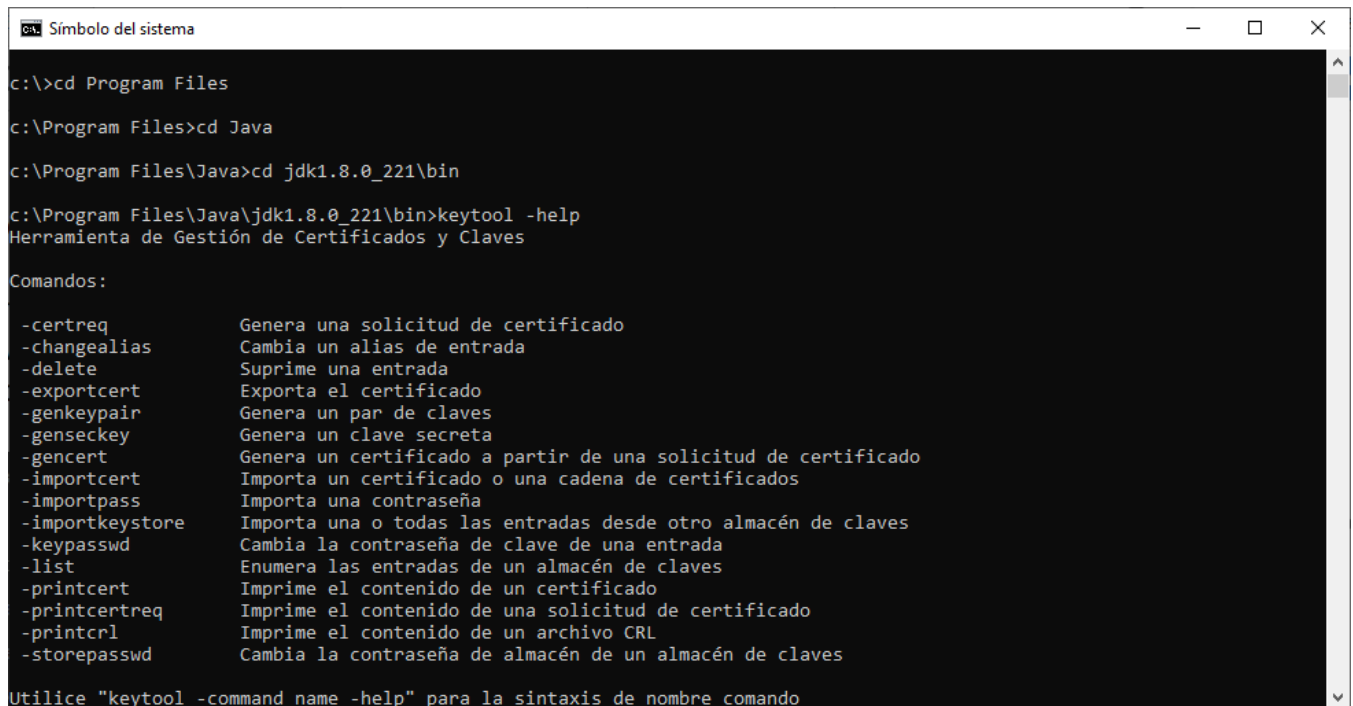


Práctica Lección 5. Mensajería de última Milla II

Parte 1:

