All information herein is either public information or is the property of and owned solely by Gemalto and/or its subsidiaries who shall have and keep the sole right to file patent applications or any other kind of intellectual property protection in connection with such information.

Nothing herein shall be construed as implying or granting to you any rights, by license, grant or otherwise, under any intellectual and/or industrial property rights of or concerning any of Gemalto’s information.

This document can be used for informational, non-commercial, internal and personal use only provided that:

- The copyright notice below, the confidentiality and proprietary legend and this full warning notice appear in all copies.
- This document shall not be posted on any network computer or broadcast in any media and no modification of any part of this document shall be made.

Use for any other purpose is expressly prohibited and may result in severe civil and criminal liabilities.

The information contained in this document is provided “AS IS” without any warranty of any kind. Unless otherwise expressly agreed in writing, Gemalto makes no warranty as to the value or accuracy of information contained herein.

The document could include technical inaccuracies or typographical errors. Changes are periodically added to the information herein. Furthermore, Gemalto reserves the right to make any change or improvement in the specifications data, information, and the like described herein, at any time.

Gemalto hereby disclaims all warranties and conditions with regard to the information contained herein, including all implied warranties of merchantability, fitness for a particular purpose, title and non-infringement. In no event shall Gemalto be liable, whether in contract, tort or otherwise, for any indirect, special or consequential damages or any damages whatsoever including but not limited to damages resulting from loss of use, data, profits, revenues, or customers, arising out of or in connection with the use or performance of information contained in this document.

Gemalto does not and shall not warrant that this product will be resistant to all possible attacks and shall not incur, and disclaims, any liability in this respect. Even if each product is compliant with current security standards in force on the date of their design, security mechanisms' resistance necessarily evolves according to the state of the art in security and notably under the emergence of new attacks. Under no circumstances, shall Gemalto be held liable for any third party actions and in particular in case of any successful attack against systems or equipment incorporating Gemalto products. Gemalto disclaims any liability with respect to security for direct, indirect, incidental or consequential damages that result from any use of its products. It is further stressed that independent testing and verification by the person using the product is particularly encouraged, especially in any application in which defective, incorrect or insecure functioning could result in damage to persons or property, denial of service or loss of privacy.

© 2010 - 2017 Gemalto. All rights reserved. Gemalto and the Gemalto logo are trademarks and service marks of Gemalto and/or its subsidiaries and are registered in certain countries. All other trademarks and service marks, whether registered or not in specific countries, are the property of their respective owners.

**Document Number:** 007-012690-001, Rev. B  
**Release Date:** October 2017
Contents

Third-Party Software Acknowledgement .................................................................................. 4
Description .......................................................................................................................... 4
Applicability ........................................................................................................................ 5
Environment ......................................................................................................................... 5
Audience ............................................................................................................................... 5
Authentication Flow ............................................................................................................. 6
Prerequisites .......................................................................................................................... 7
Supported Tokens and Smart Cards in SafeNet Authentication Client .................................. 7
Configuring BitLocker .......................................................................................................... 8
Running the Solution ........................................................................................................... 11
    Enabling BitLocker and Encrypting a Drive .................................................................... 11
    Unlocking the Drive ....................................................................................................... 25
Appendix ................................................................................................................................ 31
Support Contacts .................................................................................................................. 42
    Customer Support Portal ............................................................................................... 42
    Telephone Support ........................................................................................................ 42
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as BitLocker.

Material from third-party software is being used solely for the purpose of making instructions clear. Screen images and content obtained from third-party software will be acknowledged as such.

Description

SafeNet Authentication Client (SAC) is a 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. SAC enables the implementation of strong two-factor authentication using standard certificates, as well as encryption and digital signing of data. The SAC generic integration with CAPI, CNG, and PKCS#11 security interfaces enables out-of-the-box interoperability with a variety of security applications, offering security for web access, network logon, email, and data. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

BitLocker (formerly BitLocker Drive Encryption) is a full-disk encryption feature included with the Ultimate and Enterprise editions of Windows Vista and Windows 7, the Pro and Enterprise editions of Windows 8 and Windows 8.1, and Windows Server 2008 and later. BitLocker protects data by providing encryption for entire volumes. By default, BitLocker uses the AES encryption algorithm in cipher block chaining (CBC) mode with a 128-bit or 256-bit key, and can be combined with the Elephant diffuser for additional disk encryption-specific security, which is not provided by AES. CBC is not used over the entire disk, but rather for each disk sector.

An effective strong authentication solution must be able to address data breaches on the rise for companies to protect their information assets and comply with privacy regulations. Data encryption is a common technique used by enterprises today, but to be most effective, it must be accompanied by strong two factor user authentication to desktop, mobile, and laptop computer applications. Working together, encryption and authentication reduce risk and stop unauthorized access to sensitive data.

