SafeNet Authentication Client

RELEASE NOTES

Version:	10.4 – Windows (Post GA)
Build:	40
Issue Date:	November 2017
Document Number:	007-013559-006 Rev A

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 10.4 (Post GA) introduces the ROCA vulnerability solution and bug fixes.

New Features and Enhancements

SafeNet Authentication Client 10.4 (Post GA) offers the following new features:

- **Microsoft Credential Guard –** SAC 10.4 (Post GA) is now compliant with Microsoft Credential Guard and code integrity is now enabled.
- **ROCA Vulnerability Solution –** this solution is available when using SAC 10.4 (Post GA) customized using IDGo 800 Compatible Mode. For more information, see the ROCA Vulnerability Solution on page 17.
- **Bug fixes -** this release includes bug fixes from previous SAC versions.

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/.

NOTE: Using the Gemalto IDGo 800 Minidriver as a standalone component does not require SAC licensing.

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

SafeNet Authentication Client 10.4 (GA) Windows supports the following browsers:

- Firefox 56.02
- Internet Explorer 11.332.15063.0
- Chrome version 62
- Microsoft Edge 42.17035

Operating Systems

SafeNet Authentication Client 10.4 (GA) Windows supports the following operating systems:

- Windows Server 2008 R2 SP1 (32-bit, 64-bit)
- Windows Server 2008 SP2 (32-bit, 64-bit)
- Windows Server 2012 and 2012 R2 (64-bit)
- Windows Server 2016 (64-bit)
- Windows 7 SP1 (32-bit, 64-bit)
- Windows 8 (32-bit, 64-bit)
- Windows 8.1 (32-bit, 64-bit)
- Windows 10 (32-bit, 64-bit)

Tokens

SafeNet Authentication Client 10.4 (GA) supports the following tokens:

Certificate-based USB Tokens

- SafeNet eToken 5110
- SafeNet eToken 5110 CC
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 FIPS HID
- SafeNet eToken 5110 HID

Software Tokens

- SafeNet Virtual Token
- SafeNet Rescue Token

Smart Cards

- 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)

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

End-of-Sale Tokens/Smart Cards

- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID
- SafeNet eToken 4100
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
- SafeNet eToken 7300
- SafeNet eToken 7300-HID

NOTE: SafeNet HID tokens are not compatible with Smart Card Logon and CAPI based VPN applications.

End-of-Life Tokens/Smart Cards

- SafeNet eToken PRO 32K v4.2B
- SafeNet eToken PRO 64K v4.2B
- SafeNet eToken Pro SC 32K v4.2B
- SafeNet eToken Pro SC 64K v4.2B
- SafeNet eToken 7100 (SafeNet eToken NG-Flash)
- SafeNet iKey: 2032, 2032u, 2032i (Windows and Mac only)
- SafeNet smart cards: SC330, SC330u, SC330i
- SafeNet eToken 5000 (iKey 4000)
- SafeNet eToken 4000 (SC400)
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken PRO Smartcard 72K

External Smart Card Readers

SafeNet Authentication Client 10.4 (GA) supports the following smart card readers:

- Gemalto IDBridge K30
- Gemalto IDBridge K50
- Gemalto IDBridge CT30
- Gemalto IDBridge CT40
- Gemalto IDBridge CL 3000 (ex Prox-DU)
- Athena AESDrive IIIe USB v2 and v3
- Advanced Card System ACR 1281U
- Dell Broadcom (This reader is found only in laptops)

NOTE: SC Reader drivers must be compatible with the extended APDU format in order to be used with RSA-2048 (relevant to SafeNet eToken 4100).

Mobile PKI Bluetooth Readers:

- SafeNet Reader CT1100
- SafeNet Reader K1100

Secure PIN Pad Readers:

SafeNet Authentication Client 10.4 (GA) supports the following PIN pad readers:

- Gemalto IDBridge CT700
- Gemalto IDBridge CT710
- Ezio Shield Pro
- Ezio Bluetooth Reader
- Ezio BLE

NOTE: The Secure PIN Pad readers listed above are subject to limitations. Certain readers may not fully support all Smartcards. See the Administrator Guide for full details of supported Smartcard and PIN Pad reader combinations.