Primero se verifica la ayuda de keytool,



```

C:\>cd Program Files
C:\Program Files>cd Java
C:\Program Files\Java>cd jdk1.8.0_221\bin
C:\Program Files\Java\jdk1.8.0_221\bin>keytool -help
Herramienta de Gestión de Certificados y Claves

Comandos:

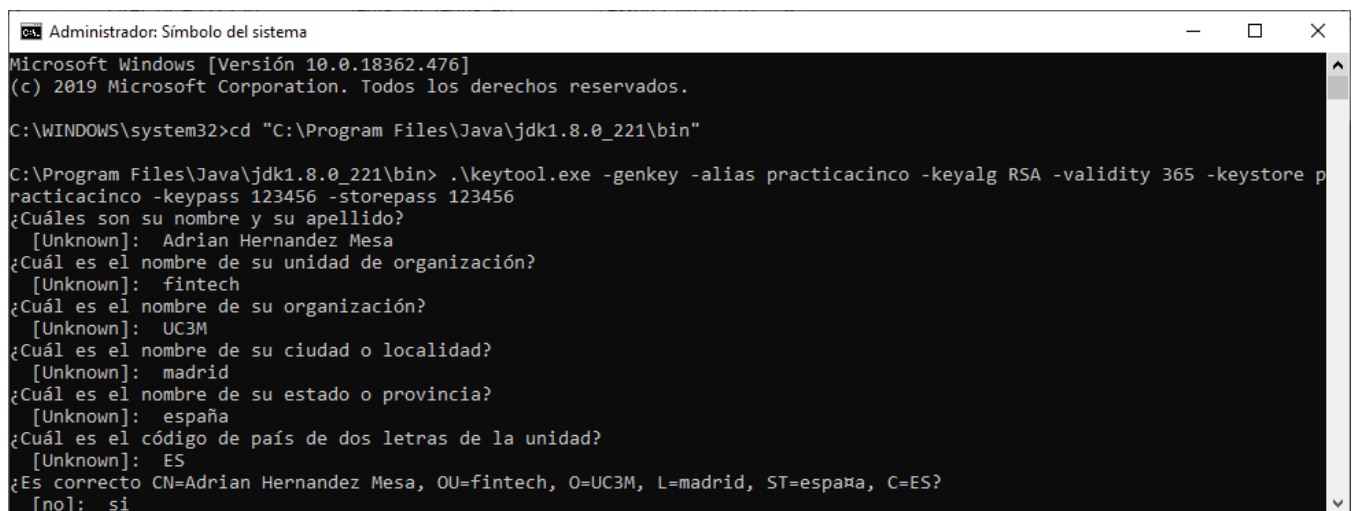
-certreq          Genera una solicitud de certificado
-changealias      Cambia un alias de entrada
-delete          Suprime una entrada
-exportcert       Exporta el certificado
-genkeypair       Genera un par de claves
-genseckey        Genera un clave secreta
-gencert          Genera un certificado a partir de una solicitud de certificado
-importcert       Importa un certificado o una cadena de certificados
-importpass       Importa una contraseña
-importkeystore   Importa una o todas las entradas desde otro almacén de claves
-keypasswd        Cambia la contraseña de clave de una entrada
-list            Enumera las entradas de un almacén de claves
-printcert        Imprime el contenido de un certificado
-printcertreq     Imprime el contenido de una solicitud de certificado
-printcrl         Imprime el contenido de un archivo CRL
-storepasswd      Cambia la contraseña de almacén de un almacén de claves

Utilice "keytool -command_name -help" para la sintaxis de nombre_comando

```

Creación de certificados

Para desarrollar la práctica primero deberemos crear un certificado. Utilizaremos la herramienta keytools de la JDK. Dado que mi entorno es en Windows invocaré la herramienta desde el PowerShell.



```

Microsoft Windows [Versión 10.0.18362.476]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>cd "C:\Program Files\Java\jdk1.8.0_221\bin"

C:\Program Files\Java\jdk1.8.0_221\bin>.\keytool.exe -genkey -alias practiacinco -keyalg RSA -validity 365 -keystore p
racticacinco -keypass 123456 -storepass 123456
¿Cuáles son su nombre y su apellido?
[Unknown]: Adrian Hernandez Mesa
¿Cuál es el nombre de su unidad de organización?
[Unknown]: fintech
¿Cuál es el nombre de su organización?
[Unknown]: UC3M
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: madrid
¿Cuál es el nombre de su estado o provincia?
[Unknown]: españa
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: ES
¿Es correcto CN=Adrian Hernandez Mesa, OU=fintech, O=UC3M, L=madrid, ST=españa, C=ES?
[no]: si

