MINISTERIO
DE EDUCACIÓN
Y CIENCIA

SECRETARÍA GENERAL
DE EDUCACIÓN
Y FORMACIÓN PROFESIONAL

DIRECCIÓN GENERAL
DE EDUCACIÓN,
FORMACIÓN PROFESIONAL
E INNOVACIÓN EDUCATIVA

CENTRO NACIONAL
DE INFORMACIÓN Y
COMUNICACIÓN EDUCATIVA

Redes de área local
Aplicaciones y Servicios Linux

Entidad certificadora

C/ TORRELAGUNA, 58
28027 - MADRID

Índice de contenido

Entidad Certificadora

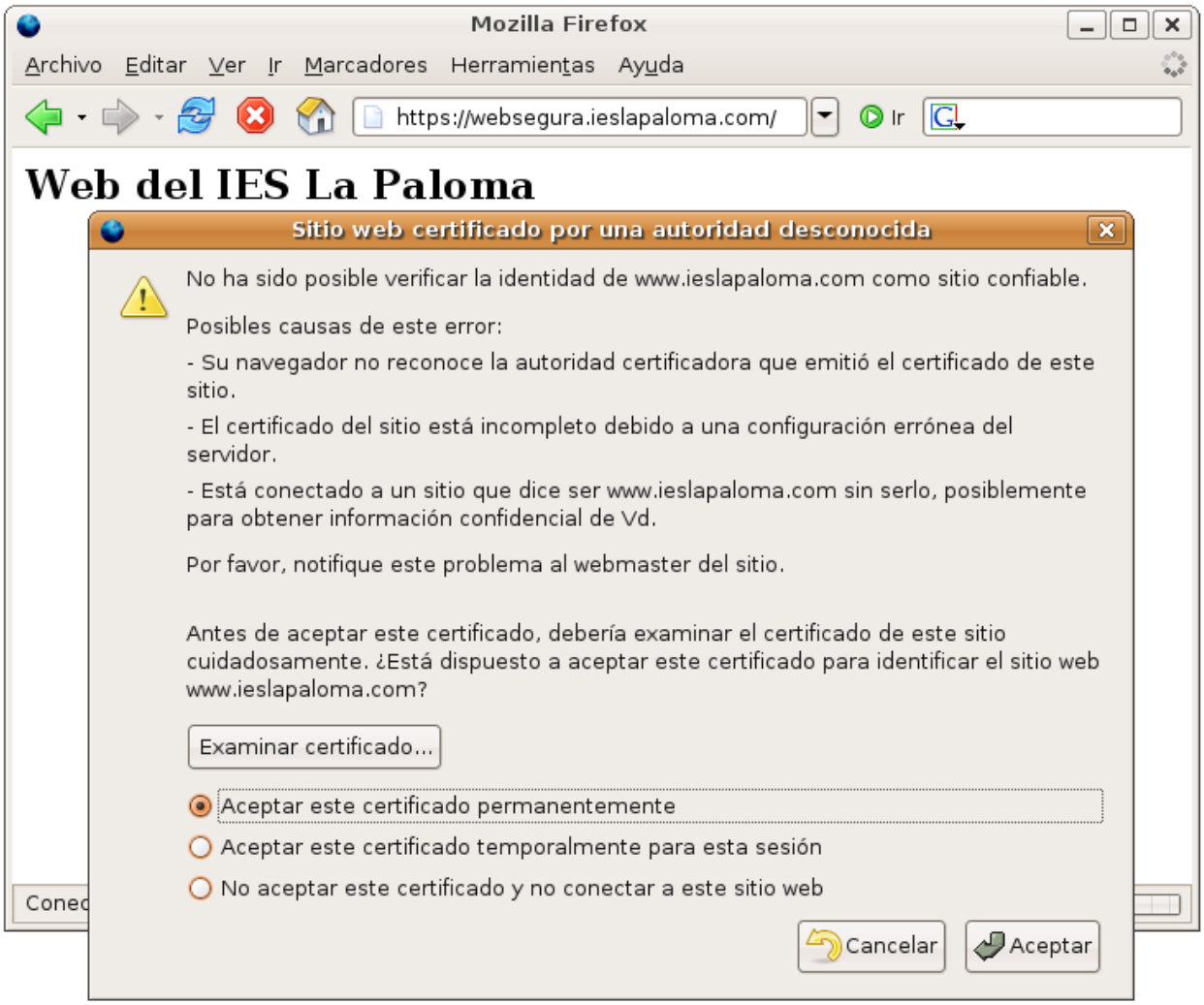
Una entidad certificadora (en inglés CA Certification Authority) es alguien que puede firmar certificados de usuarios y garantizar su autenticidad. Por ejemplo en España, una entidad certificadora es la FNMT - Fábrica Nacional de Moneda y timbre http://www.cert.fnmt.es

