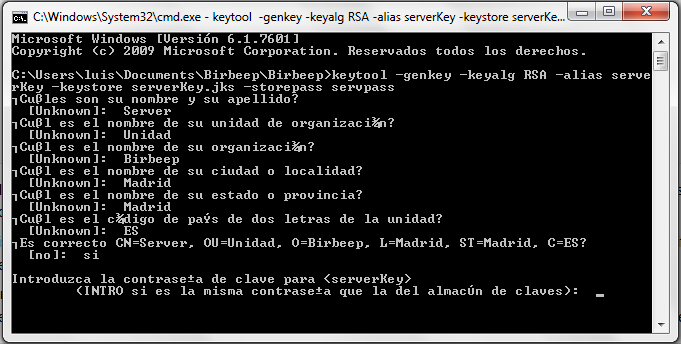
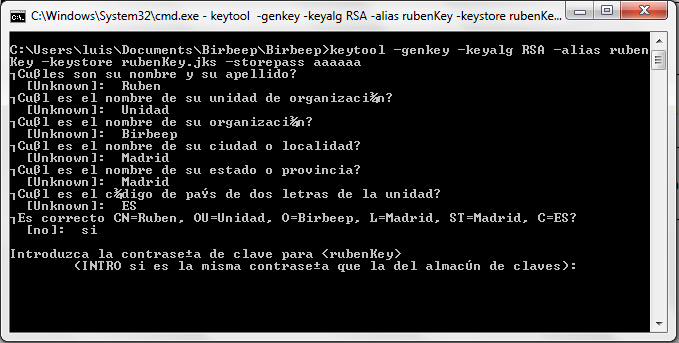
|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **SERVER** | **CLIENT1** | **CLIENT2** | **CLIENT3** |
| **Alias Certificado** | serverKey | sebasKey | luismiKey | rubenKey |
| **Password Certificado** | servpass | 123456 | 567890 | aaaaaa |
| **Nombre Almacén Certificado** | serverKey.jks | sebasKey.jks | luismiKey.jks | rubenKey.jks |
| **Password Almacén Certificado** | servpass | 123456 | 567890 | aaaaaa |
| **Nombre Fichero Exportación/Importación** | ServerPublicKey.cer | SebasPublicKey.cer | LuismiPublicKey.cer | RubenPublicKey.cer |
| **Nombre Almacén Certificados Confianza** | serverTrustedCerts.jks | sebasTrustedCerts.jks | luismiTrustedCerts.jks | rubenTrustedCerts.jks |
| **Password Almacén Certificados Confianza** | 000000 | 111111 | 222222 | 333333 |

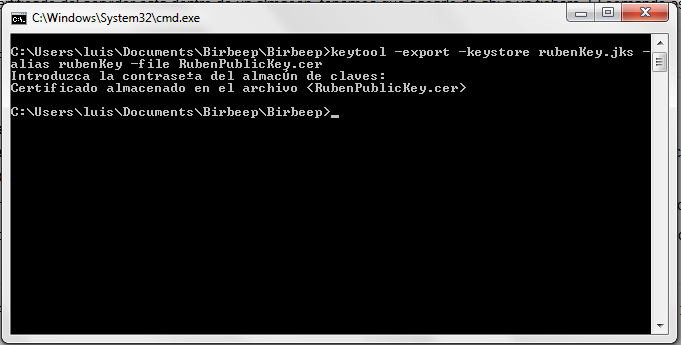
# 1.-Creamos el certificado del Servidor con su almacén de certificados correspondiente:



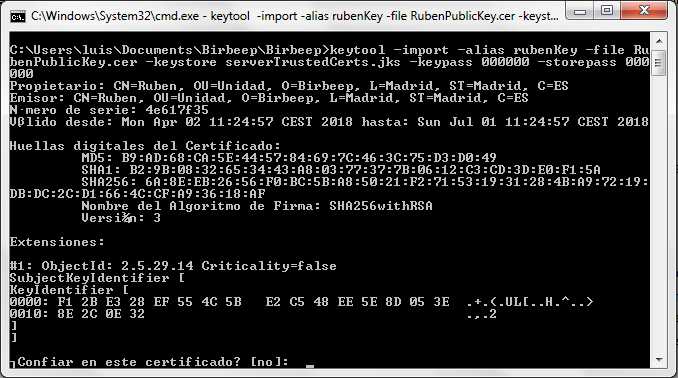
# 2.-Creamos el certificado del primer cliente con su almacén correspondiente (en este caso se crea en la misma máquina):



