LA-04-09-2020

Como convertir un certificado PFX de Macroseguridad.org-Sectigo a JKS utilizando Keytool

Usted puede convertir un certificado de CodeSigning de Macroseguridad.org-Sectigo en formato PFX a un certificado JKS utilizando Keytool de Oracle Java.

Requisitos:

- Certificado PFX/P12 exportado desde el navegador web donde lo haya generado.
- JRE / JDK
- OpenSSL
- Sistema Operativo Windows

Nota: Java 1.6 y posterior incluye soporte para archivos PFX, por lo que no es necesario convertir el certificado PFX a JKS para firmar con **jarsigner**.

Convertir un certificado PFX a JKS

Ejecute el siguiente comando de keytool para convertir el certificado PFX a JKS:

```
keytool -importkeystore -srckeystore [Ruta al archivo]\micertificado.pfx -srcstoretype pkcs12 -destkeystore [Ruta al archivo]\micertificado.jks -deststoretype JKS
```

Donde "*micertificado.pfx*" es el nombre del certificado de CodeSiging y "*micertificado.jks*" es el certificado de CodeSigning con nuevo formato. Durante el proceso le pedirá que defina una contraseña para el nuevo certificado JKS y que ingrese la contraseña del certificado PFX. Si la contraseña del certificado JKS es diferente a la contraseña del certificado PFX, al momento de firmar con el certificado JKS le pedirá la contraseña del certificado PFX.

Nota: El certificado PFX/P12 debe haber sido exportado con toda su cadena de certificación. Para más información refiérase al boletín "**Boletin_CodeSigning_Exportar_Certificado_CodeSigning_Generado_en_Internet_Explorer_Microsoft_Macroseguridad**", el mismo se encuentra en www.macroseguridad.net/soporte/codesigning

Importar cadena de certificación

Si el certificado PFX no fue exportado junto con la cadena de certificación, el certificado JKS no tendrá la correspondiente cadena.

Para importar la cadena de certificación dentro del archivo JKS realice los siguientes pasos:

1) Exporte la llave pública (certificado en Base64) del certificado PFX. Una forma es ejecutando la siguiente línea de comandos de OpenSSL:

```
openssl pkcs12 -in [Ruta al archivo]\micertificado.pfx -out [Ruta al archivo]\micertificado.crt -nodes -nokeys
```

Donde "*certificado.crt*" será la llave pública de su certificado de CodeSigning.

2) Ejecute el siguiente comando de keytool para conocer el alias del certificado:

```
keytool -v -list -keystore [Ruta al archivo]\micertificado.jks -storetype JKS
```

3) Concatene su llave pública (micertificado.crt) con la cadena de certificación utilizando un editor de texto que no agregue caracteres (como por ejemplo notepad) de la siguiente forma:

```
----- BEGIN CERTIFICATE -----
(La llave pública del certificado de CodeSigning)
----- END CERTIFICATE -----
----- BEGIN CERTIFICATE -----
(El certificado intermedio 2)
----- END CERTIFICATE -----
----- BEGIN CERTIFICATE -----
(El certificado intermedio 1)
----- END CERTIFICATE -----
----- BEGIN CERTIFICATE -----
(El certificado raíz)
----- END CERTIFICATE ----
```

Para obtener mayor información sobre la cadena de certificación visite www.macroseguridad.net/root.

4) Ejecute el siguiente comando para importar el certificado con la cadena de certificación al JKS:

```
keytool -import -alias AliasObtenidoEnElPaso2 -file [Ruta al archivo]\micertificado.crt -keystore [Ruta al archivo]\micertificado.jks
```

Para mayor información contacte al equipo de Tecnología de MacroSeguridad por el medio que usted prefiera

- Mail: soporte@macroseguridad.net
- Portal de Soporte: https://soporte.macroseguridad.la
- Web: www.MacroSeguridad.net