

MiddleWare y Applet

Manual de Aplicación de escritorio Demostrativa en C#

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 C# 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 C#

- **DotNet v4.0 Framework**

- **Microsoft Visual C++ 2010 Redistributable Package**

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

- **Net.Pkcs11.dll** (Wrapper PKCS11 para utilizar beidpkcs11.dll en C#)

ver: <https://svn.code.sf.net/p/pkcs11net/code/>

- **BouncyCastle.Crypto.dll** (Dependencia de Net.Pkcs11.dll para Cryptoki)

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

- **asepkcs.dll** (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.soportefirmadigital.com/sfd/default.aspx>

Aplicación

La solución: **CSmwEIDTest.sln** que se encuentra en:

\trunk\aplicaciones_demostrativas\CS\CSmwEIDTest_VisualStudio-2010

, contiene el proyecto de la Aplicación Demostrativa en C#.

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

- **Net.Pkcs11.dll** (Wrapper PKCS11 para utilizar beidpkcs11.dll en C#)

ver: <https://svn.code.sf.net/p/pkcs11net/code/>

- **BouncyCastle.Crypto.dll** (Dependencia de Net.Pkcs11.dll para Cryptoki)

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

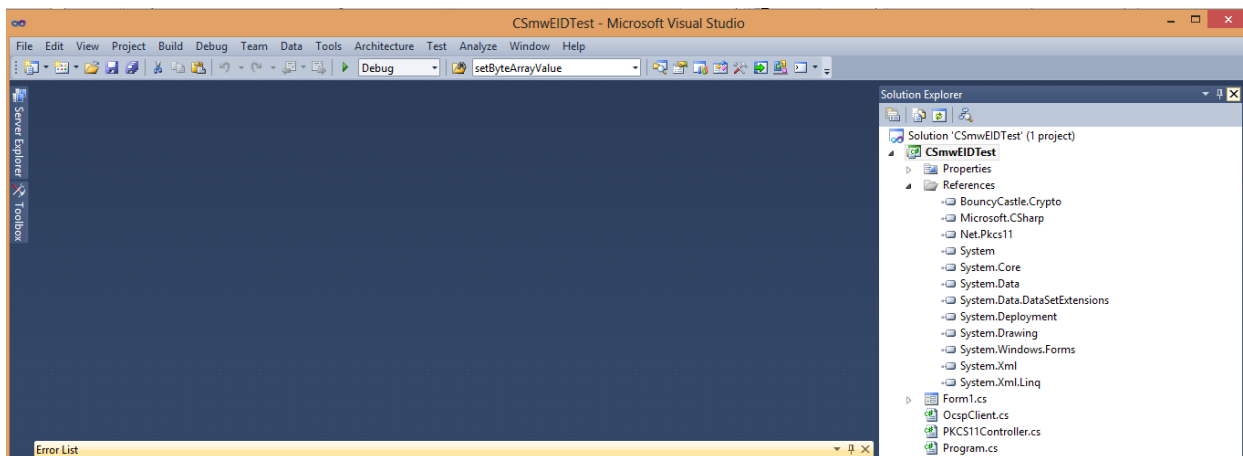
Ambas librerías tienen que ser copiadas dentro del directorio:

\trunk\aplicaciones_demostrativas\CS\CSmwEIDTest_VisualStudio-2010\CSmwEIDTest\References

Tomar en cuenta que el Wrapper Net.Pkcs11.dll tiene que ser el producto de las modificaciones realizadas y descritas en el documento:

Instalación y Configuración.pdf

Una vez que las librerías de referencia han sido copiadas, asegurarse que Visual Studio las muestra sin ningún problema como se muestra a continuación:



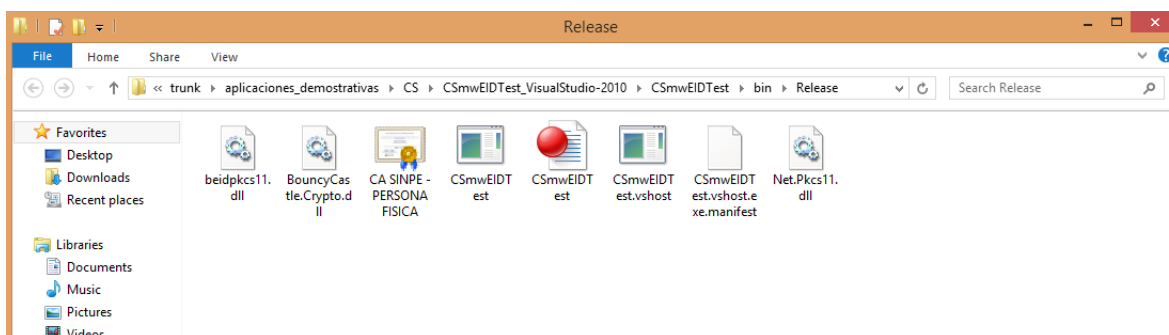
Luego de realizar la compilación del proyecto, es necesario copiar los archivos:

- beidpkcs11.dll
- CA SINPE - PERSONA FISICA.cer

dentro de los directorios tanto en Debug como en Release:

trunk\aplicaciones_demostrativas\CS\CSmwEIDTest_VisualStudio-2010\CSmwEIDTest\bin\Release

Asegurarse que la estructura de archivos sea como se muestra en la siguiente figura:



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

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

1. Configuración

Card Reader: Athena ASEDive V3CR 0

PIN: ****

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

Card Info

2. PKCS#11 - Autenticación

Autenticar

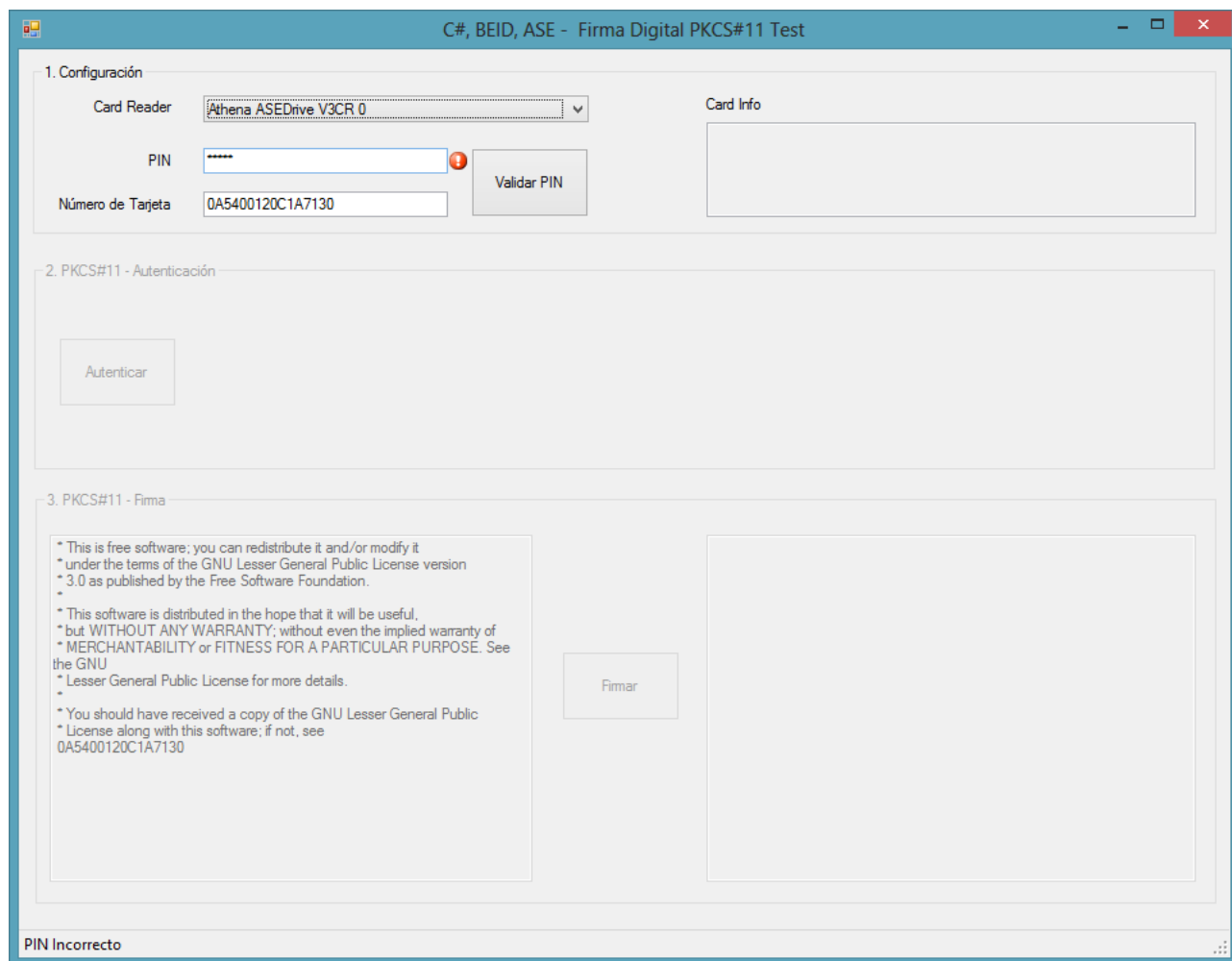
3. PKCS#11 - Firma

* 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.
*
* This software is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the GNU
* Lesser General Public License for more details.
*
* You should have received a copy of the GNU Lesser General Public
* License along with this software; if not, see
0A5400120C1A7130

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:



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

1. Configuración

Card Reader: Athena ASEDrive V3CR 0

PIN: *****

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

Card Info

2. PKCS#11 - Autenticación

Autenticar

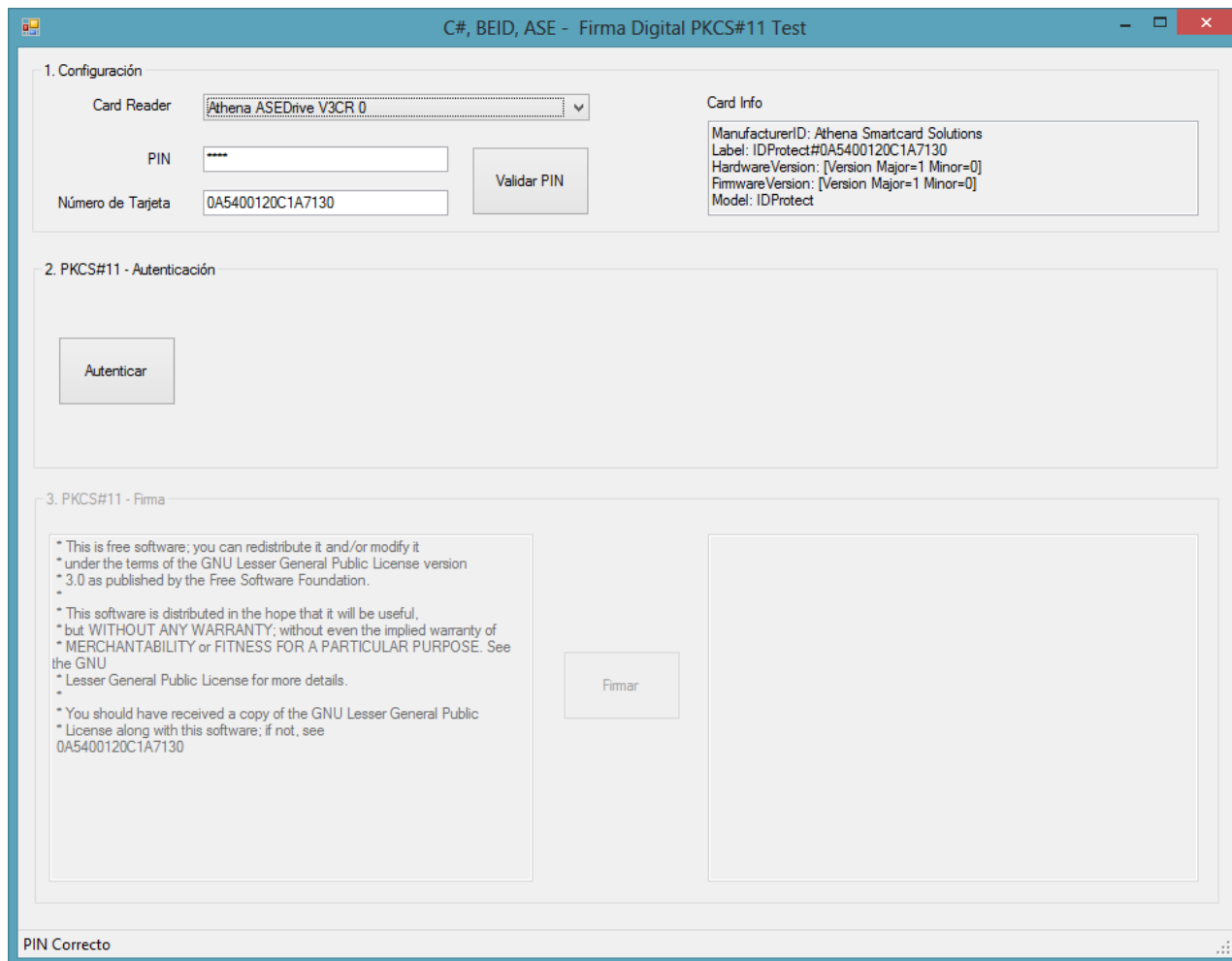
3. PKCS#11 - Firma

* 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.
 *
 * This software is distributed in the hope that it will be useful,
 * but WITHOUT ANY WARRANTY; without even the implied warranty of
 * MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
 the GNU
 * Lesser General Public License for more details.
 *
 * You should have received a copy of the GNU Lesser General Public
 * License along with this software; if not, see
 0A5400120C1A7130

Firmar

PIN Incorrecto

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



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

1. Configuración

Card Reader:

PIN:

Número de Tarjeta:

Card Info

ManufacturerID: Athena Smartcard Solutions
Label: IDProtect#0A5400120C1A7130
HardwareVersion: [Version Major=1 Minor=0]
FirmwareVersion: [Version Major=1 Minor=0]
Model: IDProtect

