SafeNet Authentication Client

MAC RELEASE NOTES

Version: 10.1 – Mac (GA)
Build 44
Issue Date: November 2017
Document Number: 007-013724-002 Revision A

Contents

Product Description

SafeNet Authentication Client is public key infrastructure (PKI) middleware that provides a secure method for exchanging information based on public key cryptography, enabling trusted third-party verification of user identities. It utilizes a system of digital certificates, certificate authorities, and other registration authorities that verify and authenticate the validity of each party involved in an Internet transaction.

Release Description

SafeNet Authentication Client 10.1 Mac introduces support for PIN Pad reads including the See What You Sign (SWYS) Pin Pad reader with IDPrime MD cards as well as support for Mac OSx new Crypto Token Kit (CTK).

IDPrime MD cards are PKI smart cards. Administrators and users can use and manage IDPrime MD smart cards seamlessly via the standard PKCS#11 interface and without the need for any additional middleware. They offer secure IT Security and ID access and are compatible with the NFC standard.

New Features and Enhancements

SafeNet Authentication Client 10.1 Mac offers the following new features:

- **Support for PIN Pad readers including the See What You Sign (SWYS) Pin Pad reader with IDPrime MD cards:**
  - SWYS acts as a regular PIN Pad reader and in addition provides the ability to sign documents or transactions using the See What You Sign (SWYS) feature.
  - The functionality of SWYS is available via SAC SDK PKCS#11 Extended API.
  - SAC supports both PKI (certificate) and OCRA OTP mechanisms with the SWYS feature. Ensure that your reader supports the required (PKI / OCRA OTP) configuration.
- **Support for Mac new Crypto Token Kit (CTK)** - Enables accessing Smart Cards and manages user interactions, the CTK module provides programmatic access to smart cards. (for more information see the SafeNet Authentication Client Mac 10.1 Administrator Guide).
- **Support for Common Criteria with CTK** –Common Criteria is supported with the Mac new Crypto Token Kit (CTK) in addition to the PKCS#11 support introduced in SAC 10.0 Mac.
- **Bug fixes** – this release includes bug fixes from previous SAC Mac versions.

Advisory Notes

- The new Crypto Token Kit (CTK) and Tokend are independent modules that may run in parallel on the same machine.

  NOTE: Ensure that all used applications are supported with the CTK module.

  To disable the Tokend module, see Chapter 3 - Tokend and Crypto Token Kit Modules in the SafeNet Authentication Client Mac 10.1 Administrator Guide.
- EZIO Shield PRO reader does not support Secure Messaging (SM) protected operations such as import key pair, generate key pair and change administrator key.

- Working with SafeNet Authentication Client together with Gemalto Bluetooth Device Manager may be slower than using a USB connection.
- Working with both Crypto kit and Tokend modules side-by-side results in one certificate displayed twice.

Licensing

The use of this product is subject to the terms and conditions as stated in the End User License Agreement. A valid license must be obtained from the SafeNet License Center: https://lc.cis-app.com/.

Default Password

SafeNet eToken devices are supplied with the following default token password: 1234567890**.**

IDPrime cards are supplied with the following default token password: “0000” (4 digits). The administrator password must be entered using 48 hexadecimal zeros (24 binary zeros).

For IDPrime MD 840/3840/eToken 5110 CC devices:

- The default Digital Signature PIN is “000000” (6 digits)
- The default Digital Signature PUK is “000000” (6 digits)

Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/smart card according to the following:

- User PIN should include at least 8 characters of different types.
- Admin PIN should include at least16 characters of different types.
- Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.

NOTE: Character types include upper case, lower case, numbers, and special characters.

Compatibility Information

Browsers

SafeNet Authentication Client 10.1 Mac supports the following browsers:

- Safari 11.01
- Firefox (up to and including version 56)
- Chrome version 62, for authentication only (does not support certificate enrollment)

Operating Systems

SafeNet Authentication Client 10.1 Mac supports the following operating systems:

- OSX 10.12.6 Sierra
- OSX 10.13.1 High Sierra

Tokens

SafeNet Authentication Client 10.1 Mac supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 FIPS HID
- SafeNet eToken 5110 HID

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810

- Gemalto IDPrime MD 3811
- Gemalto IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)

> **NOTE:** For more information on IDPrime MD Smart Cards, see the IDPrime MD Configuration Guide.

