Universidad
Carlos III de Madrid

TECNOLOGÍAS *DEL* SECTOR FINANCIERO

Práctica 5: Mensajería de última milla 2

Andoni Alcelay

MÁSTER UNIVERSITARIO EN TECNOLOGÍAS DEL SECTOR FINANCIERO: FINTECH

Introducción

En este documento se encontrará el desarrollo de la práctica 5, mensajería de última milla 2. La cual está dividida en 2 partes. La primera, la creación de un certificado para la práctica a realizar, y la segunda, la comparación de las mediciones entre los resultados de la práctica anterior y esta.

Certificado generado con keytool

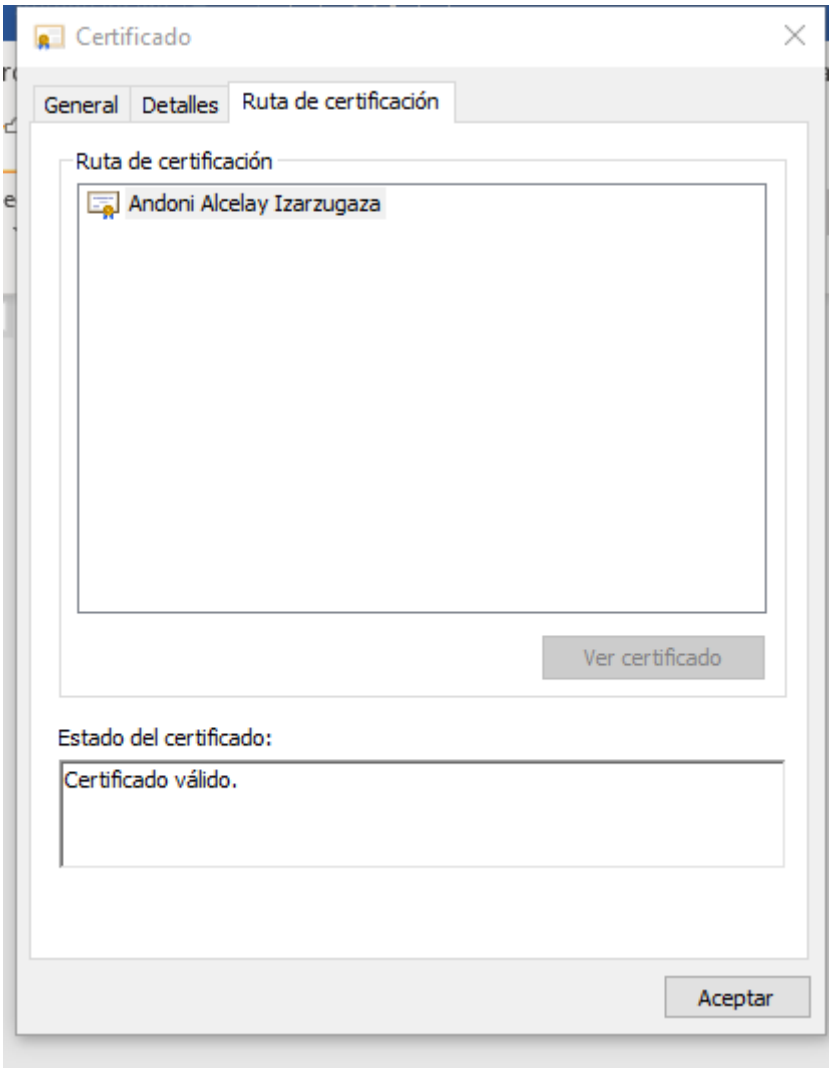
Creación del certificado

```
C:\Program Files\Java\jdk1.8.0_191\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: 11-nov-2018
Tipo de Entrada: PrivateKeyEntry
Longitud de la Cadena de Certificado: 1
Certificado[1]:
Propietario: CN=Andoni Alcelay Izarzugaza, OU=BSTPRG, O=BestProgramming, L=Durango, ST=Bizkaia, C=ES
Emisor: CN=Andoni Alcelay Izarzugaza, OU=BSTPRG, O=BestProgramming, L=Durango, ST=Bizkaia, C=ES
Número de serie: e1fd82d
Válido desde: Sun Nov 11 20:54:54 CET 2018 hasta: Mon Nov 11 20:54:54 CET 2019
Huellas digitales del certificado:
         MD5: 65:4C:44:92:7A:A4:B8:23:18:61:E7:06:5C:D0:0B:2D
         SHA1: 80:19:DB:FB:28:2E:DD:FC:2B:6A:4E:6B:FF:17:42:4A:4D:15:25:FB
         SHA256: DB:17:37:F5:E5:ED:DD:83:D3:DD:39:FE:85:26:AA:E3:1B:79:61:31:FE:2D:D1:B8:B4:86:FC:75:AE:A7:38:C7
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: 90 E6 0B F5 95 8E 5A 53   4E 81 F0 2E DC B4 0F C0  ......ZSN.......
0010: 34 6E 21 FD                                        4n!.
]
]



*******************************************
*******************************************
```

Exportación del certificado

```
C:\Program Files\Java\jdk1.8.0_191\bin>keytool -export -alias practicefive -keystore practicefive -rfc -file PracticeFivePublica.cer
Introduzca la contraseña del almacén de claves:
Certificado almacenado en el archivo <PracticeFivePublica.cer>
```

Imagen del certificado generado, y la confirmación de que el certificado es válido



Resultados de mediciones

Para esto usaremos dos mediciones, en la parte superior se encuentran las mediciones correspondientes a la práctica 4. Y en la parte inferior en las de la actual, de manera que estas se puedan comparar.

RESULTADOS DE LA PRÁCTICA 4		
LONG POLLING	**WEBSOCKET**	**SLEEP TIME**
		0
		1
		10

RESULTADOS DE LA PRÁCTICA 5		
LONG POLLING	**WEBSOCKET**	**SLEEP TIME**
		0
		1
		10

Como puede observarse en los tiempos, en la conexión segura todo va más despacio. Esto se debe a que al realizar una conexión https, cada paquete enviado tiene que verificar si la conexión segura está activa, lo que produce que la velocidad de envío de los mensajes en cualquier caso disminuya considerablemente.