Sinatura electrónica en entornos libres

3º Ciclo Sábados Libres na Altamar

José María Casanova Crespo (@txenoo)

jmcasanova@igalia.com

11 Abril 2015

C9FC 273B E9BE 5464 0BAA 8F97 9C19 DB3C 039A CDF0

http://piratepad.net/AltamarSeguridade

contidos

Que é a sinatura dixital?

A sinatura dixital permítenos identificarnos a través de Internet da mesma forma que a nosa sinatura manuscrita nos identifica nos actos documentais fora da contorna dixital.

A sinatura dixital actualmente baséase no cifrado asimétrico e a existencia dun par de clave pública e clave cifrada.

Marco Lexislativo

A sinatura electrónica en España ten o soporte xurídico da **Lei Orgánica 59/2003**, de 19 de decembro de 2003, de sinatura electrónica.

A lei regula a validez xurídica da sinatura dixital, os **certificados electrónicos**, as entidades certificadoras, como se crea e verifica a sinatura.

A lei non fai referencia a tecnoloxías específicas, pero si os requirimentos.

Definición de e-sinatura

Segundo a Lei a **Sinatura electrónica** é o conxunto de datos en forma electrónica consignados xunto a outros ou asociados con eles, que poden ser empregados como medio de identificación do asinante.

Sinatura electrónica avanzada

A Sinatura electrónica avanzada é a sinatura electrónica que permite identificar ao asinante e detectar calquera cambio ulterior dos datos asinados, que está vinculada ao asinante de xeito único e aos datos aos que se refire e que foi creada por medios que o asinante pode manter baixo o seu exclusivo control.

Sinatura electrónica recoñecida

Considerase **Sinatura electrónica recoñecida** á sinatura electrónica avanzada baseada nun certificado recoñecido e xerada mediante un dispositivo seguro de creación de sinatura.

A **sinatura electrónica recoñecida** terá respecto dos datos consignados en forma electrónica o **mesmo valor que a sinatura manuscrita** en relación cos consignados en papel.

O Certificado dixital

Un certificado dixital é un documento asinado electronicamente por un prestador de servizos de certificación que vincula uns datos de verificación de firma a un asinante e confirma a súa identidade.

Son **certificados recoñecidos** os certificados electrónicos expedidos por un prestador de servizos de certificación que cumpra os requirimentos establecidos na lei en canto á **comprobación da identidade** e demais circunstancias dos solicitante e á fiabilidade e as garantías dos servizos de certificación que presten.

O DNI electrónico

O DNI electrónico é o documento nacional de identidade que **acredita electronicamente a identidade** persoal do seu titular e **permite a sinatura electrónica** de documentos.

Todas as persoas físicas ou xurídicas, públicas ou privadas, **recoñecerán a eficacia do DNI electrónico** para acreditar a **identidade** e os demais datos persoais dun titular que consten no mesmo, e para acreditar a **identidade do asinante** e a **integridade dos documentos asinados** cos dispositivos de sinatura electrónica nel incluídos.

Creación da sinatura electrónica

Un dispositivo seguro de creación de sinatura é un programa informático que ofrece, como mínimo, as seguintes garantías:

1. Que os datos empregados para a xeración da sinatura poden producirse unha única vez e se asegura de forma razoable o seu segredo.
2. Que existe unha seguridade razoable de que os datos empregados para a xeración da sinatura non poden ser derivados dos de verificación de sinatura ou da propia sinatura e que a sinatura está protexida contra a falsificación coa tecnoloxía existente en cada momento.
3. Que os datos de creación da sinatura poden ser protexidos de forma fiable polo asinante contra a súa utilización por terceiros.
4. Que o dispositivo empregado non altera os datos ou o documento que debe asinarse nin impide que este se mostre ao asinante antes do proceso de sinatura.

CERES

A FNMT-RCM, a través do seu departamento CERES (CERtificación ESpañola) ofrece certificados electrónicos recoñecidos pola maioría das Administracións Públicas, o certificado FNMT Clase 2CA e o certificado AC FNMT Usuarios.

http://www.cert.fnmt.es/gl/home

Ademais dos certificados de usuario a FNMT-RCM ofrece a Administracións Públicas e Empresas servizos de Certificación que garanten os principios de Autenticación, Integridade, Confidencialidade e Non repudio nas comunicacións a través das redes.

Como solicitar un certificado dixital

Solicitar un certificado dixital da FNMT-RCM é gratuito é serve para comunicarse con case todas as administracións públicas en España.

http://www.cert.fnmt.es/gl/home

Formato X.509

O X.509 é un formato estándar da ITU-T que define o formato dos certificados. Actualmente empregase a versión 3 publicada en 1996.

Os certificados teñen varios niveis:

- Clase 1: asocia persoa e correo electrónico.
- Clase 2: ademais comproba a identidade cun documento de identidade.
- Clase 3: ademais realizase unha validación de crédito.
- Clase 4: ademais verificase o seu cargo ou posición nunha organización.

Formatos de sinatura dixital

- CMS (Cryptographic Message Syntax) PCK#7
- PDF/A (PDF con sinatura electrónica).
- XML Signature (Enveloped, Enveloping, Detached)
- S/MINE
- Sinatura avanzada: PadES, XAdES, CadES.

Almacén de certificados

- PKCS#12 Almacén de cable privada protexido por unha cable simétrica.
- PKCS#11 Dispositivo de almacenamento criptográfico. (DNI-e)

Asinando documentos en GNU/Linux: @firma, ecofirma, etc...

Existen varias ferramentas de sinatura electrónica:

- Ecofirma
- Cliente @firma
- Sinadura

Todas estas opcións supoñen que temos unha VM Java. Funcionan con OpenJDK coa versión libre sen moitos problemas.

