eID Trust Service

Documentación del proceso de instalación, configuración y

puesta en marcha del eID Trust Service

Rolosa HyJ S.A. - MICITT

13 de Junio de 2014

Resumen

El presente manual permite la instalación, configuración y puesta en marcha de la solución de eID Trust Service del Micitt para el DCFD

Tabla de contenido

Introducción

El Trust Service provee dos servicios principales:

eID Trust Service Portal

Vía este portal web, los ciudadanos pueden revisar la validez de sus certificados

eID Web Service

Vía este web service SOPA, los Proveedores de Servicios pueden revisar la validez de rutas de certificados. Este web service está construido de acuerdo al estándar W3C XKMS2.

A parte de estos dos artefactos, el eID Trust Service también viene con un portal de Administración que permite a los administradores utilizar y configurar el eID Trust Service a través de una interfaz web. En los siguientes párrafos utilizaremos el $EID_TRUST_SERVICE_ADDRESS como la dirección web interna de el eID Trust Service que ha sido desplegado.

El código del eID Trust Service está actualmente ubicado en un servidor SVN de Google:

http://dcfd-mw-applet.googlecode.com

Para obtener una copia del código se debe utilizar un cliente SVN y realizar la operación de Checkout:

svn checkout http://dcfd-mw-applet.googlecode.com/svn/trunk/trust-service

El eID Trust Service depende de la librería jTrust la cual es una librería para validaciones de confianza de certificados X509. Esta librería puede ser encontrada en un servidor SVN de google:

http://code.googlecode.com/p/jtrust

El eID Trust Service también presenta una dependencia con el Applet de Bélgica, el cual ya ha sido modificado para trabajar con las tarjetas del SNCD, este Applet puede ser encontrado en:

http://dcfd-mw-applet.googlecode.com/

Para obtener una copia del código se debe utilizar un cliente SVN y realizar la operación de Checkout:

svn checkout http://dcfd-mw-applet.googlecode.com/svn/trunk/applet

Para obtener una copia de todo el código de la solución, se debe utilizar un cliente SVN y realizar la operación de Checkout, ej.:

svn checkout http://dcfd-mw-applet.googlecode.com/svn/trunk/

A continuación se muestra un ejemplo de cómo realizar el procedimiento de Checkout utilizando el código de la solución del Applet.

Para este ejemplo, se utilizará el cliente SVN del IDE NetBeans, este procedimiento es válido para todos los Sistemas Operativos actualmente soportados por el IDE NetBeans, y ha sido verificado en Windows (8) y Linux (Ubuntu 12.10). En la Figura 1, NetBeans SVN Checkout, podemos observar cómo realizar el procedimiento de descarga del código.