Tablets

- Lenovo ThinkPad Tablet running Windows 8.
- Microsoft Surface Pro 4 running Windows 8.1 and Windows 10.

Localizations

SafeNet Authentication Client 10.4 (GA) Windows supports the following languages:

• Chinese (Simplified) • Chinese (Traditional)	• Hungarian • Italian	• Romanian • Russian

• Czech • English • French (Canadian) • French (European) • German	• Japanese • Korean • Lithuanian • Polish • Portuguese (Brazilian)	• Spanish • Thai • Vietnamese • Turkish

NOTE:

- When using IDPrime MD, .Net cards and eToken 5110 CC, the user PIN and Admin Pin can be in English only.
- IDPrime features are available in English localization only (e.g. Initializing Common Criteria devices and PIN Pad functionality).

Compatibility with Gemalto Applications

IDPrime MD cards can be used with the following products:

- Gemalto Bluetooth Device Manager (GBDM) (V3.1)
- IDGo 800 Credential Provider (V1.2.4)
- IDGo 800 User Tool for Windows (V1.1.30)
- IDGo 800 Cert Tool (V 1.0.7)
- IDGo 800 Minidriver (V 1.2.10) (dll – V 8.5.0.7)
- Classic Client (V 6.3.12)
  For more information refer to the compatibility guide *Using SafeNet Authentication Client with IDGo 300.*
- eSigner (V 6.5.0)

To work with these products, install IDGo 800 Minidriver by generating an .msi file using the SAC Customization Tool. See the SafeNet Authentication Client 10.4 (GA) Administrator Guide for more details on how to generate the MSI installation file.

SafeNet Authentication Client can be used with the following products:

- SafeNet Network Logon 8.3
- SafeNet Authentication Manager 9.0 (Gemalto IDPrime MD 840 / 3840 and .Net devices are not supported on this version of SAM).

Installing SAC with eToken SafeNet Network Logon 8.3

When installing SafeNet Authentication Client together with SafeNet Network Logon, perform the tasks in the following order:

1. Install SafeNet Authentication Client.
2. Install SafeNet Network Logon.
3. You may be required to restart the computer.

NOTE: When installing SAC together with SafeNet Network Logon, you must install SAC as a *Custom* installation (instead of *Typical*) and enable the eTSapi component.

Compatibility with Third-Party Applications

Most of the third-party applications listed below have been validated and tested with SafeNet Authentication Client 10.4 (GA).

Solution Type	Vendor	Product Version
Remote Access VPN	Check Point	Client E-80 (Security Gateway)
	Microsoft	Windows Server 2008 SP2 and later
	Cisco	NAM
		AnyConnect
	Palo Alto	PA-200 GW Appliance
	Juniper	Juniper MAG 2600 GW Appliance
Virtual Desktop Infrastructure (VDI)	Citrix	XenApp/XenDesktop 7.9
	Microsoft	Remote Desktop
	VMware View	Horizon 7.0
Identity Access Management (IAM) Identity Management (IDM)	IBM	ISAM for Web 9.0 (eToken only)
	Intercede	MyID (eToken only)
	Microsoft	MIM 2016
	IDnomic	OpenTrust CMS 4.9.1
Pre Boot Authentication (PBA)	Sophos	SafeGuard Easy (eToken only)
	Microsoft	BitLocker (RSA only)
Certificate Authority (CA)	Entrust	SMA 8.1 (eToken only)
	Check Point (Local CA)	For All Check Point platforms
	Microsoft (Local CA)	For All Windows platforms
Local Access	Microsoft	All supported OS
	Evidian	ESSO (eToken only)
Digital Signatures	Entrust	ESP 9.2 (eToken only)
	Adobe	Reader XI and DC
	Microsoft	Outlook 2010 and 2013
	Mozilla	Thunderbird 45

Installation and Upgrade Information

Installation

SafeNet Authentication Client must be installed on each computer on which IDPrime MD 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

For earlier versions of SafeNet Authentication Client, it is recommended that an upgrade is performed to the latest version on each computer that uses a Token or Smart Card. Local administrator rights are required to upgrade SafeNet Authentication Client.

