Instalación de certificados SSL en Web Server TOMCAT

22/06/2017

Departamento ID Digital.
Gerencia de Negocios.

Índice

1 Creación del CSR con keytool.

El CSR (Certificate Signing Request) es un formato de archivo que contiene un texto cifrado con la información necesaria para la creación de un certificado SSL. Primero debemos ubicarnos en el fichero que contendrá el almacén de certificados que utilizaremos durante toda la operación. Normalmente se encuentra en "**$TOMCAT_HOME/appserver/domains/MiDominio/config/**".

Donde:

- **$TOMCAT_HOME :** Es el fichero home configurado para la instancia de la aplicación tomcat.
- **MiDominio:** Es el fichero correspondiente a la instancia del dominio en el que instalaremos el certificado SSL.

A continuación, deberá seguir los siguientes pasos:

1- Para generar dicho archivo en primera instancia se debe crear el almacén de certificados, que en un futuro contendrá el certificado SSL. El comando para la creación del llamado KEYSTORE (almacén de claves) será el siguiente:

```
keytool -keysize 2048 -genkey -alias aliasclave -keyalg RSA -keystore almacen.jks
```

Donde:

- **aliasclave :** Será el alias que tendrá la clave privada que se genere dentro del almacén .
- **almacen.jks:** es el nombre del almacén de certificados generados.

2- Ingrese una contraseña para el almacén de certificados. La contraseña por defecto es **changeit**.(para evitar problemas futuros, asigne una contraseña diferente a este archivo)

3- Ingrese la información correspondiente a su organización:

- **First and Last 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.
- **Organizational Unit** (OU) — Deberá mencionar aquí el sector que solicita dicho certificado. Puede ser por ejemplo: Departamento de Informática.
- **Organization** (O)— En este campo debe mencionar la razón social de la empresa registrada en DGI.

- **City/Locality** — Ciudad o localidad en la que se encuentra.
- **State/Province** —Estado o Provincia. Ejemplo: Montevideo
- **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

4- Una vez se crea el almacén de certificados se genera el archivo .csr :

```
keytool -certreq -keyalg RSA -alias aliasclave -file CSR.csr -keystore almacen.jks
```

Le solicitaran la contraseña del almacén de claves ingresada en los pasos anteriores. Al finalizar en el mismo fichero en que se encuentra ubicada tendrá creado el archivo .csr

5- Abrimos el archivo generado con nuestro editor de texto favorito y copiamos el contenido del mismo.

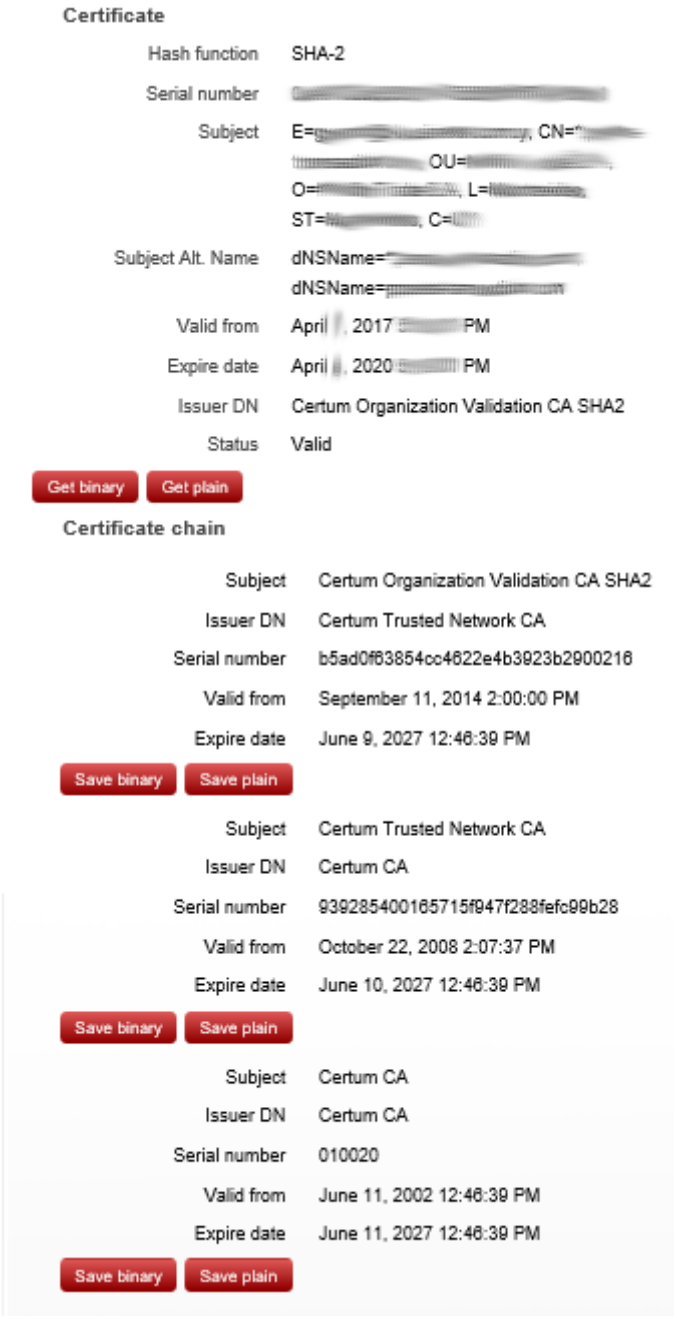
6- Cuando realice el formulario web de solicitud para el certificado SSL, se le solicitara que ingrese el .csr , pegue el texto copiado en el anterior paso para poder continuar con dicha solicitud.

