THALES

SafeNet Minidriver 10.8 R6 (Post GA)
RELEASE NOTES

Issue Date: February 2022

Build: 2164
Document Part Number: 007-013868-002 Rev. J

Contents

Product Description

SafeNet Minidriver a simple alternative to developing a legacy cryptographic service provider (CSP) by encapsulating the complex cryptographic operations from the card Minidriver vendor.

SafeNet Minidriver presents a consistent interface between Thales PKI authenticators and Microsoft's Smart Card Base Cryptographic Service Provider (CSP) or Crypto Next Generation (CNG) Key Storage Provider (KSP) and to the Smart Card Management Interface).

Release Description

SafeNet Minidriver 10.8 R6 (Post GA) includes enhancements and bug fixes from previous versions.

The initial part of the document covers the SafeNet Minidriver as a single solution, whereas the second part of the document covers the information relevant to each Minidriver solution separately.

> **NOTE** This release of SafeNet Minidriver is not Microsoft Certified. Below screen is displayed while installing the Minidriver, click **Install** to continue.
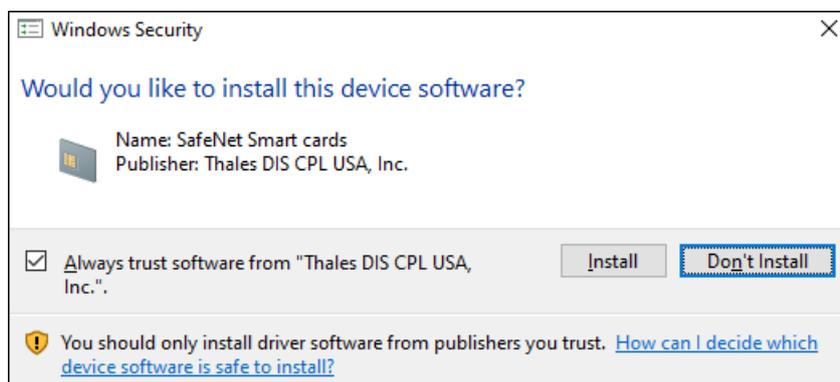
New Features and Enhancements

This release offers the following:

> Support for the SafeNet IDPrime 940B smart card.

> Improvements in Microsoft Certificate renewal failing with SAC 10.7.

   For details, refer to "Resolved Issues" on page 16.

Advisory Notes

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

> 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:

- Supported on OpenTrust versions 4.9.2 or 5.6

- 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.

> SafeNet eToken 5300:

- To retrieve touch sense capabilities using the SafeNet Minidriver API, refer tosee the `CCP_TS_CONTAINER` and `CP_CARD_TS_FEATURE` properties in the *SafeNet Authentication Client Developer Guide*.

- In the event of a time out (due to the SafeNet eToken 5300 not being touched in time), the following specific API error messages are shown:

  - `PKCS11 - CKR_FUNCTION_CANCELED(0x00000050)`

  - SafeNet Minidriver - `SCARD_E_CANCELLED (0x80100002)`

    These error messages replace the previous Generic error message.

Enabling SafeNet Minidriver Logs

To enable SafeNet Minidriver logs, you need to create a Registry value **Enabled** with value as 1 at the following path `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\Log`.
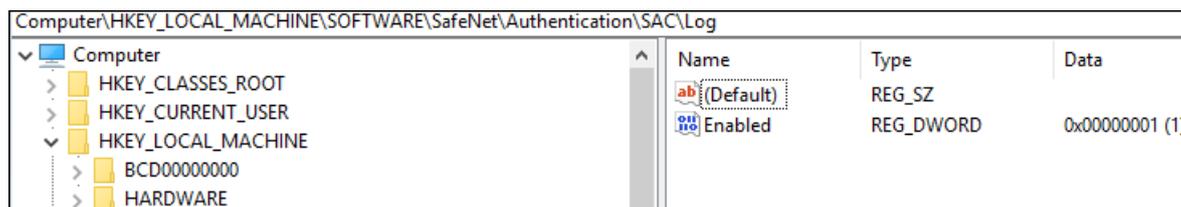
Compatibility Information

Operating Systems

Following operating systems are supported:

> Windows Server 2019 (64-bit)

> Windows Server 2016 (64-bit)

> Windows Server 2012 and 2012 R2 (64-bit)

> Windows 11 (21H2)

