

# SafeNet Authentication Client 10.8 R2 (GA)

## MAC RELEASE NOTES

**Issue Date:** October 2023

**Build:** 10.8.267.0

**Document Part Number:** 007-013724-004 Rev. D

### Contents

<b>Product Description</b>	<b>2</b>
Release Description	2
New Features and Enhancements	2
Advisory Notes	2
Licensing	3
Default Password	3
Password Recommendations	3
Initialization Key Recommendations	4
Compatibility Information	4
Browsers	4
Operating Systems	4
Tokens	4
Device Features Supported by SAC	6
PIN Pad Readers	7
Localizations	8
Compatibility with Third-Party and Native Applications	8
Installation	9
Upgrade	9
<b>Resolved and Known Issues</b>	<b>10</b>
Issue Severity and Classification	10
Resolved Issues	10
Known Issues	11
Known Limitations	14
<b>Product Documentation</b>	<b>17</b>
<b>Support Contacts</b>	<b>18</b>

# Product Description

SafeNet Authentication Client (SAC) 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 10.8 R2 (GA) Mac includes new features and bug fixes from previous SAC versions.

## New Features and Enhancements

This release offers the following:

- > Support for macOS 14 (Sonoma) and macOS 13.3.1 (a) (Ventura).
- > Provides CCID driver package version 1.5.2 and installation instructions to support SafeNet eToken Fusion CC token and SafeNet eToken 5110 FIPS (Java Applet 1.7.7, 1.8.5) To download the driver, visit [https://supportportal.gemalto.com/csm?id=kb\\_article\\_view&sysparm\\_article=KB0027738](https://supportportal.gemalto.com/csm?id=kb_article_view&sysparm_article=KB0027738).
- > Support for new cards and tokens.
- > Support for new contact and contactless card readers.
- > Performance improvements and bug fixes.

## Advisory Notes

Before deploying this release, note the following high-level requirements and limitations:

- > **TokenD 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 10.8 onwards supports Crypto Token Kit (CTK) framework only. When CTK is enabled:
  - Tokens and certificates under keychain GUI: Not Displayed
  - Sign only certificate usage: Applicable
- > **Notarization**- This release is notarized. For more details, refer to [https://developer.apple.com/documentation/xcode/notarizing\\_macos\\_software\\_before\\_distribution](https://developer.apple.com/documentation/xcode/notarizing_macos_software_before_distribution)  
As of January 2020, macOS Catalina notarized software is mandatory. SAC 10.8 R2 (GA) is notarized and verified using the following command line: `xcrun stapler validate myapp.app`.  
For more information, refer to <https://help.apple.com/xcode/mac/current/#/dev88332a81e?sub=dev68b6e38a3>
- > **AKS drivers deprecated**- SAC 10.8 onwards removes the support for AKS drivers.
- > **RSA 1024 key size deprecated**- SAC 10.8 onwards removes the support for RSA 1024 key size signing with SHA-1.

If you need it, use the `Disable-Crypto` setting mentioned in *SafeNet Authentication Client Administrator Guide*

> SafeNet IDPrime 930/3930:

- SafeNet IDPrime 930 has different profiles. A non-managed profile has no Administrator PIN and therefore, cannot be used in Managed environments (CMS).
- After deleting a key from a SafeNet IDPrime 930/3930 device, the available memory size may be reduced.

For more information, refer to *IDPrime 930/3930 Card Configuration Guide*.

> eToken 5110 FIPS:

- Due to an eToken applet limitation, the User PIN Retry counter cannot be set on SafeNet eToken 5110 FIPS or SafeNet eToken 5110, unless they are initialized.

## Licensing

From SAC 10.8 release onwards, no license is required for SAC on Mac.

