

MiddleWare y Applet

Manual de Aplicación de escritorio Demostrativa en Java

Consumiendo funcionalidades del MiddleWare

Rolosa HyJ S.A. - MICITT

20 de Enero de 2014



Resumen

El presente documento es una para la utilización de la Aplicación de escritorio Demostrativa en Java que consume la Librería resultante de la compilación del MiddleWare que sigue el estándar RSA - PKCS#11.

Tabla de contenido

| | |
|---------------------|---|
| Pre-requisitos..... | 1 |
| Aplicación | 2 |

Pre-requisitos

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

- **Java Runtime Environment 6 update 45**

- **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)

- **iaikPkcs11Wrapper.jar** (Wrapper PKCS11 para utilizar beidpkcs11.dll en Java)

- **PKCS11Wrapper.dll** (Wrapper PKCS11 para JNI en Java - Windows)

- **libpkcs11wrapper.so** (Wrapper PKCS11 para JNI en Java - Linux)

- **bcprov-jdk15on-150.jar** (Dependencia de AIK para Cryptoki - BouncyCastle)

ver: <http://www.bouncycastle.org/java>

- **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).

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.soportefimadigital.com/sfd/default.aspx>

Aplicación

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

`\trunk\aplicaciones_demostrativas\JAVA\JAVAmwEIDTest_NetBeans-6.8\`

, contiene el la Aplicación Demostrativa en Java.

Las siguientes librerías fueron utilizadas para la creación de esta aplicación demostrativa:

- **bcprov-jdk15on-150.jar** (Libreria BouncyCastle para JAVA - Criptoki)

ver: <http://www.bouncycastle.org/java.html>

- **iaikPkcs11Wrapper.jar** (Wrapper ASIK PKCS11 para JAVA)

- **PKCS11Wrapper.dll** (Wrapper para JNI JAVA - Windows, importante utilizar librería x86)

- **libpkcs11wrapper.so** (Wrapper para JNI JAVA - Linux)

ver: http://ice.iaik.tugraz.at/sic/Products/Core-Crypto-Toolkits/PKCS_11_Wrapper

Todas las librerías tienen que ser copiadas dentro del directorio:

`\trunk\aplicaciones_demostrativas\JAVA\JAVAmwEIDTest_NetBeans-6.8\lib`

Para la creación de esta aplicación demostrativa, se requiere la existencia de los siguientes archivos en el presente directorio: `trunk/aplicaciones_demostrativas/JAVA/JAVAmwEIDTest/`

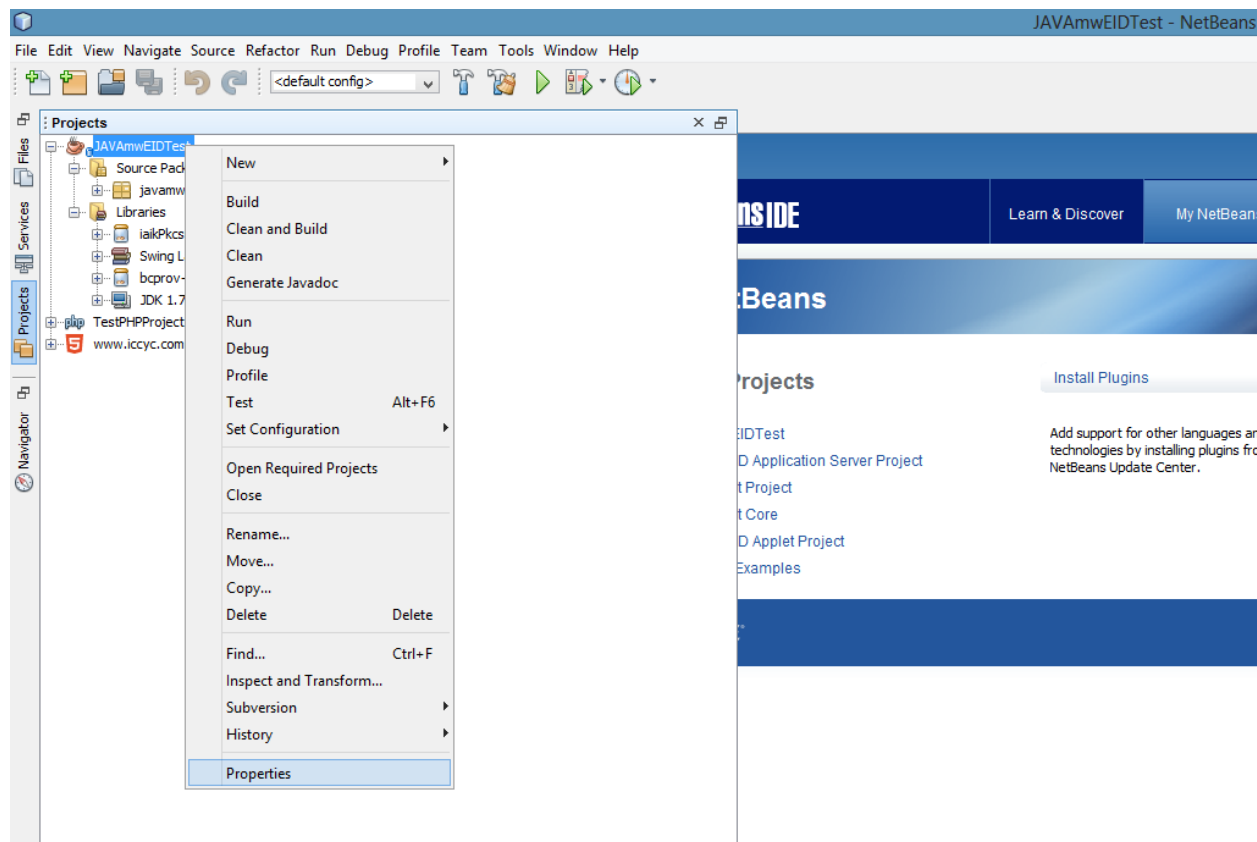
- **CA SINPE - PERSONA FISICA.cer** (Certificado del Emisor)