> Windows 10 (32-bit, 64-bit) up to 21H2

> Windows 8.1 (32-bit, 64-bit)

Tokens

Following tokens are supported:

Certificate-based USB Tokens

> SafeNet eToken 5300

> SafeNet eToken 5110

> SafeNet eToken 5110 CC

> SafeNet eToken 5110 FIPS

> SafeNet eToken 5300 C

Software Tokens

> SafeNet IDPrime Virtual Smart Card

Smart Cards

> SafeNet IDPrime 940B

> SafeNet IDPrime 940 SIS

> SafeNet IDPrime 3940 FIDO

> SafeNet IDPrime 930

> SafeNet IDPrime 3930

> SafeNet IDPrime 940

> SafeNet IDPrime 3940

> **NOTE** 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.

> Gemalto IDCore 30B eToken

> Gemalto IDPrime MD 840 (EOS)

> Gemalto IDPrime MD 840 B

> Gemalto IDPrime MD 3840 (EOS)

> Gemalto IDPrime MD 3840 B

> Gemalto IDPrime MD 830-FIPS

> Gemalto IDPrime MD 830-ICP

> Gemalto IDPrime MD 830 B

> Gemalto IDPrime MD 3810 (EOS)

> Gemalto IDPrime MD 3811

> Gemalto IDPrime MD 8840 (8GB) Micro SD card (EOS)

> Gemalto IDPrime .NET (EOS)

> Optelio R7

> **TIP** Although the majority of contactless cards mentioned in this release notes are compliant with ISO14443, 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 Cards and Tokens that Support Common Criteria

> SafeNet IDPrime 940

> SafeNet IDPrime 3940

> 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

> SafeNet eToken 5110 CC

Smart Card Readers supported in Contact and Contactless modes

> CL3000 Prox-du (EOL)

> ACR128U (EOL)

> Omnikey Cardman 5422

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

Smart Card Readers

> Gemalto IDBridge K30

> Gemalto IDBridge K50

> Gemalto IDBridge CT30

> Gemalto IDBridge CT40

> ACR128U (EOL)

> OMNIKEY 5422

> IDBridge CL3000 (EOS)

Secure PIN Pad Readers:

> Gemalto IDBridge CT700

> **NOTE** PIN Pad readers are supported only on IDPrime and .NET cards.

Compatibility with Third-Party Applications

Following third-party applications are supported:

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	Endpoint Security E80.70
	Microsoft	Windows Server 2008 SP2 and later
	Cisco	> AnyConnect Windows 4.7.00136
	Juniper	Pulse Secure
	Zone Central	Zone Central 6.1
Virtual Desktop Infrastructure (VDI)	Citrix	Virtual Apps and Desktops 7.1903 (Formerly XenDesktop)
	Microsoft	Remote Desktop
	VMware View	Horizon 7.8
Identity Access Management (IAM) Identity Management (IDM)	Intercede	MyID 11.3
	Microsoft	MIM 2016 4.5.286.0 (Supported with SAC Minidriver profile)
	Versasec	vSEC: CMS 5.8 (Supported only with SAC Minidriver profile)
	IDnomic	OpenTrust CMS 5.2 **NOTE** For eToken 5110 FIPS support, refer to "Advisory Notes" on page 3.
Pre Boot Authentication (PBA)	Microsoft	BitLocker (RSA only)
Certificate Authority (CA)	Microsoft (Local CA)	For All Windows platforms

Solution Type	Vendor	Product Version
Digital Signatures	Entrust	ESP 10
	Adobe	2020.009.20063
	Microsoft	Outlook 2016 / Office 365
	Mozilla	Thunderbird 52.9.1 **NOTE** As of SAC 10.8, the PKCS#11 module is registered automatically.
Browsers	Mozilla	Firefox 96.0.2 (TLS 1.3 supported)
	Microsoft	> Internet Explorer 11.0.9600.20139 (TLS 1.2 supported) > Edge Chromium 97.0.1072.69 (TLS 1.3 supported)
	Google	Chrome 97.0.4692.99 (TLS 1.3 supported)

Compatibility with Thales Applications

IDPrime cards can be used with the following products:

> SafeNet Authentication Service (SAS) / SafeNet Trusted Access (STA)

> IDPrime User Tool for Windows (V1.2.0)

Installation and Upgrade Information

Installing SafeNet Minidriver 10.8 R6 (Post GA)

SafeNet Minidriver can be installed in either of the following ways:

> **Automatically** – Microsoft Catalog (plug `n play). Performed only on a clean machine.

