

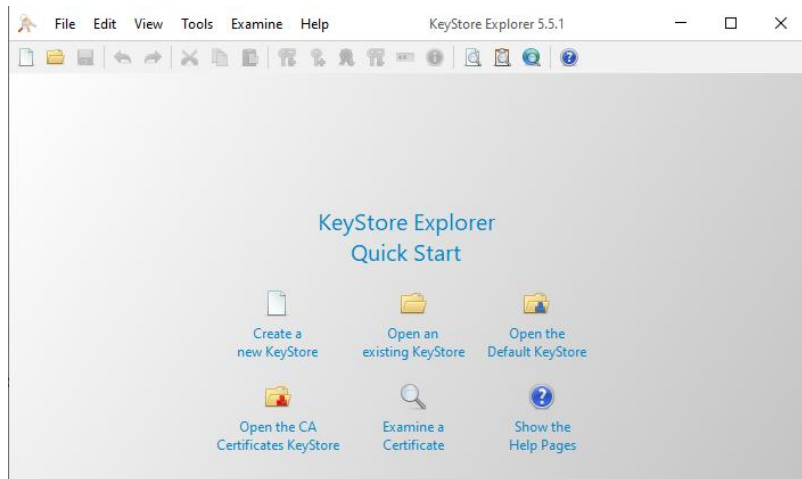
PRACTICA 2. ATW

CREACION DE CERTIFICADOS SSL CON JAVA Y TOMCAT(PARTE II)

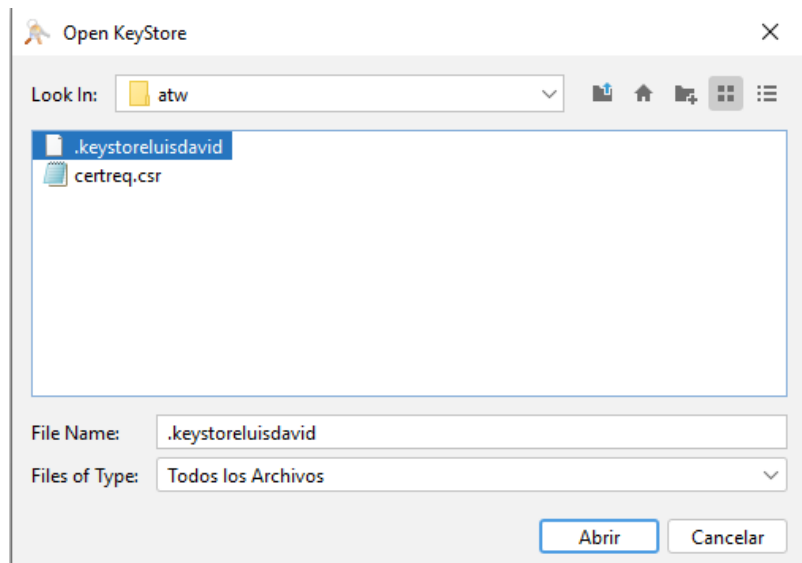
En esta parte seremos nosotros quienes generaremos nuestro propio certificado con las herramientas proporcionadas en la práctica (OpenSSL y Keystore Explorer)

Para empezar, deberemos exportar nuestra clave privada a través del programa *Keystore Explorer*. Los pasos para seguir, en este proceso se verán en las siguientes imágenes.

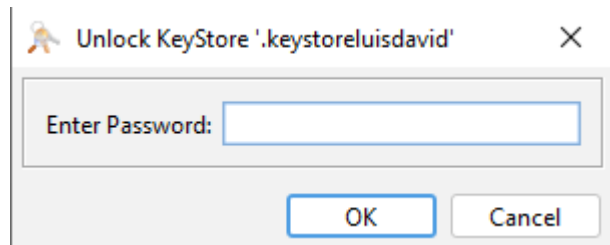
1) Abrimos el programa *keystore Explorer* y pulsamos sobre el icono de la carpeta con el título “*Open an existing KeyStore*”