SafeNet smart card certificate-based tokens and secure USB certificate-based tokens are interoperable with BitLocker, providing a solution for encryption and strong access control that prevents unauthorized access to sensitive data and stops information loss and exposure. The integrated solution delivers greater security, reduced operational costs, and improved compliance by adding smart card-based strong user authentication to BitLocker.

Gemalto’s X.509 certificate-based USB tokens and smart cards have been integrated with BitLocker, providing two-factor authentication at both pre-boot and Microsoft Windows levels.

The Gemalto’s X.509 certificate-based USB tokens and smart cards provide secure storage for the certificates needed for endpoint encryption for BitLocker functionality to boot up. If Gemalto’s X.509 certificate-based USB token or smart card is not inserted in the client machine, or if the certificates are deleted, revoked, or expired, the BitLocker software will not boot up and the data on the laptop will stay encrypted and secure.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to BitLocker using Gemalto tokens or smart cards.

It is assumed that the BitLocker environment is already configured and working with static passwords prior to implementing Gemalto multi-factor authentication.

BitLocker can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with Gemalto products.
Applicability

The information in this document applies to:

- **SafeNet Authentication Client (SAC) Typical installation mode** - SafeNet Authentication Client is public key infrastructure (PKI) middleware that manages Gemalto’s tokens and smart cards.

- **SafeNet Authentication Minidriver Package** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

- This document is intended for system administrators who are familiar with BitLocker, and those who are interested in adding certificate-based authentication (CBA) using SAC.

For more details about different SAC installation modes, please refer to the *Customization* section in the *SafeNet Authentication Client Administrator Guide*.

Environment

The integration environment that was used in this document is based on the following software versions:

- **SafeNet Authentication Client (SAC) Typical installation mode** – 10.4
- **SafeNet Authentication Minidriver Package** - 10.4
- **Windows Server 2008R2** – Active Directory and Certificate management installed

Audience

This document is targeted to system administrators who are familiar with BitLocker, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.
Authentication Flow

The diagram below illustrates the flow of certificate-based authentication for BitLocker using Smart card/Tokens:

1. The user wants to access the encrypted drive.

2. The user connects the Smart Card/Token containing the certificate.

3. The user enters the Smart card /Token pin and then the certificate on the Token/smart card is validated.

4. On successful authentication the user can log into the encrypted drive.
Prerequisites

To enable users to perform pre-boot authentication with BitLocker using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate through pre-boot from the BitLocker environment with a static password before configuring the BitLocker to use Gemalto tokens and smart cards.
- If SafeNet Authentication Manager (SAM) is used to manage the tokens, Token Policy Object (TPO) must be configured with MS CA connector. For further details, refer to the section "Connector for Microsoft CA" in the SafeNet Authentication Manager Administrator’s Guide.
- Users have a Gemalto token or smart card with valid certificate enrolled on it with the same object identifier (OID) that matches the OID configured for BitLocker.
- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. In general, any CA can be used. However, in this guide, integration is demonstrated using Microsoft CA.
- SafeNet Authentication Client (10.4) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.4) supports the following tokens and smart cards:

Certificate-based USB tokens
- SafeNet eToken 5110 GA
- SafeNet eToken 5110 FIPS
- SafeNet eToken 5110 CC

Smart Cards
- Gemalto IDPrime MD 830
- Gemalto IDPrime MD 840

For a list of all supported devices please refer to SafeNet Authentication Client Customer Release Notes.
Configuring BitLocker

Complete the procedures in this section to configure BitLocker for two-factor authentication so users can authenticate using certificates on their smart cards or eTokens.

Configuring Group Policies for BitLocker

1. To open the Local Group Policy Editor, from the Windows Start menu, in the Run box or Search programs and files box, type gpedit.msc.

2. On the Local Group Policy Editor window, select Local Computer Policy > Computer Configuration > Administrative Templates.

4. In the right panel, double-click **Validate smart card certificate usage rule compliance**

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
5. Perform the following steps:

- **Click Enabled.**
- In the **Object identifier** field, enter the certificate's object identifier (in this example: 1.3.6.1.4.1.311.67.1.1), and then click **OK**.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

---

**NOTE**: The Smart Card Certificate contains the same **Object identifier**.
Running the Solution

Enabling BitLocker and Encrypting a Drive

Windows 10

In this example Windows 10 Version 1607 is demonstrated.