## 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 zeros in hexadecimal (24 zeros in binary).

For IDPrime MD 940/3940/840/3840/eToken 5110 CC devices:

- > The default Digital Signature PIN is "000000" (6 zeros)
- > The default Digital Signature PUK is "000000" (6 zeros)

## Password Recommendations

We strongly recommend changing all device passwords upon receipt of a token/smart card as follows:

- > User PIN should include at least 8 characters of different types.
- > Admin PIN should include at least 16 characters of different types.
- > Friendly Admin Password should include at least 16 characters of different types.

For more details on the Friendly Admin Password, refer to *SafeNet Authentication Client User Guide*.

- > Digital Signature PUK, when using a friendly name, should include at least 16 characters of different types.
- > For devices running the IDPrime applet, the 3DES random key may be used instead of the administrator password. As per 3DES algorithm for 24 zeros in binary or 48 zeros in hexadecimal values (entered as Admin PIN) every LSB bit is ignored, which means if user enters any random number as the LSB, it will be ignored and more number of Admin PIN are possible.

**NOTE** It is recommended to not use 24 zeros in binary or 48 zeros in hexadecimal values for Admin PIN.

- > Use the password validity period combined with password history options.

**NOTE** Character types include upper case, lower case, numbers, and special characters. For more information, refer to the 'Security Recommendations' chapter in *SafeNet Authentication Client Administrator Guide*.

## Initialization Key Recommendations

Thales strongly recommends changing the Initialization Key using the *SAC Initialization* process.

For more details on Initialization Key settings, refer to *SafeNet Authentication Client User Guide*.

## Compatibility Information

### Browsers

Following browsers are supported:

- > Firefox (version 117.0.1) (TLS 1.3 supported)
- > Safari 17.1 (TLS 1.3 supported)
- > Chrome version 117.0.5938.132, for authentication only (does not support certificate enrollment) (TLS 1.3 supported)

### Operating Systems

Following operating systems are supported:

- > macOS 14 (Sonoma)
- > macOS 13.3.1 (a) (Ventura)
- > macOS 12.6.5 (Monterey)

### Tokens

Following tokens are supported:

#### Certificate-based USB Tokens

- > SafeNet eToken 5300 USB A
- > SafeNet eToken 5300 USB A TS
- > SafeNet eToken 5300-C
- > SafeNet eToken 5300-C TS
- > SafeNet eToken 5110
- > SafeNet eToken 5110 FIPS
- > SafeNet eToken 5110+
- > SafeNet eToken 5110+ FIPS
- > SafeNet eToken 5110 CC
- > SafeNet eToken 5110 CC (940)

- > SafeNet eToken 5110+ CC (940B)
- > SafeNet eToken Fusion CC

### Smart Cards

- > SafeNet IDPrime MD 830
- > SafeNet IDPrime MD 830nc
- > SafeNet IDPrime 930
- > SafeNet IDPrime 930nc
- > SafeNet IDPrime 3930
- > SafeNet IDPrime 3930 FIDO
- > SafeNet IDPrime 940
- > SafeNet IDPrime 940B
- > SafeNet IDPrime 940C
- > SafeNet IDPrime 3940
- > SafeNet IDPrime 3940 FIDO
- > SafeNet IDPrime 940 SIS

**NOTE** If the Admin PIN is locked on a SafeNet IDPrime 940 or 3940 smart card, the card is left in an unusable state. SafeNet IDPrime 3940 and 3930 type B smart cards can be used in contactless mode using the readers in Smart Card Readers supported in Contact and Contactless modes.

**NOTE** Although the majority of contactless cards mentioned in this release notes are compliant with ISO 14443, it is recommended to test these cards on all customer laptop models before placing an order.

For more information on IDPrime MD Smart Cards, refer to *IDPrime MD Configuration Guide*.

