

|  |  |
| --- | --- |
| **SEGURIDAD INFORMÁTICA** – 2º SMR | |
| UT5: Sistemas de identificación. Criptografía. | Práctica 5: Certificado Digital. |
| Nombre: | |
| Nota: | Observaciones: |

1. Menciona al menos dos autoridades de certificación españolas.

Firma profesional, Camerfirma

1. ¿Qué son las CA raíz y cuáles las intermedias? ¿Qué misión tienen?

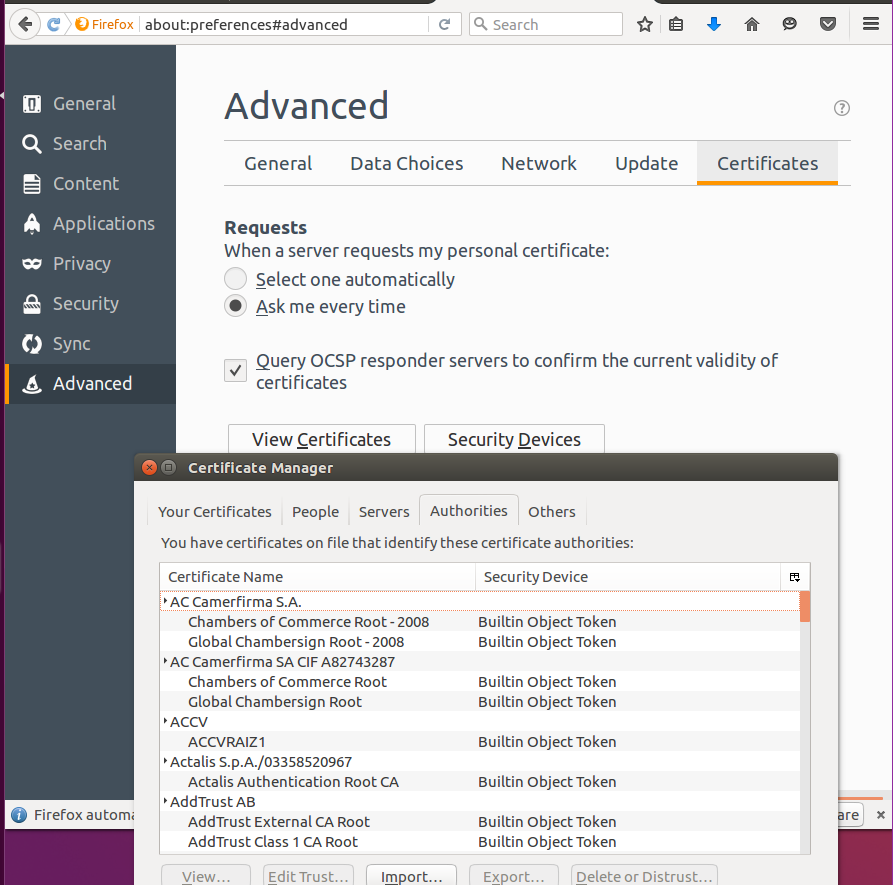
Raiz: elemento inicial de cualquier jerarquía de certificación.

Intermedias: se sientan entre un certificado de entidad final y un certificado raíz. Ellos ayudan a completar una " cadena de confianza " de su certificado de nuevo a el certificado raíz de GlobalSign .

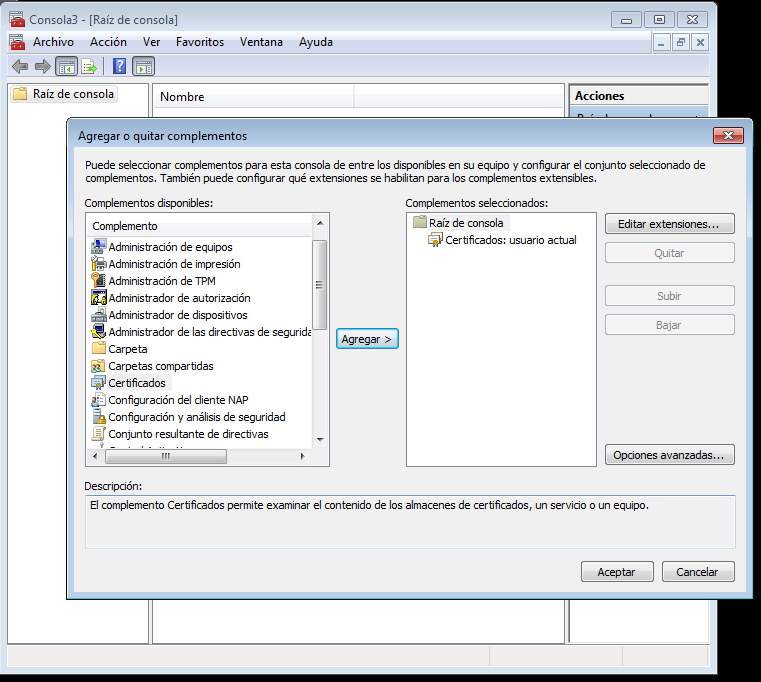
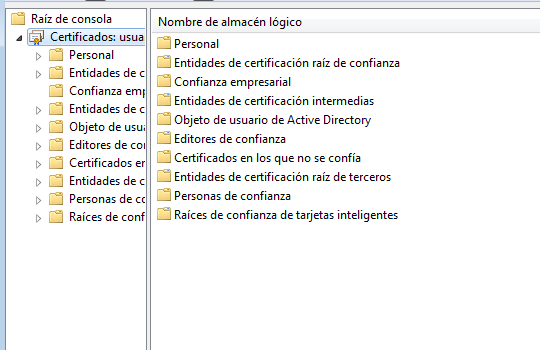
1. ¿Qué son los almacenes de certificados?