> **NOTE** Automatic installation will fetch previous version i.e. SafeNet Minidriver 10.8 R6 (GA) since this release is not Microsoft Certified.

> **Manually** – Double-click the `.msi` file.

Automatic Installation (Plug and Play)

When connecting a Thales PKI authenticator, the relevant Minidriver solution is automatically installed.

Both the IDPrime and SafeNet Minidrivers (which are part of the SafeNet Minidriver 10.8 R6 (Post GA) solution) are downloaded automatically (from the Microsoft Update Catalog site) when connecting one of the devices listed in the Supported Tokens section above.

For example:

Connected Device	Minidriver Solution Downloaded and Installed	Supported Binary Files
SafeNet IDPrime 930 SafeNet IDPrime 3930 SafeNet IDPrime 940 SafeNet IDPrime 3940 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 Optelio R7 SafeNet eToken 5110 CC SafeNet eToken 5300	SafeNet Minidriver for IDPrime	axaltocm.dll
SafeNet eToken 5110 SafeNet eToken 5110 FIPS	SafeNet Minidriver for eToken	etokenMD.dll

Manual Installation

SafeNet Minidriver 10.8 R6 (Post GA) can be installed manually on a clean machine or according to the scenarios listed in the table below:

Currently Installed	Perform the following
SafeNet Minidriver 9.0 (Plug and Play installation)	Install: **SafeNetMinidriver-10.8-R6.msi** file
SafeNet Minidriver 10.0, 10.1, 10.2, 10.7 or 10.8	Uninstall Safenet Minidriver 10.0/10.1/10.2/10.7 and then install **SafeNetMinidriver-10.8-R6.msi** file
SafeNet Minidriver 10.8 (Plug and Play installation)	Install: **SafeNetMinidriver-10.8-R6.msi** file
SafeNet Minidriver 10.8 (.msi installation)	Install: **SafeNetMinidriver-10.8-R6.msi** file

Upgrading SafeNet Minidriver

You can upgrade from SafeNet Minidriver 10.8 to 10.8 R6 (Post GA) using the MSI file wizard installation, or by using the command line installation.

> **NOTE** Upgrade from SafeNet Minidriver 10.8 R6 (GA) to 10.8 R6 (Post GA) is not supported.

> **TIP** You must restart your computer when the upgrade procedure completes.

When upgrading through the command line using the `/qn` parameter, your computer is restarted automatically.

Upgrading from Versions earlier than SafeNet Minidriver 10.8
Legacy versions of SafeNet Minidriver, earlier than 10.8 must be uninstalled before installing SafeNet Minidriver 10.8 R6 (Post GA).

Moving from SafeNet Minidriver to SAC

If you want to install SafeNet Authentication Client (SAC) on top of SafeNet Minidriver, then uninstall SafeNet Minidriver and only then install SAC.

> **NOTE** Upgrading from SafeNet Minidriver to SAC is not supported.

Applying SafeNet Minidriver using the SAC Customization Tool

SAC 10.8 R6 (Post GA) Customization Tool has been enhanced to provide you with a predefined SafeNet Minidriver installation profile. By selecting this profile, there is no need to configure and install individual elements.

SAC core Middleware services are installed, such as eToken Service and SAC Monitor that allow managing public device data for better Minidriver performance, as well as support for Single Logon.

The SafeNet Minidriver is mainly for Thales customers who want to work only with SafeNet Minidriver together with SAC services. Only the relevant SafeNet Minidriver components have been made available in the SafeNet Minidriver installation profile, all other components that are not relevant to this profile have been grayed out.

The SafeNet Minidriver profile allows editing (selecting/clearing) the following components:

> SafeNet Minidriver 9.0 (for eToken Devices)

> Applications (SAC Tools)

> Services (eToken Services and SAC Monitor)

> Core (IDPrime PKCS#11)

> eToken Drivers

SafeNet Minidriver Cryptographic Policies

The following recommendations will help you maintain a secured SAC environment as well as keep your information as safe as possible:

> User/Administrator smart card password protection: To avoid password leakage, we recommend the following:

- Use PIN Pad readers - user passwords do not pass through a computer's memory when using a PIN Pad reader.

- Use devices configured to support secured messaging - secured messaging protects the transfer of data between the middleware and the device.

> Protect the device from unauthorized usage:

- Ensure the device is disconnected when not in use.