# 3.-Exportamos el certificado del cliente para almacenarlo en un almacén de certificados de confianza del Servidor:

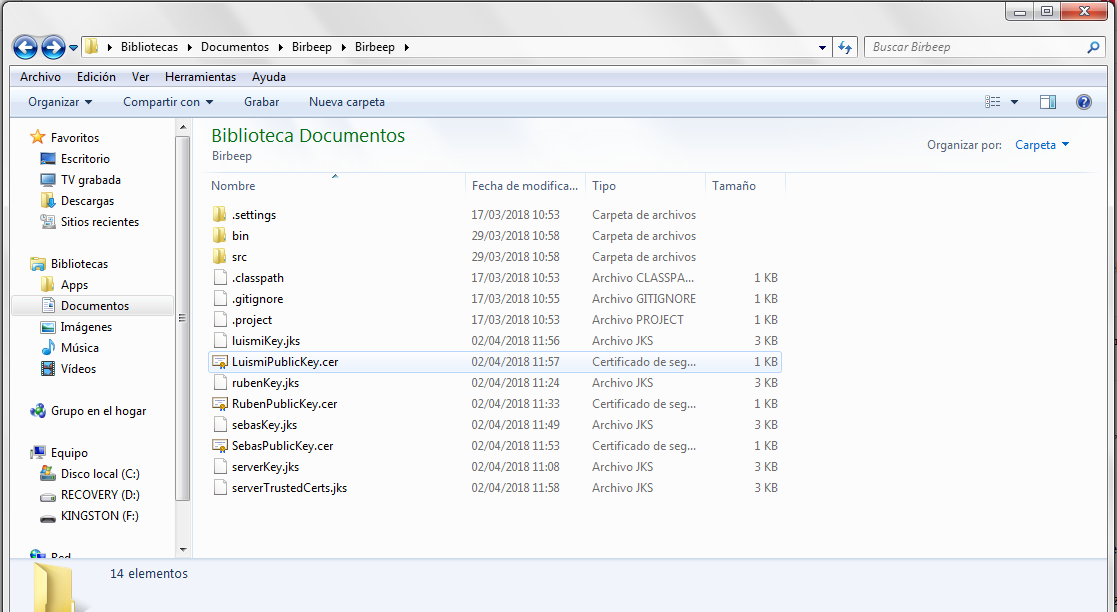


# 4.-Metemos el certificado del cliente en un almacén de certificados de confianza del Servidor:



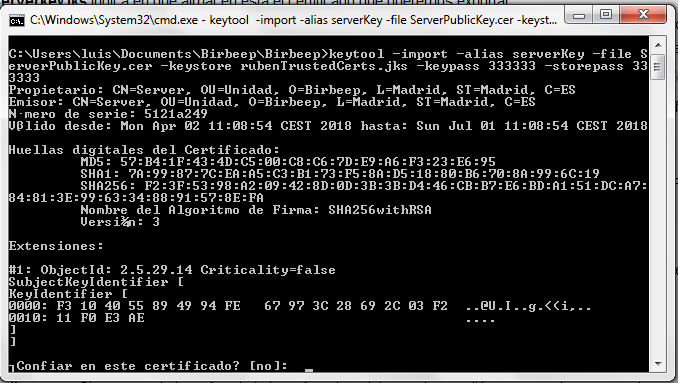
# 5.-Repetir pasos 2,3 y 4 para cada cliente.