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. A efectos del tipo de almacén de claves con el que contamos (jks) debemos descargarnos los certificados en la opción “Get plain” y “Save plain”. Al hacer esto, los archivos descargados tendrán la extensión

.pem . El primer certificado que figura, es el certificado solicitado, luego se visualizan los certificados que representan a la "Chain of Trust". Para facilitar su uso en este manual, le pondremos nombres a cada certificado descargado:

1. El certificado de la web le llamaremos: Certificado.pem
2. El primer certificado de la "Chain of Trust" será: CertumOrganization.pem
3. El segundo certificado de la "Chain of Trust" será: CertumTrusted.pem
4. El tercer certificado de la "Chain of Trust" será: CertumCA.pem

Una vez descargados y con su nombre, deben ubicar el certificado en la misma carpeta en la que se encuentra el almacén de certificados JKS.

2.2 Importación del certificado en el almacén de certificados.

Por consola nos ubicamos en la carpeta donde se encuentra el almacén de certificados. Empezaremos a importar los certificados intermedios y root en el almacén respetando el orden de la cadena de confianza. Para ello ejecutamos los siguientes comandos:

1.

```
keytool -import -alias certumorganization -keystore almacen.jks -trustcacerts -file CertumOrganization.pem
```

2.

```
keytool -import -alias certumtrusted -keystore almacen.jks -trustcacerts -file CertumTrusted.pem
```

3.

```
keytool -import -alias certumca -keystore almacen.jks -trustcacerts -file CertumCA.pem
```

El último certificado de estos, a veces no lo permite instalar dentro del almacén, en estos casos simplemente ignore el mensaje de error y no instale el certificado (por defecto muchos servidores de aplicaciones ya cuentan con este certificado integrado).

Para finalizar importaremos nuestro certificado en el almacén de certificados ejecutando el siguiente comando.

```
keytool -import -alias aliasclave -keystore almacen.jks -trustcacerts -file Certificado.pem
```

Es importante mencionar que el alias dado a este certificado debe ser el mismo que utilizaron al crear el almacén de certificados, es decir, la clave privada debe tener el mismo alias que la clave pública. Con esto tendremos un almacén de certificados listo para ser implementado.

3 Configuración Necesaria

El último paso a realizar es asegurarnos que Tomcat acceda al almacén de certificados:

1) Acceda al a través de su editor de texto preferido al archivo server.xml (generalmente ubicado en el home de Tomcat dentro de la carpeta conf).
2) En dicho archivo ubicamos el conector a utilizar por el SSL
3) Dentro del conector lo modificamos de acuerdo a la versión de TOMCAT con la que contamos:

- **En Tomcat 4.xx** :

```
<clientAuth="false" protocol="TLS"     keystoreFile="/etc/tomcat5/tomcat.keystore"
 keystorePass="changeit" />
```

- **En Tomcat 5.xx, 6.xx y 7.xx**:

```
<-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

     <Connector

          port="8443" maxThreads="200"

          scheme="https" secure="true" SSLEnabled="true"


keystoreFile="$TOMCAT_HOME/appserver/domains/MiDominio/config/almacen.jks"

           keystorePass="changeit"

           clientAuth="false" sslProtocol="TLS"/>
```

- ✓ En keystoreFile= deberá colocar el path donde se encuentra nuestro almacén de certificados.
- ✓ En port= puede ser 8443 o 443.
- ✓ Si su versión de TOMCAT es anterior a la 7.xx se deberá cambiar el keystorePASS por keypass.

4) Luego de realizar el cambio pertinente sobre server.xml, guarda los cambios realizados y reinicia el servicio de TOMCAT.

Conéctese a la aplicación y verifique si se publica correctamente.

4 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.