SafeNet Authentication Client 10.8 GA

LINUX RELEASE NOTES

Issue Date: July 2021

Build: RPM 28 / DEB 28
Document Part Number: 007-013841-003 Rev. A

Contents

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 GA Linux includes new features and bug fixes from previous SAC versions.

New Features and Enhancements

This release offers the following:

- All deliverables are rebranded to Thales.
- Added support for Ubuntu (v20.04), RedHat (v8.3), Fedora (v34), and CentOS (v8.3).
- Added support for IDPrime 930/3930 and IDPrime 3940 FIDO cards.

  See "Smart Cards" on page 4.
- Added support for GTK3.

Advisory Notes

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

- Legacy End-of-Life devices (eToken Virtual (ETV), iKey and CardOS) are no longer supported with SAC 10.8 GA Linux.
- SAC 10.8 GA Linux is compatible with all current Linux distributions, including OpenSSL 1.0 or above.
- If the Security-Enhanced Linux (SELinux) is enabled, the policy module must be updated to enable smart card logon. For more information, see the *Integration Guide: Using SafeNet Authentication Client CBA for Red Hat Enterprise Linux Workstation (Document Number: 007-000117-001, Rev A)*.
- Support and deliverable for 32-bit OS have been removed from SAC 10.8 GA onwards.

Licensing

From this release onwards, SAC on Linux does not require a license.

Localization

This release supports English only.

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 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, see *SafeNet Authentication Client User Guide*.
- 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. For more information, see ‘Security Recommendations’ chapter in *SafeNet Authentication Client Administrator Guide*.

Initialization Key Recommendation

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

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

Compatibility Information

Browsers

Following browsers are supported:

- Firefox 89.0 (TLS 1.3 supported)
- Thunderbird 78.8.1

Operating Systems

Following operating systems are supported:

- Red Hat 8.3
- CentOS 8.3
- Fedora 34(GNOME & KDE)

- Ubuntu 20.04(GNOME & KDE)

Tokens

Following tokens are supported:

Certificate-based USB Tokens

Following USB Tokens are supported:

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

Smart Cards

Following smart cards are supported:

- SafeNet IDPrime Virtual Smart Card
- SafeNet IDPrime 940
- SafeNet IDPrime 3940
- SafeNet IDPrime 930
- SafeNet IDPrime 3930

> **NOTE**
> If the Admin PIN is locked on a SafeNet IDPrime 940 or 3940 smart card, the card is left in an unusable state.
> If the SafeNet IDPrime 3940 smart card is set with the type B contactless protocol, it will be supported by the following readers only:
> - Gemalto IDBridge CL 3000 (ex Prox-DU)
> - Advanced Card System ACR 1281U

- Gemalto IDCore 30B eToken
- 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 MD 8840 (8GB) Micro SD card
- Gemalto IDPrime .NET (only SAC PKCS#11 and IDGo 800 Minidriver interfaces)

- Ezio PKI card
- Optelio R7

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

Smart Cards and Tokens that Support Common Criteria

Following devices support Common Criteria:

- Gemalto IDPrime MD 840
- Gemalto IDPrime MD 840 B
- Gemalto IDPrime MD 3840
- Gemalto IDPrime MD 3840 B
- Gemalto IDPrime MD 8840 Micro SD Card
- Gemalto IDPrime MD 940
- SafeNet eToken 5110 CC

External Smart Card Readers

Following smart card readers are supported:

- Gemalto IDBridge CT30
- Gemalto IDBridge CT40

Secure PIN Pad Readers

Following PIN Pad readers are secured:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710

> **NOTE** The Secure PIN Pad readers listed above are subject to limitations. Certain readers may not fully support all Smart cards. For details of supported Smart card and PIN Pad reader combinations, see *SafeNet Authentication Client Administrator Guide*.

Device Features Supported by SAC

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

Features	**Devices**				
	Gemalto IDPrime MD 840/3840/3840B/8840/SafeNet eToken 5110 CC	**SafeNet IDPrime 940**	**Gemalto IDPrime MD 830-FIPS/830-ICP/830B/3810/3810 MIFARE 1K/3811/SafeNet eToken 5300**	**SafeNet IDPrime 930/3930**	**SafeNet eToken 5110-FIPS**

Features	Devices				
Number of key containers	14 – default **Note 1**	20 – default **Note 1**	15	32	Dynamic **Note 5**
RSA Key sizes	1024-bit - default 2048-bit - default 3072-bit 4096-bit **Note 2 and Note 7**	1024-bit - default 2048-bit - default 3072-bit 4096-bit - default **Note 2**	1024-bit 2048-bit **Note 3**	1024-bit 2048-bit 3072-bit 4096-bit **Note 3**	1024-bit 2048-bit **Note 3**
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 **Note 4**	RAW, PKCS#1 v1.5, PSS, OAEP **Note 3 and Note 6**
ECC Key sizes	256-bit - default 384-bit 521-bit **Note 2**	256-bit - default 384-bit 521-bit **Note 2**	256-bit 384-bit 521-bit	256-bit 384-bit 521-bit	256-bit 384-bit
Hash	SHA-1 160-bit SHA-2 256-bit, 384- bit, 512-b	SHA-1 160-bit SHA-2 256- bit, 384-bit, 512-bit	SHA-1 160-bit SHA-2 256-bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256- bit, 384-bit, 512-bit **Note 3**	SHA-1 160-bit SHA-2 256- bit, 384-bit, 512-bit **Note 3**
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

Features	Devices				
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 is 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-bit and 4096-bit only key import available (no OBKG).