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

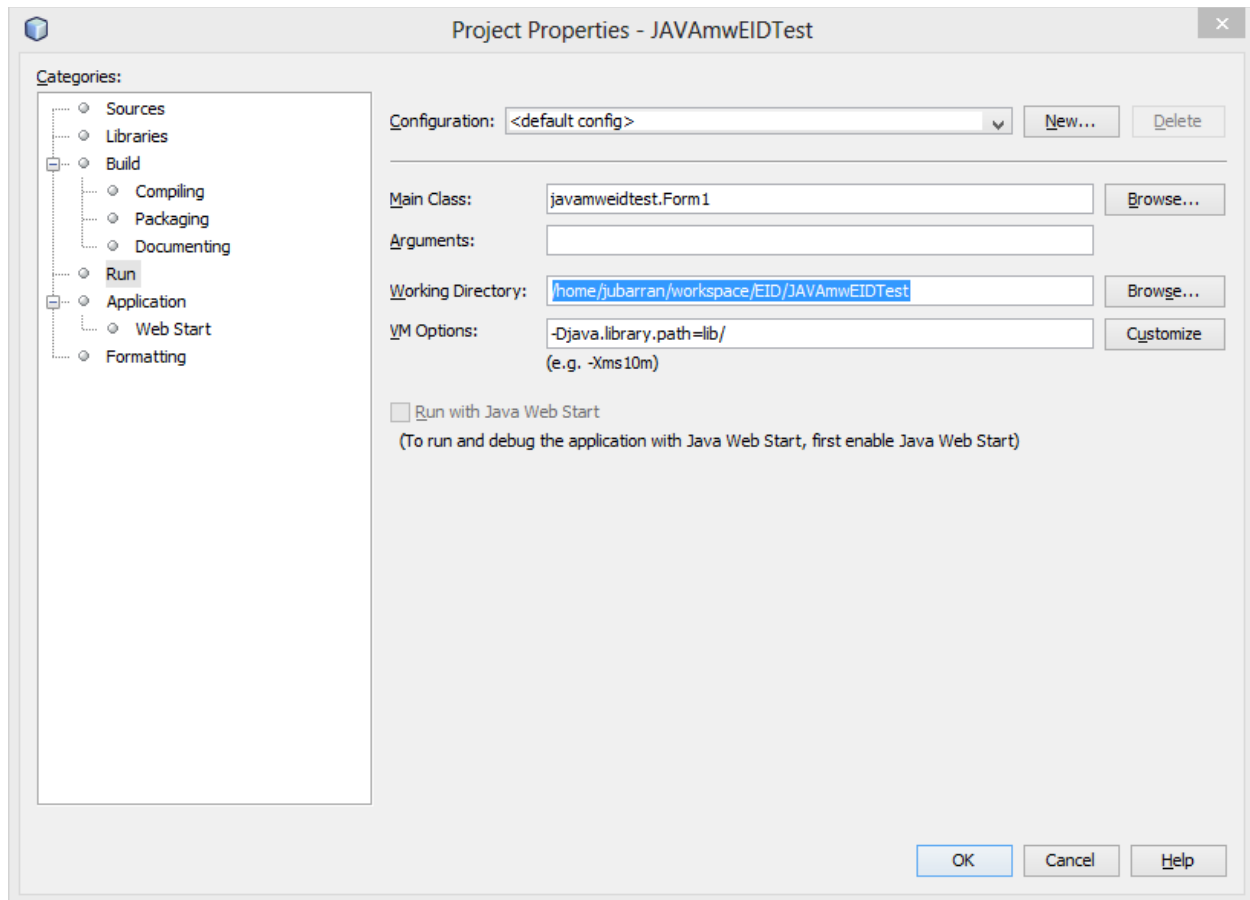
- **libbeidpkcs11.so** (Librería resultado de la compilación del BEID middleware - Linux)

- **beidpkcs11.dll** (Librería resultado de la compilación del BEID middleware - Windows)