Gemalto customers migrating from IDGo 800 must uninstall their version of IDGo 800 and install SafeNet Authentication Client 10.4 (GA).

For more Installation and Upgrade details, see the SafeNet Authentication Client 10.4 (GA) Administrator Guide.

Resolved Issues

Issue	Synopsis
ASAC-5860	SAC was not compatible with Credential Guard when code integrity was enabled.
ASAC-5349	eToken 7300 crashed during the initialization process.
ASAC-5209	When initializing an IDPrime MD 840 on SAC 10.3.25 and the “Use the same token and administrator passwords for digital signature operation” feature was selected, a general error occured.
ASAC-5184	It was not possible to set the “Must change password on first logon’ Field on an IDPrime MD 840 device with PKCS#11 extension.
ASAC-5177	Windows logon showed latency when an IDPRime MD 830 RevB card was used with SAC.
ASAC-5167	When trying to generate an RSA key pair on IDPrime MD 840 CSP via PKCS#11, errors were reported.
ASAC-5157	When using the Single Logon Timeout feature SAC remains logged on even after the timeout count is exceeded.
ASAC-4779	SAC prompted for a PIN Pad reader even though the card did not support PIN Pad.
ASAC-2643	After changing the virtual reader settings, a general error message appeared.

Known Limitations

Issue	Synopsis
ASAC-4872	IDPrime MD 840 and eToken 5110 CC do not support history size of Password Quality.

Issue	Synopsis
ASAC-4531	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	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	SafeNet eToken 5110 FIPS does not support RSA 1024 and SHA1 on board, as per FIPS/NIST regulations.
ASAC-3980	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.
ASAC-3769	The following PIN pad limitations exist: • SC Logon via eToken CSP (not supported) Customer must use Minidriver • Common Criteria Linked mode (not supported) A security contradiction exists whereby the PIN pad provides high protection, but linked mode reduces the security. • 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-2320	When 'Smart Card is required for interactive logon' is enabled, the ‘Synchronize with Domain Password’ feature of SAC is not supported (domain passwords cannot be changed when this option is enabled).

Known Issues

Issue	Synopsis
ASAC-5306	**Summary:** When trying to log onto a locked device, two messages are shown instead of one. **Workaround:** Close both windows.
ASAC-5201	**Summary:** When connecting a non-Pin Pad reader, an incorrect message is displayed in the event viewer. **Workaround:** To disable minidriver PinPAD support, create a REG_DWORD value called "NoPinPad" under the key `HKEY_LOCAL_MACHINE\SOFTWARE\SafeNet\Authentication\SAC\General` and set its value to 1. On 64-bit machines, you additionally need to do the same under the key: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\SafeNet\Authentication\SAC\General`
ASAC-4950	**Summary**: When an incorrect token password is entered on Metro IE: • The “Incorrect Token Password” message is not displayed. • The retries counter is decreased by 1. • The Token Logon window remains displayed. **Workaround**: If the **Token Logon** window remains displayed after a token password is submitted, assume that the password entered was incorrect. You can use SAC Tools to see the number of remaining retries.
ASAC-4516	Generating a customized .msi file with a previous xml file (taken from an earlier SAC version) is not supported. **Workaround:** Make sure you create a new configuration with the same settings in the current SAC version.
ASAC-4504	**Summary:** When rebooting a PC after placing an IDPrime 3811 MD contactless card on a reader, the following error message appears: “No valid certificates were found on this smart card….”. **Workaround:** Remove the card and then place it back on the reader, the certificate will be seen, and may be used.
ASAC-4497	**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-4479	**Summary:** When inserting an IDPrime MD card that contains a new certificate friendly name, SAC displays the order of the messages incorrectly. **Workaround:** None.
ASAC-4469	**Summary:** Aborting an import certificate operation (in the middle of the process) while working with a Pin Pad reader, SAC Tools ignores the request to abort and continues with the import certificate operation. **Workaround:** Press cancel on the ‘Import Certificate’ window to abort the import certificate operation.