```

Podemos comprobar el certificado:

```

Administrador: Símbolo del sistema
Microsoft Windows [Versión 10.0.18362.476]
(c) 2019 Microsoft Corporation. Todos los derechos reservados.

C:\WINDOWS\system32>cd "C:\Program Files\Java\jdk1.8.0_221\bin"

C:\Program Files\Java\jdk1.8.0_221\bin>keytool -genkey -alias practicefive -keyalg RSA -validity 365 -keystore practicefive -keypass 123456 -storepass 123456
¿Cuáles son su nombre y su apellido?
[Unknown]: Adrian Hernandez
¿Cuál es el nombre de su unidad de organización?
[Unknown]: uc3m
¿Cuál es el nombre de su organización?
[Unknown]: uc3m
¿Cuál es el nombre de su ciudad o localidad?
[Unknown]: madrid
¿Cuál es el nombre de su estado o provincia?
[Unknown]: madrid
¿Cuál es el código de país de dos letras de la unidad?
[Unknown]: ES
¿Es correcto CN=Adrian Hernandez, OU=uc3m, O=uc3m, L=madrid, ST=madrid, C=ES?
[no]: si

Warning:
El almacén de claves JKS utiliza un formato propietario. Se recomienda migrar a PKCS12, que es un formato estándar del sector que utiliza "keytool -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_221\bin>keytool -list -v -keystore practicefive
Introduzca la contraseña del almacén de claves:
Tipo de Almacén de Claves: jks
Proveedor de Almacén de Claves: SUN

Su almacén de claves contiene 1 entrada

Nombre de Alias: practicefive
Fecha de Creación: 04-dic-2019
Tipo de Entrada: PrivateKeyEntry
Longitud de la Cadena de Certificado: 1
Certificado[1]:
Propietario: CN=Adrian Hernandez, OU=uc3m, O=uc3m, L=madrid, ST=madrid, C=ES
Emisor: CN=Adrian Hernandez, OU=uc3m, O=uc3m, L=madrid, ST=madrid, C=ES
Número de serie: 70197df8
Válido desde: Wed Dec 04 10:38:00 CET 2019 hasta: Thu Dec 03 10:38:00 CET 2020
Huellas digitales del certificado:
MD5: 57:AD:00:43:C0:03:09:8C:DA:B0:8C:FC:04:2D:29:47

```

```

Seleccionar Administrador: Símbolo del sistema
C:\Program Files\Java\jdk1.8.0_221\bin>keytool -list -v -keystore practicefive
Introduzca la contraseña del almacén de claves:
Tipo de Almacén de Claves: jks
Proveedor de Almacén de Claves: SUN

Su almacén de claves contiene 1 entrada

Nombre de Alias: practicefive
Fecha de Creación: 04-dic-2019
Tipo de Entrada: PrivateKeyEntry
Longitud de la Cadena de Certificado: 1
Certificado[1]:
Propietario: CN=Adrian Hernandez, OU=uc3m, O=uc3m, L=madrid, ST=madrid, C=ES
Emisor: CN=Adrian Hernandez, OU=uc3m, O=uc3m, L=madrid, ST=madrid, C=ES
Número de serie: 70197df8
Válido desde: Wed Dec 04 10:38:00 CET 2019 hasta: Thu Dec 03 10:38:00 CET 2020
Huellas digitales del certificado:
MD5: 57:AD:00:43:C0:03:09:8C:DA:B0:8C:FC:04:2D:29:47
SHA1: 5A:9A:56:92:A8:9F:AE:71:52:21:1D:28:EC:E2:F6:69:90:B6:A5:3F
SHA256: 63:B0:A9:91:70:72:A3:F9:66:31:44:DD:63:E8:86:DB:5A:C7:02:D3:6B:0B:90:65:04:78:F8:4B:76:C0:C1:DA
Nombre del algoritmo de firma: SHA256withRSA
Algoritmo de clave pública de asunto: Clave RSA de 2048 bits
Versión: 3

Extensiones:
#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: B3 8B 0F A2 73 BA 44 81 5D 1B 81 07 3E 70 DA 74 .....s.D.]...p.t
0010: D9 24 49 E1 .....$.I.
]
]

*****
*****

Warning:
El almacén de claves JKS utiliza un formato propietario. Se recomienda migrar a PKCS12, que es un formato estándar del sector que utiliza "keytool -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

```

Se exporta el certificado:

```

Administrador: Símbolo del sistema
C:\Program Files\Java\jdk1.8.0_221\bin>keytool -export -alias practicefive -keystore practicefive -rfc -file Certpracticefive.cer
Introduzca la contraseña del almacén de claves:
Certificado almacenado en el archivo <Certpracticefive.cer>

Warning:
El almacén de claves JKS utiliza un formato propietario. Se recomienda migrar a PKCS12, que es un formato estándar del sector que utiliza "keytool -importkeystore -srckeystore practicefive -destkeystore practicefive -deststoretype pkcs12".

C:\Program Files\Java\jdk1.8.0_221\bin>_