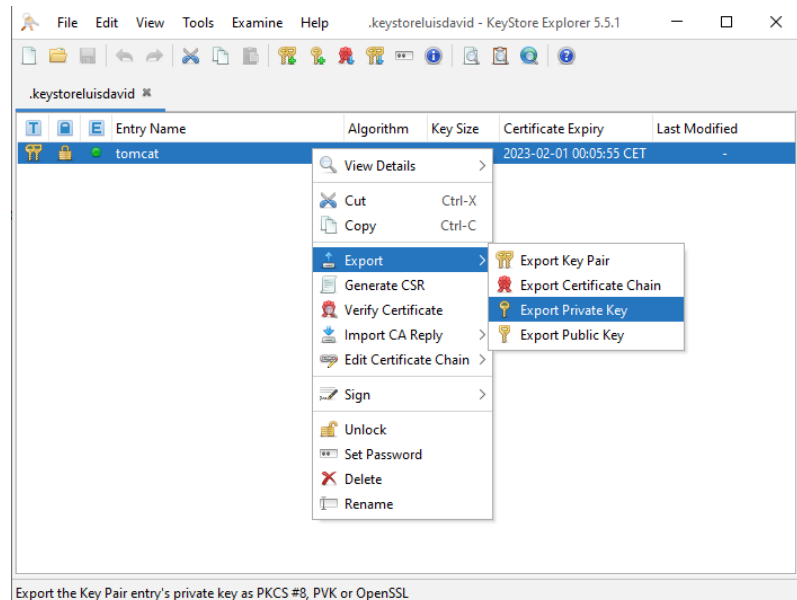
2) Buscamos la carpeta donde hemos guardado **nuestro keystore** y lo seleccionamos



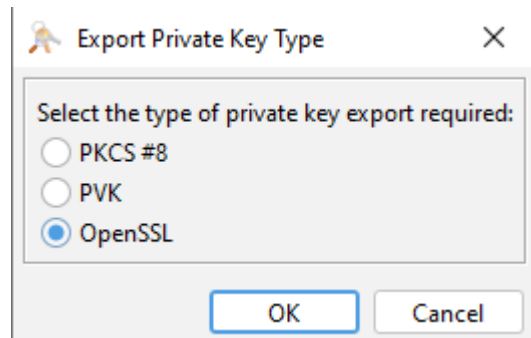
3) Se nos pedirá la contraseña del keystore, introducimos la que hemos usado durante la parte 1. En este caso "changeit".



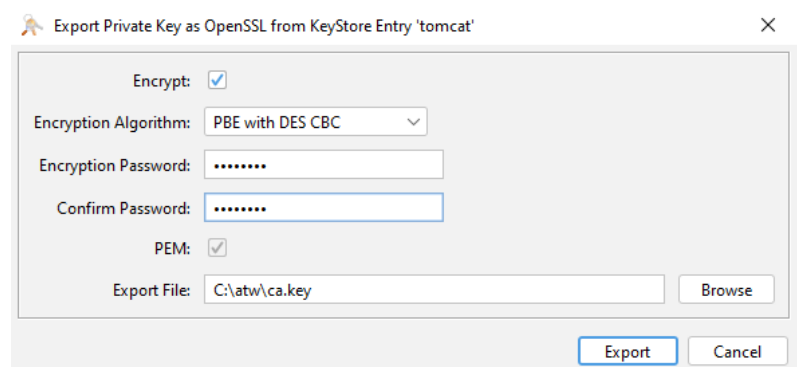
4) Una vez abierto nuestro keystore, nos aparecerá un fichero en el programa. Para exportar la clave privada, haremos clic derecho, clicamos en "Export" y seleccionamos "Export Private Key".



5) Se nos abrirá esta ventana para seleccionar el tipo de exportación y seleccionaremos OpenSSL



6) Luego de seleccionar el tipo de exportación se nos abrirá otra ventana la cual nos pedirá una contraseña para el archivo, usaremos "changeit" y en Export File introduciremos la carpeta destino ("C:\atw\") y el nombre de este al importarse ("ca.key").



7) En segundo lugar generaremos un certificado .csr que hemos exportado en la parte 1 de esta práctica, y la clave privada que hemos exportado en esta parte (ca.key), para ello usaremos OpenSSL, que abriremos desde nuestro directorio que indicamos en la parte 1 para guardar nuestra keystore.

```
OpenSSL> x509 -req -days 365 -in certreq.csr -signkey ca.key -out certificadotomcat.crt
Signature ok
subject=C = ES, ST = Alicante, L = Orihuela, O = UMH.ES, OU = UMH, CN = ATWLuisDavidDiazMesa.com
Getting Private key
Enter pass phrase for ca.key:
OpenSSL>
```

