



IDGo 500 PKCS#11 Library for Windows - Release 2.2.0.12

Release Notes

Doc Ref : D1264129A

6 July, 2012

Contents

What's New?	3
New Names.....	3
New Versions of Operating Systems and Applications Supported	3
Corrected Problems	3
Enhancements	3
What's Gone?.....	4
What's In?.....	5
Supported Operating Systems and Applications	5
Supported Readers	6
What's History?	7
What's Up?	9
Known Issues	9
Conversion from .NET PKCS#11 2.1 to 2.2.....	9
Performance Problems With Memory Management	9
Mozilla Firefox and Thunderbird	9
Remote Desktop Connection	9
CheckPoint VPN Client NGX.....	9
Citrix Server.....	10
Adobe Acrobat Reader.....	10
Where's the Doc?	10

These release notes provide particular details about release 2.2.0.12 of IDGo 500 PKCS#11 Library for Windows.

What's New?

This section describes all the differences between this release 2.2.0.12 and the previous release 2.2.0.

New Names

The .NET Smart Cards PKCS#11 Library has been renamed "IDGo 500 PKCS#11 library. Gemalto's .NET range of cards has been renamed IDPrime .NET.

New Versions of Operating Systems and Applications Supported

Some third-party applications have evolved since the previous release of IDGo 500 PKCS#11.

For details of the latest versions of applications and operating systems that are supported by this latest release, please refer to "Supported Operating Systems and Applications" in the "What's In?" section and see which appear as "added" in the second column.

Corrected Problems

- The **C_InitToken** function has been modified so that all objects are now correctly erased.
- For the IDGo 500 PKCS#11 to prompt the user to enter the User PIN via the PIN pad reader, the User PIN must be of type "External" and the PIN pad must be connected to the computer and correctly installed. A problem existed, where if the PIN type was changed to "normal alphanumeric" in the card, the IDPrime .NET PKCS#11 module was still expecting the PIN to be entered via the PIN pad (prompting the user to do so). This was because the PIN type was being stored in cache memory. This has been fixed by making the IDPrime .NET PKCS#11 module read the PIN type directly from the card, rather than from cache memory.
- The **C_Finalize** function has been modified to improve its robustness.
- Modifications have been made to the way in which card insertion and withdrawal is detected in order to overcome certain problems.

Enhancements

- The logs have been changed so that there is now one log for each process. In addition, timestamping has been added so that you can see the times that each operation is performed.

What's Gone?

For information about the old versions of applications that are no longer officially supported by IDGo 500 PKCS#11 Library for Windows, please refer to "Supported applications and operating Systems in the "What's In?" section and see which appear as "removed" in the second column.

What's In?

This section provides a full list of hardware, operating systems, peripherals and software that are supported by Gemalto for use with this current version of IDGo 500 PKCS#11 Library for Windows.

Supported Operating Systems and Applications

This section provides a full list of all the OS supported by this current version of IDGo 500 PKCS#11 Library for Windows.

The second column indicates the old versions that are no longer officially supported (removed) and new versions for which support has been added. If the second column is blank for an application version, this means that support for that version is continued.

PKCS#11 for IDPrime .NET Smart Cards comes in two versions, one for 64-bit operating systems and one for 32-bit operating systems (OS). The installation program checks your version of windows and automatically installs the correct version for you.

OS OR APPLICATIONS	
Windows 2000 Professional (up to SP5) (32-bit version only)	Removed
Windows XP Professional (up to SP3)	
Windows Server 2003 (up to SP2)	
Windows VISTA SP1 and SP2	
Windows Server 2008 (up to SP1)	
Windows Server 2008 R2 (64-bit version only)	
Windows 7 (up to SP1)	Added SP1
Browsers	
Mozilla Firefox 3.0	Removed
Mozilla Firefox 3.5	Removed
Mozilla Firefox 3.6	Removed
Mozilla Firefox 11.X	Added
Mozilla Firefox 12.X	Added
Mozilla Firefox 13.X	Added
e-mail applications	
Mozilla Thunderbird 2.0	Removed
Mozilla Thunderbird 3.X	Removed

Mozilla Thunderbird 11.X	Added
Mozilla Thunderbird 12.X	Added
Mozilla Thunderbird 13.X	Added
Other Applications	
Adobe Reader 9.X	
Adobe Reader 10.X (Tested with Windows 7 SP1)	Added

Note: Unless indicated otherwise, all Service Packs (SP) associated with the various OS are supported.

Supported Readers

The smart card reader may be integrated with the Windows system or it can be an external device that is connected via USB. The solution is compatible with most certified Chip Card Interface Device (CCID), USB class or embedded smart card reader; for example Gemalto's IDBridge K30 / K50 (ex USB Shell Token V2/V3) and IDBridge CT30 (ex PC Twin).

PIN pad readers that are compliant with the PC/SC V2.0 specification are supported but the PIN pad itself can be used only for the **Verify PIN** function.

What's History?

This section a history of the changes made in previous releases

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.2.0 (since 2.1.3.1)

New Features:

- The .NET PKCS#11 library now reads the card serial number directly from the Card ID file instead of from the CSN optional parameter.
- Instant detection of .NET USB devices. The .NET PKCS#11 can now detect insertions and withdrawals of these types of devices.
- File cache disk. This feature improves the performance of the .NET PKCS#11 by storing a copy of non-confidential data on the computer. In this way, read/write operations can be performed on the cache instead of the card's contents. (PINs and private keys are not included in the file cache).
- A configuration file has been added that enables you to activate or deactivate the cache disk feature and the log file. The configuration file specifies the location of the log file.
- The .NET PKCS#11 library now has five permanent "ready to use" virtual slots. This means however that the maximum number of simultaneous reader collections is now five instead of 16.
- The Minidriver's **Set Card Property** and **Get Card Property** can now be called at the PKCS#11 level (**C_SetCardProperty** and **C_GetCardProperty**) respectively.