# 6.-En la siguiente imagen, el Servidor confía en los tres clientes:

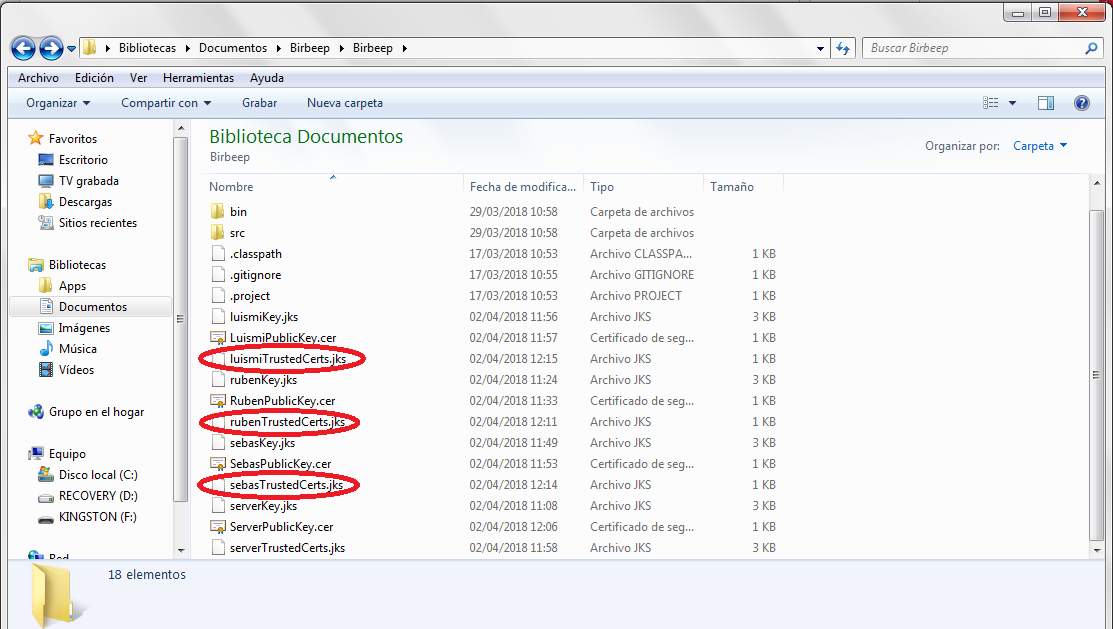


# 7.-Exportamos el certificado del Servidor como en el paso 3 (pero con las credenciales del servidor)

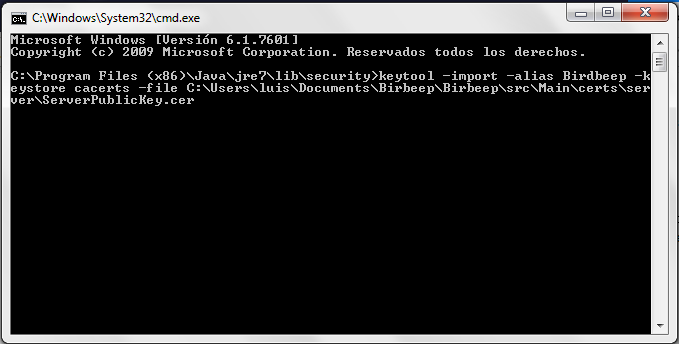
# 8.-Como en el paso 4, ahora CADA cliente tendrá su almacén de confianza en el que estará el del Servidor:



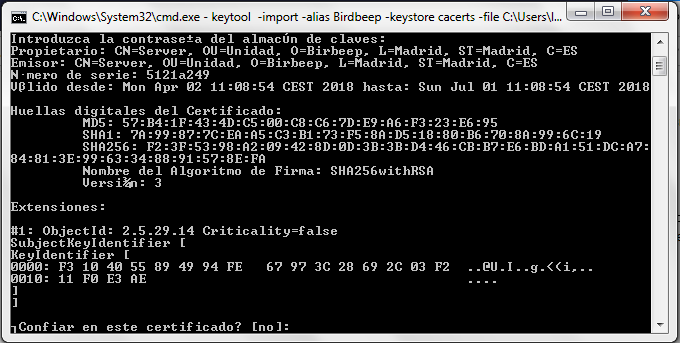
# 9.-En cada uno de los archivos marcados está el certificado del Servidor:



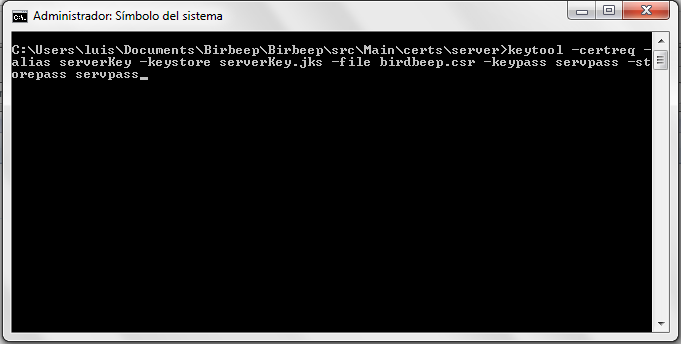
# 10.-Alamcenar el certificado del Servidor en la máquina que ejecuta la app java (Ejecutar cmd como admin):



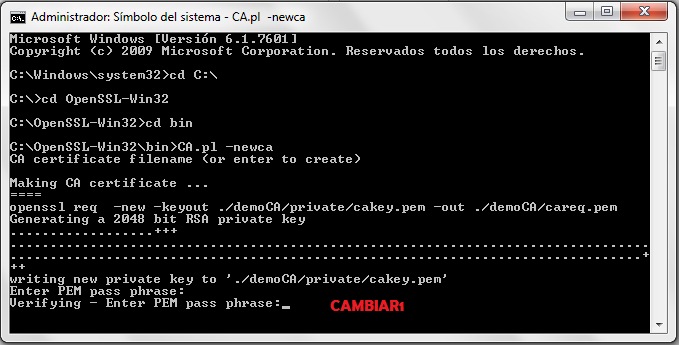
# 11.-Confirmar (Password por defecto del almacen: changeit):



