Doc Ref: D1369387A

Date: 21July 2015

This document presents information about the IDGo 800 PKCS#11 Library and Tokend for Mac OS X V1.2.3.02 and says what has changed since V1.2.

Important Note:

Even though Apple has now officially deprecated the Tokend in 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?

What's Supported?

This release supports more recent versions of some applications. For information about the new versions of applications that are now officially supported by the IDGo 800 PKCS#11 Library and Tokend for Mac V1.2.3.02, please refer to "Supported Operating Systems and Applications" on page 2.

Operating Systems

The major change in this release is that Mac OS 10.10 Yosemite is now 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

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 V1.2.3.02, 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.

Features

■ PKCS#11 auto registration in Firefox - This feature is no longer supported as the support by Mozilla is not consistent from one version of Firefox to another.

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 V1.2.3.02.

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 with applications not in this list, please contact your Gemalto technical consultant.

Table 1 - Supported OS and Applications

Mac OS Version	Supported (Added/ Removed)
10.8 Mountain Lion 64-bits	Removed
10.9 Mavericks 64-bits	Added
10.10 Yosemite 64-bits	Added
Browsers	
Safari 6 (with Mountain Lion)	Removed
Safari 7 (with Mavericks)	Added
Safari 8 (with Yosemite)	Added
Mozilla Firefox 38 ESR	Added
E-mail Applications	
Mozilla Thunderbird 38 ESR	
Microsoft Outlook 2011	
Mail 6.5 (Mac's native mail application) (with Mountain Lion)	Removed
Mail 7 (Mac's native mail application) (with Mavericks)	
Mail 8 (Mac's native mail application) (with Yosemite)	Added

Table 1 - Supported OS and Applications (continued)

Mac OS Version	Supported (Added/ Removed)
Other Applications	
Adobe Acrobat Reader 11 – 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)

Dual (Contact and Contactless)

- IDBridge CL 3000 (ex Prox-DU)

Secure PIN Pad Readers

- IDBridge CT700 (ex PC Pinpad)
- IDBridge CT710

Smart Cards

- 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=Cl (Prox DU)] 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

- 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.

- 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.

- When a card is connected to a CT30 reader (when there are two readers in use CT30 and CT710), and the card is logged onto via the Firefox Device Manager, the login process fails when attempting to connect to the second reader. Ref #56778

What's History?

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

- 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.

Note: This 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 Document Reference: D1310775A	Provides overview of Library and describes its installation and how to perform end-user tasks.
IDGo 800 Middleware Integration Guide Document Reference: D1252186C	Provides information about the PKCS#11 and Minidriver functions supported and their compliance with the PKCS#11 and Microsoft Minidriver specifications. This document covers Windows, Mac and Linux.
IDGo 800 Release Notes (this document) Document Reference: D1369387A	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.