THALES

The SafeNet Authentication Client

RELEASE NOTES

Version: 10.2 Mac (Post GA - R3)

Build: 109

Issue Date: June 2020

Document PN: 007-013724-002 - Rev E

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 (Post GA – R3) introduces support for MacOS 10.15 Catalina and includes bug fixes from previous SAC Mac versions.

Advisory Notes

- **TokenD is deprecated -** Due to Apple's decision (starting from MacOS 10.15.1 and above) to no longer support TokenD, customers should either start using Crypto Token Kit (CTK) instead of TokenD, or continue using earlier versions of MacOS (10.15.0 or below), which still supports TokenD.
  SAC Mac 10.2 (Post GA – R3) supports both TokenD and CTK, ensure that either one of the frameworks are configured.
- **Notarization -** SAC 10.2 (Post GA – R3) was notarized. For more details, see https://developer.apple.com/documentation/xcode/notarizing_macos_software_before_distribution
  As of January 2020 MacOS Catalina notarized software is mandatory.
  SAC 10.2 was notarized and verified using the following command line: `xcrun stapler validate myapp.app`

  For more information, see https://help.apple.com/xcode/mac/current/#/dev88332a81e?sub=dev68b6e38a3
- SafeNet Authentication Client Customization Tool is supported only on MacOS Mojave.
- **Working with CTK and TokenD:**

	Tokens and certificates under keychain GUI:	**Sign only certificate usage:**
CTK Enabled	Not Displayed	Applicable
TokenD Enabled	Displayed	Not Applicable

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, IDPrime 940/3940, 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 guidelines:

- 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 (Post GA – R3) (Standard Installation) supports the following browsers:

- Firefox (version 69 and earlier)
- Safari 12.1.2
- Chrome version 77, for authentication only (does not support certificate enrollment)

Operating Systems

SafeNet Authentication Client 10.2 Mac (Post GA – R3) supports the following operating systems:

- MacOS 10.15.5 Catalina
- MacOS 10.14.6 Mojave

Tokens

SafeNet Authentication Client 10.2 Mac (Post GA – R3) supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5300
- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS

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 Smart Cards, see the product Configuration Guide.

External Smart Card Readers

SafeNet Authentication Client 10.2 Mac (Post GA – R3) supports the following smart card readers:

- 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.

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 Smart Card 72K
- SafeNet Virtual Token
- SafeNet Rescue Token

PIN Pad Readers

SafeNet Authentication Client 10.2 Mac (Post GA – R3) 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 supported	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

* Secure Messaging (SM) protected operations includes import key pair, generate key pair and change administrator key.

** Cards configured with PIN/s protected by SM will not be supported by any PIN Pad reader.

> **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 (Post GA – R3) supports only English.

Compatibility with Third-Party and Native Applications

Most of the third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.2 Mac (Post GA – R3).

Solution Type	Vendor	Product Version
VPN	Pulse Secure	9.1 R2
	Cisco AnyConnect	4.8.00175
	Check Point	E80.61***
Access Management	Centrify	5.5.1**
Virtual Desktop Infrastructure (VDI)	*Citrix	XenApp/XenDesktop 7.18
	VMware Horizon Client	5.1.0*
Digital Signatures	Adobe	Reader XI and DC
	Apple	Mail app
	Mozilla	Thunderbird 60.3.1
	SETCCE proXSign	2.1.4.31

* Citrix receiver app 12.9.1 for Mac is not supported on Catalina. Instead, there is a new app called Citrix Software app v19.12.0.23 that is supported on MacOS Catalina

** Validated on MacOS Mojave

*** Validated with previous SAC version

Installation

SafeNet Authentication Client must be installed on each computer on which IDPrime 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 (Post GA – R3) uses the default PCSC-Lite that is installed with Mac OS X.) It also 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 and Known Issues

Issue Severity and Classification

The following table serves as a key to the severity and classification of the issues listed in the **Resolved Issues** table and the **Known Issues** table, which can be found in the sections that follow.

Severity	Classification	Definition
C	Critical	No reasonable workaround exists
H	High	Reasonable workaround exists
M	Medium	Medium-level priority problems
L	Low	Low-level priority problems