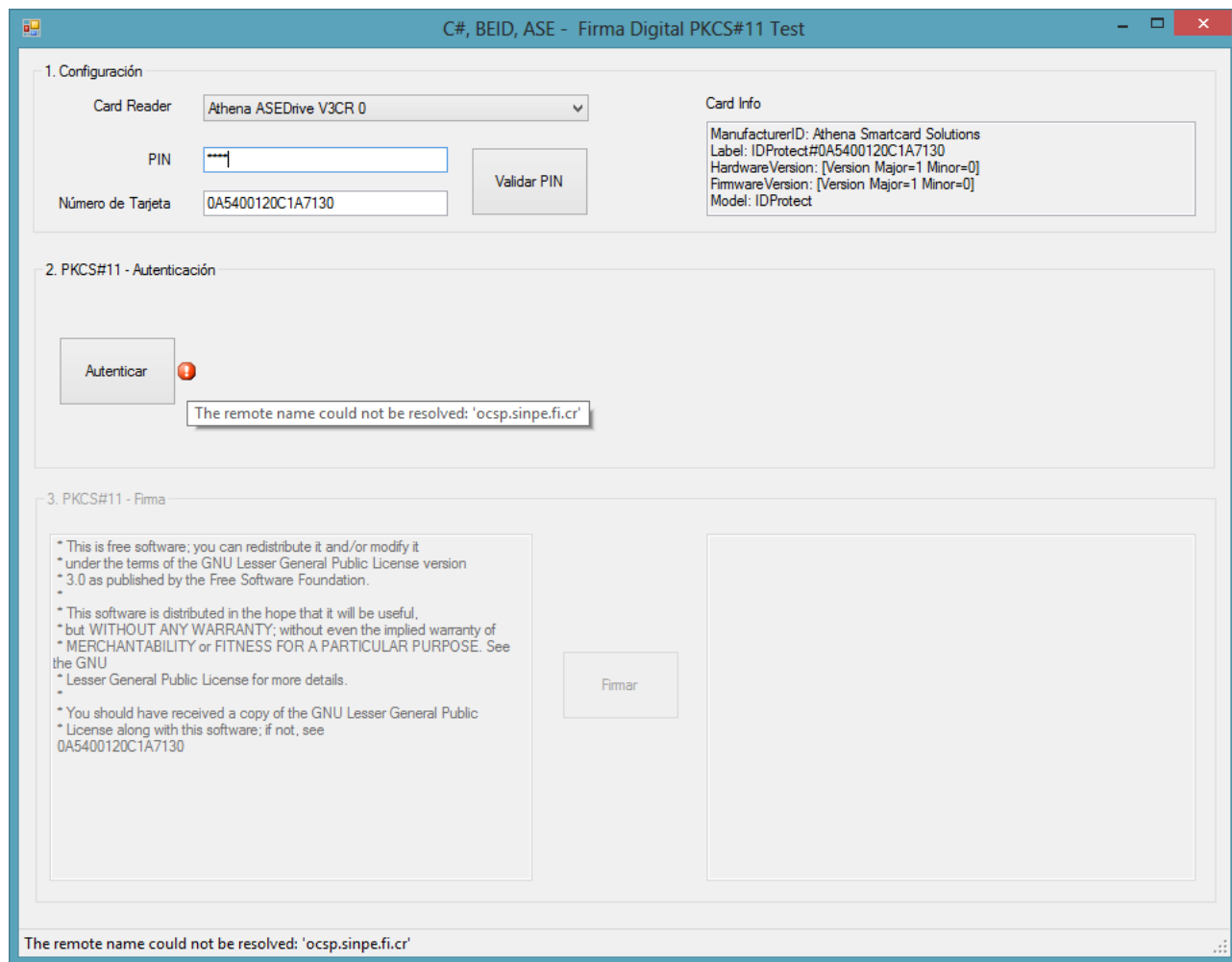
2. PKCS#11 - Autenticación

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.
*
* This software is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the GNU
* Lesser General Public License for more details.
*
* You should have received a copy of the GNU Lesser General Public
* License along with this software; if not, see
0A5400120C1A7130

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 realizara la misma utilizando el certificado del emisor “CA SINPE - PERSONA FISICA.cr”, si hubiese algún error el programa lo notificará:



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

1. Configuración

Card Reader: Athena ASEDrive V3CR 0

PIN: ****

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

Card Info

ManufacturerID: Athena Smartcard Solutions
Label: IDProtect#0A5400120C1A7130
HardwareVersion: [Version Major=1 Minor=0]
FirmwareVersion: [Version Major=1 Minor=0]
Model: IDProtect

2. PKCS#11 - Autenticación

Autenticar

The remote name could not be resolved: 'ocsp.sinpe.fi.cr'