Pueden mostrar el alamacen de certificados de un usuario, un equipo y un sonido según el propósito para el que se emitió el certificado o mediante sus categorías de almacenamiento logico

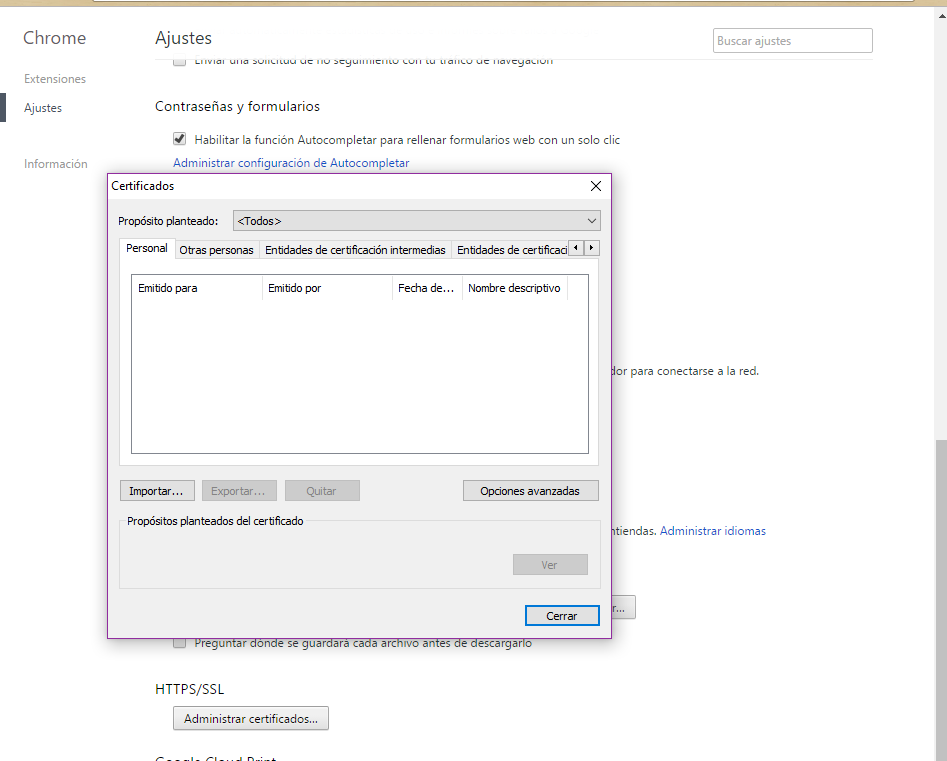
1. Localiza los certificados disponibles en el navegado Firefox.