### Smart Card Readers supported in Contact and Contactless modes

- > HID OMNIKEY 5422
- > HID OMNIKEY 5022 (Contactless only)
- > Identiv uTrust 4701 F

**NOTE** It is recommended to use Vendor drivers for the above SC Readers.

### Smart Card Readers

Following smart card readers are supported:

- > Gemalto IDBridge CT30
- > Gemalto IDBridge CT40
- > OMNIKEY 3121

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

## Device Features Supported by SAC

Below table specifies the various features that are supported by SafeNet Authentication Client:

Features:	Device:				
	<b>Gemalto IDPrime MD 840/3840/3840B/ 8840/SafeNet eToken 5110 CC</b>	<b>SafeNet IDPrime 940</b>	<b>Gemalto IDPrime MD 830-FIPS/830-ICP/830B/3810/3810 MIFARE 1K/3811/SafeNet eToken 5300</b>	<b>SafeNet IDPrime 930/3930</b>	<b>SafeNet eToken 5110-FIPS</b>
Number of key containers	14 – default <b>Note 1</b>	20 – default <b>Note 1</b>	15	32	Dynamic <b>Note 5</b>
RSA Key sizes	2048-bit - default 3072-bit 4096-bit <b>Note 2 &amp; 7</b>	2048-bit - default 3072-bit 4096-bit - default <b>Note 2</b>	2048-bit <b>Note 3</b>	2048-bit 3072-bit 4096-bit <b>Note 3</b>	2048-bit <b>Note 3</b>
RSA Padding	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP	PKCS#1 v1.5, PSS, OAEP <b>Note 4</b>	RAW, PKCS#1 v1.5, PSS, OAEP <b>Note 3 &amp; 6</b>
ECC Key sizes	256-bit - default 384-bit 521-bit <b>Note 2</b>	256-bit - default 384-bit 521-bit <b>Note 2</b>	256-bit 384-bit 521-bit	256-bit 384-bit 521-bit	256-bit 384-bit

Features:	Device:				
Hash	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit  <b>Note 3</b>	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit  <b>Note 3</b>	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit  <b>Note 3</b>
Activation PIN	N/A	Available	N/A	Available	N/A
Re-init feature	N/A	N/A	N/A	Available	Available
SKI	N/A	N/A	Available	Available	N/A
Non-managed profile	N/A	N/A	N/A	Available	Available

**NOTE**

1. The default number of containers and default container capabilities can be customized during the PERSO process.
2. The supported key sizes depend on the PERSO container customizations.
3. SHA-1 (160-bit) and RSA 1024-bit are not allowed in FIPS L3 cards.
4. PKCS#1 padding does not allow decrypt on IDPrime 930\3930 FIPS L3 cards.
5. Keys can be created as long as free memory is available.
6. Raw RSA is not available on FIPS devices.
- 7: RSA 3072 and 4096-bit only key import available (no OBKG).

## PIN Pad Readers

Following PIN Pad readers are supported:

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

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 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, refer to "[Smart Card Readers](#)" on [page 5](#)).

PIN Pad readers have different firewalls and therefore, different functional behavior. It is recommended that the reader specification document is reviewed before using the PIN Pad reader.

## Localizations

This release supports only English.

## Compatibility with Third-Party and Native Applications

Following third-party applications have been validated and tested with this release:



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	Acrobat Reader 2023.006.20320
	Apple	Mail app 16.0
	Mozilla	Thunderbird 102.15.1
	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 with SAC on Mac 10.2

## 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.

## Upgrade

It is recommended to upgrade the SafeNet Authentication Client to the latest version on each computer that uses a SafeNet eToken, or SafeNet smart card. Local administrator rights are required to upgrade SafeNet Authentication Client.

After upgrading from SAC 10.8 R1 to SAC 10.8 R2 on a Mac, it is recommended that you restart the machine in order to recognize the device.

# Resolved and Known Issues

## Issue Severity and Classification

This section lists the issues that have been resolved and known to exist in this release. The following table defines the severity of the issues listed in this section.