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7300
- SafeNet eToken 7300-HID

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K

External Smart Card Readers

SafeNet Authentication Client 10.1 Mac supports the following smart card readers:

- Gemalto IDBridge CT1100
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40

> **NOTE:** SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048.

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

Secure PIN Pad Readers

SafeNet Authentication Client 10.1 Mac supports the following PIN pad readers:

Supported Reader Name	Firmware Version	IDPrime MD 830-FIPS IDPrime MD 830 B (L2) IDPrime MD 840 IDPrime MD 840 B	IDPrime MD 830 B - FIPS L3
Ezio Shield Pro	GTO K6.14.00	SM Protected operations are not supported*,**	Not supported
Ezio Shield Pro	UKP K6.14.05	SM Protected operations are not	Not supported
Ezio Bluetooth Reader	GTO O7.04.05	Fully Supported**	Not supported
Ezio Bluetooth Reader	PKI P1.01.10	Fully Supported**	Not supported
Ezio Bluetooth Reader	PKI SWYS	Fully Supported**	Not supported
IDBridge CT710 Rev D	CT7xBarclays JA S1141693 18L13 05	Fully Supported**	Not supported
CT700	SWP113162F	Fully Supported**	Not supported

NOTE:

EZIO PKI cards (applet version 4.3.6) that have the 'Enforce PIN Pad firewall' feature enabled and are compatible with PIN Pad readers must have the FW version in the table above (or higher). Transparent readers (For the full list of transparent readers: See "External Smart Card Readers" on page 5).

PIN Pad readers have different firewalls and therefore have different functional behavior.

It is recommended that the reader specification document is reviewed before using the PIN Pad reader.

Localizations

SafeNet Authentication Client 10.1 Mac supports only English.

Compatibility with Third-Party Applications

Most of the third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.1 Mac (GA).

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.11
VPN	Checkpoint	E80.61
Digital Signatures	Adobe	Reader XI and DC
	Microsoft	Outlook 2016
	Mozilla	Thunderbird 45
Smart Card Logon	Centrify	5.1.3.482

Installation

SafeNet Authentication Client must be installed on each computer on which IDPrime MD cards, as well as SafeNet Tokens or Smart Cards are to be used. Local administrator rights are required to install or uninstall SafeNet Authentication Client.

PCSC-Lite

SafeNet Authentication Client 10.1 Mac uses the default PCSC-Lite that is installed with Mac OS X. SafeNet Authentication Client 10.1 installs a plug-in and driver for PCSC-Lite, during the normal installation process.

PCSC-Lite is managed by the Mac OS X Security Manager. When a device is inserted, the service runs automatically.

Resolved Issues

Issue	Synopsis
ASAC-5578	The ‘Delete the token content’ message did not have a ‘Cancel’ option alongside the ‘OK’ button.
ASAC-5362	After authentication was performed, the token password window couldn’t be closed.