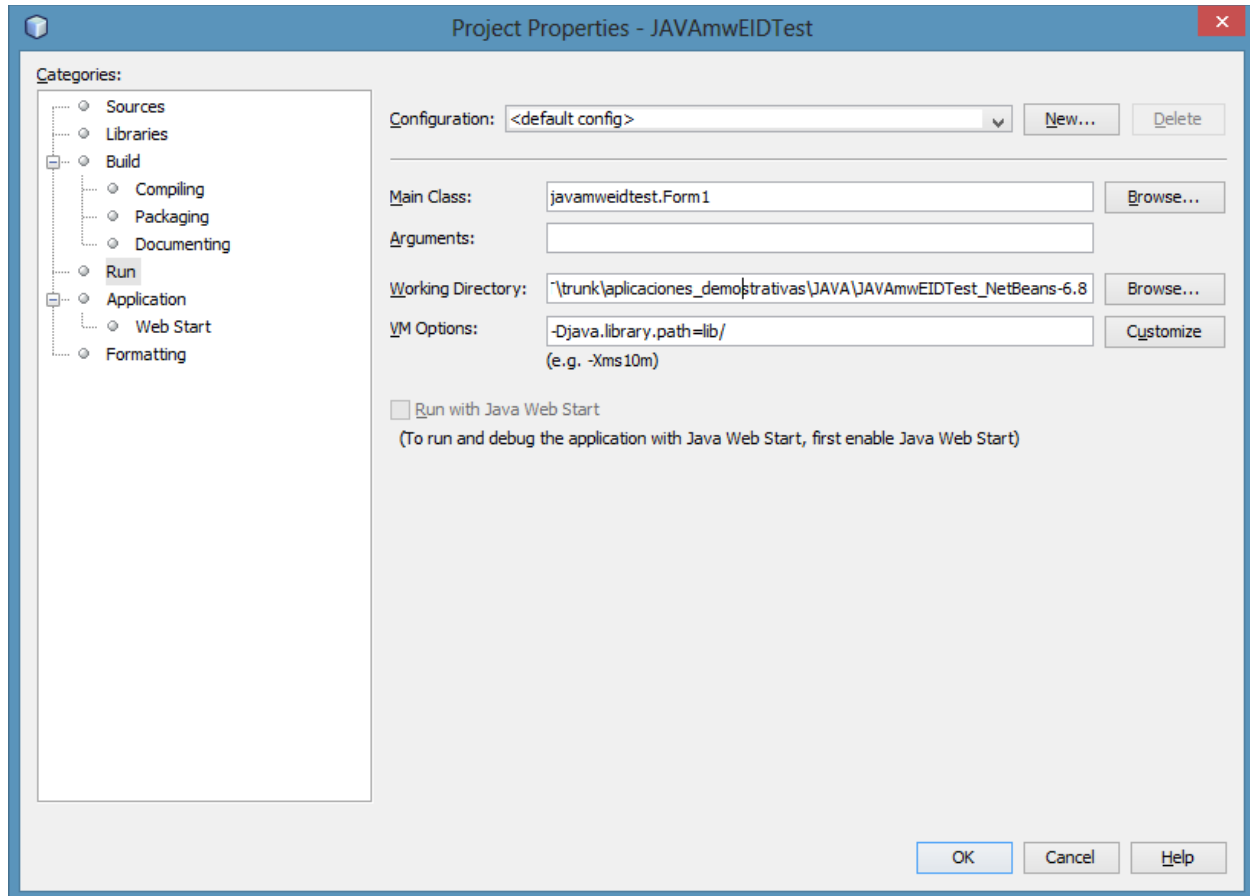
El proyecto ha sido creado con el IDE NetBeans 6.8. Luego de abrirlo, para compilar el proyecto, es necesario especificar el "**Working Directory**", ingresar a Propiedades del Proyecto:



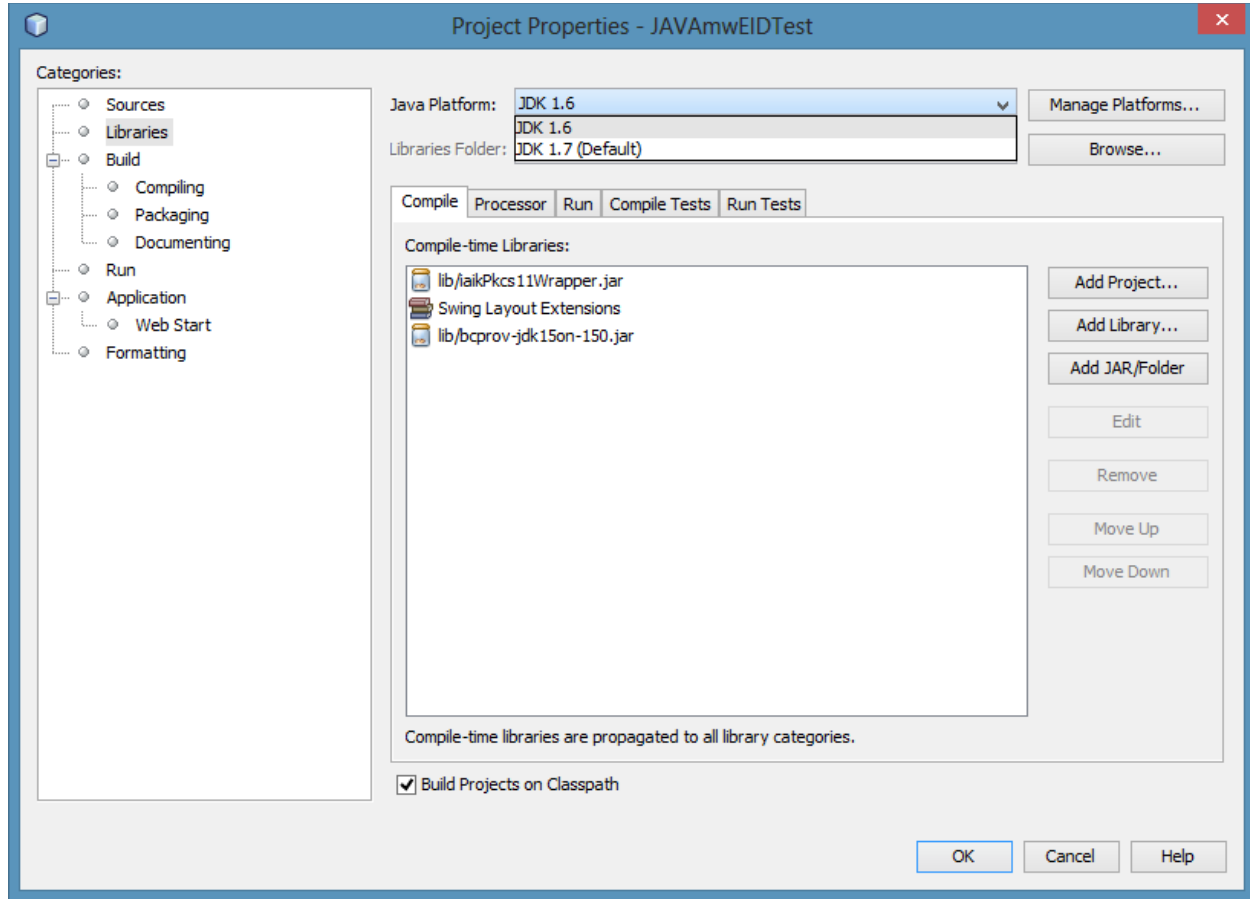
En la categoría "Run", cambia la ruta del "**Working Directory**":



