Solicitud e instalación de certificados de servidor

Referencia	--
Fecha	03/10/2022-04/10/2022
Autores	Unidad de Sistemas y Redes
Revisores	[Nombre y apellidos de los revisores]
Destinatarios	Usuarios del servicio de emisión de certificados de servidor
Descripción	Este documento describe cómo solicitar e instalar certificados de servidor.
Palabras clave	Seguridad, Certificados, TCS, RedIRIS

1 Introducción al servicio de emisión de certificados de servidor

Los certificados digitales de servidor son utilizados, principalmente, para servir contenido Web a través de conexiones cifradas. Si emitimos estos certificados desde una autoridad de certificación (CA) ampliamente reconocida, conseguimos que la navegación en los sitios que usan estos certificados sea etiquetada por los navegadores como segura.

El **Área TIC** de la **UCLM** ofrece certificados digitales de servidor a través del **Servicio TCS de RedIRIS**. Los certificados son emitidos por una autoridad de certificación ampliamente reconocida, con una vigencia de **12 meses**.

1.1 A quién va dirigido

Pueden usar este servicio todos aquellos docentes e investigadores responsables de servidores Web en el dominio DNS **uclm.es**.

1.2 Qué tipos de certificados pueden emitirse

Este servicio puede emitir certificados de servidor para nombres DNS en el dominio **uclm.es** o en alguno de sus subdominios.

1.3 Alternativas

En aquellos casos en los que los solicitantes gocen de control total sobre el servidor Web donde quieren instalar certificado, se puede optar por usar certificados emitidos por **Let's Encrypt**, que ofrece el servicio de emisión de forma gratuita.

Los certificados emitidos por **Let's Encrypt** caducan cada 3 meses. Sin embargo, **Let's Encryp't** ofrece opciones de automatización a través del agente **Certbot** (https://letsencrypt.org/es/docs/client-options/), que se encarga de renovar periódicamente el certificado sin requerir ningún tipo de intervención manual.

El resto de esta guía se refiere exclusivamente al servicio de emisión de emisión de certificados prestado por el **Área TIC** de la **UCLM**.

2 Cómo solicitar la emisión de un certificado de servidor al Área TIC

Basta con poner un caso a través del **CAU** (Centro de Atención al Usuario), indicando el nombre el nombre **DNS** del servidor para el que se solicita el certificado y adjuntando un fichero de solicitud en formato **CSR** (*Certificate Signing Request*).

3 Cómo generar el fichero CSR para hacer la solicitud

La forma más fácil de generar el fichero **CSR** para hacer la petición de un certificado firmado por una entidad de certificación reconocida, es utilizar la herramienta de línea de órdenes **OpenSSL**. **OpenSSL** está preinstalado en la mayoría de los sistemas **Linux** y disponible también para otras plataformas como Windows y macOS.

Podemos usar la utilidad en línea https://www.digicert.com/easy-csr/openssl.htm para saber qué opciones hay que suministra a OpenSSL para obtener la **CSR**. Por ejemplo, para un servidor de nombre **mi-servidor.uclm.es**, la orden sería (en una sola línea):

```
openssl req -new -newkey rsa:2048 -nodes -out mi-servidor_uclm_es.csr
-keyout mi-servidor_uclm_es.key -subj "/C=/ST=/L=/O=/CN=mi-
servidor.uclm.es"
```

Como podemos observar, en el proceso se han generado dos ficheros:

- **mi-servidor_uclm_es.csr**, que es el que hay que suministrar al **Área TIC** en el caso del **CAU** (Centro de Atención al Usuario) en el que se solicita la emisión del certificado. Este fichero contiene, codificado en un formato llamado **PEM**, tanto una clave pública como el nombre **DNS** solicitado para el servidor.
- **mi-servidor_uclm_es.key**, que contiene la clave privada que encaja con la clave pública incluida en el fichero **CSR**. Es imprescindible conservar el fichero que contiene la clave privada para que, una vez recibamos nuestro certificado, podamos configurar con éxito nuestro servidor Web.

4 Obtención del certificado para el servidor

En condiciones normales, si el fichero CSR está correctamente generado, obtendremos una respuesta a nuestro CAU en uno o dos días laborables. Esta repuesta contendrá:

- El certificado en formato **PEM** (**servidor_uclm_es.pem**). Este certificado habrá sido emitido por una autoridad de certificación de confianza.
- La cadena de certificación de la autoridad de certificación que firmó el certificado anterior, también en formato **PEM**, en el fichero **ca-chain.pem**.

