Configuración de Mozilla Thunderbird y Mozilla Firefox para usar los certificados emitidos por la CA del Laboratorio de Criptología

23 de febrero de 2006

1. Introducción

Este manual está basado en Mozilla Thunderbird 1.0.7 y Mozilla Firefox 1.5.1 aunque debería ser válido para cualquier otra versión.

2. Obtención del certificado

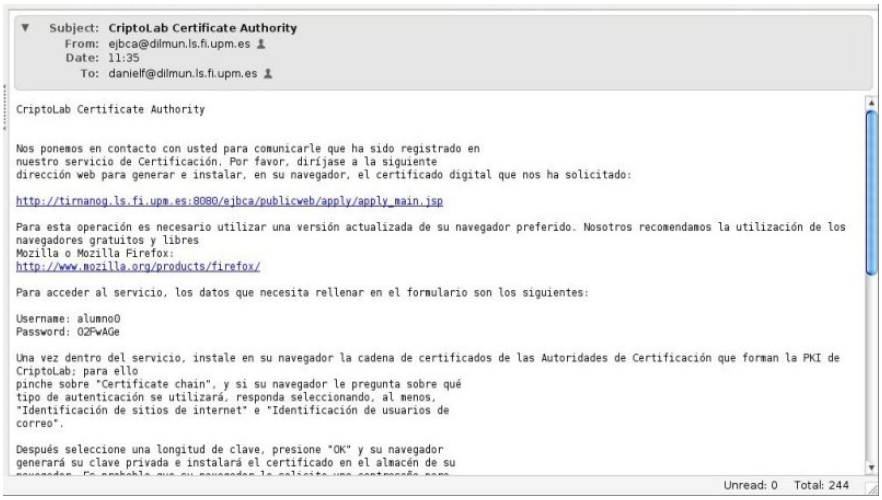
2.1. Formulario de inscripción

Para la obtención del certificado es condición necesaria el rellenar el formulario que se puede encontrar en la página de la asignatura (`http://porsche.ls.fi.upm.es/Cripto/Inicio.htm`).

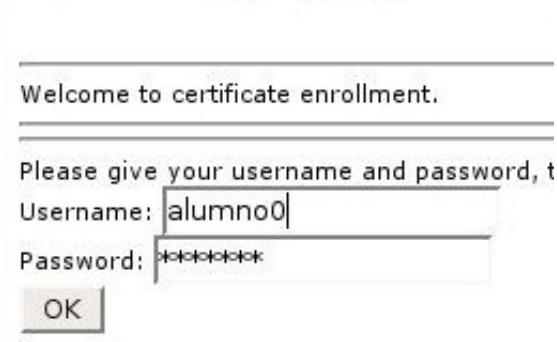
> **Nota:** Las direcciones de correo deben ser de servidores que permitan acceso vía POP3/IMAP. Los *webmail* están especialmente contraindicados.

2.2. Generación del certificado

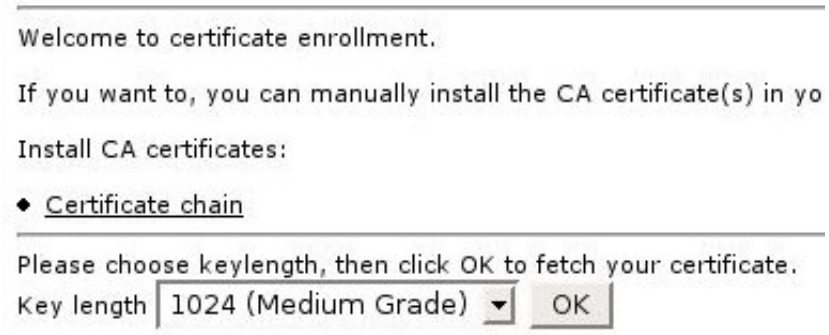
Una vez enviado el formulario y revisado para dar fe de los datos del alumno, éste será dado de alta en la Autoridad Certificadora (CA) del Laboratorio de Criptología. Una vez dado de alta en el sistema, recibirá un correo informándole del usuario y contraseña así como de la dirección web a la que acceder para obtener el certificado.



Una vez recibido el mensaje podrá ir a la dirección indicada en él autenticarse con su usuario y contraseña



y pulsar en **Certificate chain** para guardar toda la cadena de CAs involucrada en el certificado. A continuación, seleccione una clave de 1024 bits.



2.3. Exportación del certificado

Una vez generado el certificado, éste quedará insertado en el almacén de certificados del navegador.

Los pasos necesarios para exportar el certificado para poder usarlo en Mozilla Thunderbird son:

1. Seleccione el certificado a exportar y pulse Backup.
2. Seleccione un nombre y una carpeta de destino.
3. Seleccione una contraseña. Esta será la que proteja la identidad que contiene la clave privada y la pública.

Es importante seleccionar un buena contraseña ya que de ésta depende la seguridad del token.

Una vez exportada la identidad ya puede importarla en Mozilla Thunderbird, usando la opción **Import**, introduciendo como contraseña la que estableció para la identidad.

A partir de este momento, y durante el periodo de validez del mismo, el certificado podrá usarse tanto para firmar como para cifrar mensajes de correo.

3. Lista de correo de alumnos

Todos aquellos alumnos que se den de alta en la asignatura y obtengan un certificado, serán automáticamente dados de alta en la lista de correo de alumnos del año académico en curso. Para poder escribir en ella es **obligatorio** enviar los mensajes (al menos) firmados usando el certificado del laboratorio, en cualquier otro caso el mensaje será ignorado por el sistema. Los mensajes deben ser enviados a cripto2k6@dilmun.ls.fi.upm.es como si de un correo normal se tratase (teniendo en cuenta las consideraciones anteriores). Para poder leer y verificar correctamente los mensajes de la lista de correo es necesario insertar al menos los certificados de las siguientes CA:

CA de Servicios: CA que otorga los certificados a las listas de correo

CA de Personal : CA que otorga los certificados para el personal del Laboratorio de Criptología

CA de Alumnos : CA que otorga los certificados de los alumnos de Criptología.

Todos los certificados se pueden bajar de la página de la asignatura e importarse del mismo modo que su certificado.

Para el correcto uso de los certificados es necesario indicarle a Mozilla Thunderbird que confíe en la CA de Personal. Para ello, seleccione la CA correspondiente bajo la pestaña Authorities y pulsando **Edit** podremos modificar el grado de confianza en la misma.