Instructivo para la generación de claves (keystore) para la OISS.

La generación del keystore se deberá realizar tanto en el servidor 10.7.1.90 y 10.7.1.91 (actuales a este momento).

No continuar con ningún punto si el anterior no terminó correctamente.

Para la generación del keystore se deberá proceder de la siguiente manera:

1. Logearse al servidor como root y localizar el ejecutable de java ***cetificacao.jar***, por lo general se encuentra dentro de directorio de JBOSS/CDOISS.
2. Generar un directorio para que las claves queden en él y ejecutar la aplicación desde el directorio creado.
3. Ejecutar ***/<PATH>/java -jar certificacao.jar*** aparecerá el siguiente menú:

0 - Sair

1 - Gerar Par de Chaves

2 - Gerar Certificado

3 - Gerar Requisição de Certificado (CSR)

4 - Adicionar uma Chave Privada a um KeyStore

5 - Adicionar um Certificado a um KeyStore

6 - Cifrar Parâmetro

7 - Decifrar Parâmetro

Seleccionar la Opción 1.
Ingresar lo siguientes datos:

Digite o caminho do arquivo onde a chave privada gerada será armazenada: ***clave.priv***
Digite o caminho do arquivo onde a chave pública gerada será armazenada: ***clave.pub***
Digite o algoritmo das chaves (RSA, DSA): ***RSA***
Digite o tamanho, em bits, da chave (1024, 2048): ***1024***

Si el proceso ha sido correcto, mostrará el siguiente mensaje:

Par de chaves gerado com sucesso.

4. Una vez completo el paso anterior seleccionamos la opción 2.

0 - Sair

1 - Gerar Par de Chaves

2 - Gerar Certificado

3 - Gerar Requisição de Certificado (CSR)

4 - Adicionar uma Chave Privada a um KeyStore

5 - Adicionar um Certificado a um KeyStore

6 - Cifrar Parâmetro

7 - Decifrar Parâmetro

Ingresar lo siguientes datos:

Digite o caminho do arquivo onde o certificado gerado será armazenado: **cert.cer**
Digite o Distinguished Name do emissor (issuerDN) do certificado: **C=AR, ST=BA, L=BUENOS AIRES, O=DATAPREV, OU=DATAPREV, CN=localhost**
Digite o Distinguished Name do detentor (subjectDN) do certificado: **C=AR, ST=BA, L=BUENOS AIRES, O=DATAPREV, OU=DATAPREV, CN=localhost**
Digite a data de início de validade do certificado**: 01/07/2012** -→ establecer fecha de inicio
Digite a data de término de validade do certificado: **01/07/2013** -→ establecer fecha vto.
Digite o caminho do arquivo contendo a chave privada referente ao certificado a ser gerado: **clave.priv**
Digite o caminho do arquivo contendo a chave pública referente ao certificado a ser gerado: **clave.pub**
Digite o algoritmo de assinatura do certificado (SHA1withRSA, MD5withRSA, MD2withRSA): **SHA1withRSA**

Si el proceso ha sido correcto, mostrará el siguiente mensaje:

Certificado gerado com sucesso.

5. Una vez completado el paso anterior seleccionar la opción 4.

0 - Sair

1 - Gerar Par de Chaves

2 - Gerar Certificado

3 - Gerar Requisição de Certificado (CSR)

4 - Adicionar uma Chave Privada a um KeyStore

5 - Adicionar um Certificado a um KeyStore

6 - Cifrar Parâmetro

7 - Decifrar Parâmetro

Ingresar lo siguientes datos:

Digite o caminho do KeyStore: **key.jks**
Digite a senha do KeyStore: dataprev
Digite o caminho do arquivo contendo a chave privada: **clave.priv**
Digite alias que será associado a chave privada: **argentina**
Digite a senha da chave privada: **dataprev**
Digite o caminho do certificado pertencente a cadeia associada a chave privada (para parar digite 'ok'): **cert.cer**
Digite o caminho do certificado pertencente a cadeia associada a chave privada (para parar digite 'ok'): **ok**

Si el proceso ha sido correcto, mostrará el siguiente mensaje:

Chave privada adicionada com sucesso no KeyStore.

6. Una vez terminado el proceso anterior seleccionar la opción 6 para que al ejecutarlo nos entregue el PARÁMETRO DE CIFRADO. IMPORTANTE: el parámetro de cifrado no debe ser ingresado, solamente lo mostrará.

0 - Sair

1 - Gerar Par de Chaves

2 - Gerar Certificado

3 - Gerar Requisição de Certificado (CSR)

4 - Adicionar uma Chave Privada a um KeyStore

5 - Adicionar um Certificado a um KeyStore

6 - Cifrar Parâmetro

7 - Decifrar Parâmetro

Digite o valor do parâmetro: **dataprev**
Parâmetro cifrado com sucesso: DKRk3v88hdubufeeUSPdkQ==

Seleccionar la opción 0 para terminar el proceso de generación de keystore.

7. Una vez finalizado el proceso se habrán generado los siguientes archivos en el directorio que fue creado en el punto 2:

cert.cer
clave.priv
clave.pub
key.jks

8. Los mismos deberán copiarse dentro de los siguientes directorios:

el archivo key.jks copiarlo dentro del directorio:
/usr/local/jboss-4.2.1.GA/CDOISS/certificados/

Como:

keystore.jks
keystore_auth.jks
keystore_ssl.jks

copiar el certificao (cert.cer) en el directorio:

/usr/local/jboss-4.2.1.GA/CDOISS/trusted

Proceder al reinicio del Jboss.

9. Enviar a la OISS los siguientes datos:

CONTRASEÑA: dataprev
ALIAS: argentina
Cifrado: DKRk3v88hdubufeeUSPdkQ== (parámetro generado en el punto 6.)

Adjuntar además el archivo **clave.pub**.