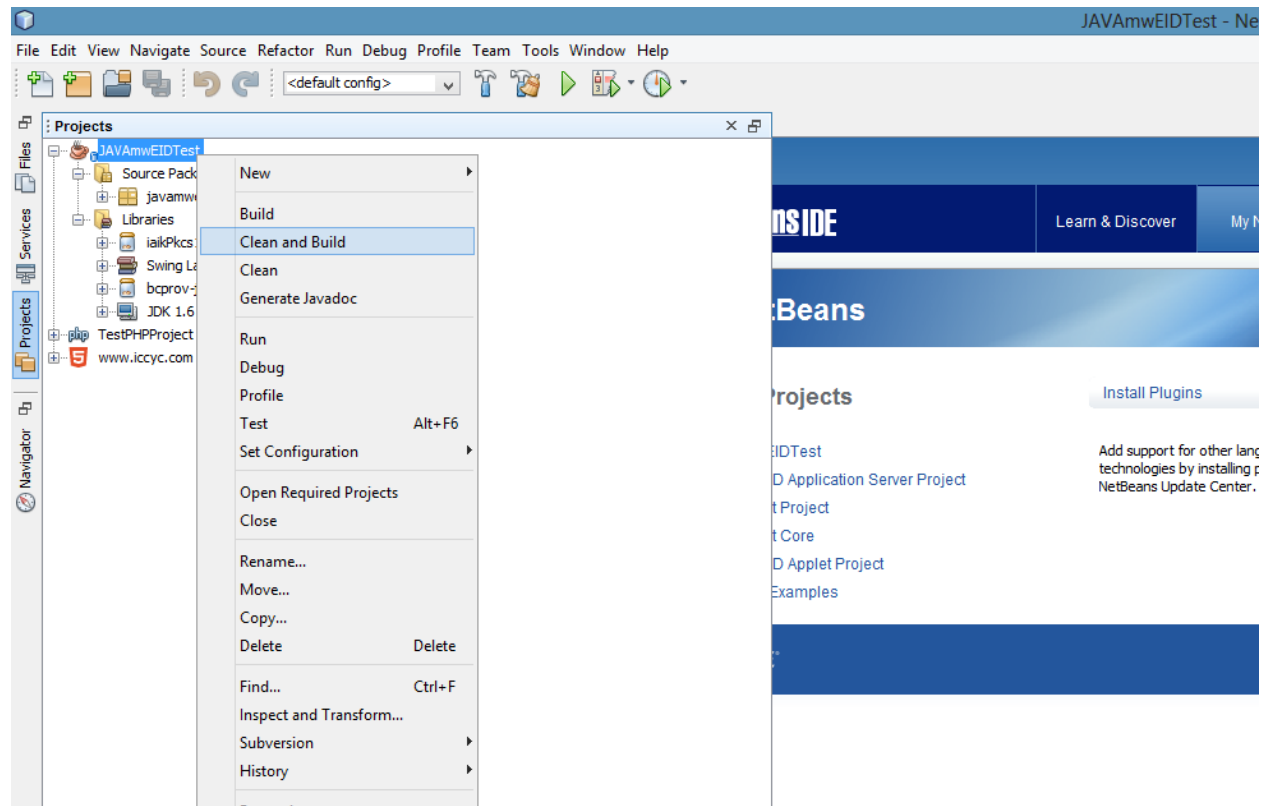
Es importante especificar la ruta que corresponde al directorio de la aplicación puesto que las referencias de las librerías serán tomadas con rutas relativas:



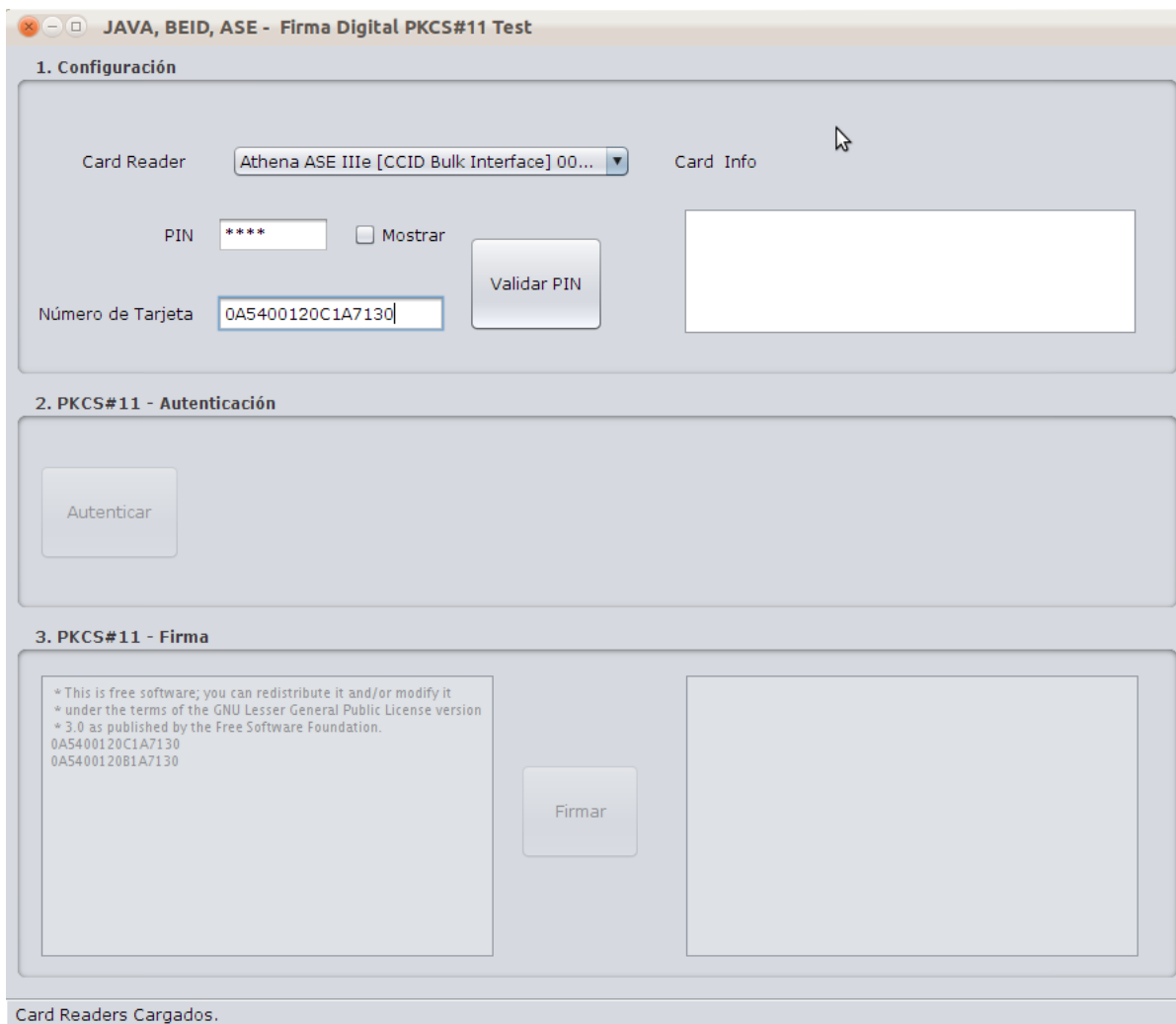
Luego, en la Categoría "**Libraries**" asegurarse que el JDK 1.6 es el especificado:



A continuación compilar el proyecto:



Una vez conectados el CardReader junto con la tarjeta inteligente, ejecutar el programa, el mismo detectará el CardReader conectado, luego introducir el PIN y el número de serie de la tarjeta:



JAVA, BEID, ASE - Firma Digital PKCS#11 Test

1. Configuración

Card Reader:

PIN: ☐ Mostrar

Número de Tarjeta:

Validar PIN

Card Info

2. PKCS#11 - Autenticación

Autenticar

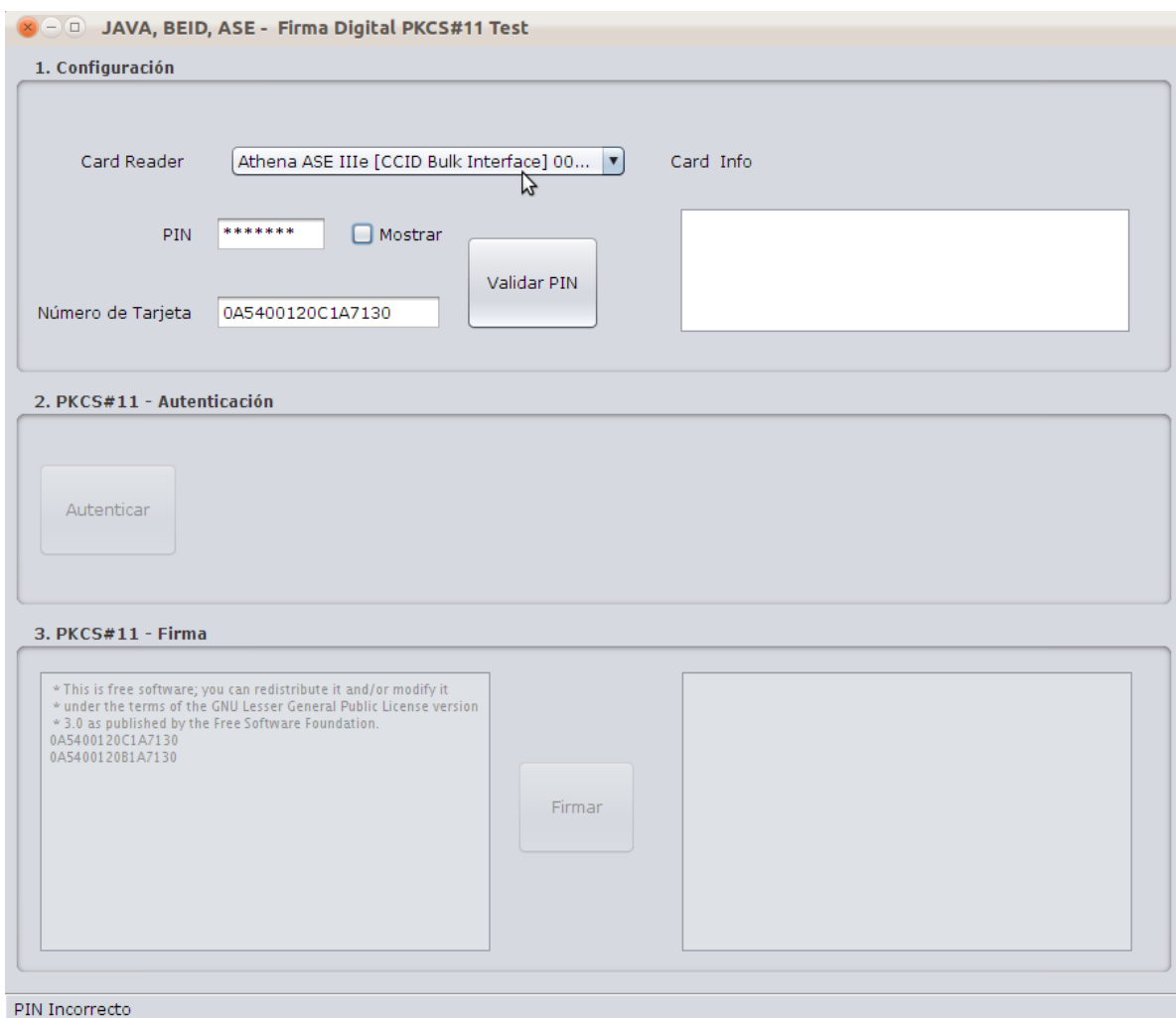
3. PKCS#11 - Firma

* This is free software; you can redistribute it and/or modify it
 * under the terms of the GNU Lesser General Public License version
 * 3.0 as published by the Free Software Foundation.
 0A5400120C1A7130
 0A5400120B1A7130

Firmar

Card Readers Cargados.

Luego de presionar el botón Validar PIN, el programar realizara las verificaciones del PIN y Número de Tarjeta, si existe algún error este será notificado:



JAVA, BEID, ASE - Firma Digital PKCS#11 Test

1. Configuración

Card Reader: Athena ASE IIIe [CCID Bulk Interface] 00...

Card Info:

PIN: ***** ☐ Mostrar

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

2. PKCS#11 - Autenticación

Autenticar

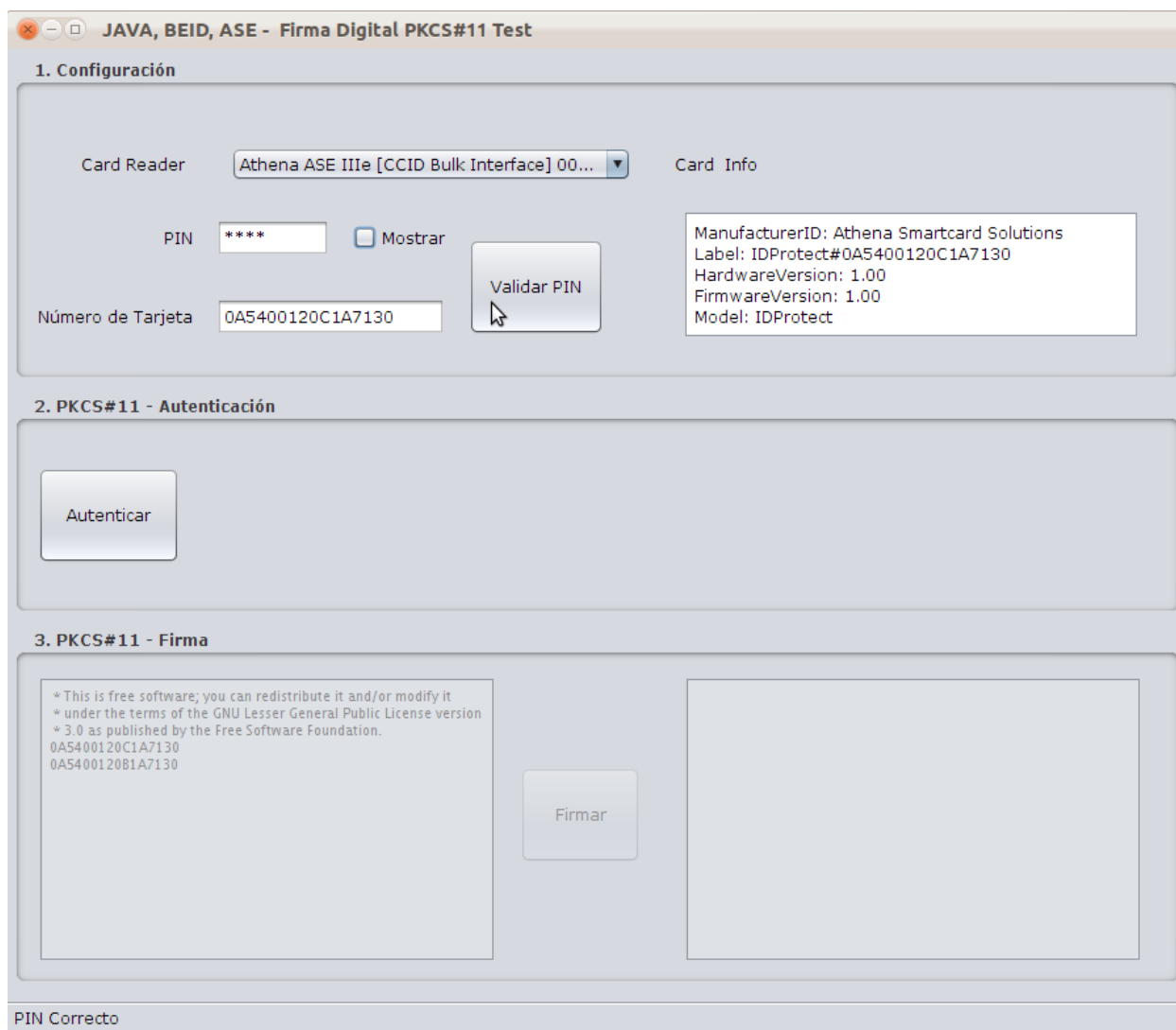
3. PKCS#11 - Firma

* This is free software; you can redistribute it and/or modify it
 * under the terms of the GNU Lesser General Public License version
 * 3.0 as published by the Free Software Foundation.
 0A5400120C1A7130
 0A5400120B1A7130

