SafeNet Authentication Client

MAC RELEASE NOTES

Version:	10.2 – Mac (GA)
Build	82
Issue Date:	December 2018
Document Number:	007-013724-002 -Revision B

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 10.2 Mac introduces support for Mac OSx Mojave, support for additional Gemalto devices and bug fixes from previous SAC Mac versions.

New Features and Enhancements

SafeNet Authentication Client 10.2 Mac offers the following new features:

- **Support for Classic Client V3 cards** – as part of the eBanking migration plan to use IDPrime MD cards, SafeNet Authentication Client 10.2 Mac introduces the support for IDClassic 340 (V3) cards in read only mode. For more details on the eBanking installation profile, see the SafeNet Authentication Client Administrator Guide.
- **Support for SafeNet IDPrime 940/3940** – the SafeNet IDPrime 940 smart card can be protected by an Activation PIN. If it is protected, it must be activated before first use.
- **Support for SafeNet eToken 5300** – this is a compact, tamper-evident USB device with presence detection, which creates a third factor of authentication.
- **Security enhancements** – as part of our initiative to continuously improve SafeNet Authentication Client security levels, enhancements and updates were performed on SAC Mac 10.2
- **New Profile supported on specific Common Criteria devices –** User PIN can now be unlocked using the PUK.
- **ITI Certification Mode –** requires the Administrator PIN to be changed on first logon and the initialization process is now protected by an Administrator PIN.
- **Bug Fixes –** this release includes bug fixes from previous SAC Mac versions.

Advisory Notes

- **SafeNet eToken 5300 driver on Mac -** SafeNet eToken 5300 is not supported by the CCID driver provided by Apple. The **ccid-installer-ccid-1.4.29.pkg** resides in the .dmg file called **ccid-installer.dmg**. Mount the .dmg and double-click the **ccid-installer-ccid-1.4.29.pkg** file to install the driver.

  

  NOTE: The CCID driver that includes the PID\VID of the TS devices must be installed in order for SafeNet eToken 5300 to work on your Mac system.

- 32-Bit applications are no longer supported on Mac.
- HID device support using PKCS#11 is disabled by default. If required, you can enable it using the HID Slots property (for more information, refer to the *General Settings* section in the *SAC 10.2 Mac Administrator Guide*).

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 940/3940/840/3840/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 10.2 Mac (Standard Installation) supports the following browsers:

- Firefox (up to and including version 63)
- Safari 12
- Chrome version 70, for authentication only (does not support certificate enrollment)

SafeNet Authentication Client 10.2 Mac (eBanking Installation) supports the following browser:

- Firefox (up to and including version 63)

Operating Systems

SafeNet Authentication Client 10.2 Mac supports the following operating systems:

- OSX 10.13.1 High Sierra
- OSX 10.14 Mojave

Tokens

SafeNet Authentication Client 10.2 Mac supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5300
- 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

- SafeNet IDPrime 940
- SafeNet IDPrime 3940

NOTE: If the Admin PIN is locked on a SafeNet IDPrime 940 or 3940 smart card, the card is left in an unusable state.

- 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-Life 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
- 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 10.2 Mac supports the following smart card readers:

- SafeNet Reader 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 10.2 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 SafeNet IDPrime 940/3940	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 10.2 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 10.2 Mac (GA).

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.18
VPN	Checkpoint	E80.61
Digital Signatures	Adobe	Reader XI and DC
	Microsoft	Outlook 2016
	Mozilla	Thunderbird 45

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 10.2 Mac uses the default PCSC-Lite that is installed with Mac OS X. SafeNet Authentication Client 10.2 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-5854	TLS 1.2 authentication to a VMView environment did not work in SAC 10.1 Mac. Customer ID: CS0450778

Known Issues

Issue	Synopsis
ASAC-8086	**Summary:** TLS and Web Signer operations could not be performed when logging in with a V3 password length that's less than 8 on a CT710 or SWAT PIN Pad reader. **Workaround:** Define the PQMinLen = 6 in SAC PQ default settings.
ASAC-8085	**Summary:** Using a PIN Pad reader and V3 card to send a signed email via Thunderbird on Mac caused the card to be logged out. **Workaround:** Reinsert the card and login when prompted.
ASAC-8081	**Summary:** TLS via Chrome and Safari (tokenD) is not supported with a CC Sign Only certificate. The TLS process fails regardless of whether the user logs in with Role 1 or Role 3. **Workaround:** To work with a CC Sign Only certificate, disable the tokenD plug-in.
ASAC-8024	**Summary:** The PIN Validity period cannot be set on IDPrime 830 Rev A cards. It is not supported by SAC if not configured already in production.
ASAC-8006	**Summary:** When importing a PFX into a token when the Password must be changed is enabled, the operation failed. **Workaround:** Change the token password and then perform the import separately.
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.

Issue	Synopsis
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.
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:**

Issue	Synopsis
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.

Known Limitations

Issue	Synopsis
ASAC-7927	Smart Card login with CryptoTokenKit (CTK) does not support Pin Pad readers. Apple Bug ID:#34655464
ASAC-7918	Smart Card login using the IDClassic 340 (V3) card is not supported.
ASAC-7895	Smart Card Pairing fails when using the Gemalto IDPrime 840B card with a Sign Only Certificate. An exchange certificate + the private key must exist on the card.
ASAC-7795	Smart Card pairing is not supported for V3 cards on Mac.
ASAC-5447	When working with multiple PIN's on a card (using Safari and Chrome), the login dialog displays a general PIN prompt instead of specifying the type of PIN to be entered. This is a Crypto Token Kit (CTK) framework limitation present on High Sierra and Mojave (Apple Bug ID 34620675).

Product Documentation

The following product documentation is associated with this release: confidence

- 007-013726-002_SafeNet Authentication Client 10.2_Mac_ Administrator Guide_Revision B
- 007-013725-002_ SafeNet Authentication Client 10.2_Mac_User Guide_Revision B

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