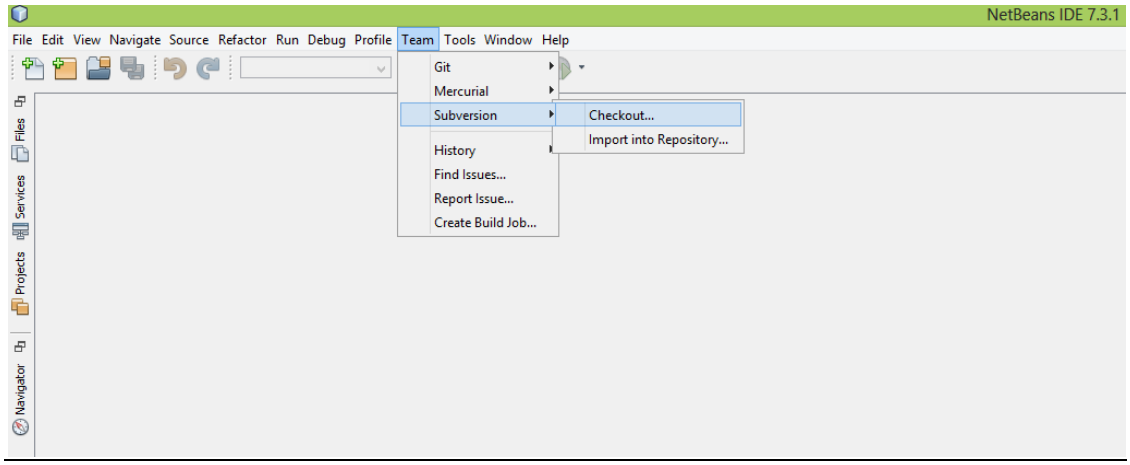

Figura 1, NetBeans SVN Checkout

Debemos especificar el URL para realizar el Checkout , esta es la URL del servidor de Google. Como se aprecia en la Figura 2, NetBeans, SVN URL, no se requiere especificar ningún Usuario ni Contraseña, puesto que el Checkout del código se realiza en modo "read-only".

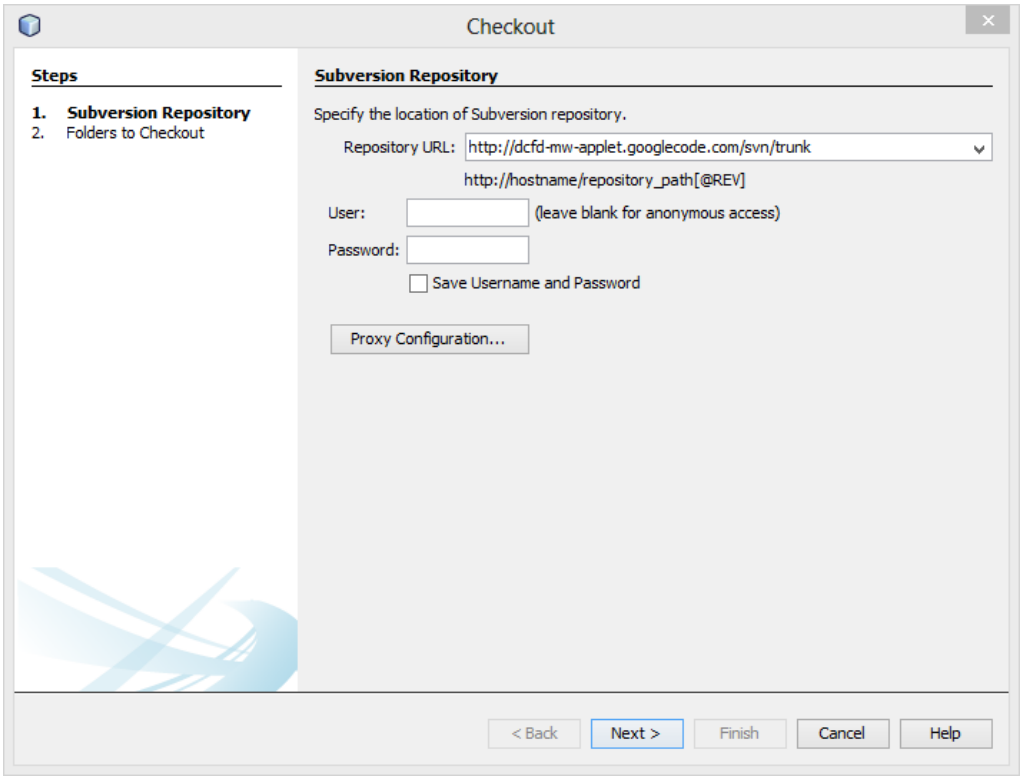

Figura 2, NetBeans, SVN URL

Para finalizar el procedimiento de Checkout es necesario especificar el directorio local donde se realizará la descarga del código. La Figura 3, NetBeans SVN Checkout - local, muestra el último paso para el Checkout.