Fimar

PIN Incorrecto

Si tanto el PIN como el Numero de Tarjeta son correctos, el programa mostrara una información básica de la tarjeta y se habilitara el Botón de Autenticar:



The screenshot shows a Java application window titled "JAVA, BEID, ASE - Firma Digital PKCS#11 Test". It is divided into three main sections:

- 1. Configuración:** This section contains a "Card Reader" dropdown menu set to "Athena ASE IIIe [CCID Bulk Interface] 00...", a "Card Info" box displaying "ManufacturerID: Athena Smartcard Solutions", "Label: IDProtect#0A5400120C1A7130", "HardwareVersion: 1.00", "FirmwareVersion: 1.00", and "Model: IDProtect". Below the dropdown is a "PIN" field with "****" and a "Mostrar" checkbox. To the right is a "Validar PIN" button. At the bottom left of this section is a "Número de Tarjeta" field containing "0A5400120C1A7130".
- 2. PKCS#11 - Autenticación:** This section contains a single "Autenticar" button.
- 3. PKCS#11 - Firma:** This section contains a text area on the left with the following text:

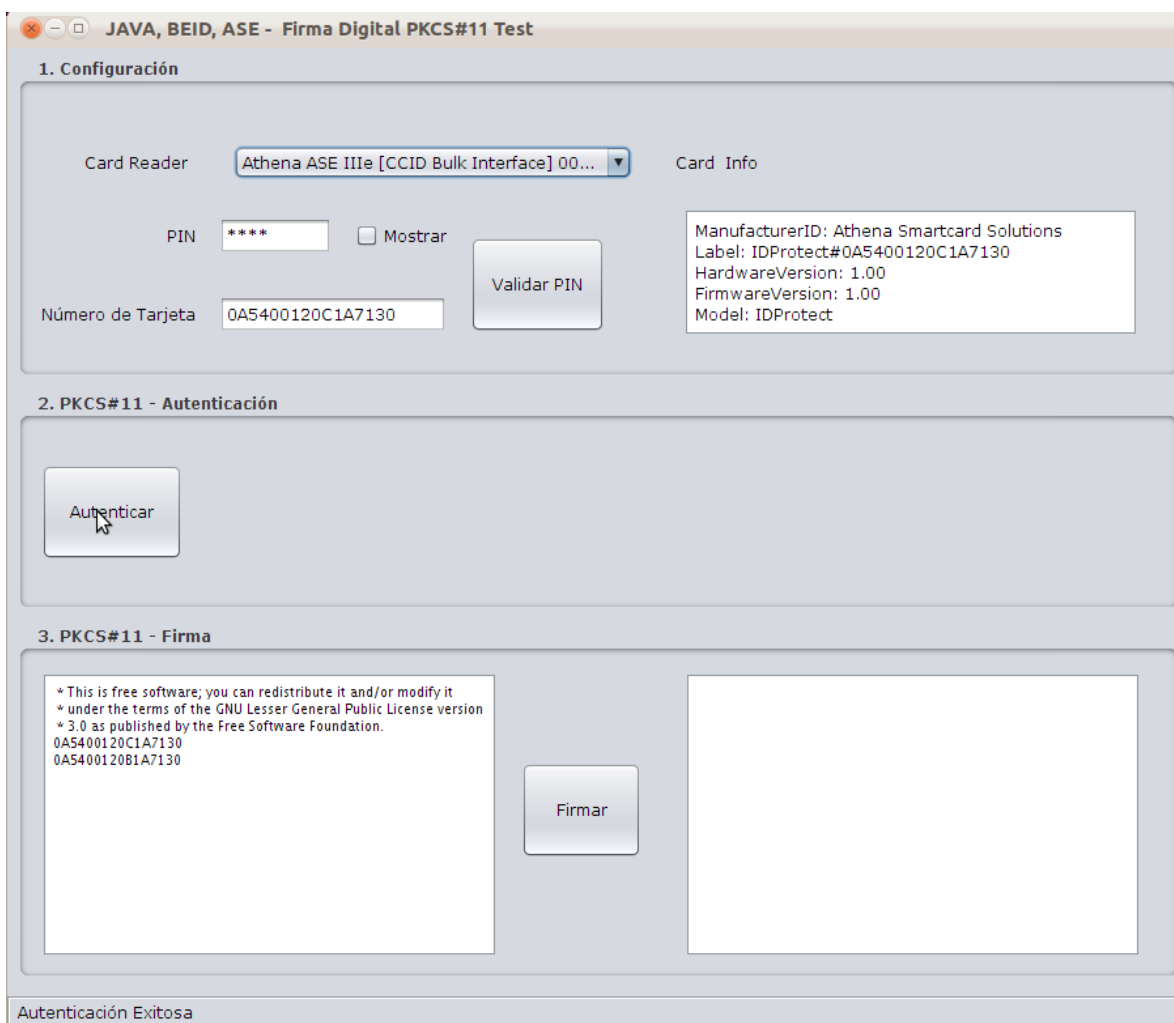

```
* This is free software; you can redistribute it and/or modify it
* under the terms of the GNU Lesser General Public License version
* 3.0 as published by the Free Software Foundation.
0A5400120C1A7130
0A5400120B1A7130
```

 In the center is a "Firmar" button, and on the right is a large empty rectangular box for the signature.

At the bottom of the window, a status bar displays "PIN Correcto".

Al presionar el Botón Autenticar, el programa leerá el Certificado de Autenticación que se encuentra en la SmartCard, extraerá la información del Servidor OCSP contra el cual tiene que realizar la verificación, y realizará la misma utilizando el certificado del emisor “CA SINPE - PERSONA FISICA.cer”, si hubiese algún error el programa lo notificará.