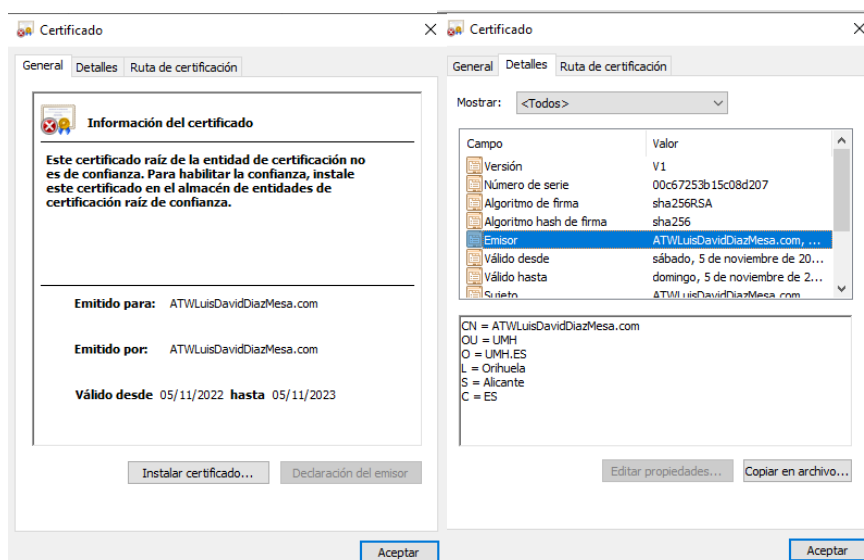
Con esa línea de comando ya habremos generado el certificado. A continuación, instalaremos el certificado y lo exportaremos.

8) Vamos a nuestro directorio y comprobamos que se ha creado el certificado.

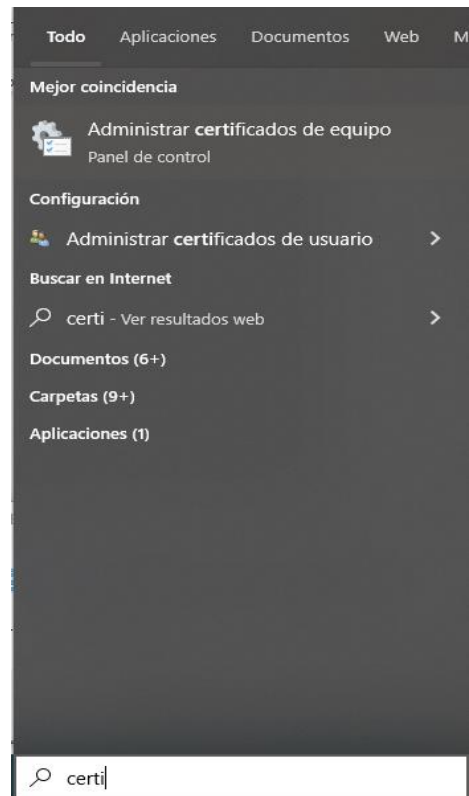
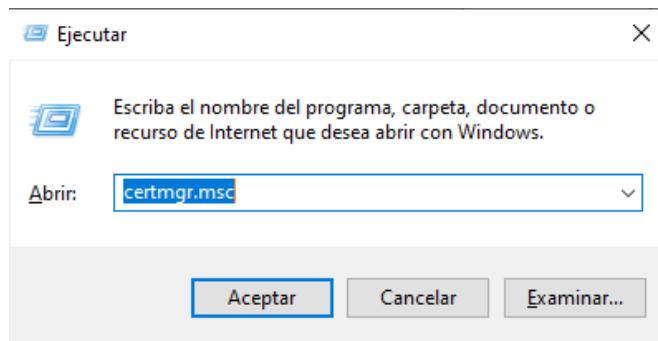
equipo > OS (C:) > atw

Nombre	Fecha de modificación	Tipo
.DS_Store	13/04/2018 21:41	Archivo DS_STORE
.gitattributes	27/03/2018 15:50	Archivo de origen ...
.gitignore	27/03/2018 15:50	Documento de te...
.keystoreluisdavid	03/11/2022 0:05	Archivo KEYSTORE...
.travis.yml	27/03/2018 15:50	Archivo de origen ...
.travis-apt-pin.preferences	27/03/2018 15:50	Archivo PREFERE...
.travis-create-release.sh	27/03/2018 15:50	Shell Script
ca.key	05/11/2022 22:59	Archivo KEY
certificadotomcat.crt	05/11/2022 23:06	Certificado de seg...
certreq.csr	03/11/2022 18:53	Archivo CSR
libcrypto-1_1-x64.dll	13/04/2018 17:29	Extensión de la ap...
libssl-1_1-x64.dll	13/04/2018 17:29	Extensión de la ap...
openssl.cnf	27/03/2018 15:50	Archivo CNF
openssl.exe	13/04/2018 17:30	Aplicación
tomcat.key	05/11/2022 22:58	Archivo KEY