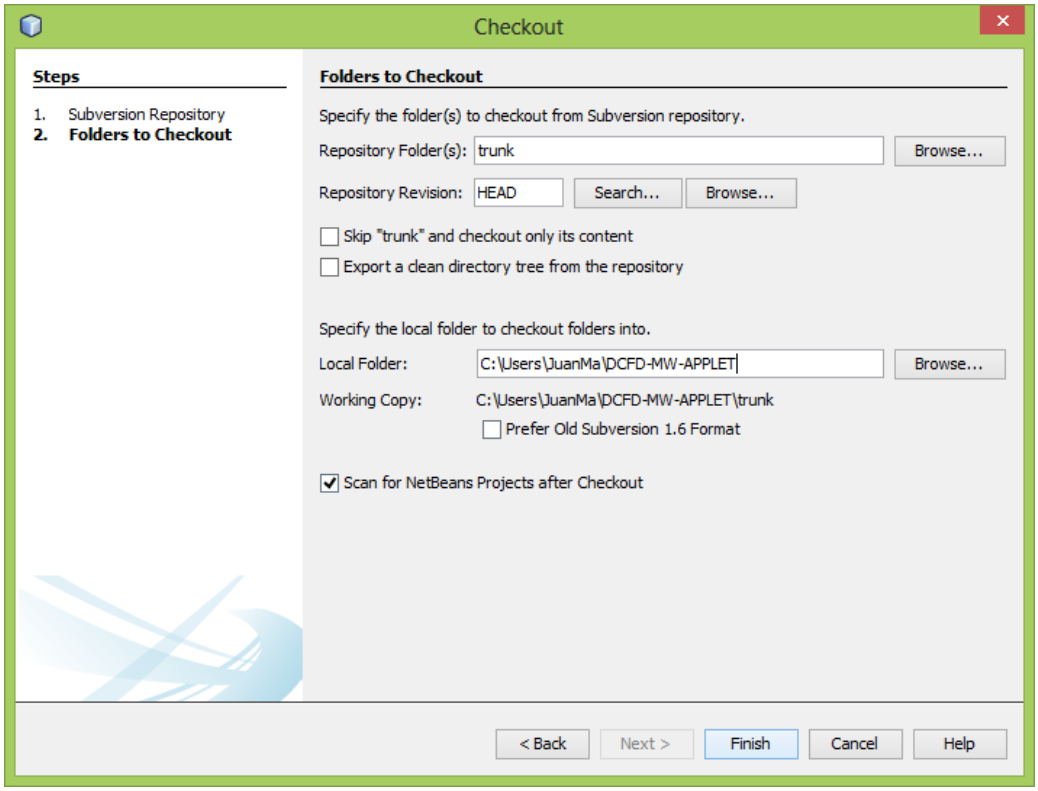

Figura 3, NetBeans SVN Checkout - local

Compilación

El eID Trust Service ha sido concebido para soportar una plataforma especifica de Java sin depender del Sistema Operativo en el que se desee utilizar el mismo. Es en este sentido que en la actualidad, solamente esta soportada la plataforma Java 6.

Pre-requisitos

1. Plataforma Java 6
    a. Oracle Java Runtime Environment 6 (update 45)
    b. Oracle Java Development Kit 6 (update 45)

    Es imprescindible asegurarse que las distribuciones de JRE y JDK correspondan a las provistas por SUN - Oracle. En varias distribuciones Linux (Ubuntu 12.04, Fedora 9, 10, 11, 12), el JRE por defecto es el IcedTea JRE basado en OpenJDK; el Applet no tiene soporte funcional completo para OpenJDK.

    Apple solamente soporta Java 6 runtime en las versiones de Mac OS X desde Snow Leopard.

    Los plugins para soporte de Java en el explorador web que se utilice, tienen que ser compatibles con Java 6

    La instalación y configuración de Oracle Java 6u45 en algún sistema operativo sale del alcance de este manual. Como referencia es posible revisar el siguiente tutorial de instalación de Java6u45 en Ubuntu 12:

    http://hendrelouw73.wordpress.com/2013/05/07/how-to-install-oracle-java-6-update-45-on-ubuntu-12-10-linux/

2. Apache Maven
    a. Apache Maven 3.0.4 o superior

    La administración del código fuente y proyecto del eID Trust Service ha sido realizada utilizando Apache Maven. La instalación y configuración de Apache Maven en algún sistema operativo sale del alcance de este manual. Existen numerosos tutoriales en Internet al respecto.

