eID Identity Provider

Documentación del proceso de instalación, configuración y

puesta en marcha del eID Identity Provider

Rolosa HyJ S.A. - MICITT

11 de Agosto de 2014

Resumen

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

Tabla de contenido

Introducción

El Digital Signature Service provee dos servicios principales:

eID Digital Signature Service Portal

Vía este portal web, los ciudadanos pueden firmar documentos y verificar firmas en documentos existentes

eID Digital Signature Service Web Service de validación de firmas

Vía este web service SOAP, los Proveedores de Servicios pueden verificar las firmas en digitales de documentos. Este web service está construido de acuerdo al estándar OASIS DSS.

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

El código del eID DSS 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/dss

El eID DSS depende del eID Trust Service modificado para el Micitt. Este puede ser encontrado en el mismo servidor SVN de google:

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

Compilación

El eID DSS 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 IDP 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 pasos de compilación que se deben realizar para el proyecto eID IDP son en esencia los mismos que se debe realizar para el proyecto eID Trust Service, para ambos proyectos es necesario especificar el perfil para el cual se desea realizar la compilación (prod-mysql o prod-oracle).

Distribución Mysql

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

Instalación

El servidor eID IDP 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. Debido a la dependencia estricta que se tiene con el eID Trust Service, la distribución del eID Trust Service es utilizada como base de la distribución del eID IDP.

Una vez descomprimido el archivo resultante de la compilación del proyecto **eID IDP 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 IDP.

Configuración de Base de Datos MySql

Antes de iniciar el servidor de aplicaciones JBoss, es necesario inicializar la base de datos. La inicialización de la base de datos es idéntica a la del producto eID Trust Service, agregando que en el directorio sql se encuentra 1 script de inicialización especifico para el DSS, llamado: **eid-idp-ddl-mysql.sql**.

Iniciar el Servidor

La Distribución JBoss del eID IDP viene en conjunto con el eID Trust Service, de manera que una instalación limpia consistiría de ambos productos. Si se desea que solamente el eID IDP sea desplegado es posible remover los siguientes archivos del eID Trust Service:

- `jboss/server/default/deploy/eid-trust-service-deploy-1.0.0.GA.ear`
- `jboss/server/all/deploy/eid-trust-service-deploy-1.0.0.GA.ear`

Inversamente, si la intención es la de desplegar el eID IDP en una distribución JBoss previa del eID trust Service, esto es posible copiando el archivo **eid-idp-deploy-1.0.6-SNAPSHOT.ear** dentro de las siguientes rutas:

- `jboss/server/default/deploy/`
- `jboss/server/all/deploy/`

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 Creación (CR)
2. Dominio de Confianza para Verificación (CR)
3. Dominio de Confianza de Registro Nacional (CR-NAT-REG) , a ser removido en el futuro
4. Dominio de Confianza para Sellado de Tiempo TSP (CR-TSA)

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

La configuración general es similar a la descrita en el documento de Instalación y Configuración del eID Trust Service.

Tamaño de los archivos

Si el tamaño por defecto de archivos POST no es suficiente para el tamaño de documentos a ser procesados por el eID DSS, este valor puede ser configurado en el archivo jboss/server/default/deploy/jbossweb.sar/server.xml

```
<Connector ...
maxPostSize="20971520"/>
```

EL valor de maxPostSIze es expresado en bytes.

Administración

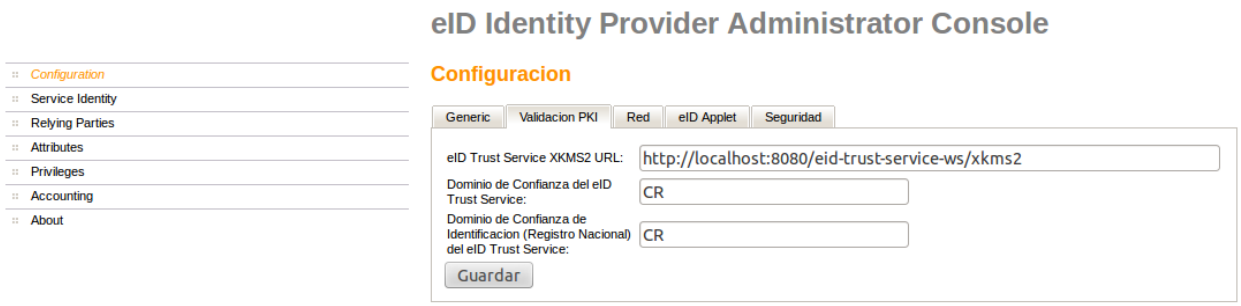
Portal de Administración

El eID IDP dispone de un portal de administración para ajustar varios aspectos del servicio. El cual puede ser accedido mediante $EID_IDP_ADDRESS/eid-idp-admin-portal.

Para iniciar 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.

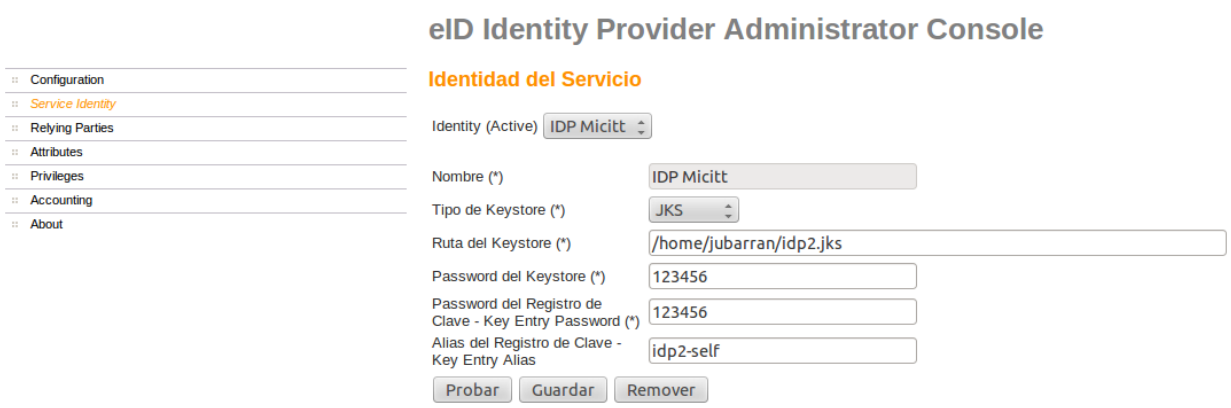
Configuración

La configuración mínima requiere de parámetros en la pestaña de Validación PKI como se muestra en la siguiente figura:



La URL del Web Service XKMS2 del eID Trust Service es necesaria para permitir al eID IDP realizar la autenticación correspondiente de los interesados en consumir el servicio. Los Dominios de Confianza son los que se encuentran disponibles en el eID Trust Service. Si el eID IDP y el eID Trust Service han sido desplegados en el mismo servidor, la URL tiene que estar en la forma $EID_IDP_ADDRESS/eid-trust-service-ws/xkms2.

En la sección de Identidad del Servicio, se debe configurar los parámetros correspondientes a los certificados del KeyStore para proveer de identidad al IDP. Este paso es mandatorio para permitir que el IDP procese correctamente solicitudes de Autenticación por el protocolo SAML v2.0.



Una vez configurado el IDP, se puede acceder a la dirección $EID_IDP_ADDRESS/eid-idp para ver un resumen de los protocolos ofrecidos por el IDP, sus correspondientes EndPoints (Puntos de Entrada) para que las aplicaciones web de los Proveedores de Servicios puedan acceder. La siguiente imagen muestra dicho resumen.