

MiddleWare y Applet

Manual de Aplicación web Demostrativa en Java EE

Consumiendo funcionalidades del Applet

Rolosa HyJ S.A. - MICITT

20 de Enero de 2014



Resumen

El presente documento es una para la utilización de la Aplicación web Demostrativa en Java que consume el Applet

Tabla de contenido

Pre-requisitos.....	1
Aplicación	3

Pre-requisitos

El siguiente software es requerido para trabajar con la aplicación demostrativa en Java:

- **Java Runtime Environment 6 update 45**

- **Apache Maven 3.0.4+**

- **GlassFish V3 Server** Servidor para la aplicación WEB

- **NetBeans 6.9.1-Java EE.** IDE de Desarrollo que permitirá compilar y ejecutar la aplicación demostrativa, incluye instancia de GlassFish V3 Server, incluye soporte nativo para Maven 3.

- **beidpkcs11.dll** (Librería resultante de la compilación del MiddleWare que sigue el estándar RSA - PKCS#11 - Windows)

- **libbeidpkcs11.so** (Librería resultante de la compilación del MiddleWare que sigue el estándar RSA - PKCS#11 - Linux)

- **asepkcs.dll** (Librería PKCS de Athena para Firma Digital del Costa Rica - Windows)

- **libasep11.so** (Librería PKCS de Athena para Firma Digital del Costa Rica)

- **CA SINPE - PERSONA FISICA.cer** (Certificado del Emisor, utilizado para autenticación del usuario con la Tarjeta inteligente).

- **CA RAIZ NACIONAL COSTA RICA.cer** (Certificado raíz, utilizado para autenticación de la SmartCard de, banco Central).

También es necesario disponer de:

- Una Tarjeta Inteligente para Firma Digital de Costa Rica
- Un lector de tarjetas apropiado
- Certificados Digitales de la cadena de la confianza de la Firma Digital de Costa Rica
- Drivers necesarios para la Tarjeta Inteligente, dependiendo el sistema operativo en el que se desee realizar los trabajos.

Los drivers y certificados digitales tienen que ser obtenidos desde el sitio de Soporte de Firma Digital de Costa Rica:

<https://www.soportefirmadigital.com/sfd/default.aspx>

IMPORTANTE, asegurarse que los certificados existan en las rutas siguiente según la versión de sistema operativo:

Linux y Mac:

/usr/lib/dcfcd/certificados

jubarran@stboltra01: /usr/lib/dcfcd/certificados

jubarran@stboltra01: /usr/lib/dcfcd/certificados

```
jubarran@stboltra01:/usr/lib/dcfcd/certificados$ ls -l
total 8
-rw-r--r-- 1 root root 1469 2014-01-16 20:13 CA RAIZ NACIONAL COSTA RICA.cer
-rw-r--r-- 1 root root 3016 2014-01-16 20:13 CA SINPE - PERSONA FISICA.cer
jubarran@stboltra01:/usr/lib/dcfcd/certificados$
```

Windows:

C:\Firma Digital\certificados

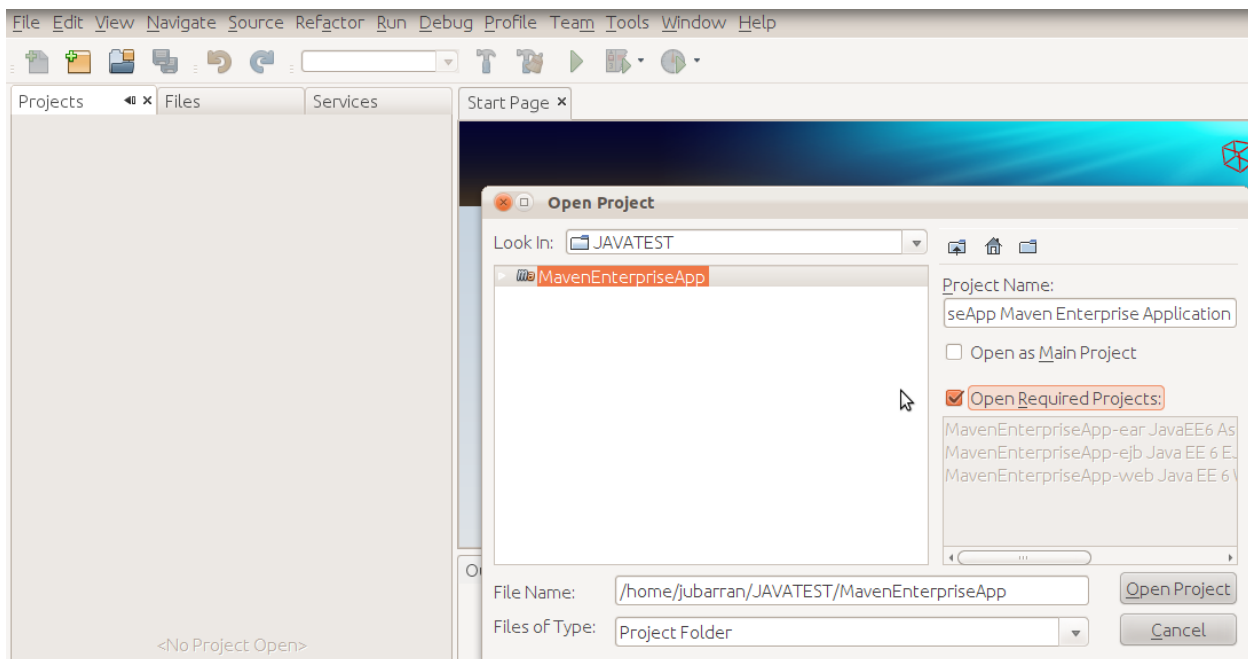
Aplicación

El proyecto: **MavenEnterpriseApp** que se encuentra en:

\trunk\aplicaciones_demostrativas\WEB\MavenEnterpriseApp

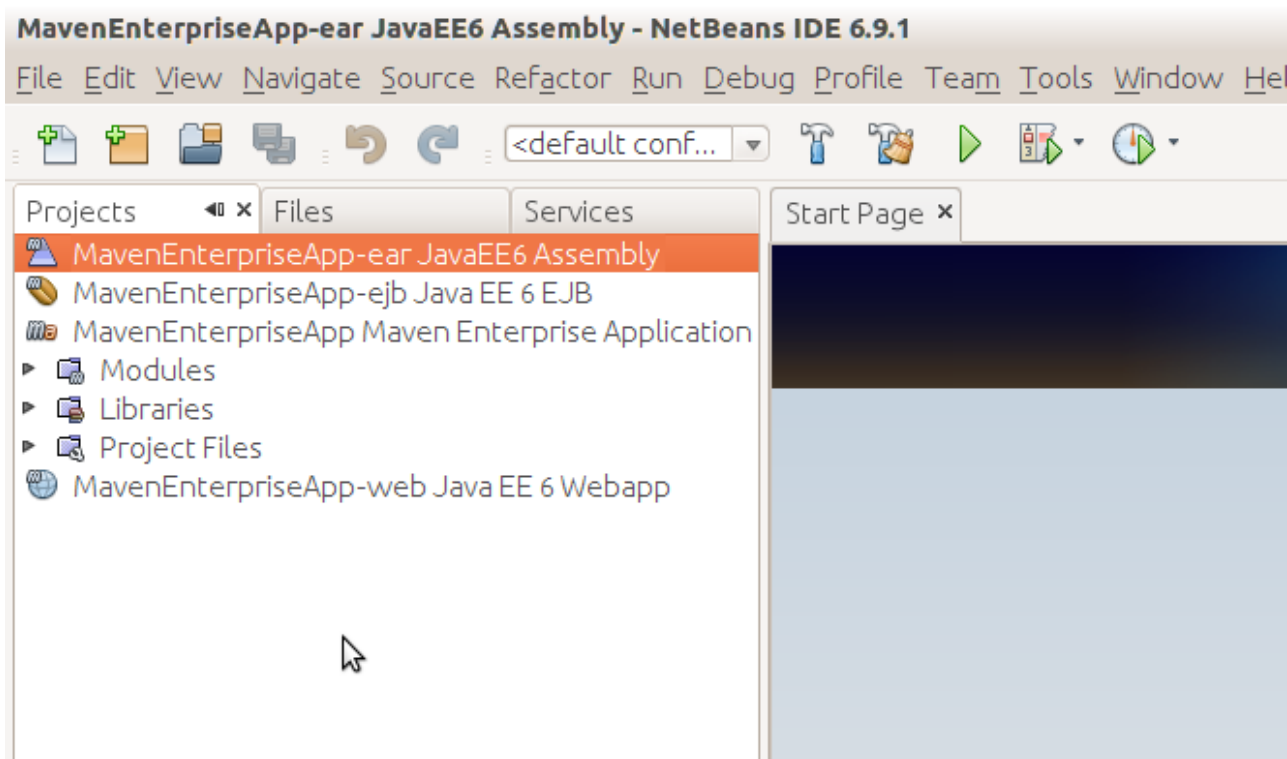
, contiene el la Aplicación Demostrativa web en Java.