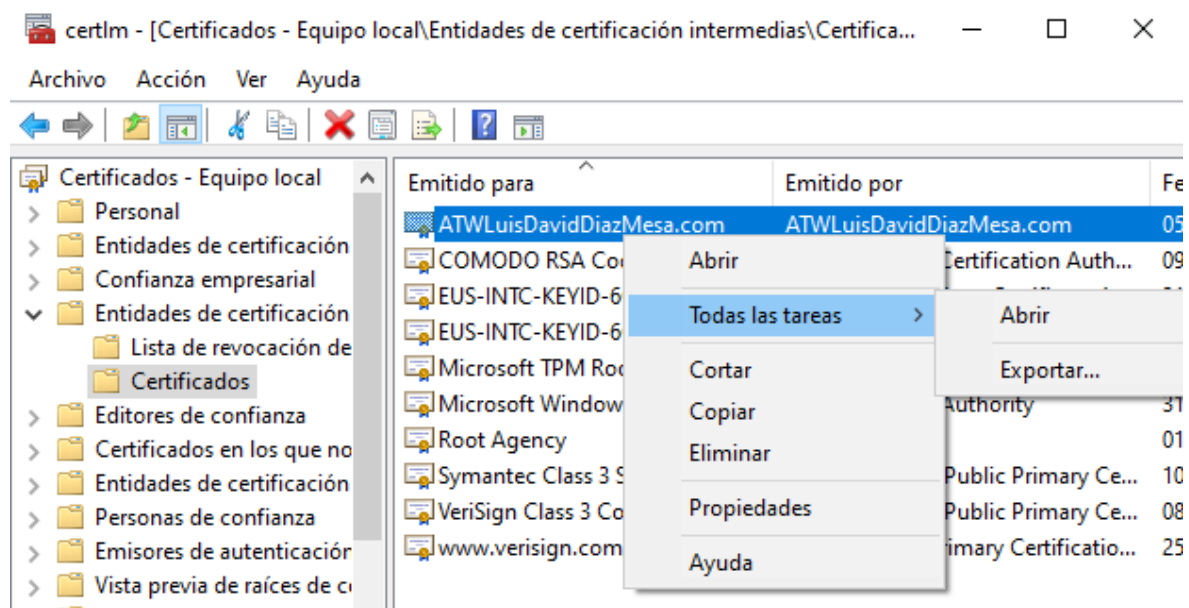
9) Hacemos doble clic en el archivo y le damos al botón “Instalar certificado”. También podemos examinar la información que contiene el certificado en la pestaña “Detalles”.



10) Para comprobar la correcta instalación del certificado usamos la herramienta de Windows, **certlm**, podremos acceder a esta herramienta en Windows pulsando Windows+R y en el buscador escribir “**certmgr.msc**”. También podemos buscar la herramienta en el buscador de Windows tan sólo con escribir “certificado”.



11) Dentro de la herramienta buscamos nuestro certificado dentro de las carpetas “Entidades de certificación intermedias” → “Certificados” y seleccionamos nuestro archivo para exportarlo y obtener nuestra clave publica .cer.



12) Al pulsar sobre “Exportar” se nos abrirá el asistente para exportar certificados y tan solo daremos a siguiente→siguiente→seleccionamos la ubicación del archivo y su nombres→siguiente→finalizar.

1

← Asistente para exportar certificados

Este es el Asistente para exportar certificados

Este asistente lo ayuda a copiar certificados, listas de certificados de confianza y listas de revocación de certificados desde un almacén de certificados a su disco.

Un certificado, que lo emite una entidad de certificación, es una confirmación de su identidad y contiene información que se usa para proteger datos o para establecer conexiones de red seguras. Un almacén de certificados es el área del sistema donde se guardan los certificados.

Para continuar, haga clic en Siguiente.