Applications Supported:

- Added Mozilla Firefox 3.6
- Added Mozilla Thunderbird 3.0

Readers Supported

- Removed Human Interface Device (HID) readers

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.1.3.1 (since 2.1.3)

New Feature:

- "No PIN" type user PINs (in the Minidriver sense of the term). This means that all key containers that are protected by the user PIN can be used without having to enter the user PIN.

Evolutions:

- Default certificate management modified (Windows 2000, XP and Server 2003 – does not apply to Vista).

The current cryptoki sets the default certificate flag to this certificate only if the smart card logon OID is present in the certificate attributes, otherwise the default certificate is unchanged. If no certificate with the smart card logon OID is present in the card, the default certificate is the first one present.

Corrected Problems:

- Serial number returned by the "C_GetTokenInfo" method changed back to v2.1.2.

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.1.3 (since 2.1.2)

New Features:

- Biometric authentication support (if .NET Bio installed) extended to include Windows 7 and Windows Server 2008 R2 (64-bit version only)

Corrected Problems:

- There was a bug fix concerning multisessions.

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.1.2 (since 2.1.1)

OS Supported:

- Added Windows 7
- Added Windows Server 2008 R2 (64-bit version only)

Applications Supported:

- Added Mozilla Firefox 3.5
- Removed Mozilla Firefox 2.0
- Added Adobe Acrobat 9.X
- Removed Adobe Acrobat 8.X

Readers Supported:

- Added PIN pad readers that are compliant with the PC/SC V2.0 specification, although only for the **Verify PIN** operation. For other PIN operations such as **Change PIN** and **Unblock PIN**, the readers act in transparent mode, that is, like an ordinary smart card reader.

Corrected Problems

- A problem was corrected in order to enable support of Firefox 3.0.13 and 3.5.2. This was done by enabling PKCS#11 templates to support attributes of "null" size. In such a case, the attribute is ignored and the rest of the template is processed.

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.1.1 (since 2.1)

OS Supported:

- Added Vista SP2 for 32-bit and 64-bit OS
- Removed support for first version of Vista (pre-SP1) for 32-bit and 64-bit OS
- Added Windows Server 2008 up to SP2 (was up to SP1) for 32-bit and 64-bit OS

Features added:

- Biometric authentication supported if .NET Bio installed
- SSO (Single Sign-On) mode supported if .NET policy configured accordingly.

Improvements in .NET Smart Cards PKCS#11 Library for Windows 2.1 (since 2.0)

- C_GetSlotList method behaves differently so PC/SC reader list is refreshed each time the method is called.

What's Up?

This section provides a list of the known issues at the time of this current release and also of the limitations of the product.

Known Issues

The following issues were known at the time of writing this release note.

Conversion from .NET PKCS#11 2.1 to 2.2

The way in which Root certificates are imported in version 2.1 causes a problem when you upgrade to version 2.2. The card's minidriver file system manages this incorrectly, which means that the card is not interpreted correctly by the host minidriver, even though it may appear to be fine as far as the card is concerned. This means that when a card that was personalized under version 2.1 of .NET PKCS#11 is read for the first time by version 2.2, the .NET PKCS#11 library corrects the card's file system automatically. Unfortunately this correction means that the garbage collector has to create new files and delete old ones which is resource intensive and can take a long time (around 20 seconds for each certificate that needs to be moved).

Note: This automatic correction of the file system is only performed once - the first time the card is read by .NET PKCS#11 2.2.

Performance Problems With Memory Management

The .NET card can be slow when performing operations that require using the card's memory such as, for example, loading a large number of certificates or keys, or large PKCS#11 data objects. This is mainly operations that involve the garbage collector.

Mozilla Firefox and Thunderbird

Simultaneous Smart Cards

When browsing the cryptographic modules on either Firefox or Thunderbird with two smart cards connected and logs on with one of the smart cards, Firefox/Thunderbird considers both smart cards as being logged on.

Fast User Switching

If the end-user switches from one account to another while Firefox/Thunderbird is running, the PC/SC context is broken.

Firefox/ Thunderbird must be restarted after the switch to communicate with the smart card.

Remote Desktop Connection

The end-user must log off from any active remote desktop connection before accessing it from the host.

CheckPoint VPN Client NGX

On a Windows 64-bit OS, CheckPoint is not able to enroll the end-user on the smart card.

Citrix Server

Applications using the PKCS#11 library (such as Firefox) remain in memory after the end-user closes the application. Check the latest hotfix on the Citrix web site.

Adobe Acrobat Reader

Adobe Acrobat Reader does not support certificate importation.

Where's the Doc?

This section describes the documentation that is provided with IDPrime .NET Smart Cards PKCS#11 Library for Windows and where to find it:

Documentation		
Document	Location	Description
IDGo 500 PKCS#11 Library for Windows User Guide	<ul style="list-style-type: none">In the ZIP file alongside the .msi that contains the library.	Describes the architecture and PKCS#11 methods and describes the main tasks to perform with the solution.
Release Notes (this document)	<ul style="list-style-type: none">In the ZIP file alongside the .msi that contains the library.	Describes the new features and cards/readers/applications supported, added since the previous release as well as known limitations.
EULA	<ul style="list-style-type: none">Appears during installation when asked to accept terms and conditions	Describes the End User License Agreement – the terms and condition of use for IDGo 500 PKCS#11 Library for Windows