de la firma que generan, puesta en marcha, incidencia sobre la empresa,...

Acrobat de Adobe Systems

Ciertas aplicaciones permiten generar documentos que incorporan firmas y/o comprobar las firmas incorporadas en dichos documentos. Entre dichas aplicaciones se encuentra Acrobat de Adobe systems. Se puede consultar la referencia , el manual de ayuda de Acrobat u otras referencias para ver cómo hacerlo. Puede realizarse con la version de visualización (reader) o con la versión PROFESIONAL.

(Opcional 1) Generar y comprobar una firma PGP.

También podemos generar y validar firmas digitales con aplicaciones netamente criptográficas como GnuPG. Se trata de verificar la firma del paquete "openssl-1.1.1.tar.gz" que contiene el código fuente y se encuentra en https://www.openssl.org/source/.

(Opcional 2) Firmar mensajes y comprobar firmas usando claves de criptomonedas

La base de funcionamiento de las denominadas criptomonedas, como Bitcoin, es la criptografía. La confianza en "la cadena de bloques" se basa en la firma de transacciones. Se puede usar una clave privada bitcoin para firmar un mensaje y la clave pública correspondiente para validar/comprobar la validez de la firma. En "how to sign a message with bitcoin private key" https://steemit.com/bitcoin/[@bitsignal/how-to-sign-a-bitcoin-message-using-your-private-key] nos indican cómo, y también podemos acceder al software en el repositorio github.

Se generará un informe que documente la actividad realizada para las tareas encomendadas. El informe deberá ir en formato pdf y estará firmado con una firma visible realizada usando el Certificado X.509 personal del estudiante generado en la práctica 3. El informe junto a otros posibles documentos (Certificado del firmante, de la Autoridad, …) se empaquetarán en un zip que se subirá a la plataforma.

Enunciado de la práctica en fichero pdf firmado digitalmente por Angel Luis Sánchez Lázaro haciendo uso de un Certificado de clave pública firmado por la Autoridad FNMT. Este documento puede servir de ejemplo de como debe quedar el informe que debe presentar el alumnos.

Condiciones de entrega

Práctica opcional

Entregar un fichero llamado firmaLegal.zip que contendrá el informe realizado en formato PDF (en el informe debe aparecer el nombre de los autores) y cuantos ficheros hayan sido necesarios para la realización de esta práctica. El fichero PDF deberá estar firmado digitalmente[1] con firma visible en la primera página.

Fecha límite de entrega: 27-noviembre-2020 Hora límite de entrega: 23:59

[1] https://www.sede.fnmt.gob.es/documents/10445900/10528353/Firmar_documento_PDF_Adobe_Acrobat_Reader_DC.pdf

Criterios para la formación de equipos

Número máximo de participantes: 2 Periodo de formación de los equipos: Desde el 18-noviembre-2020 hasta el 27-noviembre-2020