Instalación de certificados SSL en el Application Server Apache

Departamento ID Digital.

Índice

1 Creación del CSR con OpenSSL.

Para la creación del CSR (Certificate Signing Request) es necesario generar en nuestro servidor la llamada clave privada. Primero que nada, nos ubicamos en la carpeta donde queremos que se generen la clave privada y el CSR.

1- Ejecutamos el siguiente comando:

```
openssl req -out CSR.csr -new -newkey rsa:2048 -nodes -keyout claveprivada.key
```

2- Ingrese la información correspondiente a su organización:

a. Country Code — Este campo corresponde al código ISO del país de dos letras en el que se encuentra la empresa. En el caso de Uruguay por ejemplo es UY

b. State/Province —Estado o Provincia. Ejemplo: Montevideo

c. City/Locality — Ciudad o localidad en la que se encuentra.

d. Organization (O)— En este campo debe mencionar la razón social de la empresa registrada en DGI.

e. Organizational Unit (OU) — Deberá mencionar aquí el sector que solicita dicho certificado. Puede ser, por ejemplo: Departamento de Informática.

f. Common Name — Deberá ingresa el nombre del dominio en formato FQDN del dominio. Recuerde, si solicita un Wildcard deberá agregar el "*." Antes del dominio (su izquierda), por ejemplo *.midominio.com.

3- Como resultado de esto, obtendrá dos archivos uno claveprivada.key y otro CSR.csr. El CSR.csr debe abrirse con un editor de texto plano a su elección y copiar su contenido.

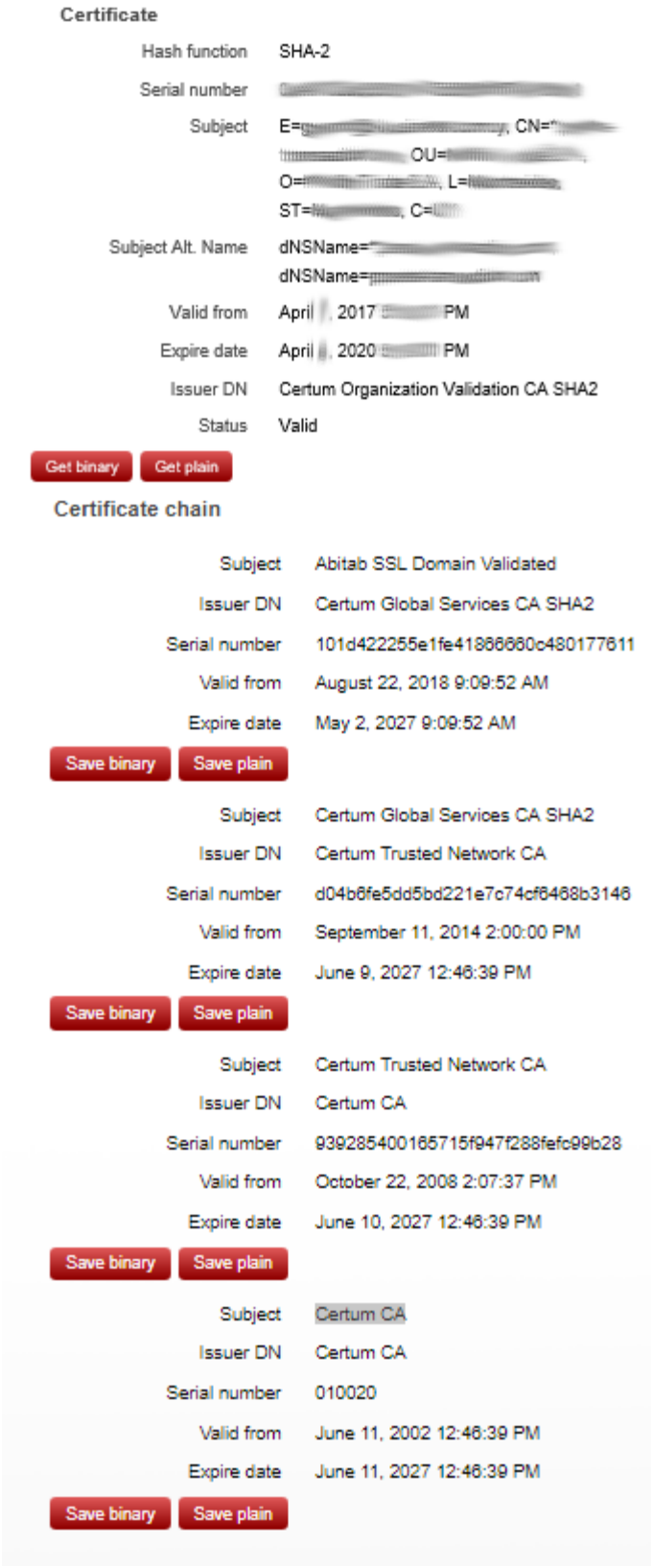
4- Cuando realice el formulario web de solicitud para el certificado SSL, se le solicitara que ingrese el .csr , pegue el texto copiado en el anterior paso para poder continuar con dicha solicitud.