> The recommended password strength is:

- User PIN should include at least 8 characters of different types.

- Admin PIN should include at least 16 characters of different character types.

> **NOTE** Character types include upper case, lower case, numbers, and special characters.

- 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 is 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.

> Configure restrictive cryptographic policies:

To allow organizations to enforce restrictive cryptographic policies when using SafeNet / Thales security devices (smart cards and USB tokens), the following policies were updated:

- Deprecated Cryptographic Algorithms and Features Policy

- Key Management Policy

  The motivation behind these policy updates:

  Legacy cryptographic schemes can cause organizations to fail current compliance requirements or expose cryptographic weakness associated with deprecated algorithms and mechanisms.

  Changes have been made to the default SafeNet Minidriver configuration to disallow the usage of cryptographic algorithms, or protocols, that are now considered to be weak.

  Default settings were updated to eliminate revealing sensitive data:

- The creation, generation and usage of exportable symmetric keys are blocked.

- The unwrapping and wrapping of asymmetric/symmetric private keys is blocked.

- Legacy and obsolete algorithms are blocked - these cryptographic algorithms conform to the National Institute of Standards and Technology (NIST), preventing third-party applications from using legacy or obsolete algorithms.

> **NOTE** Once a restrictive policy has been set, the use of SAC with the above algorithms will be blocked. This might have implications on the way in which the third-party's applications currently work.
> Administrators must make sure that the third-party applications used by the organization are configured accordingly and do no use one of the algorithms listed above, as they will be blocked.

For more information, refer to below.

Security Settings

The following settings are written to the **Crypto** section in the `SafeNet\Authentication\SAC\Crypto` registry key.

Description	Registry Value
Deprecated Cryptographic Algorithms and Features The default list of deprecated cryptographic algorithms and features may be enhanced in order to comply with NIST requirements in future versions. It is up to the customer to check that it will be compatible with third-party applications.	> **Value Name:** `Disable-Crypto` > **Values:** (String) • **None -** All SafeNet Minidriver cryptographic algorithms and features are supported. This was the default value for SafeNet Minidriver versions below 10.7. Setting this value causes SafeNet Minidriver to be compatible with previous versions of SafeNet Minidriver. It is strongly recommended you read the section: SafeNet Minidriver Cryptographic Policies. • **Obsolete -** A list of restricted and deprecated cryptographic algorithms and features. The following are deprecated: MD5, RC2, RC4, DES, 2DES, GenericSecret<112, RSA-RAW, RSA<2048, ECC<224, ECB, Sign-SHA1 • **Manual -** Create your own list of deprecated algorithms and features. (See the description below). > **Default:** Obsolete

Description	Registry Value

The following can be disabled:

> Algorithms: RSA, ECC, DES, 2DES, 3DES, AES, RC2, RC4, GenericSecret

> Hash types: MD5, SHA1, SHA2

> Padding types: RAW, PKCS1, OAEP, PSS

> Cipher modes: ECB, CBC, CTR, CCM

> Mechanisms: MAC, HMAC, ECDSA, ECDH

> Operations: Encrypt, Decrypt, Sign, Verify, Generate, Derive, Wrap, Unwrap, Digest, Create (keys only)

> Weak key size: RSA<2048

> Object types: HWEF – elementary file (EF) objects (used by eToken devices for storing exportable symmetric keys and symmetric keys without on-board implementation)

> HWALL – all types of objects implemented on token (Base Security Object (BSO) and EF)

Example of a manual configuration: Encrypt-DES-ECB, Sign-3DES-MAC, DES-CTR, HMAC-MD5, HMAC-SHA1, HMAC-SHA2, DES-CBC, Unwrap-DES-ECB, RSA-PKCS1-MD5, Verify-RSAPSS-SHA2, AES-CTR, AES-MAC, Decrypt-RC2, Wrap-ECB.