Issue	Synopsis
ASAC-4141	**Summary:** During the unblock operation, no other application can access the device until the unblock operation is finished or canceled. **Workaround:** None.
ASAC-4116	**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-4024	**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-3451 ASAC-2278 ASAC-2221 ASAC-1675	**Summary:** Upgrading from previous versions to SAC 10.4 (while a token is connected with Smart Card Logon, MS certificate or SNL profile), caused the session to lock the upgrade process automatically and the upgrade process to fail. **Workaround:** Run the following command to upgrade from previous SAC versions to SAC 10.4: `msiexec /i C:\SafeNetAuthenticationClient-x32-10.4.msi PROP_FAKEREADER=128`
ASAC-3449	**Summary**: When generating an MSI file using the SAC Customization Tool, the eToken.dll file is run over by the eTokenMD.dll when selecting IDGO 800 Minidriver. **Workaround**: Select eToken CSP\KSP provider when using eToken Devices.
ASAC-3112	**Summary**: The SAC token login window on IE11 freezes when the Enhanced Protected Mode feature is on. **Workaround**: Move the mouse cursor to the window and click inside the text box, or disable the Enhanced Protected Mode feature.
ASAC-2653	**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.

Issue	Synopsis
ASAC-2429	**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. **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
ASAC-2299	**Summary:** SafeNet Virtual devices that are locked to flash, and were enrolled on SafeNet Authentication Manager using a USB 3 port, cannot function on a USB 2 port, and vice versa. **Workaround:** If the SafeNet Virtual Token was enrolled on a USB 3 port, then use the token on a USB 3 port only. If the SafeNet Virtual Token was enrolled on a USB 2 port, then use the token on a USB 2 port only.
ASAC-2298	**Summary:** Connection problems occur when SafeNet Virtual devices are locked to flash and enrolled on a VMware environment. **Workaround:** When using a SafeNet Virtual device that is locked to flash, make sure the device is enrolled on a regular environment and not VMware.
ASAC-2295	**Summary:** SAC 9.0 does not support legacy GA configuration profiles. **Workaround:** Create new profiles using SAC 9.0 Customization Tool.
ASAC-2284	**Summary:** When a user attempts to generate a customized SAC msi file with no administrator privileges, the process fails. **Workaround:** Create customized SAC msi file with administrator privileges.
ASAC-2146	**Summary:** The process of creating a signed customized MSI with the Customization Tool takes a while. **Workaround:** Wait for the process to end.
ASAC-1992	**Summary:** Repartitioning the eToken 7300 device with a token password configured with **Maximum usage period** and **Expiration warning period**, the repartition process fails. **Workaround:** Initialize the token.

