Herramienta keyTool

Descripción de Keytool

- **Keytool** es una utilidad que permite la gestión de
  - Claves
  - Certificados

- **Keytool** permite a los usuarios:
  - Administrar pares de claves pública/privada y los certificados asociados para su uso en una autenticación.
  - Almacenar en caché las claves públicas, en forma de certificados, de las personas con las que se comunican.

- **Keytool** permite almacenar claves y certificados en un almacén denominado **Keystore(almacén de certificados).**

Keystore y Truststore

• **Keystore:** almacén de certificados. Desde la perspectiva de JSSE es una base de datos de los pares llaves y de los certificados que se utilizan para la autentificación del SSL.

• **Truststore:** almacena certificados de las Autoridades de Certificación (CA). Se utilizan para verificar las identidades de otros clientes y servidores.

- Cuando un cliente o un servidor inicia una sesión del SSL, extrae sus certificados y claves de su almacén de certificados (keystore).
- Cuando verifica las identidades de otros clientes o servidores, extraerá los certificados de la Autoridad de la Certificación de su truststore.

Creación de un certificado para utilizar con SSL (I)

El siguiente comando crea un certificado de clave pública de nombre claveSsl, con el algoritmo RSA y lo almacena en el keystore de nombre AlmacenSSL

```
keytool -genkey -alias claveSsl -keyalg RSA -keystore AlmacenSSL
```

Creación de un certificado para utilizar con SSL (II)

Al introducir el comando nos solicita la contraseña del keystore, (damos por ejemplo 123456), nombre,etc. Observa la captura:

```
C:\Users\za>keytool -genkey -alias claveSsl -keyalg RSA -keystore AlmacenSSL
Escriba la contrase±a del almacÚn de claves:
Volver a escribir la contrase±a nueva:
¿Cußles son su nombre y su apellido?
  [Unknown]:  ies alandalus
¿Cußl es el nombre de su unidad de organizaci¾n?
  [Unknown]:  edu
¿Cußl es el nombre de su organizaci¾n?
  [Unknown]:  educación
¿Cußl es el nombre de su ciudad o localidad?
  [Unknown]:  almería
¿Cußl es el nombre de su estado o provincia?
  [Unknown]:  almería
¿Cußl es el c¾digo de paŸs de dos letras de la unidad?
  [Unknown]:  es
¿Es correcto CN=ies alandalus, OU=edu, O=educación, L=almería, ST=almería, C=es?

  [no]:  si

Escriba la contrase±a clave para <claveSsl>
        (INTRO si es la misma contrase±a que la del almacÚn de claves):
```

Exportar el certificado a un archivo (I)

El siguiente comando exporta el certificado de nombre claveSsl, almacenado en el keystore de nombre AlmacenSSL al fichero de nombre claveSSL.crt

```
keytool -export -alias claveSsl -keystore AlmacenSSL -rfc -file claveSSL.crt
```

Exportar el certificado a un archivo (II)

- Al introducir el comando nos solicita la contraseña del almacén de claves.
- Una vez introducida la contraseña, nos indica el resultado de la exportación.

```
C:\Users\za> keytool -export -alias claveSsl -keystore AlmacenSSL -rfc -file cla
veSSL.crt
Escriba la contrase±a del almacÚn de claves:
Certificado almacenado en el archivo <claveSSL.crt>
```

Importar el certificado al Truststore (I)

El siguiente comando importa el certificado claveSSl.crt bajo el nombre claveTSsl al almacen de nombre TrustSSL

keytool -import -alias clave_TSsl -file claveSSL.crt -keystore TrustSSL

Importar el archivo al Truststore (II)

- Al introducir el comando nos solicita la contraseña del almacén de claves.
- Una vez introducida la contraseña, nos indica el resultado de la importación.

```
C:\Users\za>keytool -import -alias clave_TSsl -file claveSSL.crt -keystore Trust
SSL
Escriba la contrase±a del almacÚn de claves:
Propietario: CN=ies alandalus, OU=edu, O=educación, L=almería, ST=almería, C=es
Emisor: CN=ies alandalus, OU=edu, O=educación, L=almería, ST=almería, C=es
N·mero de serie: 4f04b494
Vßlido desde: Wed Jan 04 21:20:36 CET 2012 hasta: Tue Apr 03 22:20:36 CEST 2012
Huellas digitales del certificado:
         MD5:  E7:30:4F:DC:CE:AC:91:5F:2F:F7:5D:11:BA:50:A9:F9
         SHA1: 24:6E:76:F4:BF:5D:64:75:7B:90:AB:C1:58:DD:A1:33:58:D9:97:7B
         Nombre del algoritmo de firma: SHA1withRSA
         Versi¾n: 3
¬Confiar en este certificado? [no]:  si
Se ha a±adido el certificado al almacÚn de claves
```

Credenciales

Imagen	Datos de licencia
Todas las capturas de pantalla de este presentación tienen como datos de licencia: Autoría: Isabel M. Cruz Granados Licencia: Uso educativo-no comercial. Procedencia: Captura de pantalla de una consola Windows propiedad de Microsoft Corporation al ejecutar el comando keytool de Java propiedad de Oracle Corporation.	