1. Open **My Computer**.

2. Right-click the drive to be encrypted, and then select **Turn on BitLocker**.

3. Connect the smart card or eToken containing the certificate.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
4. On the **BitLocker Drive Encryption** window, select **Use my smart card to unlock the drive**, and then click **next**.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
5. Select one of the following backup methods for the recovery key, and then click **Next**:

- **Save to a file** - Save the key as a file in a folder on another drive on your computer that will not be encrypted.

- **Print the recovery key** - Print a hard copy of the recovery key.

![Screen image](image.png)

*(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).*
6. Select one of the following drive encryption options, and then click Next.
   - Encrypt used disk space only (faster and best for new PCs and drives)
   - Encrypt entire drive (slower but best for PCs and drives already in use)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
7. Choose one of the following encryption modes:
   - **New encryption mode (best for fixed devices on this device)**
   - **Compatible mode (best for drives that can be moved from this device)**

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
8. When you are ready to encrypt the drive, click **Start encrypting**.

![Start encrypting dialog](image)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

9. When encryption is complete, click **Close**.

![Encryption complete](image)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

10. Restart the machine to activate locking of the encrypted drive.
Windows 8.1

1. Open Windows My Computer.
2. Right-click the drive to be encrypted, and then select Turn on BitLocker.

![Windows 8.1 My Computer window with BitLocker Drive Encryption option](image)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

3. Connect the smart card or eToken containing the certificate.
4. On the BitLocker Drive Encryption window, select Use my smart card to unlock the drive, and then click next.

![BitLocker Drive Encryption window](image)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
5. Select one of the following methods for the recovery key, and then click **Next**:

- **Save to a file** - saves the key as a file in a folder on another drive on your computer that will not be encrypted.

- **Print the recovery key** - prints a hard copy of the recovery key.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
6. Select one of the following drive encryption options, and then click **Next**.

- **Encrypt used disk space only (faster and best for new PCs and drives)**
- **Encrypt entire drive (slower but best for PCs and drives already in use)**

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
7. When you are ready to encrypt the drive, click **Start encrypting**.

8. When encryption is complete, click **Close**.

9. Restart the machine to activate locking of the encrypted drive.
Windows 7

1. Open Windows My Computer.
2. Right-click the drive to be encrypted, and then select Turn on BitLocker.

3. Connect the smart card or eToken containing the certificate.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
4. On the **BitLocker Drive Encryption** window, select **Use my smart card to unlock the drive**, and then click **next**.

![BitLocker Drive Encryption window](image1)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

5. When the **Insert Smart Card** window opens, click **Cancel**

![Insert Smart Card window](image2)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
NOTE: When backwardly compatible IDGo 800 is installed, the Insert Smart Card prompt does not appear. Just click Next.

6. Select one of the following methods for the recovery key, and then click Next:

- **Save the recovery key to a file** - saves the key as a file in a folder on another drive on your computer that will not be encrypted.

- **Print the recovery key** - prints a hard copy of the recovery key.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
7. When you are ready to encrypt the drive, click **Start encrypting**.

![Start Encrypting](Image)

*(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).*

8. When encryption is complete, click **Close**.

![Encryption Complete](Image)

*(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).*

9. Restart the machine to activate locking of the encrypted drive.
Unlocking the Drive

Windows 8.1 and Windows 10

In this example Windows 10 Version 1607 and Windows 8.1 follow the same steps.

Before proceeding, make sure that SafeNet Authentication Client is installed on the client machine.

1. Open Windows My Computer.
2. Right-click the encrypted drive and click Unlock Drive.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
3. Connect the smart card or eToken to the machine, and then click **Use smart card**.

![Image of smart card connection](image)

*(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners)*.

4. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

**SafeNet Authentication Client**

![Image of token logon window](image)
SafeNet Minidriver Package:

If the credentials are valid, the contents of the drive are displayed.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
Windows 7

Before proceeding, make sure that SafeNet Authentication Client is installed on the client machine.

1. Open Windows My Computer.
2. Right-click the encrypted drive and click Unlock Drive.

3. Connect the smart card or eToken to the machine, and then click Unlock.
4. When the **Insert Smart Card** window opens, click **Cancel**

![Insert Smart Card Window](image)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

**NOTE**: When backwardly compatible IDGo 800 is installed, the *Insert Smart Card* prompt does not appear. Just click **Next**.

5. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

![SafeNet Authentication Client](image)
SafeNet Minidriver Package

If the credentials are valid, the contents of the drive are displayed.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
Appendix

Using Self-Signed Certificates

In this example, Windows 10 Version 1607 is demonstrated. BitLocker can be used with self-signed certificates on stand-alone SAC clients.