Known Issues

Issue	Synopsis
ASAC-5836	**Summary:** When using Safari (TLS) the PIN is requested via the keyboard instead of being entered via the PIN Pad reader. The balloon (notification window) appears for half a second and then disappears. **Workaround:** Enter a blank PIN in the 'Enter PIN' window and that will trigger the balloon notification window.
ASAC-5774	**Summary:** When working in CTK mode, the Mac built-in VPN application does not recognize the certificates on the token. **Workaround:** Use Tokend mode to work with the built-in VPN.
ASAC-4974	**Summary:** When you are logged in as a user and changes are made to the Password Quality settings, the enter Administrator password window is displayed, but the changed settings are not saved. **Workaround:** The user must log out before making Password Quality modifications.
ASAC-4394	**Summary:** When 2 iKey devices are connected simultaneously, the machine cannot detect an iKey device until a reboot is done. If there are 2 iKeys connected only one is recognized in SAC Tools. **Workaround:** Define the following in eToken.conf: [GENERAL] PcscSlots=1
ASAC-4270	**Summary:** After upgrading SAC Mac, the previous SAC version is displayed in the SAC monitor About window. **Workaround:** Perform a restart.
ASAC-2849	**Summary:** Enrolling a certificate on Mac via CheckPoint VPN E80.61 failed. **Workaround:** Use an enrolled certificate when conncecting to VPN via CheckPoint.
ASAC-2299	**Summary:** eToken Virtual devices that are locked to flash, and were enrolled on SafeNet Authenticaion Manager using a USB 3 port, cannot function on a USB 2 port, and visa versa. **Workaround:** If the eToken Virtual was enrolled on a USB 3 port, then use the token on a USB 3 port only. If the eToken Virtual was enrolled on a USB 2 port, then use the token on a USB 2 port only.
ASAC-2298	**Summary:** Connection problems occur when eToken Virtual devices are locked to flash and enrolled on a VMware environment. **Workaround:** When using an eToken Virtual device that is locked to flash, make sure the device is enrolled on a regular environment and not VMware.
ASAC-2296	**Summary:** eToken Virtual (on a Mac) is not recognized in the Keychain application, causing Safari , the default mail application and outlook not to work. See apple bug report: 19613234. **Workaround:** None.

Issue	Synopsis
ASAC-2235	**Summary**: After installing SAC, the PKCS11 module was not inserted automatically into Firefox's browser. **Workaround:** Insert the module manually.
ASAC-2233	**Summary:** After opening the KeyChain application and selecting the 'Lock all Keychains' parameter, it is not possible to log on to the token in Keychain, and SSL in Safari cannot be established. **Workaround:** Disconnect the token, and then re-connect it.
ASAC-2227	**Summary:** When two tokens are connected, one of the token's settings are not accessible in SAC Tools. **Workaround:** Work with one connected token at a time.
ASAC-2223	**Summary:** Occasionally, when an eToken is disconnected, and then a different token is connected, the first token is still shown in SAC Tools. This is due to a Mac OS X issue. **Workaround:** Restart the machine.
ASAC-2191	**Summary**: When working with a 5100 token that is recognized via the CCID driver, the token might not be recognized or the system may not respond when the machine returns from sleep mode. **Workaround:** Re-insert the token.
ASAC-2079	**Summary:** Some Keychain related functions do not work on Yosemite when using iKey 2032 and 4000. **Workaround:** Disconnect and then connect the token.
ASAC-1470	**Summary:** After updating the FW on an eToken 7300, the FW version might not be updated under Token information in SAC Tools. **Workaround:**
ASAC-1053	**Summary:** When re-decrypting an email using Microsoft Outlook on Mac, the decrypt process fails. **Workaround:** Perform the following: 1. Disconnect the token, and close Outlook. Connect the token, and reopen Outlook.

Known Issues – Deprecated Devices

Issue	Synopsis
ASAC-1315	**Summary:** When working with SafeNet smart cards and iKey 4000 using SAC Tools, the amount of unblocking codes retries remaining cannot be changed , unless the token or smart card are locked. (i.e. there is no way of determining how many unblocking code retries remain). **Workaround:** None. This is by design.

Product Documentation

The following product documentation is associated with this release:

- 007-013726-002_SafeNet Authentication Client 10.1_Mac_ Administrator Guide_Revision A
- 007-013725-002_ SafeNet Authentication Client 10.1_Mac_User Guide_Revision A

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Support Contacts

If you encounter a problem while installing, registering, or operating this product, please make sure that you have read the documentation. If you cannot resolve the issue, contact your supplier or Gemalto Customer Support. Gemalto Customer Support operates 24 hours a day, 7 days a week. Your level of access to this service is governed by the support plan arrangements made between Gemalto and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com