**ACTIVIDAD 3**

**Enunciado**

**Firmar** un fichero jar utilizando la clave privada de un almacén de claves y **generar un certificado** con clave pública, para que quien los reciba pueda importar el certificado como un certificado de confianza y pueda verificar la firma del fichero jar.

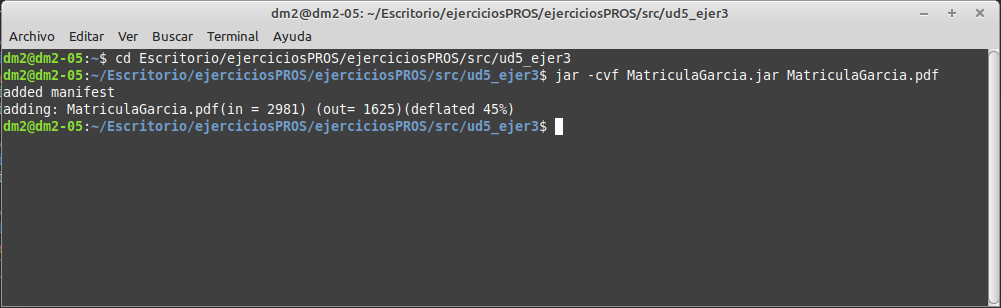
Para llevar a cabo esto, utiliza comandos disponibles en el JDK (Java Development Kit) de tu equipo del aula, de acuerdo a la siguiente secuencia de pasos:

1. Crear un archivo pdf de nombre MatriculaApellido.pdf, donde *Apellido* sea el primer apellido de la persona que realiza la actividad. Por ejemplo: MatriculaMartinezdeMarigorta.pdf.
2. Introducir dentro del archivo pdf exclusivamente tu DNI con letra. Por ejemplo: 72830262A.
3. Crear un fichero jar en base al archivo pdf, y que tenga el mismo nombre que este último. Por ejemplo: MatriculaMartinezdeMarigorta.jar. En la creación del fichero, utilizar el parámetro que permita sacar una salida verbose a través de la salida estándar de la línea de comandos
4. Generar un par de claves pública/privada mediante la herramienta keytool, creando un almacén de claves (keystore) de nombre AlmacenClavesApellido (donde *Apellido* sea el primer apellido de la persona que realiza la actividad) y creando un alias de nombre FirmaMatriculaApellido (donde *Apellido* sea el primer apellido de la persona que realiza la actividad) con el que se hará referencia al par de claves creado. Durante la ejecución del comando asociado a esta generación, proporcionar los siguientes datos:
   * Contraseña del almacén de claves
   * Nombre y primer apellido de la persona que realiza la actividad
   * Nombre de la unidad organizativa: Ciudad Jardín
   * Nombre de la organización: Educación Gobierno Vasco
   * Nombre de la ciudad o localidad: Vitoria-Gasteiz
   * Nombre de la provincia: Araba-Alava
   * Código del país de la organización: ES
   * Contraseña del par de claves (la misma que la contraseña del almacén de claves). Guardar esta contraseña en un archivo llamado ContraseñaApellido.txt (donde *Apellido* sea el primer apellido de la persona que realiza la actividad)
5. Visualizar mediante un comando de la herramienta keytool, el contenido del almacén de claves AlmacenClavesApellido recién creado.
6. Firmar el fichero jar utilizando la clave privada del almacén de claves y dejando el resultado de la firma en un fichero de nombre MatriculaApellidoFirmada.jar (donde *Apellido* sea el primer apellido de la persona que realiza la actividad).
7. Generar un certificado con clave pública (Apellido.cer), donde *Apellido* sea el primer apellido de la persona que realiza la actividad.

**Evidencias**

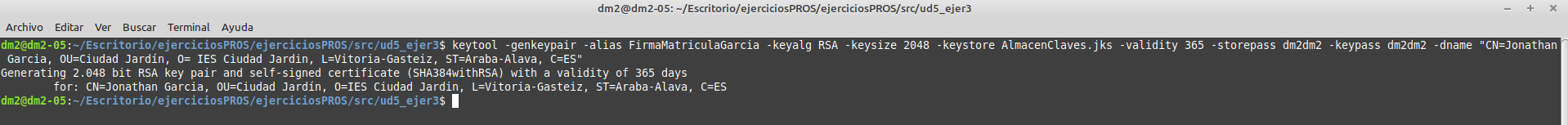
Incluye a continuación evidencias de cómo has llevado a cabo los siguientes pasos del enunciado de la actividad:

1. Crear el fichero jar



en el comando de “cd ...” vamos al directorio donde tenemos guardado el pdf

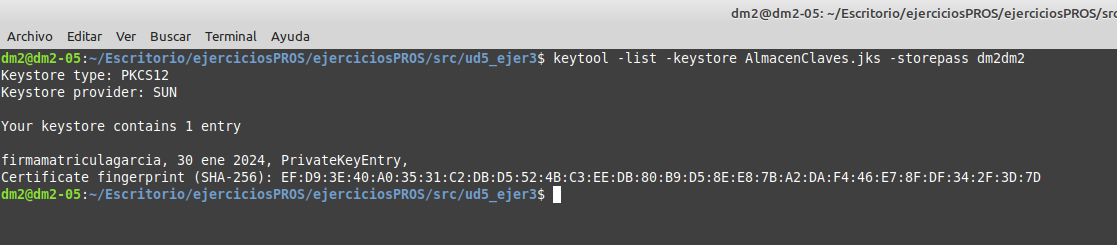
1. Generar un par de claves pública/privada



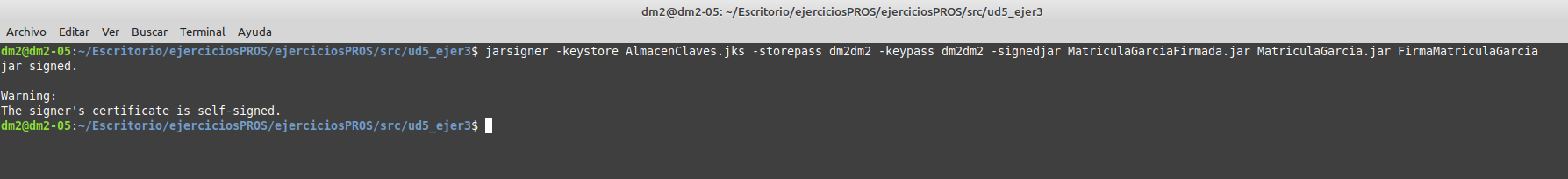
El comando es “keytool -genkeypair -alias FirmaMatriculaGarcia -keyalg RSA -keysize 2048 -keystore AlmacenClaves.jks -validity 365 -storepass dm2dm2 -keypass dm2dm2 -dname "CN=Jonathan Garcia, OU=Ciudad Jardín, O= IES Ciudad Jardin, L=Vitoria-Gasteiz, ST=Araba-Alava, C=ES"

Se puede hacer paso a paso en la consola poniendo el comando que hay en los apuntes que es “keytool -genkey -alias [ALIAS] -keystore [KEYSTORE] -keyalg RSA” (me daba error si no utilizaba el parametro extra de “-keyalg”)

1. Visualizar el contenido del almacén de claves recién creado

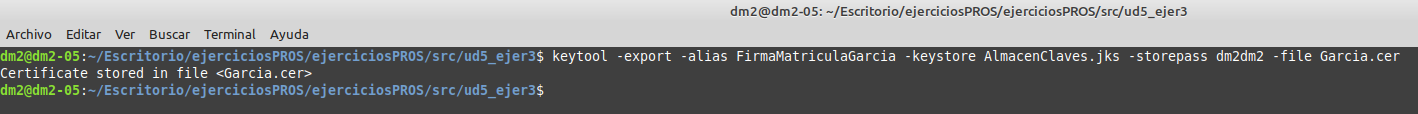


1. Firmar el fichero jar



El comando es “jarsigner -keystore AlmacenClaves.jks -storepass dm2dm2 -keypass dm2dm2 -signedjar MatriculaGarciaFirmada.jar MatriculaGarcia.jar FirmaMatriculaGarcia”

1. Generar un certificado con clave pública



El comando es “keytool -export -alias FirmaMatriculaGarcia -keystore AlmacenClaves.jks -storepass dm2dm2 -file Garcia.cer”

**Resolución de problemas**

**No he tenido problemas a la hora de realizar el ejercicio.**

**CRITERIOS DE CORRECCIÓN**

1. Nivel de ajuste a la nomenclatura de objetos definida en el enunciado de la actividad y nivel de ajuste al almacenamiento de la información requerida en las subcarpetas definidas para la actividad y unidad didáctica correspondientes (25%).
2. Hacer lo que se indica en el enunciado (25%).
3. Validez de las evidencias aportadas (25%).
4. Que sea posible importar el certificado proporcionado como un certificado de confianza y que se pueda verificar la firma del fichero jar proporcionado (25%).
5. Explicación detallada de cómo se han resuelto problemas que hayan podido surgir en la realización de la actividad (hasta un 15% adicional sobre la nota obtenida).