Página Web Segura:

Cómo solicitar un certificado y aplicarlo a su web

Cada vez es mas frecuente y necesario usar el protocolo *https* en las paginas web (en adelante, Web Segura), tanto para dar seguridad a sus visitantes como incluso para poder figurar con mayor visibilidad en los listados de las búsquedas en Google. Los navegadores más modernos indican ya que si accedemos a una página con *http*, la página es insegura y nos impiden el acceso.

Configurar una Web Segura implica que las comunicaciones entre el usuario final y nuestros servidores están encriptadas por completo, y es imposible que terceros accedan a esa información, tanto la que envían (formularios, datos personales) como la que reciben (resultados de consultas).

Esto se consigue a través de lo que se llama un *certificado*, que no es más que un conjunto de ficheros que encriptan y desencriptan la información que se transmite entre navegador y servidor, como si fuera un *password*. Estos certificados los crean las *Autoridades de Certificación (*Certificate Authority, CA), empresas que se encargan de garantizar ante terceros que los certificados suministradas identifican por completo la URL que se pretende visitar.

Este certificado será sólo válido para la URL de su página web, por lo que a la hora de crear un certificado, es necesario indicar las URL a las que va dirigido. Si su pagina web institucional tiene una redirección (por ejemplo, a la pagina personal http://www.ugr.es/local/usuario se puede acceder con http://usuario.ugr.es) el certificado tiene que crear para *ambas URLs.*

Usted puede solicitar un certificado por sí mismo a una de estas empresas CA, (pagando por el servicio) o puede solicitarlo gratuitamente, si es usuario del servicio web institucional (tanto www como wpd) de la Universidad de Granada.

1) Solicitud del certificado

El titular de la cuenta de wpd/www debe contactar mediante un correo electrónico a seguridadinformatica@ugr.es solicitando el certificado. Una vez que se verifiquen los datos de la solicitud los responsables de seguridadinformatica@ugr.es le mandarán un correo con dos ficheros, de los cuales deberá descargarse el fichero llamado **nombre_de_dominio_ugr_es_privatekey.pem**.

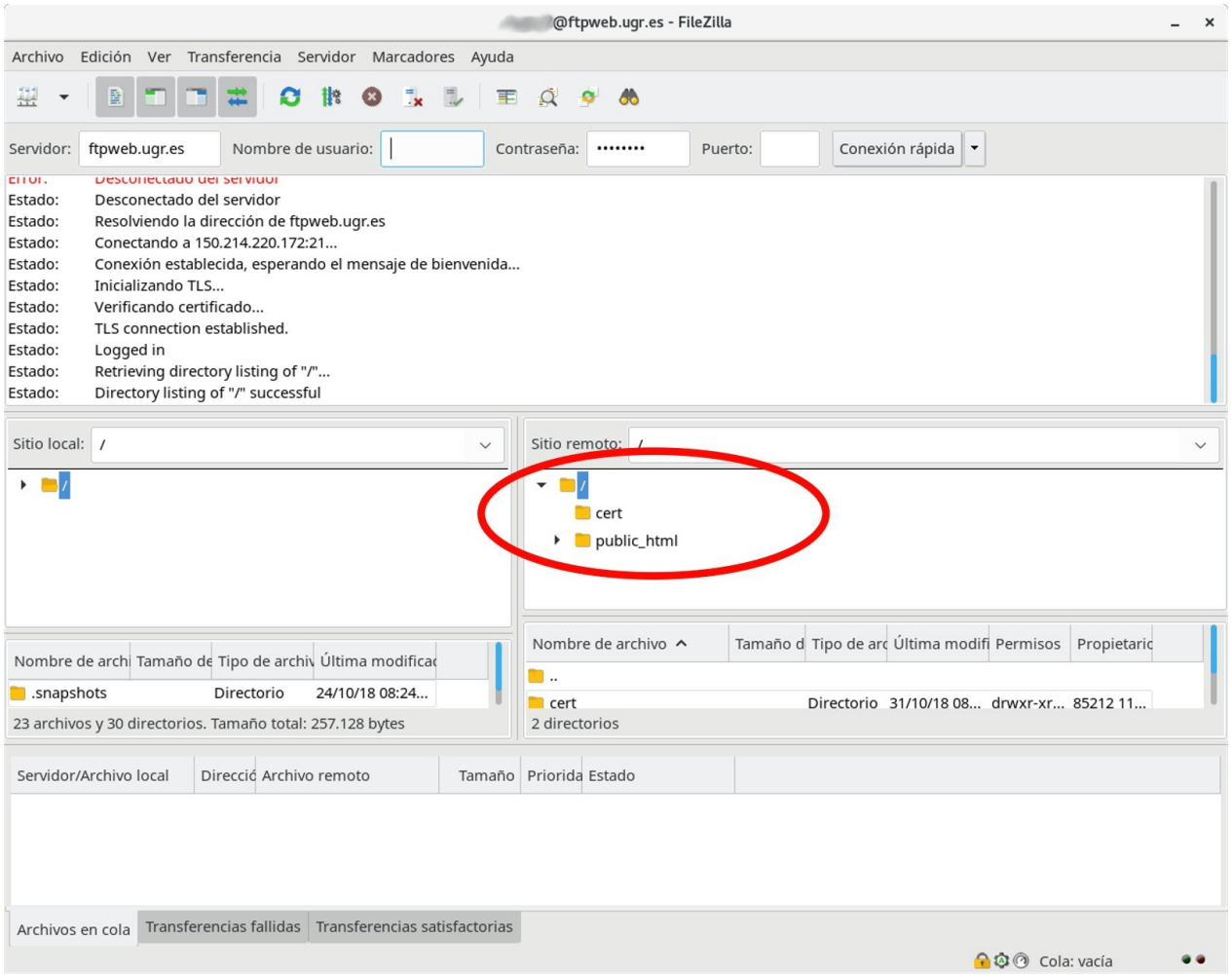
En un correo posterior proveniente de “Certificate Services Manager” pulse sobre el primer enlace que le aparece en dicho correo, justo después de la línea que comienza con “as Certificate only, PEM encoded”); se descargará un fichero con llamado **nombre_de_dominio_ugr_es_cert.cer**.