Issue	Synopsis
ASAC-1740 ASAC-2262	**Summary:** Scenario 1 - When using jarsigner.exe to sign JAR files, the jarsigner command fails to respond for a while. Scenario 2 - When performing an Identrust enrollment on Windows Server 2008, Windows 7 or Windows Server 2008 R2, the enrollment fails. **Cause:** In Windows 7 Windows Server 2008 and Windows Server 2008 R2, when an application using a smartcard has been terminated unexpectedly, it causes other applications that try to connect to the smartcard to stop responding. This occurs in both local and RDP environments. This is a Microsoft issue. Microsoft have released Hotfixes that resolve this issue. **Workaround:** Download the following two hotfixes from Microsoft: Local Scenario: http://support.microsoft.com/kb/2427997 RDP: http://support.microsoft.com/kb/2521923
ASAC-1722	**Summary**: When running the repair option from the MSI file wizard, the operation fails. **Workaround**: Use the repair option by going to **Control Panel > Add Remove Programs**.
ASAC-1702	**Summary**: When the application runs as a service without the Local System Account permissions, smart card communication fails. **Workaround**: Make sure the service runs with the Local System Account permissions by adding it manually. This is a Microsoft by-design known issue. For more details refer to the following Microsoft support ticket number: 114092811845001.
ASAC-1470	**Summary:** After updating the FW on an eToken 7300, the FW version might not be updated under Token information in SAC Tools. **Workaround:** Restart the machine.
ASAC-1419	**Summary:** When installing SAC via the GPO, SAC is installed successfully on the client computer but the tray icon doesn't appear. **Workaround:** Restart the client computer.
ASAC-1335	**Summary:** Mass storage options using an eToken 7300 protected token are not supported within an RDP session. **Workaround:** None.
ASAC-862	**Summary:** When a partitioned eToken 7300 device is connected, the SafeNet drive eToken 7300 icon is displayed on the desktop but double-clicking it does not open the device's drive. **Workaround:** Open the drive from the computer's directory window.
ASAC-819	**Summary:** When the MS KB http://support.microsoft.com/kb/2830477 is installed in a Windows 7 environment, you are prompted for the token password when you start the RDP. But after entering the remote machine, you are prompted for the standard user name and password. **Workaround:** Uninstall the MS KB.

Issue	Synopsis
ASAC-800	**Summary:** If the token was initialized as Common Criteria: • The Challenge Code created during the Unlocking procedure is 13 characters, not 16 characters as expected. • The Response Code created during the Unlocking procedure is 39 characters, not 16 characters as expected. **Workaround:** When unlocking a CC token, the user must be sure to copy the entire **Response Code** string.
AHWENG - 775	**Summary:** When a protected eToken 7300 is connected with the flash partition accessible, the flash partition may not be accessible after returning from sleep mode. **Workaround:** Disconnect and reconnect the device.
ASAC-446	**Summary:** SAC interfered with Citrix's debugging application. **Workaround:** Use Citrix' "Hotfix Rollup Pack 2 for Citrix XenApp 6.5 for Microsoft Windows Server 2008 R2", found at http://support.citrix.com/article/CTX136248.
ASAC-378	**Summary:** Smart card logon is not supported by default when using tokens with ECC certificates. **Workaround:** Perform the following: In the **Local Group Policy Editor**, under **Local Computer Policy\Administrative Templates\Windows Components\Smart Card**, enable **Allow ECC certificates to be used for logon and authentication**.
ASAC-281	**Summary:** Upon successful eToken 7300 partitioning, a Microsoft Windows message opens prompting you to format the disk. **Workaround:** Click **Cancel** to close the message window.
ASAC-277 ASAC-525	**Summary:** The SAC installation does not load the PKCS#11 module for 32-bit Firefox on a 64-bit OS. **Workaround:** Use 64-bit Firefox, or load the 32-bit PKCS#11 module manually from the **System32** folder.
SACINT-38	**Summary:** Unable to sign a Word document via Office 365 (Office on Demand) using SAC. **Workaround:** Open the saved document from the local machine itself. This enables you to sign the document successfully.

Known Issues – Deprecated Devices

Issue	Synopsis
ASAC-4326	**Summary:** The iKey reader is not installed when upgrading to SAC 10.4. **Workaround:** Uninstall SAC and re-install SAC 10.4.
ASAC-1315	**Summary:** When working with SafeNet smart cards SC330u, iKey 2032u, SC400, and iKey 4000 using SAC Tools, the number of unblocking code retries remaining cannot be changed , unless the token or smart card are locked. (i.e. there is no way of determining how many unblocking code retries remain). **Workaround:** None. This is by design.