Key Management	
Defines key creation, export, unwrap, and off board crypto policies. SAC default behavior may be updated in future versions in order to comply with NIST requirements.	> **Registry Value Name:** `Key-Management-Security`
It is up to the customer to check that it will be compatible with third-party applications.	> **Values:** (String)

> **Registry Value Name:** `Key-Management-Security`
> **Values:** (String)
> • **Compatible:** enables the use of features that are deprecated in the Optimized and Strict configurations below. This was the default value for SafeNet Minidriver versions below 10.8. Setting this value will cause SafeNet Minidriver to be compatible with SafeNet Minidriver 10.8 and below. It is strongly recommended to read the section: SafeNet Minidriver Cryptographic Policies before applying legacy values.
> • **Optimized:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable the unwrap-PKCS1.5 and unwrap-AES-CBC on hardware tokens (session enable).
> • **Strict:** Disable the generation or creation of exportable keys. Disable the exporting of keys, regardless of how they were generated. Disable any usage of symmetric keys off-board including unwrap. Disable all unwrap-PKCS1.5 and unwrap-AES-CBC operations.
> **Default:** Optimized

Description	Registry Value

DotNetOBKGType
 	
This key enables the generation of the RSA key pairs using BCrypt API on the local computer instead of On Board Key Generation. If the value of this key is set to 0 or is absent (default installation), then the RSA key pairs on IDPrime.NET cards are generated using the standard On Board Key Generation mechanism.
 	
If this key is created and set to 1, the Minidriver creates the RSA key pairs using the BCrypt API on the local computer and keys are imported into the IDPrime.NET smart card.
	> **Setting Name:** `DotNetOBKGType`
	> **Values:**
	  • 0 = Generate on board (key pair)
	  • 1 (and above) = Key pair generation is done by software (that is: disable on board key generation)
	> **Default:** 0

Specific IDPrime Minidriver Information

This section covers specific information related to IDPrime Minidriver (previously known as IDGo 800 Minidriver).

This section lists the ATRs for the supported smart cards. Those figures indicated in bold and red can differ from one card to another in the same family (other IDPrime MD cards may be added for later versions). All values are in hexadecimal.

ATRs

> SafeNet eToken 5110 CC USB Token

> SafeNet IDPrime 940, 3940 Cards

> Gemalto IDPrime MD 830-FIPS, 830-ICP, 830 B, 840, 840 B, 3810, 3811, 3840, 3840 B and 8840 Cards Ezio PKI Cards

  • [IDPrime MD T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 0**0 12 0F FE 82 90 00

  • [IDPrime MD T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 00 00 00 00 12 0F FE 82 90 00 00

  • [IDPrime MD Contactless] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FE 82 90 00 **00**

  • [IDPrime MD Contactless B] 3B 88 80 01 31 F3 5E 11 **00** 87 95 **00 00**

> SafeNet IDPrime 930, 3930 Cards

  • [IDPrime v2 T=0] 3B 7F **00** 00 00 80 31 80 65 B0 **00 00 00 0**0 12 0F FD 82 90 00

  • [IDPrime v2 T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 0F FD 82 90 00 **00**

  • [IDPrime v2 contactless type A] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 0F FD 82 90 00 **00**

  • [IDPrime v2 contactless type B] 3B 88 80 01 32 F3 5E 11 **00** 87 95 **00 00**

> SafeNet eToken 5300 USB Token

  • [eToken5300] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 01 78 82 90 00 **00**

> Gemalto IDPrime .NET Cards

  • [Axalto Cryptoflex .NET] 3B **00 00** 41 73 74 72 69 64

> Optelio R7 Cards

- [Optelio D72 FXR1 (MD) T=0] 3B 6E 00 00 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00

- [Optelio D72 FXR1 (MD) T=1] 3B EE 00 00 81 31 80 43 80 31 80 66 B1 A1 11 01 A0 F6 83 00 90 00 8F

- [Optelio R7 Contact] 3B 6E 00 00 80 31 80 66 B0 87 0C 01 6E 01 83 00 90 00

- [Optelio R7 Contactless] 3B 8E 80 01 80 31 80 66 B1 84 0C 01 6E 01 83 00 90 00 **00**

- [Optelio R7 with WG10 Contact] 3B 68 00 00 80 66 B0 07 01 01 07 07

- [Optelio R7 with WG10 Contactless] 3B 88 80 01 80 66 B0 07 01 01 07 **00 00**

- [Optelio R7 with WG10+2F10 contact] 3B 6F 00 00 80 66 B0 07 01 01 07 **00 00 00 00 00 0**0 90 00

- [Optelio R7 with WG10+2F10 contactless] 3B 8F 80 01 80 66 B0 07 01 01 07 **00 00 00 00 00 00** 90 00 **00**

> SafeNet IDPrime Virtual Smart Card

- [IDPrime Virtual] 3B FF 96 00 00 81 31 FE 43 80 31 80 65 B0 00 00 00 00 12 91 78 82 90 00 69