IDE - NetBeans

Para hacer más eficiente el trabajo con el proyecto del eID Trust Service es recomendable utilizar el **IDE NetBeans** el cual en su **versión 6.9.1 para Java EE**, El IDE NetBeans 6.9.1 para Java EE, este puede ser obtenido desde:

https://netbeans.org/downloads/6.9.1/index.html

Los siguientes pasos de compilación se deben realizar para el proyecto eID Trust Service y las dependencias jTrust y Applet. Para el eID TrustService es necesario especificar el perfil para el cual se desea realizar la compilación (prod-mysql p prod-oracle).

Una vez instalado el IDE, abrir NetBeans 6.9.1, y luego abrir el proyecto eID Trust Service que se encuentra dentro del directorio que se acaba de descargar del repositorio SVN (**Menu File > Open Project..)** como se indica en la Figura 4, Abrir proyecto

Con el proyecto abierto, seleccionar el Proyecto **eID Trust Service** y luego presionar la tecla [**F11**] o hacer click derecho sobre el proyecto y elegir "**Build**" del menú contextual, **Netbeans** realizará el proceso de compilación, para lo cual también realizará varias descargas de las dependencias que el presente proyecto tiene (ver Figura 5, Compilación - Descarga de Dependencias) este proceso puede demorar varios minutos dependiendo de la velocidad de su conexión de Internet.