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-15223	H	Smartcard login not working after SAC 10.8.66 upgrade.  (Customer ID: CS1341932, CS1437229)
ASAC-16139	H	SAC on Mac unlocking with PUK code.  (Customer ID: CS1458282)
ASAC-15908	H	Strong web Authentication operations see a delay of 3-10s with SAC 10.8 R1 Linux and SAC 10.8 R1 MAC in comparison to SAC 10.7 Linux and SAC 10.8 MAC respectively  (Customer ID: CS1450847, CS1465807)
ASAC-13477	H	SAC 10.8 on macOS 10.15.7 (Catalina) does not recognize tokens/ smartcards.  (Customer ID: CS1062000, CS1061923, CS1060911)
ASAC-14116	H	PDF signing failed while using SAC 10.8 on macOS 12 (Monterey).  (Customer ID: CS1090410)
ASAC-13776	H	Insufficient memory issue on IDPrime 830 rev A and IDPrime 830 rev B smart cards using SAC 10.8 (R6) GA.  (Customer ID: CS1023930)

Issue	Severity	Synopsis
ASAC-13031	H	Review maximum password length setting in SAC.  (Customer ID: CS0998552)
ASAC-13034	H	In SAC 10.8, TLS 1.3 failing the authentication request due to PSS mechanisms.  (Customer ID: CS1006242, CS1001654)
ASAC-13087	H	Login process with IDCore 340 cards is slower than IDPrime MD 940 cards.  (Customer ID: CS1029120)
ASAC-13617	M	SAC installation package reports wrong version number.  (Customer ID: CS1074642)
ASAC-13104	M	Need SAC minimal drivers for IDPrime MD 830 smart card to work on macOS Big Sur.  (Customer ID: CS1032445)

## Known Issues

Issue	Severity	Synopsis
ASAC-16176	M	<b>Summary:</b> SAC Tools crashes while initializing certain tokens (Intermittent). <b>Workaround:</b> Reinstall the SAC.
ASAC-15929	M	<b>Summary:</b> Kerberos login fails, after at least ONE use of CC certificate for signature <b>Workaround:</b> Disconnect the token/card and reconnect it again.
ASAC-11163	H	<b>Summary:</b> After locking the Administrator Key (due to an incorrect password being entered too many times), the IDPrime 940/3940 smart card switches to a locked state and as a result the device cannot be used (device is unrecognized). <b>Workaround:</b> None – this is a smart card design feature.
ASAC-9843	M	<b>Summary:</b> Outlook 2019 stops responding while trying to enter token's PIN on Mac OSX 10.15. <b>Workaround:</b> Use native Apple Mail app instead.
ASAC-8338	M	<b>Summary:</b> 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. <b>Workaround:</b> Define the PQMinLen = 6 in SAC PQ default settings.

Issue	Severity	Synopsis
ASAC-2849	M	<p><b>Summary:</b> Enrolling a certificate on Mac via Check Point VPN E80.61 failed.</p> <p><b>Workaround:</b> Use an enrolled certificate when connecting to VPN via Check Point.</p>
ASAC-2235	M	<p><b>Summary:</b> After installing SAC, the PKCS11 module was not inserted automatically into Firefox's browser.</p> <p><b>Workaround:</b> Insert the module manually.</p>
ASAC-2227	M	<p><b>Summary:</b> When two tokens are connected, one of the token's settings are not accessible in SAC Tools.</p> <p><b>Workaround:</b> Work with one connected token at a time.</p>
ASAC-2223	M	<p><b>Summary:</b> 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.</p> <p><b>Workaround:</b> Restart the machine.</p>
ASAC-1053	M	<p><b>Summary:</b> When re-decrypting an email using Microsoft Outlook on Mac, the decrypt process fails.</p> <p><b>Workaround:</b> Perform the following:</p> <ol style="list-style-type: none"> <li>1. Disconnect the token, and close Outlook.</li> <li>2. Connect the token, and reopen Outlook.</li> </ol>
ASAC-11099	M	<p><b>Summary:</b> Using the salt length in the PSS parameter that is not equal to the hash length of the appropriate PSS mechanism, causes the C_Verify() command to fail with the CKR_SIGNATURE_INVALID return value. Effected environment: All IDPrime based devices and any of the following mechanisms: CKM_SHA1_RSA_PKCS_PSS, CKM_SHA256_RSA_PKCS_PSS, CKM_SHA384_RSA_PKCS_PSS and CKM_SHA512_RSA_PKCS_PSS.</p> <p><b>Workaround:</b> On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length.</p>
ASAC-9288	M	<p><b>Summary:</b> By default, the retry counter cache causes the following problem in SAC: when switching the card between different machines, the true retry counter is not shown until it is changed on the current machine and the cache is updated.</p> <p><b>Workaround:</b> Add the property RetryCountCached=0 under the [General] section in the file <code>/etc/eToken.conf</code>.</p>
ASAC-8267	M	<p><b>Summary:</b> A Digital Signature PIN operation fails if the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have different PINPad configurations (PIN Type and Extended PIN Flags)</p> <p><b>Workaround:</b> Ensure that the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have the same PINPad configuration.</p>

