Release Notes

Doc Ref: D1426864A

Date: March 22, 2017

This document presents information about the IDGo 800 PKCS#11 Library and Tokend for Mac OS X V1.2.9 and says what has changed since V1.2.8

**Important Note**:

Even though Apple has now officially deprecated the Tokend from OS X Lion onwards:

http://smartcardservices.macosforge.org/post/apple-deprecates-smart-card-services-in-os-x-lion-v107/

Gemalto has decided to include a Tokend in the IDGo 800 for Mac package, in order to ease the migration of its customers.

Nevertheless, Gemalto cannot commit to provide maintenance for this Tokend security module, due to the official lack of support from Apple from now on.

Gemalto recommends its customers to use the PKCS#11 security module of IDGo 800 for Mac, for which the maintenance can be ensured by Gemalto.

# What's New?

## Corrected Problems

- During the installation of IDGo 800 Mac 1.2.8, a warning message appeared warning the user that the package was signed with an expired certificate. After updating the certificate, the message did not appear. IDGOD-373

## New Locations of PKCS#11 Security Module and Tokend

El Capitan introduces a new security feature called "System Integrity Protection" (see https://support.apple.com/en-us/HT204899.

This means that the Gemalto PKCS11 library is installed in a different location for El Captian:

- The IDGo800 PKCS#11 library file **libidprimepkcs11.dylib** is installed in **/usr/local/lib/pkcs11/** instead of **/usr/lib/pkcs11/**. The new location must be updated in applications using the Gemalto PKCS#11 module, such as Mozilla Firefox, Thunderbird or Adobe Reader.

# What's Gone?

For information about the old versions of applications that are no longer officially supported by the IDGo 800 PKCS#11 Library and Tokend for Mac, please refer to “Supported Operating Systems and Applications” on page 2.

Versions of applications which are updated often and are automatically replaced by the new versions, such as Mozilla Firefox are not listed in this note as "removed". For those applications "Table 1" on page 2 just lists the new versions that are supported.

# What's In?

This section provides a full list of hardware, middleware, operating systems, peripherals and software that are supported by Gemalto for use with the IDGo 800 PKCS#11 Library and Tokend for Mac V1.2.8.

## Supported Operating Systems and Applications

The following table lists the versions that are supported and indicates if a version has been added or removed. Other applications may also work successfully, but have not been validated. For information about the compatibility of IDGo 800 PKCS#11 Library and Tokend for Mac V1.2.8 with applications not in this list, please contact your Gemalto technical consultant.

***Table 1 - Supported OS and Applications***

| **Mac OS Version** | **Supported (Added/ Removed)** |
|---|---|
| 10.10 Yosemite 64-bits | |
| 10.11 El Capitan | |
| MacOS Sierra 10.12 | |
| **Browsers** | |
| Safari 8 (Yosemite) | |
| Safari 9 (El Capitan) | |
| Safari 10 (Sierra) | |
| Mozilla Firefox 45 ESR | |
| Mozilla Firefox 52 | |
| Mozilla Firefox 52.01 | |
| Google Chrome 57 | |

*Table 1 - Supported OS and Applications (continued)*

| Mac OS Version | Supported (Added/ Removed) |
|---|---|
| **E-mail Applications** | |
| Mozilla Thunderbird 45.8 | |
| Mozilla Thunderbird 45 ESR | |
| Microsoft Outlook 2011 | |
| Mail 8 (Mac's native mail application) (with Yosemite) | |
| Mail 9 (Mac's native mail application) (with El Capitan) | |
| Mail 10 (with Sierra) | |
| **Other Applications** | |
| Adobe Acrobat Reader 11 – for document signature | |
| Adobe Acrobat Reader 2015– for document signature | |
| Microsoft Office for Mac 2011 | |

# Readers

This section provides a list of the readers supported by IDGo 800 for Mac. The drivers for the Contact and Secure PIN Pad readers can be downloaded from http://support.gemalto.com/ in the "Download Reader Drivers" section. Click "PC-Link Readers".