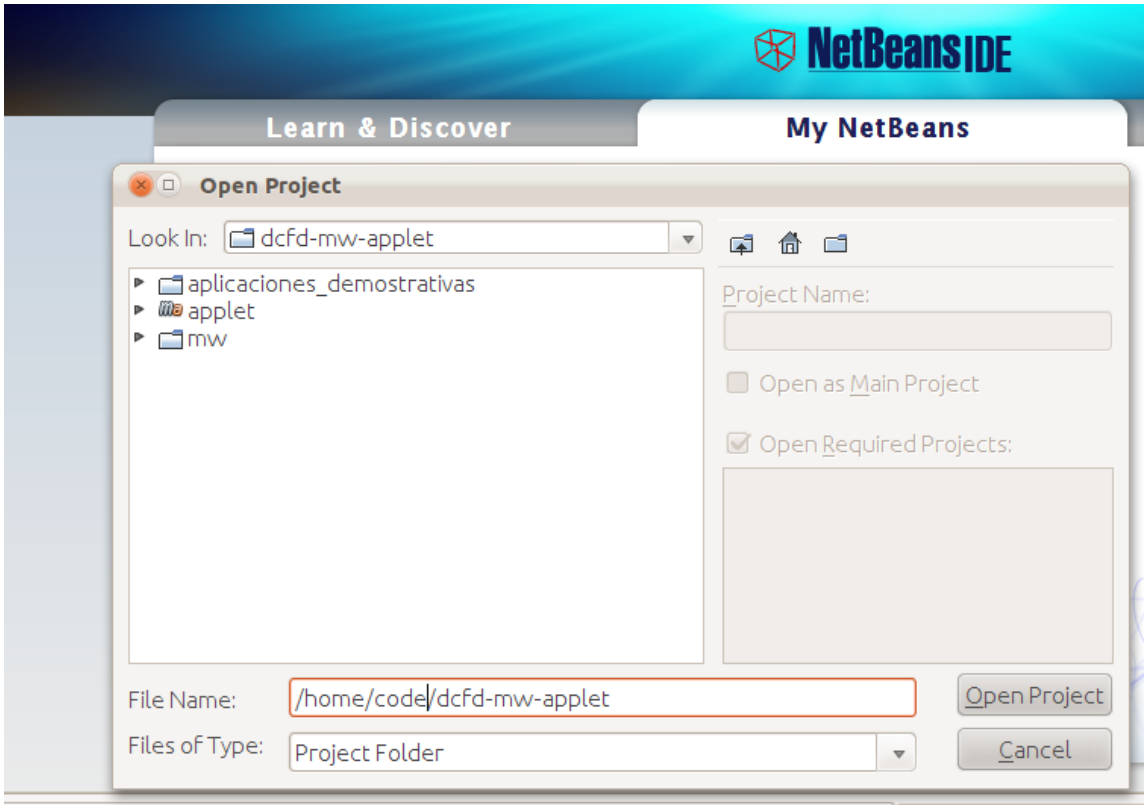

Figura 4, Abrir proyecto

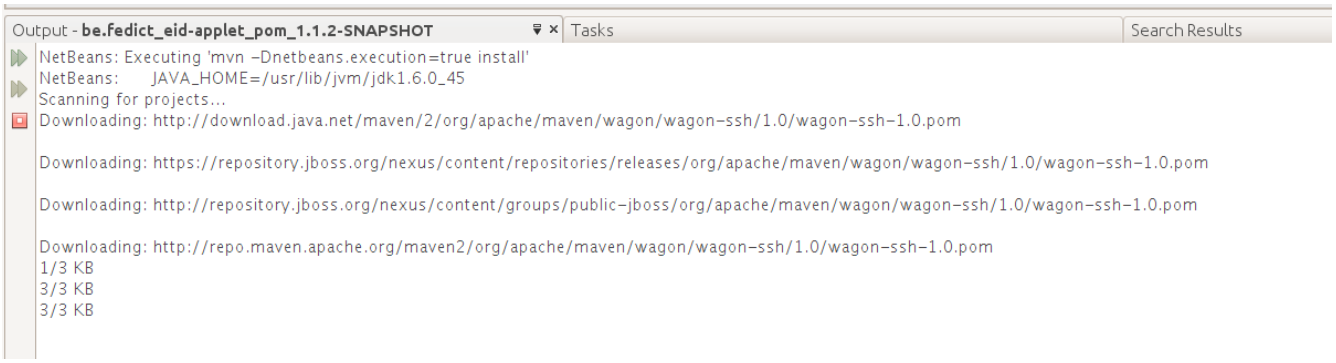

Figura 5, Compilación - Descarga de Dependencias

Una vez finalizada la compilación del proyecto, se obtendrá un resumen como el que se muestra en la Figura 6, Compilación - Exitosa.