2) Subir certificado a su página web

Una vez que tenga descargados los ficheros, deberá subirlos a su espacio web via FTP, ya sea www o wpd, a los servidores ftp ftp://ftpweb.ugr.es o ftp://ftpwpd.ugr.es, respectivamente.

Consulte cómo subir archivos vía FTP en la sección de "Proceso de publicación" a través de este enlace https://csirc.ugr.es/personal/servicios-web/alojamiento-web. Una vez conectado por ftp al servidor (ftp://ftpweb.ugr.es o ftp://ftpwpd.ugr.es) deberá crear una carpeta nueva llamada **cert** en la carpeta raíz de su usuario (la carpeta inicial, que ya debe contener public_html).

Preste especial atención a que estén en el sitio correcto, dicha carpeta **NO** debe estar dentro de la carpeta public_html; los ficheros *html* van en la carpeta public_html, los archivos *cer y key* van en la carpeta **cert** que está **FUERA** de public_html. En la imagen puede ver como deben estar las carpeta si usa el cliente filezilla para subir los archivos:

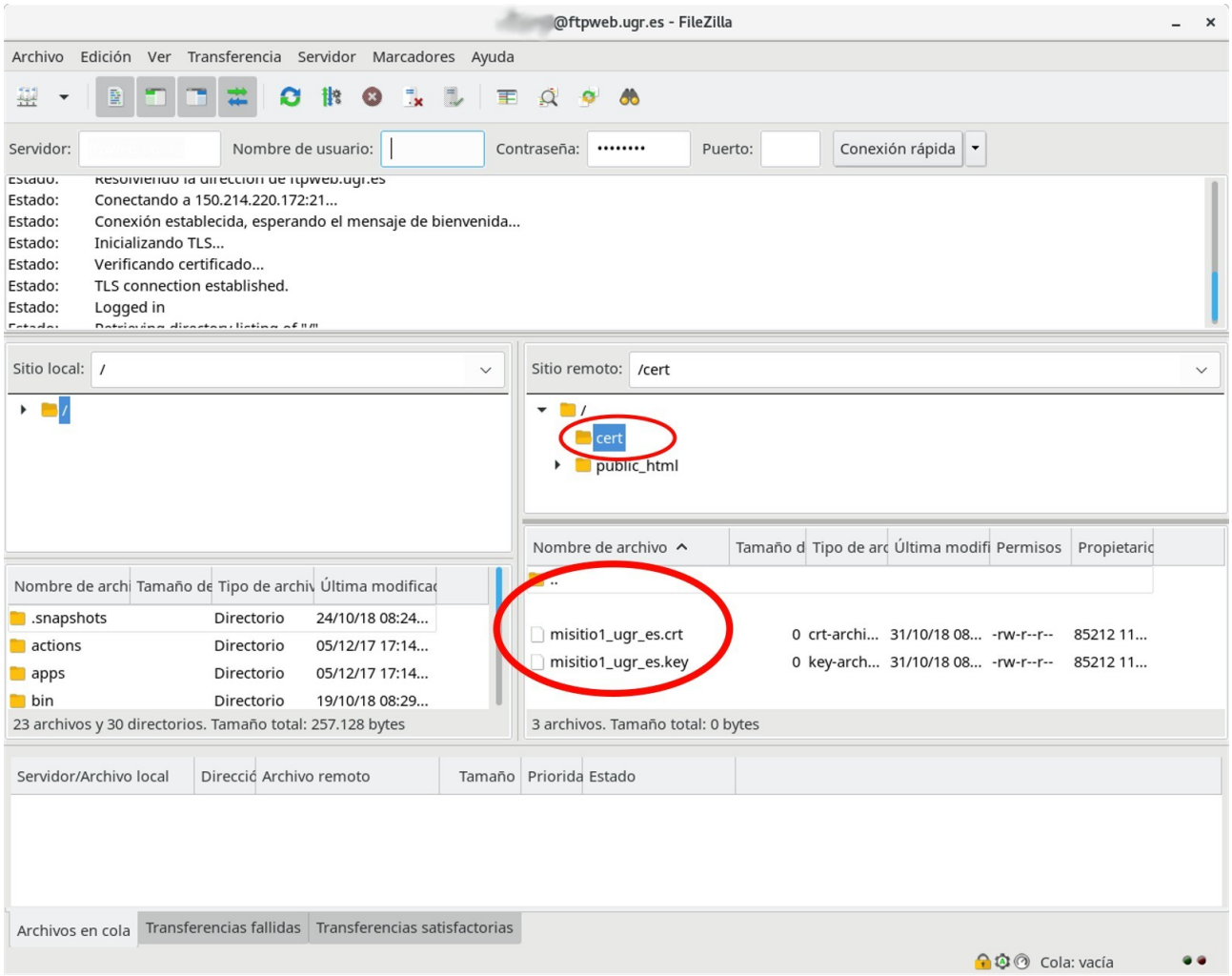


Centro de Servicios de Informática y Redes de Comunicaciones
Edificio Mecenas * Campus Fuentenueva * 18071 Granada
Telf. 958 241010 * Fax 958 244221 * Web http://csirc.ugr.es * eMail csirc@ugr

Por tanto, deberá tener dos archivos relacionados con el certificado. Por ejemplo, si el dominio para el que solicitó los certificados fuese **misitio1**.ugr.es le habrán llegado los siguientes archivos (entre otros):

- CERTIFICADO: **misitio1**_ugr_es_cert.**cer** y