La solicitud será procesada y en breve le llegará a un mail de acuerdo al método de verificación seleccionado.

2 Instalación del certificado.

2.1 Descarga del certificado.

Cuando CERTUM emita el certificado SSL, le llegará un mail a la casilla de correo seleccionada por usted. Este mail contendrá un enlace con los certificados necesarios para la instalación del SSL.



En esta página, observamos que un certificado se puede descargar tipo binary o plain (archivos tipo .cer y otro. pem). A efectos de implementar en nuestro servidor de aplicaciones, solo descargaremos el primer certificado en formato .cer.

Al certificado de la web le llamaremos: Certificado.cer

Al certificado "Certificado.cer" le cambiaremos el formato a .crt
Para ello utilizaremos nuevamente la herramienta OpenSSL:

```
openssl x509 -inform der -in Certificado.cer -out Certificado.crt
```

Ahora nos faltará descargar el ca-bundle de acuerdo a nuestro tipo de certificado SSL: Para

Certificados DV debe descargar el certificado del siguiente enlace:

DVSSLChain-SHA2.crt

Para Certificados OV debe descargar el certificado del siguiente enlace:

OVSSLChain-SHA2.crt

Para Certificados EV debe descargar el certificado del siguiente enlace:

EVSSLChain-SHA2.crt

Una vez descargados simplemente los ubicamos en una carpeta dentro de nuestro sistema, la cual debe ser accesible. Por ejemplo /etc/ssl. A efectos de este manual, vamos a utilizar un certificado OV, por tanto, dentro de la carpeta /etc/ssl finalmente tendremos 3 archivos:

- Clave privada: claveprivada.key
- Clave pública: Certificado.crt
- Certificados Intermedios: OVSSLChain-SHA2.crt

2.2 Configuración del conector.

Para la configurar el servidor y uso del certificado SSL, se debe acceder al archivo de configuración de nuestro servidor web. El mismo se puede ubicar en uno de los siguientes sitios:

- Fedora/CentOS/RHEL: /etc/httpd/conf/httpd.conf
- Debian and Debian based: /etc/apache2/apache2.conf

Los nombres más comunes de este archivo pueden ser:

- httpd-ssl.conf
- ssl.conf
- o en el directorio: /etc/apache2/sites-enabled/

Dentro de este archivo sobre la configuración del VirtualHost del sitio deberíamos tener los siguientes parámetros configurados:

SSLEngine on

SSLCertificateKeyFile /etc/ssl/ssl.key/claveprivada.key

SSLCertificateFile /etc/ssl/ssl.crt/Certificado.crt

SSLCertificateChainFile /etc/ssl/ssl.crt/ OVSSLChain-SHA2.crt

(Los paths presentados son solo de ejemplo, estos paths deben coincidir con la ubicación de los

certificados) Configuración Adicional:

SSLProtocol all

En Apache 2.4 habilitar los protocolos SSLv3 y TLSv1 y opcionalmente TLSv1.1 y TLSv1.2 (en OpenSSL
1.0.1 y superiores versiones).

En Apache 2.2. SSLProtocol All -SSLv2.

SSLHonorCipherOrder On - server enforcement of the ciphers use order

SSLCipherSuite
ECDH+AESGCM:DH+AESGCM:ECDH+AES256:DH+AES256:ECDH+AES128:DH+AES:ECDH+3DES:DH+3DES:RSA+AESGCM:RSA+AES:RSA+3DES:!aNULL:!MD5:!DSS - setting priority for the strong ciphers while at the same time disabling the weak and obsolete ones.

2.3 Reinicio del servidor.

Para que el servidor tome su nueva configuración es necesario el reinicio del servicio apache2.

- En Debian o Ubuntu : /etc/init./apache2 restart
- En RedHat/Fedora/CentOS: apachectl restart
- Otra forma: /usr/sbin/httpsd restart o /etc/init.d/apache restart

3 Verificación del sitio

Existen diferentes tipos de herramientas online que nos permiten verificar el estado del certificado SSL que protege nuestro sitio. Si este sitio se encuentra en producción, podemos verificar a través de la herramienta que nos brinda la web:

https://www.ssllabs.com/ssltest/index.html

Allí no informara del nivel de seguridad que nos brinda nuestro certificado y si este se encuentra correctamente configurado.