Luego de iniciar NetBeans 6.9.1, abrir el proyecto **MavenEnterpriseApp** que se encuentra dentro del directorio de la aplicación demostrativa: (**Menu File > Open Project..**), seleccionar la opción **“Open Required Projects”**

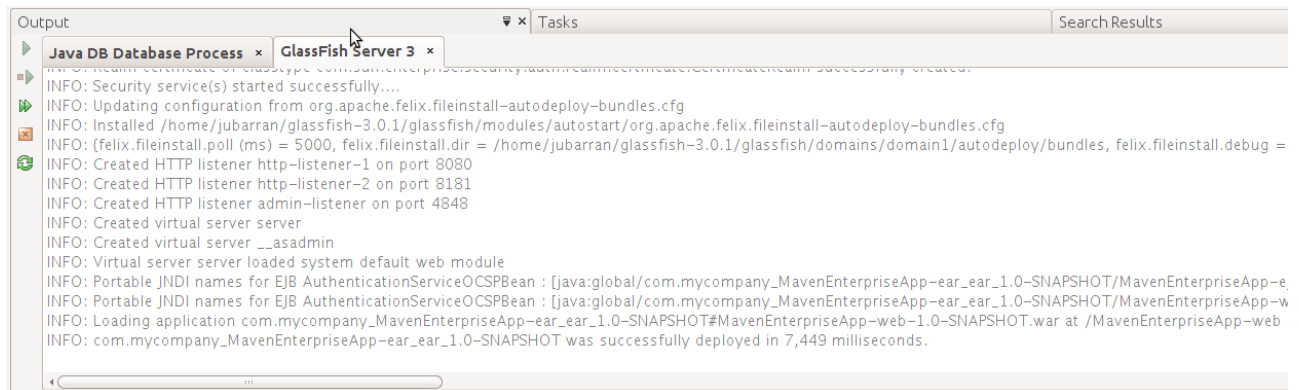


A continuación compilar el proyecto eligiendo la opción **“Clean and Build”** del menú contextual.

Una vez terminada la compilación, se debe seleccionar el Proyecto **MavenEnterpriseApp-ear JavaEE6 Assembly** y luego presionar la tecla [F6] o hacer click derecho sobre el proyecto y elegir “Run” del menú contextual:



Verificar que el servidor **GlassFish 3** esta siendo iniciado y el proyecto está siendo desplegado. El proceso de despliegue habrá finalizado una vez que en la ventana de output verifiquemos que el ultimo mensaje es: “...was successfully deployed in....”