Issue	Severity	Synopsis
ASAC-7969	M	<p><b>Summary:</b> Using the eToken Pro (no hash on-board functionality) and eToken 5110 FIPS (both hash and sign functionalities on-board) device when there are two or more threads running two PKCS#11 sessions in the same application, the signing operation fails.</p> <p><b>Workaround:</b> Perform either one of the following:</p> <ul style="list-style-type: none"> <li>&gt; Update the application to use the hash off-board mechanism and then perform the RSA operation with the token.</li> <li>&gt; Update the application to synchronize between threads - make the <code>C_SignInit</code> - <code>C_SignUpdate</code> - <code>C_SignFinal</code> a solid block.</li> <li>&gt; If there is no option to update the application, enable the hash offboard property: <i>HashOffboard</i> in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.</li> </ul>
ASAC-7932	M	<p><b>Summary:</b> Changing the PIN on Firefox using the CT710 PIN Pad does not work.</p> <p><b>Workaround:</b> Change the PIN using SAC Tools or SAC tray icon.</p>
ASAC-6214	M	<p><b>Summary:</b> VMView client may not work properly with SAC when using a smart card certificate.</p> <p><b>Workaround:</b> Install SAC before installing the VMView Client.</p>
ASAC-5815	M	<p><b>Summary:</b> When working with a token or a PIN pad reader on a VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM &gt; Removable Devices menu.</p> <p><b>Workaround:</b> Connect the device that is not under the "Shared" devices list in order to work with the eToken/reader device.</p>
ASAC-5343	M	<p><b>Summary:</b> When using a PIN Pad reader with the Smart Card initialized with the 'Must change password' flag enabled, and the password is changed on the same machine, the user may encounter an issue and receive an "Incorrect password" message. The issue will not occur if the card is initialized on one machine and the password is changed on another.</p> <p><b>Workaround:</b> Delete the cache folder (<code>/var/tmp/eToken.cache</code>) after initialization and before changing the password.</p>
ASAC-2653	M	<p><b>Summary:</b> When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM &gt; Removable Devices menu.</p> <p><b>Workaround:</b> Connect the device that is not under the "Shared" devices list in order to work with the eToken device.</p>
ASAC-4497	M	<p><b>Summary:</b> When Configuring the Maximum Password Usage value to a value other than zero (0), the password will expire a day later than was defined. For example: set it to 166 days, SAC will show 167 days.</p> <p><b>Workaround:</b> None.</p>