## Contact

- IDBridge CT 30 (ex PC Twin)
- IDBridge CT 40 (ex PC USB-SL)
- SafeNet CT1100

## Dual (Contact and Contactless)

- IDBridge CL 3000 (ex Prox-DU)
- Advanced Card System ACR 128

## Secure PIN Pad Readers

- IDBridge CT700 (ex PC PIN Pad) (Refer to Ref #66411 on page page 5 below)
- IDBridge CT710

# Smart Cards

- IDPrime MD 3811
- IDPrime MD 3810
- IDPrime MD 830
- IDPrime MD 3840
- IDPrime MD 840
- IDPrime .NET

### ATRs

This section lists the ATRs for the supported smart cards. Those figures indicated in bold and red can differ from one card to another in the same family (other IDPrime MD cards may be added for later versions). All values are in hexadecimal.

**IDPrime MD 3840, 3810, 840 and 830 Cards**

[IDPrime MD T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00

[IDPrime MD T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

[IDPrime MD 3810 T=CI] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

[IDPrime MD 3840 T=CI] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

[IDPrime MD 3811 T=CI] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

IDPrime .NET Cards

[Axalto Cryptoflex .NET] 3B **00 00** 41 73 74 72 69 64

**Optelio / Desineo Cards (Only for PKCS#11)**

[Optelio D72 FXR1 (MD) T=0] 3B 6E 00 00 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00

[Optelio D72 FXR1 (MD) T=1] 3B EE 00 00 81 31 80 43 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00

# 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 this product version.

## Known Issues

- It is not possible to change the PIN of .NET cards using the a Pin PAD reader and IDGo 800 P11. If you attempt to change the PIN of a .NET card using a Pin PAD reader, a warning message appears in the IDGo 800 Pin Management application and the process fails. IDGOD-38.
- When enrolling a certificate on Firefox, the GUI prompt for entering a new PIN is not displayed automatically. Workaround - Activate the application via the task bar to see the PIN prompt. Ref #67935.
- When entering an incorrect PIN via a PIN pad, the error message does not display the number of remaining attempts. Ref #155734
- After connecting the CT 30 reader, and logging into the card on Firefox and Keychain, to perform a PC/SC transaction, the card was visible on Firefox, but not on Keychain.
  This is a Mac problem, which occurs only on the Yosemite OS. One PC/SC transaction can block another PC/SC transaction, so users should avoid using 2 applications at the same time. Even if using one application only at a time, users should take care to avoid card movement.
  Ref #55993.

## Known Limitations

The following limitations were known at the time of writing this release note. Some of these are problems in the applications used with IDGo 800 rather than IDGo 800 itself.

- After disconnecting the reader, user certificates continue to be displayed and Firefox requests a PIN. IDGOD-130
- Certificates associated with Digital Signature PIN are not displayed in Keychain access. In Keychain access, only certificates associated with the user PIN are displayed. IDGOD-131
- If an incorrect or invalid Card PIN is entered (e.g. Safari, Mac Mail and Microsoft Office), the Tokend fails to work. Workaround - remove the card and then reinsert it. For more information on the Tokend being deprecated, see the note on page 1. Ref #68060.
- If the PIN is not initialized on the card, the PIN cannot be set in Firefox or Thunderbird. Workaround - Use the change PIN Tool to set the PIN. Ref #67987.
- The CT700 pin pad reader is not supported as connecting it blocks further actions with IDGo 800. This happens only on El Capitan and is due to a problem with the Apple CCID drivers. Gemalto has reported this bug to Apple under the reference #23515984: "Connecting a CT700 Gemalto smart card reader renders PC/SC useless”. #66411
- Auto-registration of the IDGo 800 PKCS#11 library and TokenD is not supported as the support by Mozilla is not consistent from one version of Firefox to another.
- Due to limitations of Mac OS X the IDBridge CL 3000 works only in the contactless interface.
- Firefox behaves strangely when the PIN is blocked, for example it may continue to prompt for a PIN instead of displaying a message to say that the PIN is blocked. In the event of strange behavior, check to see whether the PIN is in fact blocked. Refs #148272-4.
- When using the Mozilla applications Firefox and Thunderbird, the application prompts the user for all PINs that are linked to certificates, instead of just the one linked to the cryptographic operation.
- It is not possible to sign an e-mail in Mozilla Thunderbird using an elliptic curve certificate.
- It is not possible to sign Adobe Reader 10 documents using an elliptic curve certificate. it is possible with Adobe Reader 11 documents. Ref #148368
- The Tokend security module does not support secure PIN Pad readers, except in transparent mode.
- The Tokend security module is unable to read the contents of the smart card if the card contains any elliptic curve certificates.
- The Tokend security module can be used only to perform “read-only” operations, i.e. it cannot update the card.