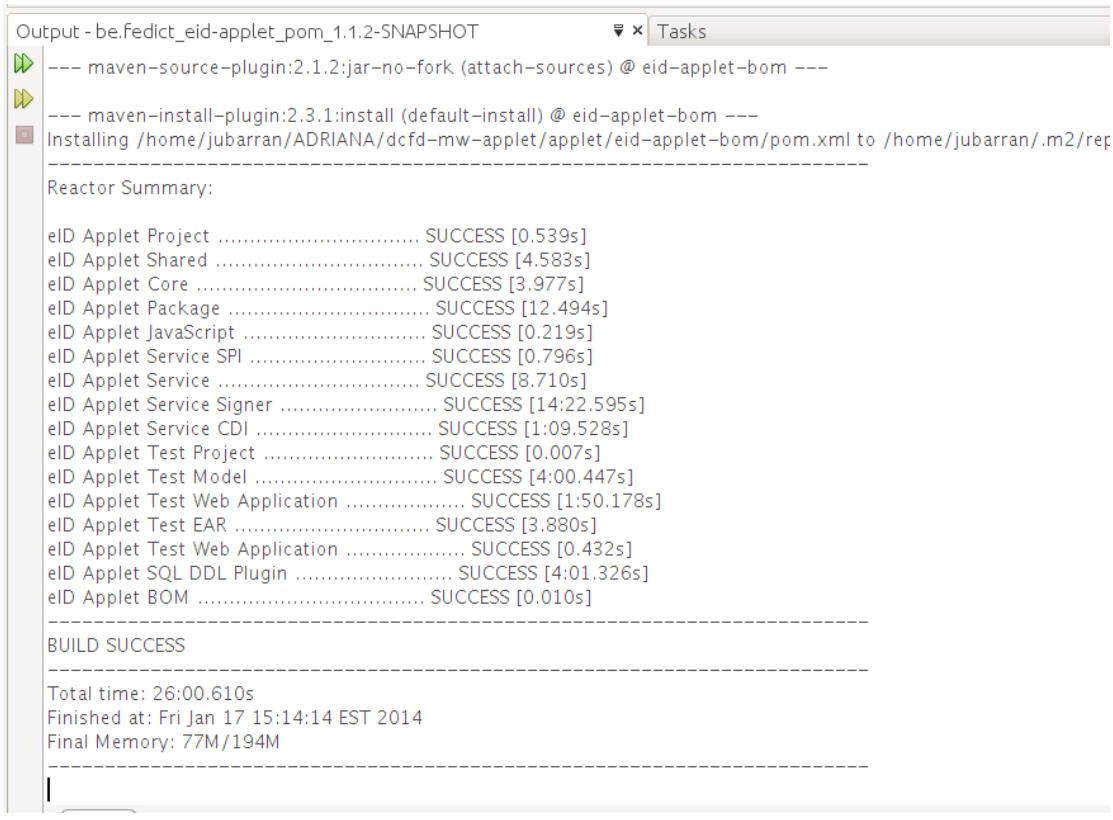

Figura 6, Compilación - Exitosa

Si por alguna motivo, la compilación es detenida a la mitad del proceso, ya sea por acción del usuario o problemas con la conexión de Internet, sin permitir que todos los sub-proyectos sea compilados, se debe seleccionar el Proyecto eID Trust Service y luego presionar la tecla [**Shift+F11**] o hacer click derecho sobre el proyecto y elegir "**Clean and Build**" del menú contextual, NetBeans realizará el proceso de borrado de los archivos de la compilación anterior e iniciara una compilación nueva, para lo cual realizará varias descargas de las dependencias que el presente proyecto tiene (ver Figura 5, Compilación - Descarga de Dependencias) este proceso puede demorar varios minutos dependiendo de la velocidad de su conexión de Internet.

```
--- maven-jar-plugin:2.3.1:jar (default-jar) @ eid-applet-package ---
Building jar: /home/jubarran/ADRIANA/dcfd-mw-applet/applet/eid-applet-package/target/eid-applet-package-1.1.2-SNAPSHOT.jar

--- keytool-maven-plugin:1.0:genkey (default) @ eid-applet-package ---
keytool error: java.lang.Exception: Key pair not generated, alias <SIGN> already exists
java.lang.Exception: Key pair not generated, alias <SIGN> already exists
      at sun.security.tools.KeyTool.doGenKeyPair(KeyTool.java:1129)
      at sun.security.tools.KeyTool.doCommands(KeyTool.java:786)
      at sun.security.tools.KeyTool.run(KeyTool.java:172)
      at sun.security.tools.KeyTool.main(KeyTool.java:166)
------------------------------------------------------------------------
Reactor Summary:

eID Applet Project ..... SUCCESS [0.570s]
eID Applet Shared ..... SUCCESS [2.867s]
eID Applet Core ..... SUCCESS [2.556s]
eID Applet Package ..... FAILURE [1.718s]
eID Applet JavaScript ..... SKIPPED
eID Applet Service SPI ..... SKIPPED
eID Applet Service ..... SKIPPED
eID Applet Service Signer ..... SKIPPED
eID Applet Service CDI ..... SKIPPED
eID Applet Test Project ..... SKIPPED
eID Applet Test Model ..... SKIPPED
eID Applet Test Web Application ..... SKIPPED
eID Applet Test EAR ..... SKIPPED
eID Applet Test Web Application ..... SKIPPED
eID Applet SQL DDL Plugin ..... SKIPPED
eID Applet BOM ..... SKIPPED
------------------------------------------------------------------------
BUILD FAILURE
------------------------------------------------------------------------
```

Figura 7, Compilación del Applet - Error

El resultado de la compilación del código del proyecto es un conjunto de archivos JAR los cuales podrán ser utilizados para la creación de aplicaciones web.

