Procedimiento de generación de fichero CSR para la solicitud de certificados digitales

Los pasos para la generación de un Certificado Digital SSL de servidor son los siguientes:

1) El responsable del servidor debe generar la petición de certificado (CSR) mediante el script Linux (bash) proporcionado por el Servicio de Informática.
2) El usuario enviará al Servicio de Informática, y si todo es correcto, se aprueba dicha petición y se envía el certificado al responsable del servidor.
3) El responsable del servidor instalará y configurará el certificado en dicho servidor.

Generar una petición de certificado (CSR) y la clave privada

Comenzaremos generando una petición de certificado (CSR). Para ello utilizaremos uno de los siguientes scripts disponibles para su descarga desde la web del Servicio de Informática (**Catálogo de Servicios > Servicio de Certificados Digitales**):

- tcs-genCSR.sh (para versiones recientes de OpenSSL)
- tcs-genCSR-20150217.sh (para versiones de OpenSSL anteriores a la 1.1.0)

Este script genera certificados con clave de 2048 bits, hash SHA-256 y utiliza UTF-8. En negrita aparecen los valores que se han cumplimentado para un certificado de ejemplo: servidor.ujaen.es.

```
# tcs-genCSR.sh
```

```
¿Para qué tipo de certificado desea generar la solicitud?
1. Certificado simple (sólo CN)
2. Certificado con múltiples dominios (CN y Subject Alternative Names)
3. Certificado Wildcard
Seleccione una opcion [1]: 1
Certificado simple (sólo CN) seleccionado
FQDN/CommonName (p. ej. www.example.com): servidor.ujaen.es
OrganisationName (p. ej. RedIRIS): Universidad de Jaen
Juego de caracteres para el DN del certificado
(p. ej. default, pkix, utf8only, nombstr) [utf8only]:
Running OpenSSL...
Generating a 2048 bit RSA private key
.....................+++
writing new private key to servidor.ujaen.es_privatekey.pem'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (Código ISO 3166) [ES]:
State or Province of the Organization (Guadalajara) [opcional] []:Jaen
Locality of the Organisation (Villabado de arriba) [opcional] []:Jaen
Organization Name (p. ej. RedIRIS) [Universidad de Jaen]:
Organisational Unit Name (Departamento de ciencias aplicadas) [optional] []:
Common Name (eg, www.example.com) [servidor.ujaen.es]:
```

```
unstructuredName MUST contains a FQDN/CommonName (eg, www.example.com)
[opcional] []:
```

Al finalizar se crearán dos ficheros:

- **`servidor.ujaen.es_csr.pem`** (petición de certificado)
- **`servidor.ujaen.es_privatekey.pem`** (clave privada)

IMPORTANTE: el fichero de clave privada (**`servidor.ujaen.es_privatekey.pem`**) **NO SE DEBE ENVIAR.** Se debe conservar de forma segura para configurar el certificado posteriormente en el servidor. Únicamente se enviará el fichero de petición (**`servidor.ujaen.es_csr.pem`**) al Servicio de Informática, quien solicitará y facilitará al administrador del servidor solicitante la descarga del certificado final desde la Autoridad de Certificación (CA).

Configurar el certificado en el servidor web (Apache)

En este apartado se documenta una instalación de certificado para Apache, por ser el servidor web más usado. Para otro tipo de servidores, consultar con el Servicio de Informática.

Una vez se tenga el certificado digital y la clave, la instalación en Apache pasa por los siguientes pasos:

En el archivo de configuración SSL de Apache (**`/etc/httpd/conf.d/ssl.conf`**), encontraremos las directivas para especificar dónde están los certificados. En Redhat y distribuciones similares, las directivas son estas (en otras distribuciones Linux, las rutas pueden cambiar):

- **`SSLCertificateFile /etc/pki/tls/certs/servidor_ujaen_es.crt`**
  - Contiene el certificado firmado por la CA. Recibido en el mensaje de correo de la CA incluyendo todos los enlaces de descarga.

- **`SSLCertificateKeyFile /etc/pki/tls/private/servidor.ujaen.es_privatekey.pem`**
  - Contiene la clave privada generada en el paso anterior.

- **`SSLCertificateChainFile /etc/pki/tls/certs/servidor_ujaen_es_interm.cer`**
  - Contiene la cadena de certificación raíz e intermedia de la CA. Recibido en el mensaje de correo de la CA incluyendo todos los enlaces de descarga.

Una vez actualizados los ficheros, reiniciamos Apache y hacemos las comprobaciones oportunas.

Más información: https://sectigo.com/resource-library/install-certificates-apache-open-ssl