1. Firmar digitalmente la aplicación:

- Necesito generar el par de claves (privada y pública).
- Necesito obtener el certificado a partir de la clave pública para enviarle al destinatario de la aplicación y que pueda comprobar su veracidad.

Uso *keytool* y trabajo desde la consola:

a) Genero el par de claves privada/pública:

D:\prueba\claves> keytool –genkey –alias firma –keystore DAM

```
D:\prueba\claves>keytool -genkey -alias firma -keystore DAM
Introduzca la contraseña del almacén de claves:
Volver a escribir la contraseña nueva:
¿Cuáles son su nombre y su apellido?
  [Unknown]:  Marina
¿Cuál es el nombre de su unidad de organización?
  [Unknown]:  INF
¿Cuál es el nombre de su organización?
  [Unknown]:  AGL
¿Cuál es el nombre de su ciudad o localidad?
  [Unknown]:  Santander
¿Cuál es el nombre de su estado o provincia?
  [Unknown]:  Cantabria
¿Cuál es el código de país de dos letras de la unidad?
  [Unknown]:  ES
¿Es correcto CN=Marina, OU=INF, O=AGL, L=Santander, ST=Cantabria, C=ES?
  [no]:  s

Introduzca la contraseña de clave para <firma>
        (INTRO si es la misma contraseña que la del almacén de claves):
```

b) Voy a firmar la aplicación TareaEjer2.jar y a la aplicación firmada la voy a llamar tareasegura.jar

D:\prueba\claves> jarsigner –keystore DAM –signedjar tareasegura.jar TareaEjer2.jar firma

```
D:\prueba\claves>jarsigner -keystore DAM -signedjar tareasegura.jar TareaEjer2.j
ar firma
Enter Passphrase for keystore:
jar signed.

Warning:
The signer certificate will expire within six months.
No -tsa or -tsacert is provided and this jar is not timestamped. Without a times
tamp, users may not be able to validate this jar after the signer certificate's
expiration date (2016-05-21) or after any future revocation date.

D:\prueba\claves>
```

c) Generar certificado con la clave pública: Quién vaya a recibir la aplicación necesita autentificar la firma del emisor. Por eso exporto la clave pública para generar el certificado que se enviará al receptor:

D:\prueba\claves> keytool –export –keystore DAM –alias firma –file tarea2.cert

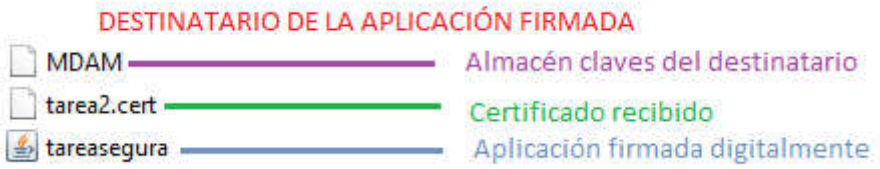
```
D:\prueba\claves>keytool -export -keystore DAM -alias firma -file tarea2.cert
Introduzca la contraseña del almacén de claves:
Certificado almacenado en el archivo <tarea2.cert>

D:\prueba\claves>_
```

2. Enviar la aplicación firmada y el certificado público para que pueda ser verificada la firma.

Lo único que tengo que enviar al destinatario es:

- La aplicación firmada. En mi caso tareasegura.jar
- El certificado. En mi caso tarea2.cert

Comprobación desde el punto de vista del destinatario.



Trabajo que tiene que hacer el destinatario:

1- Importar el certificado que contiene la clave pública, para que sea reconocido como un certificado de confianza:

User.home> keytool –import –alias tarea2 –file tarea2.cert –keystore MDAM

```
c:\datos>keytool -import -alias tarea2 -file tarea2.cert -keystore MDAM
Introduzca la contraseña del almacén de claves:
Propietario: CN=Marina, OU=INF, O=AGL, L=Santander, ST=Cantabria, C=ES
Emisor: CN=Marina, OU=INF, O=AGL, L=Santander, ST=Cantabria, C=ES
Número de serie: 452c78be
Válido desde: Sun Feb 21 17:48:40 CET 2016 hasta: Sat May 21 18:48:40 CEST 2016
Huellas digitales del Certificado:
         MD5: 66:44:CE:E2:22:8D:EE:F9:78:1C:9C:4B:3C:E3:C9:65
         SHA1: 9E:29:A5:40:69:76:B2:E0:D1:7E:DC:08:A1:49:5D:BF:92:55:41:10
         SHA256: D8:DA:58:CB:0A:5F:0E:F7:2E:05:DC:04:23:AA:81:34:7A:94:30:1F:E9:
F5:80:18:3B:A2:EF:33:20:7A:5A:65
         Nombre del Algoritmo de Firma: SHA1withDSA
         Versión: 3

Extensiones:

#1: ObjectId: 2.5.29.14 Criticality=false
SubjectKeyIdentifier [
KeyIdentifier [
0000: 94 21 7A F9 D0 4B 9F 17   F3 35 37 E7 5C A1 DD 1A  .!z..K...57.\...
0010: 64 59 30 42                                        dY0B
]
]

¿Confiar en este certificado? [no]:  s
Se ha agregado el certificado al almacén de claves

c:\datos>_
```