Siguiente

Cancelar

2

← Asistente para exportar certificados

Formato de archivo de exportación

Los certificados pueden ser exportados en diversos formatos de archivo.

Seleccione el formato que desea usar:

☒ DER binario codificado X.509 (.CER)

☐ X.509 codificado base 64 (.CER)

☐ Estándar de sintaxis de cifrado de mensajes: certificados PKCS #7 (.P7B)

☐ Incluir todos los certificados en la ruta de certificación (si es posible)

☐ Intercambio de información personal: PKCS #12 (.PFX)

☐ Incluir todos los certificados en la ruta de certificación (si es posible)

☐ Eliminar la clave privada si la exportación es correcta

☐ Exportar todas las propiedades extendidas

☐ Habilitar privacidad de certificado

☐ Almacén de certificados en serie de Microsoft (.SST)

Siguiente

Cancelar

3

← Asistente para exportar certificados

Archivo que se va a exportar

Especifique el nombre del archivo que desea exportar

Nombre de archivo:

C:\atw\publica.cer

Examinar...

Siguiente

Cancelar

4

← Asistente para exportar certificados

Finalización del Asistente para exportar certificados

El Asistente para exportar certificados se completó correctamente.

Especificó la siguiente configuración:

Nombre de archivo	C:\atw\publica.cer
Exportar claves	No
Incluir todos los certificados en la ruta de certificación	No
Formato de archivo	DER binario codificado X.509 (

Finalizar

Cancelar

13) Por último para importar la clave pública, copiaremos este último archivo en el directorio donde se encuentra el programa “Keytool” e introduciremos lo siguiente en este último programa. Se nos pedirá la contraseña y una vez puesta ya tendremos el certificado importado en nuestro *keystore*.

C:\Windows\System32\cmd.exe

```
C:\Program Files\Java\jdk-19\bin>keytool -import -trustcacerts -alias tomcat -file "C:\Program Files\Java\jdk-19\bin\publica.cer" -keystore C:\atw\keystoreluisdavid_
```

14) Para terminar, cambiaremos el nombre de nuestro host para acceder a nuestro servidor a través del nombre de nuestro dominio en vez de *localhost*. Para ello modificaremos el nombre de nuestro host cambiándolo en un archivo ubicado en ...\\System32\\drivers\\etc\\hosts

equipo > OS (C:) > Windows > System32 > drivers > etc

Nombre	Fecha de modificación	Tipo	Ti
hosts	18/03/2017 22:01	Archivo	
hosts.ics	10/10/2022 10:32	Archivo iCalendar	
lmhosts.sam	07/12/2019 10:12	Archivo SAM	
networks	18/03/2017 22:01	Archivo	
protocol	18/03/2017 22:01	Archivo	
services	18/03/2017 22:01	Archivo	

15) Abrimos el archivo con un editor y modificamos la línea comentada donde aparece el nombre de nuestro servidor como localhost

```
# Copyright (c) 1993-2009 Microsoft Corp.
#
# This is a sample HOSTS file used by Microsoft TCP/IP for Windows.
#
# This file contains the mappings of IP addresses to host names. Each
# entry should be kept on an individual line. The IP address should
# be placed in the first column followed by the corresponding host name.
# The IP address and the host name should be separated by at least one
# space.
#
# Additionally, comments (such as these) may be inserted on individual
# lines or following the machine name denoted by a '#' symbol.
#
# For example:
#
#       102.54.94.97       rhino.acme.com       # source server
#       38.25.63.10       x.acme.com          # x client host
#
# localhost name resolution is handled within DNS itself.
#       127.0.0.1         ATWLuisDavidDiazMesa.com
#       ::1               localhost
```

16) Por último comprobamos si el cambio ha funcionado intentando acceder a nuestro servidor desde el navegador con nuestro dominio.

Apache Tomcat/10.1.1

Home Documentation Configuration Examples Wiki Mailing Lists Find Help

If you're seeing this, you've successfully installed Tomcat. Congratulations!

Recommended Reading:

- [Security Considerations How-To](#)
- [Manager Application How-To](#)
- [Clustering/Session Replication How-To](#)

Server Status
Manager App
Host Manager

Developer Quick Start

- [Tomcat Setup](#)
- [First Web Application](#)
- [Realms & AAA](#)
- [JDBC Data Sources](#)
- [Examples](#)
- [Servlet Specifications](#)
- [Tomcat Versions](#)