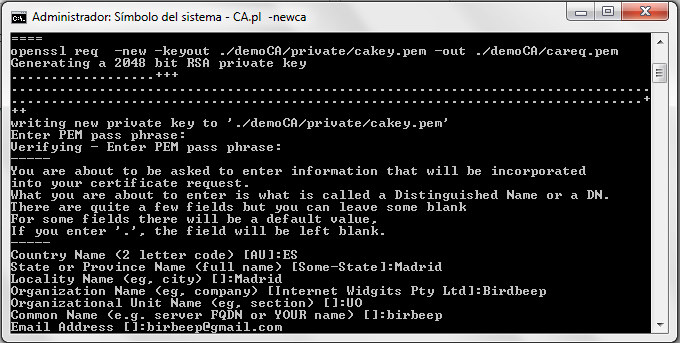
# Crear una petición de certificado (Certificate Signing Request):

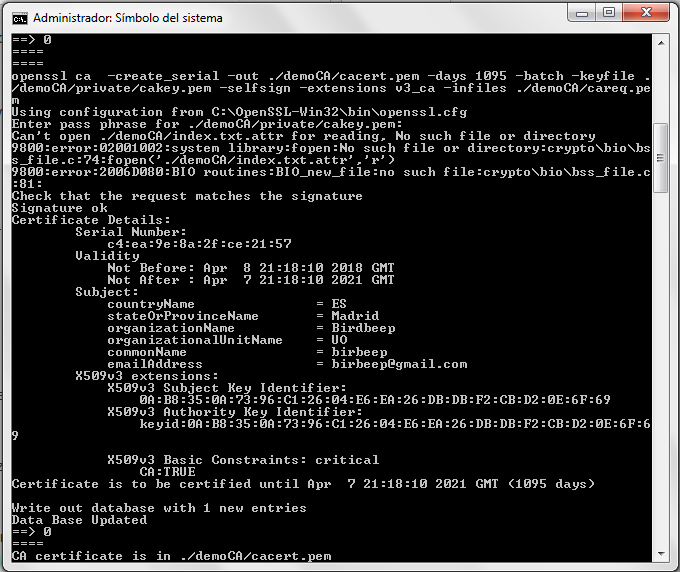


# Crear CA propia:

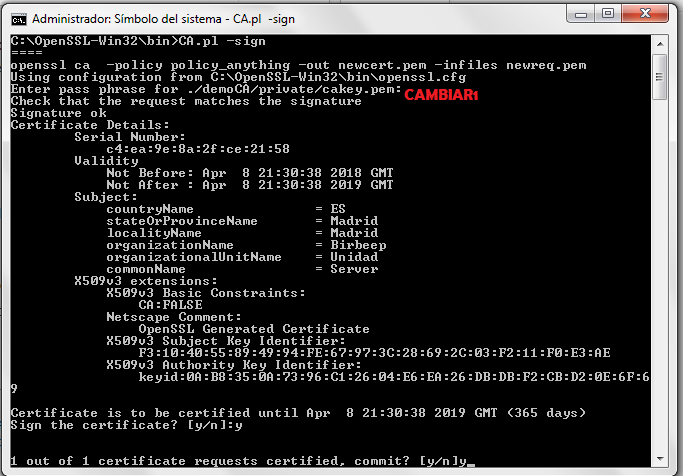


# Datos del certificado de CA:





# Firmar la CSR

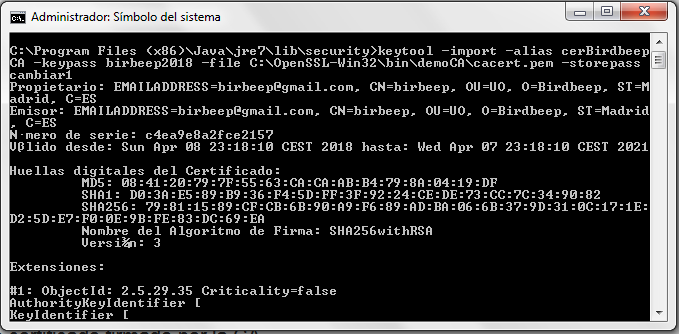


# En la ruta C:\OpenSSL-Win32\bin\demoCA copiamos el CSR con el nombre “newreq.pem”

# CA.pl –sign

# El archivo resultante , su contenido, se copia en un archivo .pem

# Importar :



# Importar al almacen del servidor y de los clientes el .pem

https://www.adictosaltrabajo.com/tutoriales/security-ssl-keytool/