Compatibility with Third-Party Applications

Following third-party applications are supported:

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	Citrix	Virtual Apps and Desktops 7.1903 (Formerly XenDesktop)*
VMware View	Horizon 7.8	VMware View*
Digital Signatures	Mozilla	Thunderbird 78.8.1
Browsers	Mozilla	Firefox 89.0

* Validated with previous SAC version (SAC on Linux 10.7)

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 10.7 to SAC 10.8 on Linux, 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-9982	H	The CKA_ALWAYS_AUTHENTICATE attribute did not function properly. (Customer ID: CS0936052)
ASAC-13297	H	RPM GPG key file missing in the package. (Customer ID: CS1053042)
ASAC-10038	H	Installer/Uninstaller not to search on the root for Mozilla plugins. (Customer ID: CS0937591)
ASAC-11632	M	The CKA_HW_FEATURE_TYPE attribute did not return a valid result. (Customer ID: CS0978602)

Known Issues

Issue	Severity	Synopsis
ASAC-11163	H	**Summary:** 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). **Workaround:** None – this is a smart card design feature.

Issue	Severity	Synopsis
ASAC-9244	H	**Summary:** When the *Must change password* flag is set and the password is changed using a Pin Pad reader through the SAC Monitor, the balloon notification appears for only a second. **Workaround:** To disable the balloon notification, add the property *PinPadNotify=2* under the *General* section of the configuration file `/etc/eToken.conf`.
ASAC-9306	M	**Summary:** Using Ubuntu 19.04 x64 KDE, SAC Monitor does not start automatically after logging in. **Workaround:** SAC Monitor must be started manually via the GUI/command line.
ASAC-9288 ASAC-9281	M	**Summary:** By default, the retry counter is cached causing 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. **Workaround:** Add the property *RetryCountCached=0* under the *General* section of the configuration file `/etc/eToken.conf`.
ASAC-9108 ASAC-6191	H M	**Summary:** Sign operations using IDPrime MD smart cards with PKCS#1 v1.5 padding with hash mechanisms SHA256, SHA384 and SHA512 require input data to be prefix with the hash object identifier (OID). The use of SHA1 does not require this prefix. **Workaround:** Ensure the following OID’s are prefixed to the hash of data to be signed: `SHA_256_HEADER [] = {0x30,0x31,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x02,0x01,0x05,0x00,0x04,0x20}; SHA_384_HEADER [] = {0x30,0x41,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x02,0x02,0x05,0x00,0x04,0x30}; SHA_512_HEADER [] = {0x30,0x51,0x30,0x0D,0x06,0x09,0x60,0x86,0x48,0x01,0x65,0x03,0x04,0x02,0x03,0x05,0x00,0x04,0x40};`
ASAC-11099	M	**Summary:** 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. **Workaround:** On IDPrime based devices, use the PSS parameters with the salt length equal to the hash length.
ASAC-8267	M	**Summary:** 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) **Workaround:** Ensure that the Digital Signature PIN (Role#3) and Digital Signature PUK (Role#4) have the same PINPad configuration.

Issue	Severity	Synopsis
ASAC-7969	M	**Summary:** 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. **Workaround:** Peform either one of the following: > Update the application to use the hash off-board mechanism and then perform the RSA operation with the token. > Update the application to synchronize between threads - make the `C_SignInit - C_SignUpdate - C_SignFinal` a solid block. > If there is no option to update the application, enable the hash offboard property: *HashOffboard* in SAC. This allows SAC PKCS#11 to perform the hash off-board instead of the token.
ASAC-7932	M	**Summary:** Changing the PIN on Firefox using the CT710 PIN Pad does not work. **Workaround:** Change the PIN using SAC Tools or SAC tray icon.
ASAC-6214	M	**Summary:** VMView client may not work properly with SAC when using a smart card certificate. **Workaround:** Install SAC before installing the VMView Client.
ASAC-5815	M	**Summary:** 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 > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken/reader device.
ASAC-5343	M	**Summary:** 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. **Workaround:** Delete the cache folder (C:\Windows\Temp\eToken.cache) after initialization and before changing the password.
ASAC-2653	M	**Summary:** When working with a token on VM Workstation, the token might be unrecognized when selecting the "Shared" device in VM > Removable Devices menu. **Workaround:** Connect the device that is not under the "Shared" devices list in order to work with the eToken device.
ASAC-4497	M	**Summary:** 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. **Workaround:** None.
ASAC-4141	M	**Summary:** During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. **Workaround:** None.

Issue	Severity	Synopsis
ASAC-4024	M	**Summary:** 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. **Workaround:** None.
ASAC-5306	M	**Summary:** When trying to log onto a locked device, two messages are shown instead of one. **Workaround:** Close both windows.
ASAC-4116	M	**Summary:** When entering an incorrect Digital Signature PIN while enrolling a CC Certificate onto a CC device in unlinked mode, the enrollment process fails. **Workaround:** Retry enrolling the certificate with the correct Digital Signature PIN.
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.

Known Limitations

Issue	Severity	Synopsis
ASAC-12144	H	When working in a VDI environment, configure the `CacheMarkerTimeout` property on the host machine under the *General* section: CacheMarkerTimeout=1 For more details, refer to *SafeNet Authentication Client Administrator Guide*.
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.

Issue	Severity	Synopsis
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, see the smart card specification guide.
ASAC-3769	M	The following PIN pad limitations exist: > 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. > Performing a “Change PIN” operation via PKCS#11 (C_SetPIN) requires the PIN to be entered again at the end of the process. > Single Sign On is not supported with PIN Pad readers.
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:

- 007-013842-002_SafeNet Authentication Client_10.8_Linux_GA_Administrator_Guide_Rev A
- 007-013843-002_SafeNet Authentication Client_10.8_Linux_GA_User_Guide_Rev 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 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).