2- Verificar autenticidad de la firma del .jar, aprovechando que ya he importado el certificado de clave pública en el almacén de claves:

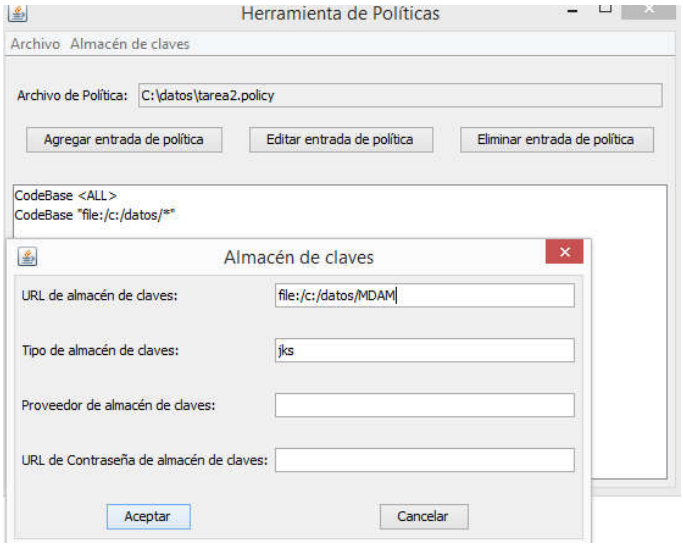
User.home> jarsigner –verify –verbose –certs –keystore MDAM tareasegura.jar

```
c:\datos>jarsigner -verify -verbose -certs -keystore MDAM tareasegura.jar

s k      311 Sun Feb 21 17:56:08 CET 2016 META-INF/MANIFEST.MF

     X.509, CN=Marina, OU=INF, O=AGL, L=Santander, ST=Cantabria, C=ES (tarea2)
     [certificate will expire on 21/05/16 18:48]

       329 Sun Feb 21 17:56:08 CET 2016 META-INF/FIRMA.SF
      1049 Sun Feb 21 17:56:08 CET 2016 META-INF/FIRMA.DSA
         0 Sun Feb 21 17:31:34 CET 2016 META-INF/
         0 Sun Feb 21 17:31:34 CET 2016 tareaejer2/
smk     4537 Sun Feb 21 17:31:34 CET 2016 tareaejer2/TareaEjer2.class

     X.509, CN=Marina, OU=INF, O=AGL, L=Santander, ST=Cantabria, C=ES (tarea2)
     [certificate will expire on 21/05/16 18:48]


  s = signature was verified
  m = entry is listed in manifest
  k = at least one certificate was found in keystore
  i = at least one certificate was found in identity scope

jar verified.

Warning:
This jar contains entries whose signer certificate will expire within six months
.
This jar contains signatures that does not include a timestamp. Without a timest
amp, users may not be able to validate this jar after the signer certificate's e
xpiration date (2016-05-21) or after any future revocation date.
```

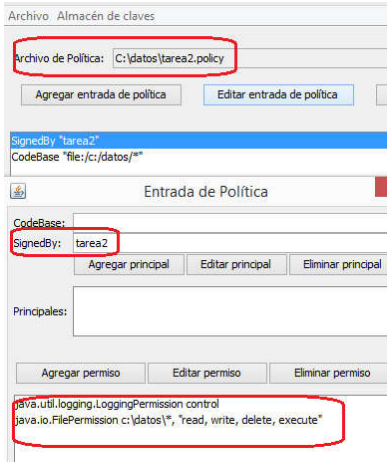
3- Ejecución de la aplicación:

```
c:\datos>java -jar tareasegura.jar
Nombre de usuario en minúsculas (no más de 8 caracteres):
marinana
Usuario marinana se ha conectado
Escribe el nombre del fichero.extension:
hola.txt
El usuario quiere ver el fichero: hola.txt
hola mundo
```

4- Al aplicar la seguridad, veo las excepciones y me aplico la política de seguridad necesaria en un archivo de nombre ***tarea2.policy***:
   - Control de acceso para la aplicación segura, teniendo en cuenta mi almacén de claves.
   - Acceso al directorio user.home



Asigno permiso de acceso o control a la clave pública (tarea2) obtenida del certificado digital que he recibido:



Finalmente compruebo que puedo ejecutar la aplicación firmada, aplicando la política de seguridad en el nuevo archivo tarea2.policy en un entorno de ejecución seguro:

```
c:\datos>java -jar -Djava.security.policy=tarea2.policy  -Djava.security.manager
 tareasegura.jar
Nombre de usuario en minúsculas (no más de 8 caracteres):
marinana
Usuario marinana se ha conectado
Escribe el nombre del fichero.extension:
hola.txt
El usuario quiere ver el fichero: hola.txt
hola mundo
```