Distribución Mysql

Una vez compilado el proyecto eID Trust Service bajo el perfil **prod-MySql**, es posible proceder a compilar la distribución correspondiente, para eso es necesario abrir el proyecto **eID Trust Service Mysql Distribution** y compilarlo de igual forma a los anterior proyectos.

Instalación

El servidor eID Trust Service está basado en JBoss Aplication Server [http://www.jboss.org/jbossas] versión 6.1.0 .Final. y viene personalizado para un motor de base de datos especifico. Una vez descomprimido el archivo resultante de la compilación del proyecto **eID Trust Service Mysql Distribution** se pueden observar 2 directorios, jboss y sql. El directorio jboss contiene al servidor de aplicaciones configurado para el motor de base de datos especificado. El directorio sql contiene los scripts de inicialización de la base de datos. Se soportan MySqL, PostgreSql y Oracle, dependiendo del Perfil de compilación elegido durante la compilación del eID Trust Service.

Configuración de Base de Datos MySql

Antes de iniciar el servidor de aplicaciones JBoss, es necesario inicializar la base de datos. En el directorio sql se encuentran 3 scripts de inicialización, uno para crear la cuenta de base de datos, otro para crear la base de datos y el ultimo para inicializar las tablas. El nombre de usuario y contraseña por defecto es trust/trust para la base de datos trust.

Una vez instalado el servidor de base de datos, los siguientes comandos permiten la completa configuración:

```
mysql -u root -p < mysql-create-account.sql
mysql -u trust -p < mysql-create-database.sql
mysql -u trust -p trust < mysql-trust-service-ddl.sql
```

Recursos

Debido a que el Harvester puede demorar mucho debido al tamaño de algunos CRLs, el consumo de memoria puede ser intensivo. El servidor de aplicaciones ha sido ajustado para que el JVM disponga de mayor memoria. Por defecto se ha reservado un total de 1GB de espacio en el "heap". Esta configuración puede ser encontrada en jboss/bin/run.conf. El servidor debe contar con al menos 2 GB de memoria disponible.

La utilización de la red está relacionada a la configuración de caching con la que se dispone. El pool de conexiones está configurado a 20. El tamaño máximo de la base de datos depende del DBMS elegido y es aproximadamente 4 GB. La base de datos consiste principalmente en datos que están disponibles públicamente en CRLs públicos, no se necesita ninguna estrategia de backups.

La aplicación utiliza almacenamiento local para descargas temporales de CRLs.

La aplicación también requiere de claves privadas (JKS, PKCS#12 o PKCS#11) para poder firmar respuestas salientes de XKMS (basado en la WS-Security).

Se pueden resumir los siguientes requerimientos técnicos como recursos de hardware:

- Memoria RAM mínimo 2 GB, recomendado 8GB

- Almacenamiento local disponible mínimo 4GB, recomendado 20GB

- Almacenamiento disponible para servidor de Base de datos mínimo 4GB, recomendado 20GB

- Procesador recomendado Intel 2.4 Ghz (multi-núcleo)

- Conexión a Internet

Iniciar el Servidor

Después de haber configurado la base de datos, se puede arrancar la aplicación ejecutando el comando:

```
./jboss/bin/run.sh -b 0.0.0.0 &
```

La opción -b 0.0.0.0 cambia el enlace de la dirección del servidor así la aplicación se hace disponible en todas las interfaces.

Una vez iniciada la aplicación, esta tendrá inicializados 4 dominios de confianza por defecto:

1. Dominio de Confianza para Autenticación (CR-AUTH)
2. Dominio de Confianza de No-Repudio (CR)
3. Dominio de Confianza de Registro Nacional (CR-NET-REG) , a ser removido en el futuro
4. Dominio de Confianza para Sellado de Tiempo (CR-TSA)

El dominio de confianza por defecto es establecido como Dominio de Confianza para Autenticación.

Para el correcto funcionamiento de la aplicación, se necesita que la misma disponga de salida a internet, si se está ubicado detrás de un proxy esto puede ser configurado utilizando el portal de administración.