Enrolling a Self-signed Certificate on the Smart Card or eToken

To enroll a self-signed certificate on the SafeNet eToken so that it can be used with BitLocker:

1. From the Windows Start menu, open Control Panel.
2. Search on the keyword, encryption, and then select Manage file encryption certificates.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
3. On the Encrypting File System window, click **Next**.

4. Select **Create a new certificate**, and then click **Next**.

5. Connect the Token/Smart Card

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
6. Select **Make a self-signed certificate and store it on my smart card**, and then click **Next**.

![Image](image1.png)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

7. On the **Token Logon** window (**SafeNet Authentication Client** or **SafeNet Minidriver Package**), enter the eToken password or PIN in the **Token Password** field, and then click **OK**.

![Image](image2.png)
SafeNet Minidriver Package:

A self-signed certificate will be generated on the eToken

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
8. After the certificate is created, do one of the following and click **Next**.
   - Under **Folders**: select previously encrypted files and folders to switch to your new certificate and key.
   - Select **I'll update my encrypted files later** to use the self-signed certificate only for BitLocker.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
9. Enter the eToken/Smart card password or PIN in the **Token Password** Click **OK**

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).

The wizard confirms the creation of the certificate.

10. Click **Close** to exit the wizard

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
Configuring Group Policies for BitLocker

1. Open the Local Group Policy Editor - from the Windows Start menu, in the Run box or Search programs and files box, type `gpedit.msc`.

2. On the Local Group Policy Editor window, select Local Computer Policy > Computer Configuration > Administrative Templates.

![Local Group Policy Editor](image1.jpg)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).


![Local Group Policy Editor](image2.jpg)

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
4. In the right panel, double-click **Validate smart card certificate usage rule compliance**.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
5. Perform the following steps:

- **Click Enabled**
- Enter the **Object identifier** setting to match the object identifier of the certificate you just created (in this example the OID for EFD certificate is 1.3.6.1.4.1.311.10.6.4)
- **Click OK** to apply the settings.

(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners).
Allowing Self-signed Certificates

By default, self-signed certificates are not allowed with BitLocker.

To enable the use of self-signed certificates, perform the following steps:

1. From the Windows Start menu, in the Run box, type **regedit.exe**, and then click **OK**.

   ![Image of regedit.exe](image1.png)

   *(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners.)*

2. Browse to **HKEY_LOCAL_MACHINE\SOFTWARE\Policies\Microsoft**, and then right-click **Microsoft**.

   ![Image of Registry Editor](image2.png)

   *(The screen image above is from Microsoft Corporation®. Trademarks are the property of their respective owners.)*
3. Select **New > Key**, and then name the key **FVE**. (If Key FVE already exists, skip this step).

4. Right-click **FVE**.

5. Select **New > DWORD (32-bit) Value**, name the value **SelfSignedCertificates**, and then enter a value of 1.

6. Close the Registry Editor.
Support Contacts

If you encounter a problem while installing, registering, or operating this product, refer to 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 a 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 Customer Support by telephone. Calls to Customer Support are handled on a priority basis.

<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Global</td>
<td>+1-410-931-7520</td>
</tr>
<tr>
<td>Australia</td>
<td>1800.020.183</td>
</tr>
</tbody>
</table>
| China   | North: 10800-713-1971  
<pre><code>       | South: 10800-1301-932 |
</code></pre>
<p>| France  | 0800-912-857     |
| Germany | 0800-181-6374    |
| India   | 000.800.100.4290 |
| Israel  | 180-931-5798    |
| Italy   | 800-786-421     |
| Japan   | 0066 3382 1699  |</p>
<table>
<thead>
<tr>
<th>Region</th>
<th>Telephone number</th>
</tr>
</thead>
<tbody>
<tr>
<td>Korea</td>
<td>+82 2 3429 1055</td>
</tr>
<tr>
<td>Netherlands</td>
<td>0800.022.2996</td>
</tr>
<tr>
<td>New Zealand</td>
<td>0800.440.359</td>
</tr>
<tr>
<td>Portugal</td>
<td>800.863.499</td>
</tr>
<tr>
<td>Singapore</td>
<td>800.1302.029</td>
</tr>
<tr>
<td>Spain</td>
<td>900.938.717</td>
</tr>
<tr>
<td>Sweden</td>
<td>020.791.028</td>
</tr>
<tr>
<td>Switzerland</td>
<td>0800.564.849</td>
</tr>
<tr>
<td>United Kingdom</td>
<td>0800.056.3158</td>
</tr>
<tr>
<td>United States</td>
<td>(800) 545-6608</td>
</tr>
</tbody>
</table>

(Subject to change. An up-to-date list is maintained on the Customer Support Portal)