# What's History?

This section describes the corrected problems, enhancements made in previous versions and the version numbers of the components.

## Improvements in IDGo 800 V1.2.8 since IDGo 800 1.2.5

Enhancements were made to PKCS#11 to support custom specific profiles with PUK instead of the Admin Key.

### Corrected Problems

- When enrolling certificates or performing digital signature operations with Firefox, the PIN dialog box was displayed incorrectly. IDGOD-21
- After reinserting the smart card in Thunderbird 45.1 caused an issue with the propagation of certificates. When selecting the user's certificate in Thunderbird settings, the signed or encrypted email could be sent, but reinserting the smart card in the reader failed to send a digitally signed email. IDGOD-143/185/186

## Improvements in IDGo 800 V1.2.5 since IDGo 800 1.2.4

### Corrected Problems

- When using Safari it was not possible to use a card with a signature key configured to request the PIN before each use of the key. IDGOD-37
- There was a login problem with Firefox Device Manager. This issue was linked to Firefox, not IDGo 800. If the Firefox Device Manager was opened, and a card was inserted into a reader, the user could log into the card with no problem. However, if the card was removed and reinserted into a different reader, it was no longer possible to login to the card.
- After enrolling a new certificate on Firefox with a PIN that was different to the user PIN, the certificate manager was not refreshed automatically. This was a Firefox limitation. Ref #68037.
- When two applications tried to access the smart card, one application was sometimes blocked due to a Mac PC/SC layer limitation. Ref #65170.
- When a card was connected to a CT30 reader (when two readers were in use CT30 and CT710), and the card was logged onto via the Firefox Device Manager, the login process failed when attempting to connect to the second reader. Ref #56778

## Improvements in IDGo 800 V1.2.4 since IDGo 800 1.2.3

### Operating Systems

The major change in this release was that Mac OS 10.11 El Capitan was supported.

## Improvements in IDGo 800 V1.2.3 since IDGo 800 1.2

### Operating Systems

The major change in this release was that Mac OS 10.10 Yosemite was supported.

### Corrected Problems

- When unblocking a PIN with a PUK using a pin pad reader, the PUK had to be entered twice instead of once. Ref#56419

### Features

- PKCS#11 auto registration in Firefox - This feature was removed as the support by Mozilla is not consistent from one version of Firefox to another.
- When you install the IDGo 800 PKCS#11 Library and Tokend for Mac OS X V1.2, it can be automatically registered in Firefox, avoiding the need to do this manually. To do this, all you need to do is make sure that Firefox is closed when installing IDGo 800. The support for this feature has since been removed.

## Improvements in IDGo 800 V1.2 since IDGo 800 1.1

### Operating Systems

Added support:

- Mac OS X 10.9 (Mavericks)

### Smart Cards

Added support for:

- IDPrime MD 3840
- IDPrime MD 840

### Readers

Added support for:

- IDBridge CL 3000 (ex Prox-DU):

### New Features

Automatic registration of IDGo 800 PKCS#11 Library and TokenD in Firefox.

### Improved Features

- Secure PIN Pad readers now support Change PIN and Unblock PIN operations.

# What Documentation is There?

| Document | Description |
|---|---|
| IDGo 800 PKCS#11 Library & Tokend for Mac User Guide<br>Document Reference: D1310775B | Provides overview of Library and describes its installation and how to perform end-user tasks. |
| IDGo 800 Middleware Integration Guide<br>Document Reference: D1285415I | Provides information about the PKCS#11 and Minidriver functions supported and their compliance with the PKCS#11 and Microsoft Minidriver specifications.<br>This document covers Windows, Mac and Linux. |
| IDGo 800 Release Notes (this document)<br>Document Reference: D1426864A | Describes the new features and cards/ readers/applications supported, as well as known limitations. |
| EULA | Describes the End User License Agreement - the terms and condition of use for IDGo 800. |