Luego se debe abrir una ventana del navegador web, escribir la **URL** que se muestra abajo y presionar la tecla **[Enter]**:

<https://localhost:8181/MavenEnterpriseApp-web/>

Es importante recalcar que el Applet necesita SSL, motivo por el cual abrimos con: “**https**” y al puerto **8181**.

Es probable que el explorador web muestre una alerta de seguridad, esto se debe a que el sitio <https://localhost:8181>..... no es reconocido como un sitio de confianza. Esto no es problema puesto que estamos ejecutando una aplicación de prueba.

De ser necesario, agregar una excepción para el sitio actual. Luego la aplicación demostrativa es mostrada:



Asegurarse de tener conectado el CardReader y que contenga una tarjeta inteligente válida.

Hacer click en el link “**Autenticación**” esto nos llevará a la página que carga el Applet.

Debemos permitir que el explorador cargue el Applet:



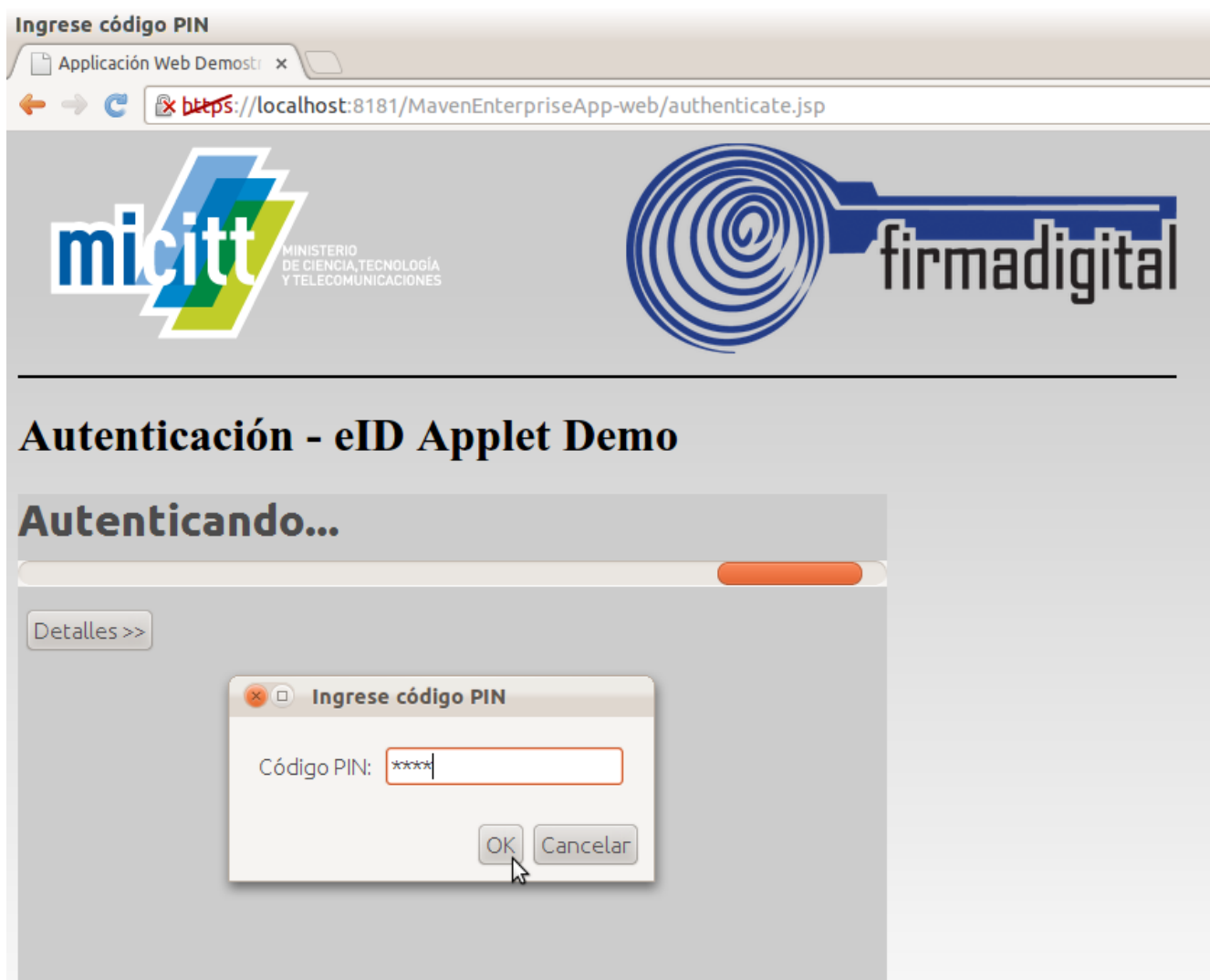
Puesto que el Applet ha sido firmado con un certificado de prueba, tendremos 2 advertencias las cuales debemos aceptar para proseguir con la ejecución de la aplicación:



La segunda advertencia la debemos aceptar de igual forma:



Una vez cargado el Applet, este detectará la presencia del Card Reader, Tarjeta, y pedirá el código PIN:

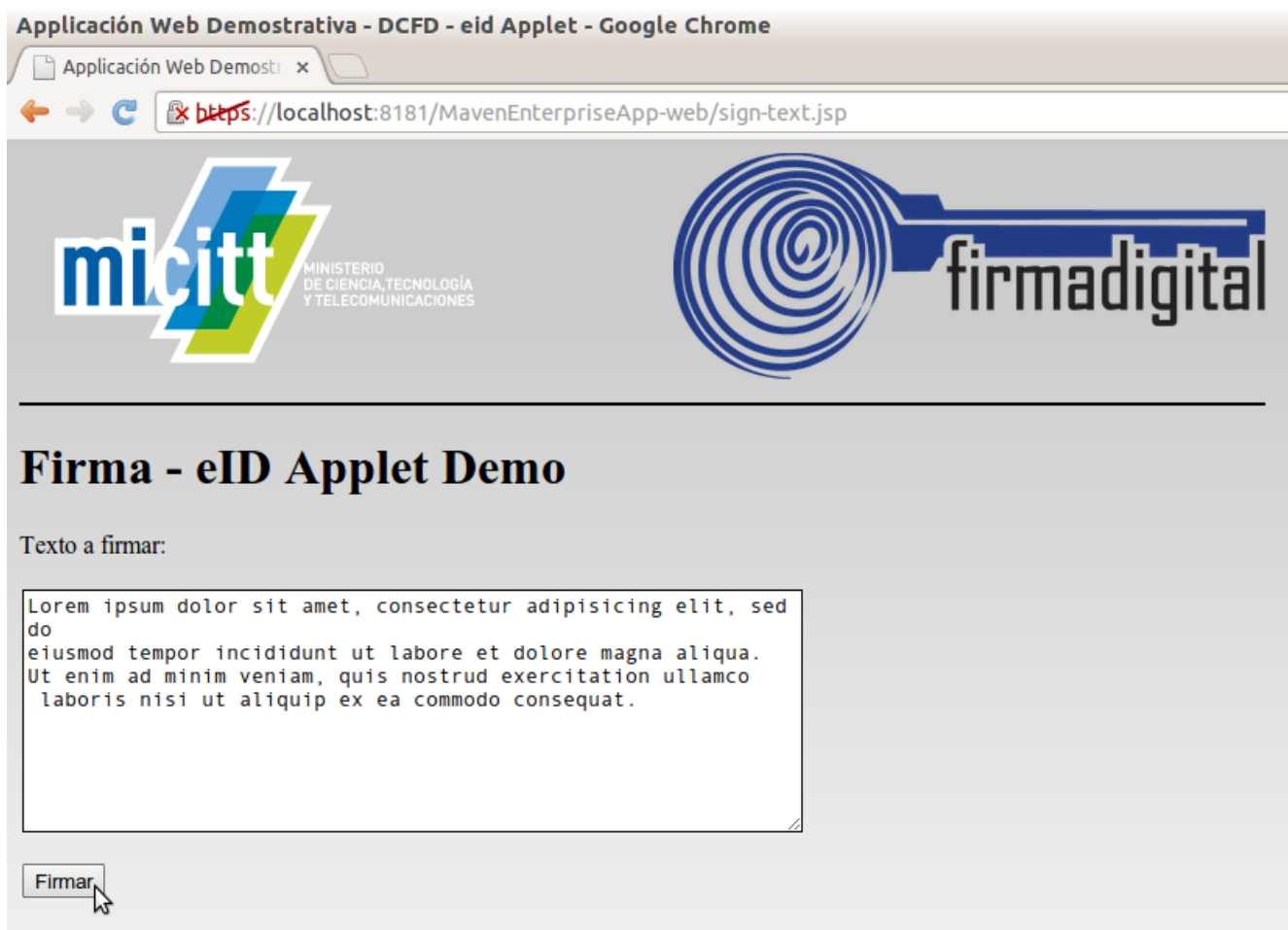


Con el PIN correcto, se procederá a la autenticación y mostrará el resultado:



Hacer click en el link “**Página de Inicio**” para volver a la página principal.

Para probar la funcionalidad de la Firma, hacer click en el link “**Firma**” esto nos llevará a la página en la que podemos especificar el texto a firmar:



Al hacer click en el botón Firmar, esto nos llevará a la página que carga el Applet.

Debemos permitir que el explorador cargue el Applet:



Cuando aparezcan las advertencias como en los pasos anteriores debemos aceptarlas.

Luego de Introducir el PIN, el Applet pedirá la confirmación para el proceso de Firma:





Luego de introducir el PIN correcto nuevamente, se procederá a la firma y mostrara el resultado:

Applicación Web Demostrativa - DCFD - eid Applet - Google Chrome

Applicación Web Demostrativa x