5 Ejemplo de instalación del certificado en el servidor Web Apache

5.1 Requisitos para seguir la guía

Esta guía asume que:

- Vamos a instalar el certificado en un servidor **Apache** que se ejecuta sobre la distribución **CentOS 7** de **GNU/Linux**. La traducción de los pasos a otras plataformas requerirá algunos ajustes, pero las órdenes básicas serán idénticas.

- El servidor **Apache** ya tiene instalado y debidamente configurado el módulo de cifrado **mod_ssl**.
- Se utiliza el directorio **/etc/pki/tls** para albergar los certificados y sus claves privadas.
- Se utilizan los siguientes ficheros relacionados con el certificado:
  - **mi-servidor_uclm_es.key**, que contiene la clave privada que debimos conservar durante el proceso de generación de la **CSR**.
  - **servidor_uclm_es.pem**, que contiene el certificado devuelto por el Área TIC en respuesta al caso en el que se suministró la **CSR**.
  - **ca-chain.pem**, que contiene la cadena de certificación devuelta por el Área TIC en respuesta al caso en el que se suministró la **CSR**.
- El nombre DNS del servidor es **mi-servidor.uclm.es**.

Queda fuera del ámbito de esta guía el establecimiento de los permisos adecuados sobre el fichero que contiene la clave privada del certificado (que deberían ser los mínimos necesarios para que el proceso de Apache pudiera leer dicha clave privada).

5.2 Configurar el servidor Apache

- Movemos los ficheros obtenidos a los directorios donde los localizará Apache:

```
mv mi-servidor_uclm_es.key /etc/pki/tls/private/

mv servidor_uclm_es.pem /etc/pki/tls/certs/

mv ca-chain.pem /etc/pki/tls/certs/
```

- Ahora realizamos la configuración del servidor Apache. En una configuración por defecto, editamos el fichero **/etc/httpd/conf.d/ssl.conf** y añadimos nuestro nuevo sitio cifrado:

```
<VirtualHost *:443>

DocumentRoot /var/www/html

ServerName mi-servidor.uclm.es

SSLEngine on

SSLCertificateKeyFile /etc/pki/tls/private/mi-servidor_uclm_es.key

SSLCertificateChainFile /etc/pki/tls/certs/ca-chain.pem

SSLCertificateFile /etc/pki/tls/certs/servidor_uclm_es.pem

</VirtualHost>
```

- Antes de reiniciar Apache, comprobamos que la sintaxis de los archivos de configuración es correcta:

```
apachectl configtest
```

- En caso afirmativo, reiniciamos Apache para que ejecute los cambios:

```
systemctl restart httpd
```

5.3 Comprobación del funcionamiento

- Para comprobar que el servidor está entregando tanto su certificado como los certificados intermedios, usamos:

```
openssl s_client -connect mi-servidor.uclm.es:443 -servername mi-servidor.uclm.es -showcerts
```

- Y observamos que el servidor está entregando:
  - Primero el certificado del servidor.
  - Después los certificados intermedios, excluyendo la CA raíz.
- Si se trata de un servidor público, también podemos usar la herramienta en línea SSL Server Test (Powered by Qualys SSL Labs) para realizar esta validación de una forma más cómoda.

6 Renovación de los certificados

Alrededor de **30 días** antes de que caduque el certificado, el **Área TIC** de la **UCLM** se pondrá en contacto con el solicitante del certificado para proceder a su renovación.

A nivel técnico, el proceso de renovación es idéntico al de emisión:

- Los administradores del servidor generan una nueva **CSR**.
- El **Área TIC** envía a firmar la **CSR** y devuelve al solicitante un certificado y una cadena de certificación.
- Los administradores del servidor proceden a instalar la nueva clave privada, el nuevo certificado y la nueva cadena de certificación en su servidor Web.

7 Referencias

- Implementaciones de cliente ACME - Let's Encrypt - Certificados SSL/TLS Gratuitos (letsencrypt.org)
- OpenSSL CSR Tool - Create Your CSR Faster | DigiCert.com
- Extracting the certificate and keys from a .pfx file (ibm.com)
- openssl - How to export CA certificate chain from PFX in PEM format without bag attributes - Unix & Linux Stack Exchange
- How To install SSL Certificate on Apache for CentOS 7 | by Hakan Bayraktar | Medium
- How to troubleshoot SSL connections with the openssl program (a2hosting.com)
- SSL Server Test (Powered by Qualys SSL Labs)