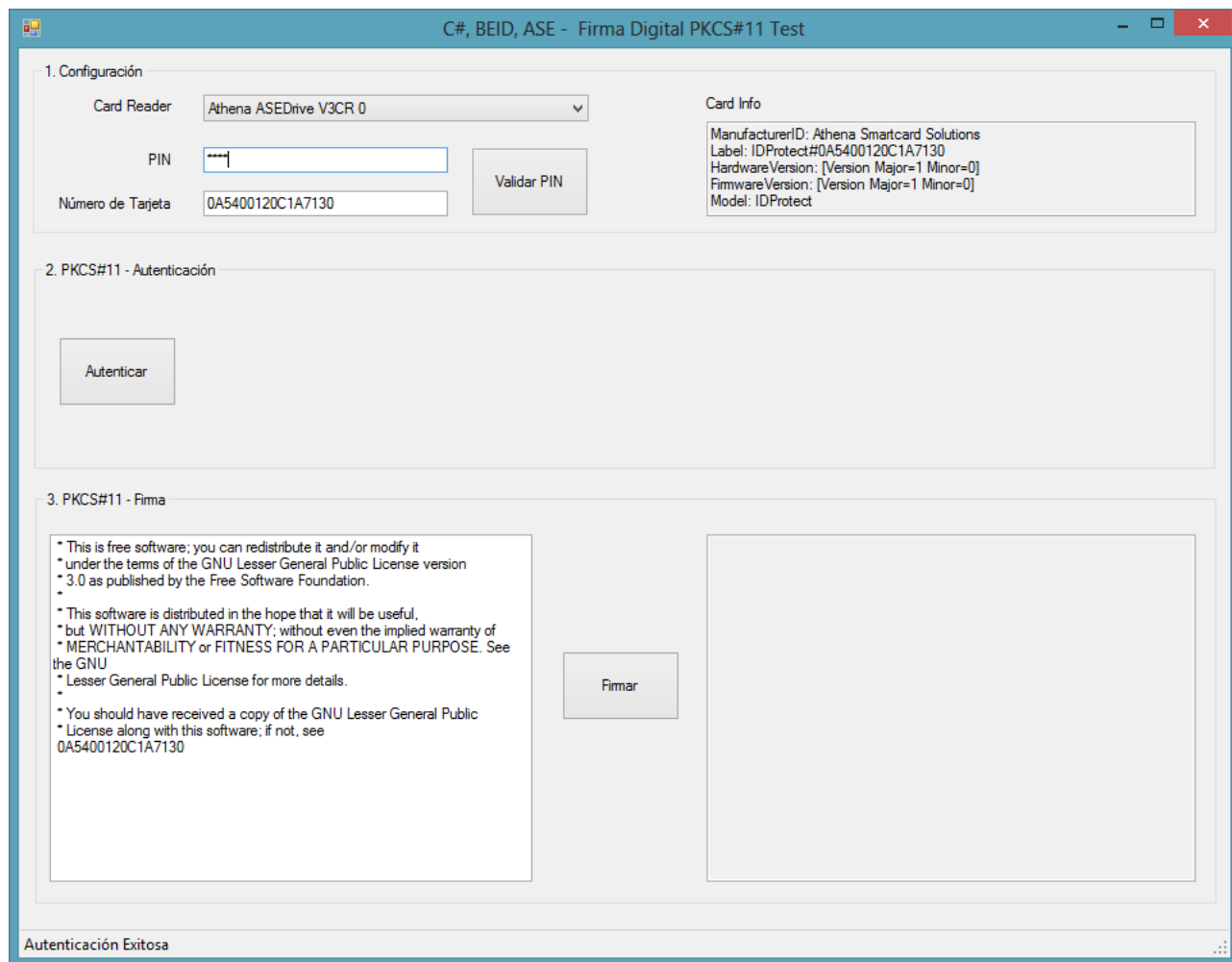
3. PKCS#11 - Firma

* 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.
*
* This software is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the GNU
* Lesser General Public License for more details.
*
* You should have received a copy of the GNU Lesser General Public
* License along with this software; if not, see
0A5400120C1A7130

Firmar

The remote name could not be resolved: 'ocsp.sinpe.fi.cr'

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:



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

1. Configuración

Card Reader: Athena ASEDrive V3CR 0

PIN: ****

Número de Tarjeta: 0A5400120C1A7130

Validar PIN

Card Info

ManufacturerID: Athena Smartcard Solutions
Label: IDProtect#0A5400120C1A7130
HardwareVersion: [Version Major=1 Minor=0]
FirmwareVersion: [Version Major=1 Minor=0]
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.
* This software is distributed in the hope that it will be useful,
* but WITHOUT ANY WARRANTY; without even the implied warranty of
* MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See
the GNU
* Lesser General Public License for more details.
* You should have received a copy of the GNU Lesser General Public
* License along with this software; if not, see
0A5400120C1A7130

Firmar

Autenticación Exitosa

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

1. Configuración

Card ReaderAthena ASEDive V3CR 0

PIN****

Validar PIN

Número de Tarjeta0A5400120C1A7130

Card Info

ManufacturerID: Athena Smartcard Solutions
Label: IDProtect#0A5400120C1A7130
HardwareVersion: [Version Major=1 Minor=0]
FirmwareVersion: [Version Major=1 Minor=0]
Model: IDProtect

2. PKCS#11 - Autenticación

Autenticar

3. PKCS#11 - Fima

* 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.

* This software is distributed in the hope that it will be useful,
but WITHOUT ANY WARRANTY; without even the implied warranty of
MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU
Lesser General Public License for more details.

* You should have received a copy of the GNU Lesser General Public
License along with this software; if not, see
0A5400120C1A7130

Fimar

%?P%k!-+??O????J0???dSw!!!5????|Xfb>
[H-?Ageh???L@Q[M?????:?)@_yg?c?=x%?-|??y(?%3???<p?
[?4U????##B L?(?! O+Q"&Y8V?
??---(?!(?!)29?E?)???XTW?KR
SD???????HMJ???7QU?nPN-P?T.?2?m<)SIC?" I?
%?C%?J {pu??pS

Texto Firmado Correctamente