← → ↺ <https://localhost:8181/MavenEnterpriseApp-web/sign-result.jsp>

Firma - eID Applet Demo

Firma exitosa!!

Valor Firma:

```
05c5ce293f7c6c7e3b0b08e96249a87cbf092b077139507e2cc8029f56ee315eefb63c960b5ea4f8e72ea193c61f03da4
```

Signing Certificate Chain:

```
[[
[
  Version: V3
  Subject: CN=HERBERT FRANCISCO RODRIGUEZ CHAVES (FIRMA), OU=CIUDADANO, O=PERSONA FISICA, C=CR, G
  Signature Algorithm: SHA1withRSA, OID = 1.2.840.113549.1.1.5

  Key: Sun RSA public key, 2048 bits
  modulus: 25862474558620109661552778405048841199808286093887884964318826124792250819207437765631
  public exponent: 65537
  Validity: [From: Thu Oct 10 11:54:31 EDT 2013,
             To: Sat Oct 10 11:54:31 EDT 2015]
  Issuer: CN=CA SINPE - PERSONA FISICA, OU=DIVISION DE SERVICIOS FINANCIEROS, O=BANCO CENTRAL DE
  SerialNumber: [ 31c28d1a 00000001 b2a5]

  Certificate Extensions: 8
  [1]: ObjectId: 1.3.6.1.4.1.311.21.10 Criticality=false
  Extension unknown: DER encoded OCTET string =
  0000: 04 0E 30 0C 30 0A 06 08  2B 06 01 05 05 07 03 04  ..0.0...+.....

```

[Firmar Nuevamente](#) | [Página de Inicio](#)