Los certificados permiten identificar y autenticar a sus titulares (usuarios, equipos, servidores,...), siempre y cuando estén firmados por una CA de confianza. Ejemplo, el usuario Pepe puede tener un certificado firmado por la FNMT que le sirve para autentificarse en la Agencia Tributaria. La Agencia Tributaria le permitirá el acceso ya que confía en los certificados firmados por la FNMT.

Si confiamos en una CA, debemos aceptar (instalar) su certificado raíz y de ésta forma confiaremos en todos los certificados firmados por dicha CA. Un certificado raíz es un certificado autofirmado por una CA.

Cuando accedemos a una página web segura mediante el protocolo https, el servidor deberá demostrar su autenticidad mediante un certificado firmado por una CA de nuestra confianza. Si la CA no es de nuestra confianza, el navegador preguntará al usuario si desea continuar o por el contrario, cancela la comunicación.

La comunicación se realiza de forma segura ya que se utilizan algoritmos de cifrado asimétrico. Para saber más del cifrado asimétrico, consultar el apartado Autentificacion segura con OpenLDAP



Nuestro servidor Linux puede comportarse como una CA y ofrecer certificados a un solicitante. Crearemos nuestra propia CA para poder utilizar páginas web seguras en nuestro servidor web Apache y para otros servicios como LDAP, mediante el protocolo SSL. Nuestra CA no será válida en Internet y sólo tendrá vigencia en el ámbito de nuestro dominio (ejemplo: 'ieslapaloma.com') pero obviamente es suficiente para el fin que pretendemos.

Instalación y configuración de OpenSSL

A nuestro servidor no acceden solamente los alumnos sino que también lo hacen los profesores y dentro de ellos los miembros del equipo directivo, accediendo a documentos privados y confidenciales. Nosotros como administradores debemos garantizar que esa información siga siendo privada, para lo cual vamos a definir en el servidor carpetas seguras que mediante el protocolo SSL proporcionen el cifrado de los datos que se intercambian entre el ordenador servidor y el cliente, como hacen en los bancos y cajas de ahorro para garantizar el acceso a nuestras cuentas.

Para ello debemos disponer de un certificado de seguridad que puede ser expedido por una entidad certificadora con el consiguiente coste económico o bien crear y utilizar nuestra propia entidad certificadora, que expedirá certificados válidos en su ámbito de actuación; el dominio de nuestro centro, ámbito suficiente para lograr la seguridad en nuestra Intranet.

Instalación de OpenSSL

Utilizaremos apt-get para instalar el software que necesitamos para crear una entidad certificadora. Deberemos instalar el paquete openssl:

```
// Instalación de OpenSSL
     # apt-get install openssl
```

Configuración de OpenSSL

El archivo de configuración de openssl es **/etc/ssl/openssl.cnf**. En dicho archivo únicamente vamos a configurar los valores por defecto de nuestra organización para que el resto de aplicaciones y programas que usen openssl tomen dichos valores por defecto de forma automática. Dichos valores debemos configurarlos en la sección [req_distinguished_name]. En el resto de secciones no es necesario que modifiquemos nada ya que nos sirve con las opciones configuradas por defecto.

```
// Configuración particular de nuestra CA. Archivo /etc/ssl/openssl.cnf


     [ req_distinguished_name ]

     countryName = Country Name (2 letter code)

     countryName_default = ES

     countryName_min = 2

     countryName_max = 2

     stateOrProvinceName = State or Province Name (full name)

     stateOrProvinceName_default = Soria

     localityName = Soria

     0.organizationName = Organization Name (eg, company)

     0.organizationName_default = I.E.S. La Paloma

     # we can do this but it is not needed normally #1.organizationName =
     Second Organization Name (eg, company)

     #1.organizationName_default = World Wide Web Pty Ltd
```

```
organizationalUnitName = I.E.S. La Paloma

#organizationalUnitName_default =

commonName = www.ieslapaloma.com

commonName_max = 64

emailAddress = root@ieslapaloma.com

emailAddress_max = 64
```

En las siguientes secciones se utiliza openssl para permitir páginas web seguras y autentificación segura:

- Acceso_a_carpetas_seguras
- Autentificacion_segura_OpenSSL_y_OpenLDAP