Resolved Issues

Issue	Severity	Synopsis
ASAC-11382	H	Cisco AnyConnect did not work as MAC OS was not able to read certificates from the token. (Customer ID: CS0971683, CS0977459)
ASAC-10889	M	When generating RSA key pair with a private key that required a Digital Signature PIN for authentication, the `CKA_ALWAYS_AUTHENTICATE` attribute always returned a `CK_FALSE`. (Customer ID: CS0936052)
ASAC-10829	H	The C_Sign function had unpredictable behavior issues on different platforms. (Customer ID: CS0938212, CS0948288)
ASAC-10194	H	On Catalina 10.15.1, CryptoTokenKit or PKCS#11 lib failed to load due to Apple's OpenSSL update. (Customer ID:CS0941837)
ASAC-10032	VH	When using SAC with MacOS Catalina, the smart card certificate was not visible in the browser and command security list and also did not display Gemalto's installed CryptoTokenKit plugin. (Customer IDs: CS0934793, CS0934054, CS0939562 ,CS0936737, CS0938180, CS0939783, CS0907041, CS0944281, CS0947702)
ASAC-9809	H	The libeTpkcs11.dylib library crashed when using the C_GetAttributeValue() API, or when calling the C_GetAttributeValue() API (Customer ID:CS0921296)
ASAC-9738	M	The C_GetAttributeValue() function failed when using ECC Keys. (Customer ID: CS0912609)
ASAC-9678	M	After saving a pdf file on Mac Mojave, the error message: "Error encountered while signing: The credential selected for signing is invalid" appeared after performing a digital signing operation. (Customer ID: CS0915903)

Issue	Severity	Synopsis
ASAC-9365	H	ProXSign components failed when performing XML signing on Mojave. (Customer ID: CS0902421)
ASAC-9363	H	When performing a Smart Card logon, Centrify failed to authenticate user against DC. (Customer ID: CS0905736)
ASAC-8271	H	Smart Card (Certificate) authentication fails with Pulse Desktop Client 9.0R3 after SafeNet Authentication Client is upgraded to 10.2. (Customer ID: CS0859798, CS0895643)
ASAC-8266	M	If more than one certificate was assigned to the same username, only the last certificate could be chosen and viewed in SAC Tools. All other certificates could not be seen. (Customer ID: CS0866930)
ASAC-5854	H	On Mac High Sierra, entering a PIN on VMware Horizon View Client failed with an SSL error. (Customer ID: CS0450778)

Known Issues

Issue	Severity	Synopsis
ASAC-9878	M	**Summary:** Native VPN does not work with a smart card via TokenD. The certificates are seen and can be chosen, but the connection will fail. **Workaround:** Use other supported VPN applications listed in the Compatibility with Third-Party and Native Applications section
ASAC-9843	M	**Summary:** Outlook 2019 stops responding while trying to enter token's PIN on Mac OSX 10.15. **Workaround:** Use native Apple Mail app instead.
ASAC-8086	M	**Summary:** TLS and Web Signer operations could not be performed when logging in with an IDClassic 340 (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-8081	L	**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	M	**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-5836	M	**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.

Issue	Severity	Synopsis
		Workaround: Enter a blank PIN in the 'Enter PIN' window and that will trigger the balloon notification window.
ASAC-5774	M	**Summary:** When working in CTK mode, the Mac built-in VPN application does not recognize the certificates on the token. Apple introduced a fix for this issue in 10.15.4 public beta. Apple Ref : https://feedbackassistant.apple.com/feedback/5738151
ASAC-4974	L	**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-4270	M	**Summary:** After upgrading SAC Mac, the previous SAC version is displayed in the SAC monitor About window. **Workaround:** Perform a restart.
ASAC-2849	M	**Summary:** Enrolling a certificate on Mac via Check Point VPN E80.61 failed. **Workaround:** Use an enrolled certificate when connecting to VPN via Check Point.
ASAC-2235	M	**Summary**: After installing SAC, the PKCS11 module was not inserted automatically into Firefox's browser. **Workaround:** Insert the module manually.
ASAC-2233	M	**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	M	**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	M	**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	M	**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-1053	M	**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. 2. Connect the token, and reopen Outlook.

Known Limitations

Issue	Severity	Synopsis
ASAC-10576	M	It is not possible to create a SAC Customization Tool package using MacOS Catalina 10.15. However, running a Customized package that was created on an earlier version of MacOS will work.
ASAC-7927	M	Smart Card login with CryptoTokenKit (CTK) does not support Pin Pad readers. Apple Bug ID:#34655464
ASAC-5447	M	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:

> 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 Thales Customer Support.

Thales 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 Thales and your organization. Please consult this support plan for further information about your entitlements, including the hours when telephone support is available to you.

Customer Support Portal

The Customer Support Portal, at https://supportportal.thalesgroup.com, is where you can find solutions for most common problems. The Customer Support Portal is a comprehensive, fully searchable database of support resources, including software and firmware downloads, release notes listing known problems and workarounds, a knowledge base, FAQs, product documentation, technical notes, and more. You can also use the portal to create and manage support cases.

> **NOTE** You require an account to access the Customer Support Portal. To create a new account, go to the portal and click on the **REGISTER** link.

Telephone Support

If you have an urgent problem, or cannot access the Customer Support Portal, you can contact Thales Customer Support by telephone at +1 410-931-7520. Additional local telephone support numbers are listed on the support portal.

Email Support

You can also contact technical support by email at technical.support.DIS@thalesgroup.com.