ROCA Vulnerability Solution

The IDGo 800 Minidriver v1.2.10 implements a solution to the recently published vulnerability CVE-2017-15361, commonly referred to as ROCA (https://cve.mitre.org/cgi-bin/cvename.cgi?name=CVE-2017-15361), which has an impact on the end of life of IDPrime .NET cards, depending on the customer use case.

For more details, please refer to the related Gemalto security bulletin:

https://safenet.gemalto.com/technical-support/security-updates/

Gemalto is proposing different technical options to address the different implementations and use cases of our customers.

This release note refers to a temporary workaround which is available with this updated version of the IDGo 800 v1.2.10 Minidriver (available via the SAC 10.4 Post GA Customization Tool), which supports the ability to generate keys on the local computer and push them into the smart card. This workaround is intended for cases when the CMS (for instance Microsoft FIM) cannot generate all the types of keys on the server. When using this version 1.2.10 of the Minidriver, it behaves differently: when it receives a CMS request to generate keys on-board, it actually generates the keys on the local computer and pushes them into the smart card. The keys are then secured within the smart card.

Please be aware that this is a temporary solution that should be used only as an intermediate step as part of a migration plan to IDPrime MD, and only after evaluating the risks & limitations of using this approach in each specific customer environment.

NOTE: This workaround is designed to affect only the IDPrime .NET smart cards and does not affect other Gemalto smart cards (IDPrime MD).

The PKCS#11 library is unchanged. We recommend that you contact your PKCS#11 based CMS provider to identify the CMS settings to create the keys out of the smart card.

Technical Description - RSA Local Key Generation (outside of the IDPrime .NET Smart Card)

This new RSA Local Key Generation mechanism uses the CNG API implemented by bcryptprimitives.dll and exposed through bcrypt.dll which is FIPS 140-2 validated on Windows 7 and later (see https://technet.microsoft.com/en-us/library/cc750357.aspx##IDFVCM).

The RSA Local Key Generation mechanism functions as follow:

- The minidriver explicitly loads the dll bcrypt.dll from Windows system directory (usually C:\Windows\System32) and retrieves BCrypt API entry points. This ensures that the legitimate FIPS implementation is used.
- An RSA keypair with the requested size is generated using BCryptGenerateKeyPair.
- The keypair is exported using BCryptExportKey and then injected into the .NET card using key import mechanism.
- All keypair materials are securely erased from memory and BCrypt API context is properly cleared.

Registry Settings - Enabling BCrypt RSA Local Key Generation in the SAC 10.4 (Post GA) IDGo 800 Compatible Mode

The **DotNetOBKGType** registry key has been introduced to securely generate RSA keypairs using BCrypt API and import them to IDPrime.NET cards instead of using On Board Key Generation.

On Windows 32-bit and Windows 64-bit systems, create DotNetOBKGType (DWORD) registry entry under:

HKEY_LOCAL_MACHINE\SOFTWARE\Gemalto\Cryptography\Minidriver

Additionally on Windows 64-bit this entry should also be created under:

HKEY_LOCAL_MACHINE \SOFTWARE\Wow6432Node\Gemalto\Cryptography\Minidriver

DotNetOBKGType:

This key enables the generation of the RSA keypairs 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 keypairs 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 keypairs using the BCrypt API on the local computer and keys are imported into the IDPrime .NET smart card.

- Type: REG_DWORD
- Value:
  - 1 to enable generation of RSA key pairs using the BCrypt API on the local computer before import to the IDPrime.NET cards.
  - 0 or absent (default) On Board Key Generation remains active as before

Product Documentation

The following product documentation is associated with this release:

- 007-013560-004_SafeNet Authentication Client 10.4 Windows (GA) Administrator Guide
- 007-013561-004_ SafeNet Authentication Client 10.4 Windows (GA) User Guide

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.

Contact Method	Contact Information
Customer Support Portal	https://supportportal.gemalto.com Existing customers with a Technical Support Customer Portal account can log in to manage incidents, get the latest software upgrades, and access the Gemalto Knowledge Base.
Technical Support contact email	technical.support@gemalto.com