THALES

gemalto
a Thales company

SafeNet Authentication Client

RELEASE NOTES

Version: 10.7 – Linux
Build: RPM 77 / DEB 77
Issue Date: 25 June 2019
Document Part Number: 007-013841-002, Rev D

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 10.7 Linux (GA) includes bug fixes and other newly supported features.

New Features and Enhancements

SafeNet Authentication Client 10.7 Linux (GA) offers the following new features:

- **Support for eToken 5300 –** The eToken 5300 is a compact, tamper-evident USB with presence detection, which creates a third factor of authentication.
- **IDPrime MD Read Only Certificates mode –** enabling this parameter prohibits deleting certificates from a connected device. The new read-only feature affects all certificates and keys on the smart card.
- **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 Pin Pad readers with IDPrime MD cards –** See the Secure PIN Pad Readers section for a list of supported PIN Pad Readers.
- **Security enhancements –** as part of our initiative to continuously improve SafeNet Authentication Client security levels, enhancements and updates were performed on SAC 10.7.
- **Bug fixes –** this release includes bug fixes from previous SAC Linux versions.

Advisory Notes

- **Legacy End-of-Life devices (eToken Virtual (ETV), iKey and CardOS) are no longer supported with SAC 10.7 Linux.**
- SAC 10.7 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 following Integration Guide: Using SafeNet Authentication Client CBA for Red Hat Enterprise Linux Workstation (Document Number: 007-000117-001, Rev A).

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 as follows:

- User PIN should include at least 8 characters of different types.
- Admin PIN should include at least 16 characters of different types.
- The Friendly Admin Password should include at least 16 characters of different types (See the SafeNet Authentication Client User Guide for more details on the Friendly Admin Password)
- 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.

Initialization Key Recommendation

We strongly recommend changing the Initialization Key using either one of the following methods:

- The customization process (CPB)
- The SAC Initialization process (See the SafeNet Authentication Client User Guide for more details on Initialization Key settings)

Compatibility Information

Browsers and Applications

SafeNet Authentication Client 10.7 Linux (GA) supports the following browsers:

- Firefox 67.04
- Thunderbird 60.7.0

Operating Systems

SafeNet Authentication Client 10.7 Linux (GA) supports the following operating systems:

- Red Hat 8 (and 7.6)
- CentOS 7.6 (and 6.10)
- SUSE 15
- Debian 9
- Fedora 30
- Ubuntu 18.04.2 LTS and 19.04

Tokens

SafeNet Authentication Client 10.7 Linux (GA) 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 Virtual Smart Card
- 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.
- 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

- 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

Smart Cards and Tokens that Support ECC Certificates

ECC Certificates are supported by eTokens and Gemalto IDPrime MD cards.

The following devices support ECC Certificates:

- SafeNet eToken 5110
- Gemalto IDPrime MD 830-FIPS
- Gemalto IDPrime MD 830-ICP
- Gemalto IDPrime MD 830 B
- Gemalto IDPrime MD 3810
- Gemalto IDPrime MD 3810 MIFARE 1K
- Gemalto IDPrime MD 3811

External Smart Card Readers

SafeNet Authentication Client 10.7 Linux (GA) supports the following smart card readers:

- Gemalto IDBridge CT30
- Gemalto IDBridge CT40

Secure PIN Pad Readers

SafeNet Authentication Client 10.7 Linux (GA) supports the following PIN pad readers:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710
- Ezio BLE

> **NOTE:** The Secure PIN Pad readers listed above are subject to limitations. Certain readers may not fully support all Smart cards. See the Administrator Guide for details of supported Smart card and PIN Pad reader combinations.

End-of-Life Tokens/Smart Cards

- SafeNet Virtual Token
- SafeNet Rescue Token
- 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 Java 72K ECC
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 5100/5105
- SafeNet eToken 5100 CC
- 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
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- Gemalto IDBridge CT710

End-of-Sale Tokens/Smart Cards

- SafeNet Reader CT1100
- SafeNet Reader K1100

Localizations

SafeNet Authentication Client 10.7 Linux 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 10.7 Linux (GA).

Solution Type	Vendor	Product Version
Virtual Desktop Infrastructure (VDI)	Citrix	Virtual Apps and Desktops 7.1903 (Formerly XenDesktop)
	VMware View	Horizon 7.8
Secure Shell (SSH)	-	-
Linux Pluggable Authentication Modules (PAM)	-	-

Installation

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

Upgrade

Upgrade is supported from previous versions of SafeNet Authentication Client Linux.

For more Installation and Upgrade details, see the SafeNet Authentication Client 10.7 Linux (GA) Administrator Guide.

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

Severity	Issue	Synopsis
H	ASAC-9241	Performing a 'Change Password' operation using the PIN Pad Reader failed. The PIN Pad could not be used to enter a password, only the keyboard could be used. (Customer ID: CS0879202)
H	ASAC-8980	Gdm-session-worker process had 100% CPU usage when logged on to Centos using SC Logon. (Customer ID: CS0878648)
L	ASAC-7442	When an eToken 5110 was inserted after the session had started, the device was not visible. (Customer ID: CS0816851)

Known Issues

Severity	Issue	Synopsis
H	ASAC-9244	**Summary:** When the 'Must change password' flag is set and the password is changed using a Pin Pad reader via 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`.
M	ASAC-9306	**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.
M	ASAC-9288 ASAC-9281	**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`.

H
M
	ASAC-9108
	ASAC-6191
		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 prepended with the hash object identifier (OID). The use of SHA1 does not require this prefix.
		Workaround: Ensure the following OID's are prepended 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};`

Product Documentation

The following product documentation is associated with this release:

- SafeNet Authentication Client 10.7 Linux GA Administrator Guide (Document PN: 007-013842-001, Rev C)
- SafeNet Authentication Client 10.7 Linux GA User Guide (Document PN: 007-013843-001, Rev 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 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.

Customer Support Portal

The Customer Support Portal, at https://supportportal.gemalto.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 Gemalto 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@gemalto.com.