```

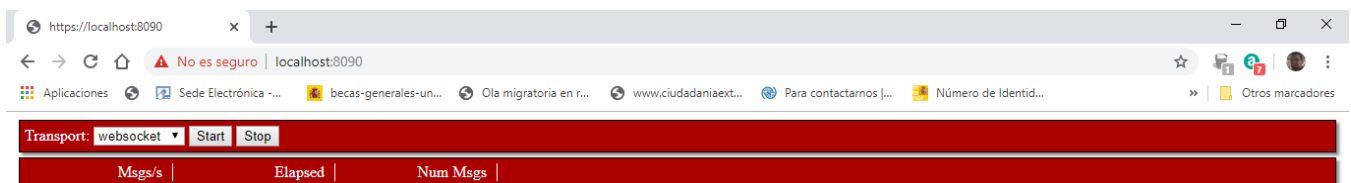
```

C:\Program Files\Java\jdk1.8.0_221\bin>.keytool.exe -export -alias practiacinco -keystore practiacinco -rfc -file pra
cticacincoPublica.cer
Introduzca la contraseña del almacén de claves:
Certificado almacenado en el archivo <practicacincoPublica.cer>
  
```

Se obtiene el siguiente certificado:



Luego de instalado el certificado el mismo abre sin problema en el navegador:



Práctica de medición de mensajes por segundo

SleepTime	Msg/seg		Time	Msgs		Transport
	http	https		http	https	
0	292	131	15	4387	1966	websocket
0	30	17	15	443	251	Long-polling
1	97	109	15	1454	1641	websocket
1	11	17	15	166	248	Long-polling
10	94	62	15	1413	97	websocket
10	10	17	15	153	254	Long-polling

SleepTime 0

Transport: websocket Start Stop	Transport: long-polling Start Stop
292 msg/s 4387 msg/s	30 msg/s 443 msg/s
15 time	15 time

SleepTime 1

Transport: websocket Start Stop	Transport: long-polling Start Stop
97 msg/s 1454 msg/s	11 msg/s 166 msg/s
15 time	15 time

SleepTime 10

Transport: websocket Start Stop	Transport: long-polling Start Stop
94 msg/s 1413 msg/s	10 msg/s 153 msg/s
15 time	15 time

Comparando con los valores de la práctica 4 podemos ver que usando una conexión segura la tasa de envío/recepción de mensajes es menor.

Cifrado y Descifrado simétrico/asimétrico

En modo de cifrado simétrico se envía "Hello world!":

```
practicas - Lesson5/src/main/java/com/cnebrera/uc3/tech/lesson5/LauncherCryptoAES.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help

LauncherWeb.java LauncherCryptoAES.java LauncherCryptoRSA.java AESEncrypt.java
24 System.out.println("Message to be encoded: " + msg);
25
26 // Create a new instance of AESCrypto
27 final AESCrypto aesCrypto = AESCrypto.createNewInstance();
28
29 // Encode directly to the array
30 final byte[] msgEncoded = aesCrypto.encode(msg.getBytes());
31
32 // Printout the encoded message
33 System.out.println("Message encoded: " + new String(msgEncoded));
34
35 // Decode the encoded message
36 final byte[] msgDecoded = aesCrypto.decode(msgEncoded);
37
```

Console

```
<terminated> LauncherCryptoAES [Java Application] C:\Program Files\Java\jdk1.8.0_221\bin\javaw.exe (9 dic. 2019 22:07:25)
Message to be encoded: Hello world!
Message encoded: =<ps@>*9*+&@
Message decoded: Hello world!
```

En modo de cifrado asimétrico se envía "Hello world!":

```
practicas - Lesson5/src/main/java/com/cnebrera/uc3/tech/lesson5/LauncherCryptoRSA.java - Eclipse IDE
File Edit Source Refactor Navigate Search Project Run Window Help

LauncherWeb.java LauncherCryptoAES.java LauncherCryptoRSA.java
11 /*
12 public class LauncherCryptoRSA
13 {
14     /**
15      * @throws Lesson5Exception with an occurred exception
16      *
17      */
18     private void doExample() throws Lesson5Exception
19     {
20         // Message to encode/decode
21         final String msg = "Hello world!";
22
23         // Printout the message
24         System.out.println("Message to be encoded: " + msg);
```

Console

```
<terminated> LauncherCryptoAES [Java Application] C:\Program Files\Java\jdk1.8.0_221\bin\javaw.exe
Message to be encoded: Hello world!
Message encoded: M*Pn%&@*+*****
Message decoded: Hello world!
```