Contents

Descripción de la práctica Correo Electrónico Seguro Usando Certificados Práctica 2: Correo electrónico seguro usando certificados Objetivos

```
Ser capaces de familiarizarse con el proceso de obtención de un certificado X.509
Experimentar con el correo electrónico seguro basado en S/MIME
Ser capaces de firmar digitalmente mensajes
Ser capaces de cifrar/descifrar los mensajes enviados/recibidos
```

Entorno

En la realización de esta práctica se empleará como

```
Cliente de correo de Microsoft Outlook Express o el de Mozilla Thunderbird
Microsoft Internet Explorer o Mozilla Firefox
Autoridad de Certificación (AC)  http://www.CAcert.org
```

Si el alumno lo desea puede usar navegadores o clientes de correo alternativos.
Enunciado

La práctica comenzará con la obtención e instalación de los certificados digitales, como paso previo a la firma y cifrado de mensajes. Después se procederá a la firma de un mensaje de correo y al envío de un mensaje cifrado.

Obtención de certificados X.509 vía web

Para la realización de la práctica usaremos como Autoridad de Certificación (AC) http://www.CAcert.org

Acceder a la página http://www.cacert.org descargar e instalar el certificado raíz en nuestro navegador. Comprobar que una vez instalado ya no recibimos advertencia alguna de seguridad.

Adicionalmente, localizaremos el certificado en el almacén de certificados (pestaña Entidades emisoras raíz de confianza) de IE y trataremos de:

```
Comprobar para qué propósitos  sirve (en propiedades)
Editar las propiedades y modificar algún propósito de uso
Anular la confianza en esta CA para identificar sitios web (servidores)
Volver a acceder a la página de CAcert en modo https
Restaurar las propiedades originales
```

¿Se ve igual en distintos navegadores/almacenes?

Solicitar un certificado digital personal (usuario)

Para que una AC pueda asegurar la identidad digital del sujeto y firmar un certificado personal hay que seguir un proceso para que la entidad emisora pueda verificar la información que contenga el certificado. Cada Autoridad procede de una manera. En el caso de los certificados emitidos por la Fábrica Nacional de Moneda y Timbre (FNMT) se valida el nombre y el NIF (campo CN del subject), pero no se verifica la dirección de correo electrónico (campo E del subject). En el caso de CAcert no verifica el nombre pero sí la dirección de correo electrónico. Para ello hay que hacer uso de peticiones estándar CSR (Certificate Signing Request).

Obtener e instalar en nuestro navegador un certificado personal de la autoridad CAcert (solo funciona en FireFox).

Comprobar que el certificado se ha instalado correctamente en el almacén de certificados de manera análoga a cómo comprobamos la instalación del certificado de la autoridad de Certificación. Verificar sus campos. Crear copia de seguridad del certificado que contiene el par de claves publica y privada (formato pk12) y el que contiene únicamente la clave pública (formato crt).

Acceder al sitio CAcert desde el navegador CHROME validando la identidad con certificado personal, no mediante usuario y contraseña.

Visualizar la información de los certificados de sitio mediante la herramienta openssl y con visores de certificados de interfaz gráfica.

Documento auxilar para generar el Certificado personal usando una peticion firmada (csr).

Firma y cifrado de mensajes de correo electrónico

Instalar los certificados obtenidos en nuestra aplicación cliente de correo.

Enviar correos con las distintas funciones de seguridad (firmado y/o cifrado) al compañero de prácticas.

Comprobar en el lado receptor su autenticidad y obtener el mensaje claro si se recibe cifrado.

Para autenticar es necesaria la clave pública del receptor que estará en un certificado dentro del almacén de certificados de otras personas. Para ello tenemos que haber obtenido y cargado el certificado del destinatario del correo. Se procederá de manera similar a la instalación del certificado propio.

Usar un cliente de correo web para tratar de ver los correos firmados y/o cifrados que hayan llegado al buzón.

Condiciones de entrega Práctica opcional

Entregar un informe en formato PDF con todos los pasos realizados. En el informe debe aparecer el nombre de los autores. Adjuntar todos los ficheros que se hayan utilizado durante el desarrollo de la práctica. el fichero debe llamarse firma.zip Fecha límite de entrega: 24-noviembre-2020 Hora límite de entrega: 23:59

Criterios para la formación de equipos Número máximo de participantes: 2 Periodo de formación de los equipos: Desde el 04-noviembre-2020 hasta el 24-noviembre-2020