O reto de acceder á administración electrónica con Software Libre

A Lei 11/2007, de acceso electrónico dos cidadáns aos servizos públicos, no seu artigo 13 enumera as formas de identificación e autenticación das administracións públicas nas súas relacións por medios electrónicos.

No caso das persoas físicas recoñecese:

- Sinatura electrónica do DNI-e para persoas físicas.
- Sistemas de sinatura electrónica avanzada baseada en certificados electrónicos recoñecidos.
- Outros sistemas de sinatura electrónica como a utilización de claves concertadas nun rexistro previo como usuario.

Autenticación HTTPS con certificado

As sedes electrónicas soen empregar o que se coñece como autenticación de cliente X509 mediante HTTPS.

En software libre a autenticación mediante certificado dixital funciona ben sempre que só se empregue o navegador web.... o problema chega cos coñecidos Applets Java...

Os Applet Java

En España o proxecto máis popular é en servidor para sinatura electrónica é o @firma.

@firma é unha plataforma de sinatura electrónica que ten un cliente para o usuario en forma de Applet Java. O applet entra en acción cando precisamos realizar unha sinatura dixital de documentos.

Polo tanto temos que ter funcionando Java e os Applets Java no noso navegador. En GNU/Linux isto só funciona en Firefox... outros navegadores como Chromium non soportan NAPI.

Os Applet Java

O soporte de Aplets Java en OpenJDK achégao o proxecto Icedtea.
En principio só é preciso instalalo... pero podes ter problemas...

- Arquitecturas 32bits/64bits.
- Múltiples máquinas virtuais Java instaladas no sistema.
- Os applets supoñen cousas do teu sistema operativo.

Historias para non durmir

O Certificado raíz da FNMT-RCM

Non vos esquezades de instalar o certificado raíz da FNMT. Que non se considera unha entidade certificadora fiable polos navegadores serios como Firefox ou Chromium.

Bug 435736 - Add Spanish FNMT root certificate

Que é un servidor OCSP ?

Historias para non durmir

O DNI electrónico

Existe alguén que lle funcione o DNI-e en todas as páxinas?

O DNI Electrónico

O DNI electrónico expídese dende 2006 co obxectivo de achegar a identidade dixital permitindo o seu uso electrónico.

O DNI-e é unha SmartCard que dispón dun chip criptográfico co deseño e medidas dun DNI.

O DNI-e permite a acreditación da identidade da persoa física de forma electrónica e a sinatura de documentos electrónicos con validez xurídica equiparable á sinatura manuscrita.

http://www.dnielectronico.es/

DNIe

O Chip do DNIe

O chip do DNIe almacena dixitalmente a mesma información impresa na tarxeta, xunto as imaxes dixitalizadas da fotografía, sinatura manuscrita e pegadas dactilares.

Pero tamén inclúe dos certificados dixitais de usuario asinados pola Dirección Xeral de Policía. Un para autenticación e outro para sinatura electrónica.

Os datos do chip están cifrados e protexidos por un PIN. As chaves criptográficas nunca saen do chip.

O Chip do DNIe

- **O certificado de autenticación** garante a identidade do cidadán nas transaccións telemáticas. Este certificado non está habilitado para operacións que requiran non repudio.
- **O certificado de sinatura** é o que se emprega para operacións de sinatura de documentos e garante a integridade dos documentos así como o non repudio en orixe. Este é un certificado X509v3 estándar. É un certificado recoñecido e creado nun Dispositivo Seguro de Creación de Sinaturas. O par de claves RSA pública e privada xéranse no interior do CHIP do DNIe.

O lector de DNIe

Para empregar o DNIe precisamos dun **Lector de tarxetas intelixentes** (*SmartCards*) conectado o noso ordenador. Os lectores válidos para o DNIe deben ser compatibles coa norma ISO 7816.

Os modelos máis populares son os integrados no teclado e os lectores externos mediante interface USB. O seu custe ronda os 10EUR.

O driver do DNIe

Unha vez temos o DNIe e temos un lector o seguinte paso é que o sistema operativo o recoñeza. No noso caso GNU/Linux.

OpenSC é o proxecto de referencia para o soporte de Smart Cards en GNU/Linux. Actualmente conta cun certo soporte para o DNIe grazas a integración dalgúns dos parches do proxecto OpenDNI.

OpenSC inclúe a ferramenta dnie-tool que permite consultar os datos básicos do DNIe.

O OpenDNI é o proxecto de Software Libre para soportar DNIe apoiado por CENATIC. https://forja.cenatic.es/projects/opendnie/

HOW TO de Instalación de OpenDNI.

https://forja.cenatic.es/plugins/mediawiki/wiki/opendnie/index.php/Documentacion_OpenDNIe_Instalacion_Linux

Descargar Drivers DNIe

- Driver `www.dnielectronico.es` Área de Descargas (OpenDNIe).
- Driver `http://www.sede.fnmt.gob.es` Área de Descargas (Código fonte non dispoñible)

Problemas con DNI-e

- Problemas de acceso as bibliotecas do DNI-e.
- Interacción co almacén de Firefox.
- 32bits vs 64bits.

Cousas para trebellar

- "Tentar"presentar un documento a través dunha sede dixital.
- Analizar o tráfico HTTPS (OWASP Zed Attack Proxy)
- Crear a nosa entidade de certificación que expida certificados SSL.

Dúbidas / Preguntas

Sinatura electrónica en entornos libres

3º Ciclo Sábados Libres na Altamar

José María Casanova Crespo (@txenoo)

jmcasanova@igalia.com

11 Abril 2015