- CLAVE PRIVADA: **misitio1**_ugr_es_privatekey.pem

El lugar donde debe subir estos ficheros es en la carpeta **cert** que habíamos creado previamente.



3) Solicitar la activación de los certificados en la web

Una vez que los certificados están en su sitio, debe solicitar la *activación* de los certificados. Esto significa que nuestros servidores se percaten de la presencia de los certificados, y comience a responder a las peticiones *https* de los navegadores.

Para ello, envíe un correo a csirc@ugr.es , o contacte con el Centro de Atención al Usuario al n.º Tfno 36000, indicando su nombre de usuario, la web a la que le quiere activar la Web Segura, y que desea que se le activen los certificados que ha subido previamente a su espacio web.

Renovación de certificados

Habitualmente los certificados generados tienen una caducidad de un año, por lo cada año tendrá que realizar los pasos:

1) Solicitud del certificado y el paso
2) Subir certificado a su página web.

Estos pasos deberá hacerlos cada año antes de caduque su certificado.

El paso "3)Solicitar la activación de los certificados" no será necesario realizarlo si el archivo recibido en la renovación tienen el mismo nombre y **extensión** :

- Si cambian los nombres pero no de extensión. Simplemente renombre el archivo al antiguo nombre antes de subirlo en el paso 2.
- Si cambia la extensión tendrá que contactar de nuevo con el CSIRC solicitando la activación.