> SafeNet IDPrime 940 SIS, 3940 SIS Cards

- [IDPrime 940 SIS T=0] 3B 7F **00** 00 00 80 31 80 65 B0 00 00 00 00 12 02 F0 82 90 00

- [IDPrime 940 SIS T=1] 3B FF **00** 00 00 81 31 **00** 43 80 31 80 65 B0 **00 00 00 00** 12 02 F0 82 90 00 **00**

- [IDPrime 940 SIS contactless type A] 3B 8F 80 01 80 31 80 65 B0 **00 00 00 00** 12 02 F0 82 90 00 **00**

> SafeNet IDPrime 3940 FIDO

- [IDPrime Fido T=1] 3B FD 96 00 00 81 31 FE 43 80 31 80 65 B0 85 04 00 11 83 01 90 00 00

Resolved and Known Issues

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

Priority	Classification	Definition
C	Critical	No reasonable workaround exists.
H	High	Reasonable workaround exists.
M	Medium	Medium level priority problems.
L	Low	Lowest level priority problems.

Resolved Issues

Issue	Severity	Synopsis
ASAC-13030	H	Microsoft Certificate renewal failed with SAC 10.7. The *Windows Logon* gives an error that no certificate is found. (Customer ID: CS1004704, CS1050137, CS1098128)

Known Issues

The following issues are known to exist in the product at the time of release.

Issue	Severity	Synopsis
ASAC-14246	M	**Summary:** Few DLLs remain in the system after uninstalling SAC (with the SafeNet Minidriver profile- custom installation) and standalone SafeNet Minidriver on a 64-bit OS. **Workaround:** Manual deletion of the DLLs can be done.
ASAC-13766	M	**Summary:** While upgrading SafeNet Minidriver (32-bit and 64-bit) from the previous versions such as 10.2, 10.8 R2, 10.8 R3, and 10.8 R5, the DLL (etoken.dll) remains in the system after uninstallation. **Workaround:** Manual deletion of the DLL can be done.

Issue	Severity	Synopsis
ASAC-8055	M	**Summary:** Changing the Admin PIN of eToken 5110 FIPS is not supported via Minidriver API. **Workaround:** Change the Admin PIN only via the PKCS11 API.
ASAC-7489	M	**Summary:** Working with the Microsoft CCID driver caused smart card logon to fail with a .Net card in a Pin Pad CT710 and SWAT reader. When working with the Gemalto CCID driver, all worked as expected. **Workaround:** Work with the Gemalto CCID driver instead of the Microsoft CCID driver.
ASAC-7448	M	**Summary:** A warning message appears when installing SafeNet Minidriver 10.6 on a PC without the Windows Patch KB3033929. **Workaround:** Prerequisite: Before installing the Minidriver on Windows 7, ensure the following Microsoft patch KB3033929 is installed: https://docs.microsoft.com/en-us/security-updates/SecurityAdvisories/2015/3033929
ASAC-7412	M	When enrolling a signature only certificate using a CT40 and an incorrect Signature PIN is entered, the 'incorrect Signature PIN' error message does not appear.
ASAC-7405	M	**Summary:** Upgrading SAC 10.5 (installed on Windows x32 OS via the Customization Tool) with SafeNet Minidriver fails. **Workaround:** Uninstall SAC 10.5 before installing SAC 10.6.
ASAC-7398	M	The registry key that has been added in order to activate the PIN Policy Single Sign-On (SSO) feature for smart card logon is supported only for Windows 7 SP1. The registry key is called EnableLogonSSO and is under `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\`
ASAC-7397	M	The single sign-on feature is supported for the contact interface only.
ASAC-7396	M	It is not possible to encrypt an e-mail in Mozilla Thunderbird using an elliptic curve certificate.
ASAC-7394	M	There is a certificate propagation issue with Windows Server 2008 R2. Although not observed with the other supported versions of Windows Server, it could possibly occur with those too. When two users log on simultaneously on a Windows server using remote desk protocol (RDP), one of the users sometimes has the certificate of the other user propagated to his or her store in addition to his or her own certificates. This happens only rarely. The impact is only visual; the user can see the other's certificates but cannot use them. This problem is caused by Windows – not the SafeNet Minidriver.