Detener el Servidor

Para detenerlo correctamente se debe ejecutar el comando:

```
./jboss/bin/shutdown.sh -S
```

Configuración

Tiempo de Espera para transacciones

La descarga y procesamiento de CRLs de gran tamaño puede tomar mucho tiempo y esto puede llevar a errores por tiempo de espera agotado por parte del DBMS. Por defecto las distribuciones de MySQL y Oracle tienen un tiempo de espera por transacción de 1200 segundos o 20 minutos. Esto puede ser cambiado en el archivo jboss/server/default/deploy/transacion-jboss-beans.xml en la línea:

```
<property name="defaultTimeout">1200</property>
```

Después de cualquier cambio en la configuración, la aplicación tiene que ser reiniciada como se muestra a continuación:

```
./jboss/bin/shutdown.sh -S
./jboss/bin/run.sh -b 0.0.0.0
```

Bitácoras

La configuración de bitácoras de la aplicación se encuentra en jboss-logging.xml. Toda la información registrada en la bitácora por componentes del eID Trust Service se encuentra en un archivo individual en jboss/server/default/log/fedict.log. Por defecto el nivel de bitácoras está configurado a DEBUG esto puede ser cambiado en

```
<logger category="be.fedict">
 <level name="DEBUG" />
 <handlers>
  <handler-ref name="FEDICT" />
 </handlers>
</logger>
```

Administración

Portal de Administración

El eID Trust Service dispone de un portal de administración para ajustar varios aspectos del servicio.

Para inicial sesión en el portal, un proceso de autenticación será realizado, si el servicio es iniciado por primera vez el primer usuario autenticado con éxito será registrado como administrador. Cualquier usuario posterior tendrá que ser aceptado para poder ser administrador, quedándose en estado pendiente mientras no haya una aprobación explicita por parte de un administrador existente.

Configuración

Administradores

Aquí se pueden ver administradores existentes y administradores pendientes, aprobar solicitudes pendientes y remover administradores existentes.

WS-Security

El eID Trust Service utilizara el keystore configurado en esta sección para firmar las respuestas salientes utilizando WS-Security

Configuración de Red

Si se encuentra detrás de un servidor proxy, se puede configurar el mismo en esta sección

Detección de desfase del Reloj

El eID Trust Service realizara peticiones al servidor TSA que sea configurado en esta sección, la respuesta del servidor contendrá un token que será utilizado para la detección de desfase del reloj.

Mensaje de Información

Se puede configurar un mensaje de información para ser mostrado en el portal $EID_TRUST_SERVICE_ADDRESS/eid-trust-service-portal.

Dominios Virtuales de Confianza

Dominios Virtuales de Confianza son un grupo de dominios de confianza existentes. Los usuarios del eID Trust Service web service puede especificar un dominio virtual de confianza contra el que validarse.

Dominios de Confianza

Se pueden agregar, modificar y remover dominios de confianza en esta sección. También se puede establecer el dominio de confianza por defecto el cual será utilizado en el eID Trust Service web service cuando no se especifique un dominio de confianza en la petición de validación. Para cada dominio de confianza se puede especificar si se utilizara la cache CRL.

Puntos de Confianza

Para cada punto de confianza, se puede especificar una expresión cron la cual indicara el intervalo y la frecuencia de actualización de la cache de CRL. Es posible realizar una actualización manual de la cache CRL.

Cache CRL

La sesión de Cache CRL provee de una visión general del estado de la cache CRL para cada CA.

Auditoria

Los siguientes eventos será registrado por el eID Trust Service los mismos que pueden ser revisados desde el Admin portal.

- Error al contactar al servidor NTP
- Máximo desfase de reloj alcanzado
- Error al descargar CRL para una CA determinada
- CRL invalido para una CA determinada
- Error al procesar el CRL de una CA determinada
- Error al notificar al harvester para una CA determinada
- Dominio de confianza por defecto no establecido
- CA no encontrada