1. Visualiza el almacén de certificados de Windows. Para ello crea una consola y añádele el complemento Certificados.

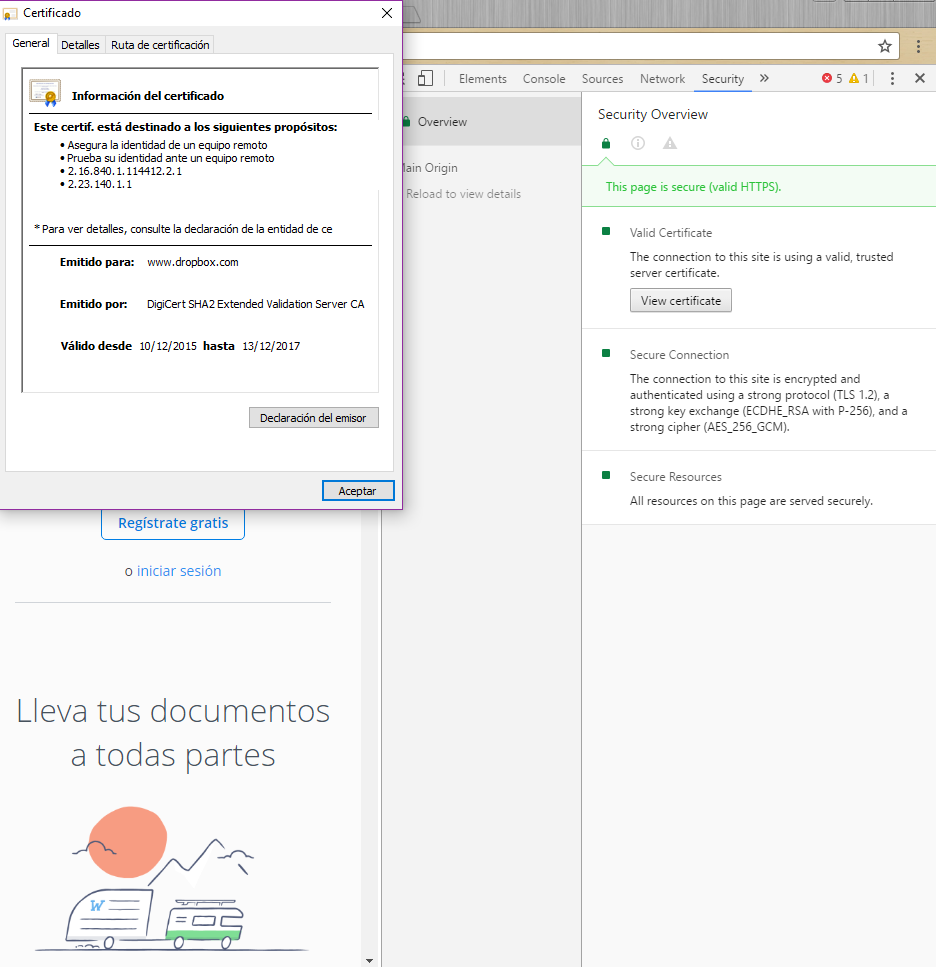
1. ¿Cómo gestiona los certificados digitales Chrome? ¿Cuál es por tanto la diferencia con Firefox?



1. Conéctate de manera segura a la web de Dropbox.
   1. ¿Qué protocolo has de utilizar para que la conexión sea segura?



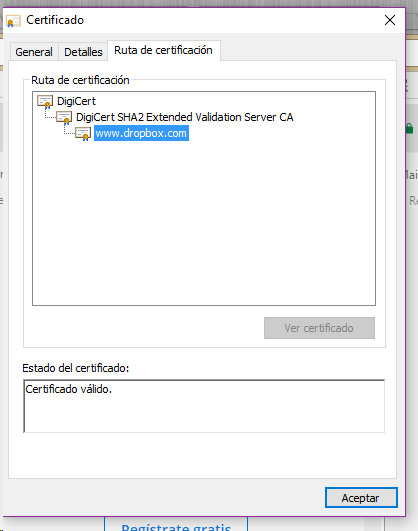
* 1. Muestra el certificado correspondiente a ese servidor web.



* 1. ¿Cuál es la finalidad del uso de los certificados?

Confirmar identidad digital

* 1. ¿Quién es la CA raíz de este certificado de Dropbox?



* 1. Confirma que dispones del certificado de dicha CA raíz y muéstralo aquí. Exporta dicho certificado.
  2. En último término, ¿qué estamos garantizando con el uso de los certificados y el https? Una conexión segura

1. Busca información acerca de qué es y para qué sirve la esteganografía.
   1. Introduce un mensaje de texto o una fotografía dentro de un archivo de música, imagen o vídeo, mediante algún software específico bajo Windows como PicCrypt, Xiao Steganography o SteganG, o bajo GNU/Linux como OpenStego.



Desde Linux con outguess

* 1. Comprueba que es posible recuperar el mensaje o archivo oculto.

1. Realiza los trámites para la obtención de tu certificado digital. ¿dónde lo tienes que descargar? ¿dónde tienes que ir a recogerlo? ¿Qué caducidad posee?

1. **Investiga acerca de la aplicación OpenSSL. ¿Qué tipo de algoritmos emplea? ¿Para qué sistemas operativos se encuentra disponible? ¿Qué utilidades posibilita?**

Open SSL: Robusto paquete de herramientas de administración y bibliotecas relacionadas con la criptografía, que suministran funciones criptográficas a otros paquetes como OpenSSH y navegadores web (para acceso seguro a sitios HTTPS)

Utiliza el algoritmo de cifrado/descrifrado

Esta disponible para UNIX/Linux, Microsoft y Java