Issue	Severity	Synopsis
ASAC-7393	M	**Summary:** Windows 8.1 does not recognize External PINs. This problem comes from the fact that Windows 8.1 uses the key storage provider instead of the Base CSP to enumerate certificates. **Workaround:** It is possible to change this by deactivating the `EnumerateECCCerts` registry key. This workaround solves the problem but means that it will no longer be possible to use ECC certificates. To deactivate the EnumerateECCCerts key, set its value to 0 in `HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft\Windows\SmartCardCredentialProvider`.
ASAC-7392	M	Adobe Reader freezes when you try to change the signature PIN (role #3). After changing the PIN, Adobe asks for the User PIN (role #1) and then freezes.
ASAC-7389	M	The IDGo 800 credential provider cannot manage more than one card connected at the same time.
ASAC-7388	M	Although multiple PINs are supported, Internet Explorer does not provide a means of associating different PIN roles with different key sets.
ASAC-7387	M	It is not possible to sign Adobe Reader 10 documents using an elliptic curve certificate. it is possible with Adobe Reader 11 documents.
ASAC-7386	M	In Word and Excel, it is not possible to sign VB macros with elliptic curve certificates.
ASAC-7385	M	When enrolling certificates in Internet Explorer (IE) with more than one card connected, it is not possible to choose the card in which the certificate is to be enrolled. This is because IE does not display a "select card" window which would allow the user to make such a choice.
ASAC-7384	M	Firefox behaves strangely when the PIN is blocked, for example it may continue to prompt for a PIN instead of displaying a message to say that the PIN is blocked. In the event of strange behavior, check to see whether the PIN is in fact blocked.
ASAC-7383	M	It is not possible to enroll a certificate in the card when using Chrome.
ASAC-7382	M	With the IDGo 800 Credential Provider, when starting a Remote Desktop Services connection the user is asked for the user PIN twice.
ASAC-7381	M	SSL authentication does not work with IE and the Modern (formerly Metro) User Interface when the SafeNet Minidriver is using secure messaging in contactless mode.

Issue	Severity	Synopsis
ASAC-7380	M	IE crashes when the certificate for SSL authentication is selected. This happens when trying to perform a remote desktop connection to the server using a smart card or with a smart card loaded in the Minidriver manager. This problem occurs only for the following configuration: 64-bit version of Windows 8.1 with Gemalto Credential Provider installed.
ASAC-7378	M	A smart card unlock operation cannot be performed in contactless mode if the smart card logon was performed in contact mode and vice-versa.
ASAC-7377	M	With Windows 8 and Server 2012 only, the smart card does not appear in Device Manager when connected via a PIN Pad reader.
ASAC-7376	M	With Windows 8 only, sometimes the computer is unable to wake up correctly from hibernation mode.
ASAC-7375	M	When using Citrix, it is not possible to perform SSL authentication with Internet Explorer in protected mode and the web site is trusted.
ASAC-7371	M	When entering an incorrect PIN via a PIN Pad, the error message will be displayed only from the point at which the user has 3 attempts remaining.
ASAC-7369	M	It is not possible to perform a smart card logon with ECC certificates when using a PIN role other than User PIN#1.
ASAC-7368	M	It is not possible to decrypt mails using the ECC certificates in Microsoft Outlook if the single sign-on feature is activated.
ASAC-7367	M	It is not possible to unblock a PIN using a PUK with the IDGo 800 Credential Provider.
ASAC-7318	M	On IDPrime MD cards, only CA private certificate objects are are supported.
ASAC-7180	M	**Summary:** When performing a secure channel via TLS on Windows 10 (1803), the PIN dialog may not be displayed. **Workaround:** Add the following registry: [HKEY_CURRENT_USER\SOFTWARE\Microsoft\Internet Explorer\Spartan] "RAC_LaunchFlags"=dword:00000023

Known Limitations

Issue	Severity	Synopsis
ASAC-7685	M	If the "Must Change Password" flag is enabled, the user will not be able to use the smart card for smart card logon until the password is changed.
ASAC-7623	M	When working with SafeNet Minidriver, the SafeNet eToken 5300 touch sense device does not have a user interface to inform the user that the device must be touched. To install the Minidriver as part of SAC 10.7 Customization Tool, add the SAC Monitor to the SafeNet Minidriver profile.
ASAC-7110	M	When a smart card is configured with the 'Must Change Password' parameter enabled, any PKI operation will fail until the password is manually changed.
ASAC-6592	M	**Summary:** When SAC (with the SafeNet Minidriver profile - custom installation) is used with an IDPrime 830 smart card on Windows 10, the PIN prompt is displayed only after 10 seconds between the signing operations. **Workaround:** This is Windows default 'Power Saving' mode. This feature sends the Power Off command (63 00 00 …) to the reader after about 20-30 seconds after any transaction to the smart card is completed. Configure the following registry key to change the delay period in seconds: `CardDisconnectPowerDownDelay` in `HK_local_ machine\software\microsoft\cryptography\calais` http://opensc.1086184.n5.nabble.com/smart-card-reset-after-5-seconds-on-Windows-td15563.html.
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.