Issue	Severity	Synopsis
ASAC-4141	M	<b>Summary:</b> During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. <b>Workaround:</b> None.
ASAC-4024	M	<b>Summary:</b> When unlocking a Common Criteria device (that's in linked mode) via SAC Tools and an incorrect Challenge Response is sent, a general error message is received. <b>Workaround:</b> None.
ASAC-11149	M	<b>Summary:</b> VPN fails using IDPrime 930 L3 (with KSP SHA2 certificate) cards. <b>Workaround:</b> None.
ASAC-5306	M	<b>Summary:</b> When trying to log onto a locked device, two messages are shown instead of one. <b>Workaround:</b> Close both windows.
ASAC-4116	M	<b>Summary:</b> When entering an incorrect Digital Signature PIN while enrolling a CC Certificate onto a CC device in unlinked mode, the enrollment process fails. <b>Workaround:</b> Retry enrolling the certificate with the correct Digital Signature PIN.
ASAC-13343	L	<b>Summary:</b> SAC binaries and packages need to be signed from Thales Apple Certificate. <b>Workaround:</b> None -no impact on SAC functionality.
ASAC-4974	L	<b>Summary:</b> 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. <b>Workaround:</b> The user must log out before making Password Quality modifications.

## Known Limitations

Issue	Severity	Synopsis
ASAC-16253	M	When multiple cards/tokens are present in reader, behaviour of CTK is unpredictable.
ASAC-16029	M	When P12 file has more certificates than available containers, "The Key container missing" message shown.
ASAC-16215	M	SIS id is not visible in Advanced view with SafeNet IDPrime 940 SIS card
ASAC-15321	M	MacOS Kerberos SSO Extension selects wrong certificate automatically.

Issue	Severity	Synopsis
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).
ASAC-8024	M	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-8203	M	After connecting and using an IDPrime 3811 device (on a contactless reader) the smart card was not recognized (loss of identification).
ASAC-6261	M	The profile whereby a PUK replaces the Admin Key does not support initializing a device.
ASAC-4872	M	IDPrime MD 840 and eToken 5110 CC do not support history size of Password Quality.
ASAC-4531	M	IDPrime MD 830B (applet 4.3.5) FIPS L3 does not support RSA 1024, ECC signing with SHA1 algorithms, as per FIPS/NIST regulations.
ASAC-4363	M	As of SAC 10.2, Symmetric keys created using PKCS#11 without the attributes: CKA_SENSITIVE = TRUE and CKA_EXTRACTABLE = FALSE, on an eToken Java device initialized in FIPS/CC mode will face backward compatibility issues on previous SAC versions.
ASAC-4081	M	SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
ASAC-3980	M	SafeNet Authentication Client does not support RSA 3072 and 4096 on IDPrime MD, .NET and eToken devices.  SafeNet Authentication Client does not support Single Sign On with IDPrime .NET and IDPrime MD cards via PKCS#11 API interface.  For more information, refer to the smart card specification guide.

Issue	Severity	Synopsis
ASAC-3769	M	<p>The following PIN pad limitations exist:</p> <ul style="list-style-type: none"><li>&gt; IDPrime MD 840 and IDPrime MD 3840 cards ignore the “Token password must be changed on first logon” parameter when working with the PIN pad reader.</li><li>&gt; Performing a “Change PIN” operation via PKCS#11 (C_SetPIN) requires the PIN to be entered again at the end of the process.</li><li>&gt; Single Sign On is not supported with PIN Pad readers.</li></ul>
ASAC-6191	M	IDPrime smart cards cannot sign plain data longer than 36 bytes for RSA or ECC keys.
ASAC-7318	M	On IDPrime MD cards, only CA private certificate objects are supported.



# Product Documentation

The following product documentation is associated with this release:

- > 007-013726-004\_SafeNet Authentication Client 10.8\_R2\_GA\_Mac\_Administrator Guide\_Revision C
- > 007-013725-004\_SafeNet Authentication Client 10.8\_R2\_GA\_Mac\_User Guide\_Revision C

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 refer to the documentation before contacting support. 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

The support portal also lists telephone numbers for voice contact ([Contact Us](#)).

## Email Support

You can also contact technical support by email at [technical.support.DIS@thalesgroup.com](mailto:technical.support.DIS@thalesgroup.com).