Si la Autenticación es exitosa, se habilitará el Botón “Firmar” para realizar la Firma Digital del texto de demostración que se encuentra en el cuadro de Texto:



JAVA, BEID, ASE - Firma Digital PKCS#11 Test

1. Configuración

Card Reader: Athena ASE IIIe [CCID Bulk Interface] 00...

PIN: **** ☐ Mostrar

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

Card Info:

- ManufacturerID: Athena Smartcard Solutions
- Label: IDProtect#0A5400120C1A7130
- HardwareVersion: 1.00
- FirmwareVersion: 1.00
- Model: IDProtect

2. PKCS#11 - Autenticación

Autenticar

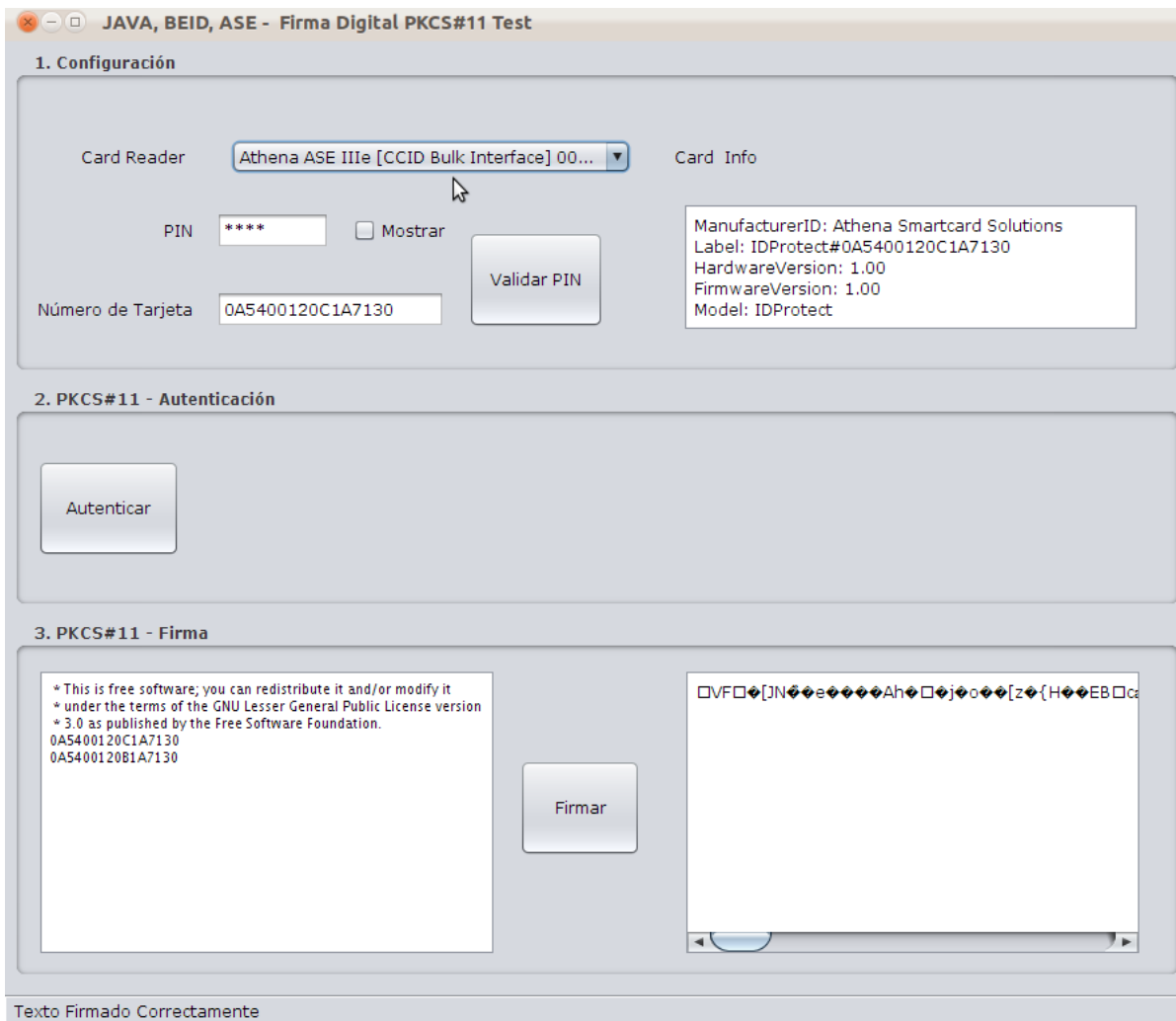
3. PKCS#11 - Firma

* This is free software; you can redistribute it and/or modify it
 * under the terms of the GNU Lesser General Public License version
 * 3.0 as published by the Free Software Foundation.
 0A5400120C1A7130
 0A5400120B1A7130

Firmar

Autenticación Exitosa

Al presionar el Botón "Firmar", se procederá a realizar la Firma del texto utilizando la Clave para Firma digital que se encuentra almacenada en la SmartCard:



1. Configuración

Card Reader: **Athena ASE IIIe [CCID Bulk Interface] 00...**

PIN: ******** ☐ Mostrar

Número de Tarjeta: **0A5400120C1A7130**

Validar PIN

Card Info

ManufacturerID: Athena Smartcard Solutions
Label: IDProtect#0A5400120C1A7130
HardwareVersion: 1.00
FirmwareVersion: 1.00
Model: IDProtect

2. PKCS#11 - Autenticación

Autenticar

3. PKCS#11 - Firma

* This is free software; you can redistribute it and/or modify it
* under the terms of the GNU Lesser General Public License version
* 3.0 as published by the Free Software Foundation.
0A5400120C1A7130
0A5400120B1A7130

Firmar

OVFO[INeAhjz{HEBcc

Texto Firmado Correctamente