Specific SafeNet Minidriver (eToken) Information

This section covers specific information related to SafeNet Minidriver (eToken). SafeNet Minidriver (eToken) refers to eToken Minidriver (Build 54).

Password Quality Limitations

Password Quality policies that are managed by SAC, are supported by SafeNet Minidriver. However, the following settings are ignored by Minidriver even though they are configured on the token:

> Maximum Length – this setting is configured and enforced by the SafeNet Authentication Client Settings on all operating systems.

> Expiry Warning Period – no alerts or warning prompts are displayed.

Smart Card Logon with ECC Certificates

To enable Smart Card logon with ECC certificates:

1. Click **Start**, and enter `gpedit.msc` in the search field.
2. In the **Local Group Policy Editor**, select **Computer Configuration** > **Administrative templates** > **Windows Components** > **Smart Card**.
3. Select **Enabled** in the **Allow ECC Certificates** to be used for logon and authentication field.

Uninstalling SafeNet Minidriver

When SafeNet Minidriver is installed from the Microsoft Update Catalog, perform the following to uninstall the Minidriver:

> On a 32-bit system, the file that defines the registry card media (`eTokenMD.dll`) must be deleted from the system32 folder.

> On a 64-bit system, these must be deleted from both `sysWOW64` and `system32` folders.

Remove the following keys from the `HKEY_LOCAL_MACHINE` registry tree:

32-bit Systems:

> `SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0`

> `SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0b`

64-bit Systems:

> `SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0`

> `SOFTWARE\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0b`

> `SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0`
> `SOFTWARE\Wow6432Node\Microsoft\Cryptography\Calais\SmartCards\eTokenCard/JC1.0b`

> **NOTE** Restart the system after uninstalling SafeNet Minidriver.

Known Issues and Limitations

Issue	Severity	Synopsis
ASAC-11057	M	**Summary:** An error message appeared when using vSec to change/unblock a connected SafeNet eToken 5110 User PIN. **Workaround:** Ensure no other processes are communicating with the device during the unblock procedure. Close SACTools and SACMonitor prior to the unblock operation.
ASAC-7121 ASAC-6788 ASAC-2429	M	**Summary:** Performing a remote desktop connection from a system which has Minidriver installed, to a system with SAC installed, causes RDP errors after entering the smart card PIN. > **NOTE** This is the default behavior of the RDP, when the CredSSP protocol is used during an RDP session, when the CSP names differ on a client and a server. https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CSSP/[MS-CSSP].pdf|https://winprotocoldoc.blob.core.windows.net/productionwindowsarchives/MS-CSSP/%5bMS-CSSP%5d.pdf CSP name is passed from the client to the server during the CredSSP handshake, which is why the first attempt fails, but the second one succeeds because it uses the CSP name that's local to the server. For more information please refer to the official document: *2.2.1.2.2 TSSmartCardCreds*. **Workaround:** 1. Upgrade the RDP version on the machine. 2. Edit the RDP file (on the Client) by following these steps: • Open the Remote Desktop connection window. • Click Show Options. • Under Connection Settings, click Save as, and save the RDP file locally. • Open the file using Notepad. • Add enablecredsspsupport:i:0 at the end of the RDP file and then save the file. • Connect to the server using the edited RDP file. For more details, see: > https://support.microsoft.com/en-us/kb/941641 > https://technet.microsoft.com/en-us/library/ff393660(v=ws.10).aspx

Issue	Severity	Synopsis
ASAC-2379	M	**Summary:** When a token is initialized with the 'Password must be changed on first logon' field, and is then connected to the operating system with SC Logon using SafeNet Minidriver, an error message is displayed as soon as a password is entered. **Workaround:** Change the password using SafeNet Authentication Client before using the Minidriver.

Product Documentation

We have attempted to make this 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.