SafeNet Authentication Client
Integration Guide

Using SafeNet Authentication Client CBA for Pulse Connect Secure
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 - 2018 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:** 007-012717-002 Rev. B  
**Release Date:** March 2018
## Contents

Third-Party Software Acknowledgement ................................................................. 4  
Description ................................................................................................................ 4  
Applicability ............................................................................................................... 5  
Environment ............................................................................................................. 5  
Audience ................................................................................................................... 5  
CBA Flow using SafeNet Authentication Client ...................................................... 6  
Prerequisites .............................................................................................................. 7  
Supported Tokens and Smart Cards in SafeNet Authentication Client .................. 7  
Configuring Pulse Connect Secure ......................................................................... 8  
  Certificate Configuration ....................................................................................... 8  
  Adding an Authentication Server ....................................................................... 11  
  Attaching Authentication Servers to User Realms ............................................ 12  
  Sign-in Policies .................................................................................................... 17  
  Configuring Pulse Connect Secure Client ........................................................ 21  
Running the Solution .............................................................................................. 23  
Support Contacts ..................................................................................................... 25  
  Customer Support Portal ...................................................................................... 25  
  Telephone Support .............................................................................................. 25
Third-Party Software Acknowledgement

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

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.

Pulse secure software enables dynamic SSL VPN connectivity, network access control (NAC), mobile security, and collaboration, through a simple end-user interface. It simplifies and optimizes connectivity to end users at the same time it check their device type and security state, location, identity, and adherence to corporate access control policies.

An effective strong authentication solution must be able to address ever more frequent data breaches, to protect a company’s 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 Pulse Connect Secure, 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 Pulse Connect Secure.

Gemalto’s X.509 certificate-based USB tokens and smart cards have been integrated with Pulse Connect Secure, 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 Pulse Connect Secure 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 Pulse Connect Secure 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 Pulse Connect Secure using Gemalto tokens or smart cards.

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

Pulse Connect Secure 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 Client (SAC) IDGo800 Compatible mode** - IDGo800 Minidriver based package, uses Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards.

- **Juniper SA MAG2600 appliance**

- **Pulse Connect Secure**

For more details about different SAC installation modes, 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)** - 10.5
- **Pulse Connect Secure** - 8.3R4 (60519)
- **Pulse Secure Windows installer Client** - 5.3.4 (1161)

Audience

This document is intended for system administrators who are familiar with Pulse Connect Secure, and are interested in adding multi-factor authentication capabilities during pre-boot using SafeNet tokens.
CBA Flow using SafeNet Authentication Client

The following diagram illustrates the flow of certificate-based authentication:

1. A user is required to authenticate to Juniper MAG2600 via the Pulse Secure application using a SafeNet certificate-based token. The SafeNet token is deployed with a user-unique client certificate for authentication. When the user is authenticated, they must provide a PIN to access the token.

2. After successful authentication, the user receives VPN/SSL access to the network.
Prerequisites

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

- Users can authenticate to the Pulse Connect Secure environment with a static password before configuring the Pulse Connect Secure 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.
- 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 (10.5) must be installed on all client machines.

Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (10.5) 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
- Gemalto IDCore 30B eToken

For all supported devices please refer to SafeNet Authentication Client Customer Release Notes.
Configuring Pulse Connect Secure

The configuration of Juniper with certificate-based authentication (CBA) requires the following:

- Certificate configuration
- Adding an authentication server
- Attaching an authentication server to user realms
- Sign-in Policies

Certificate Configuration

1. Open the Juniper Pulse Connect Secure web console (in this guide the Classic UI was Used).

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
2. In the left pane, under **System > Configuration**, click **Certificates**.

3. Under **Certificates**, select the **Trusted Client CAs** tab.
4. In the **Trusted Client CAs** list, import the root CA certificate by clicking **Import CA Certificate**.

   ![Import Trusted Client CA](image)

   (The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)

5. Browse to the root CA certificate and import by clicking **Import Certificate**.

   ![Import Trusted Client CA](image)

   (The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
Adding an Authentication Server

This section describes the creation of an authentication server. The authentication server will be configured with CBA support. Later, the authentication server will be set as the main authentication server of Juniper Pulse Connect Secure. This enables Juniper Pulse Connect Secure to be accessed with a certificate that is on a SafeNet token.

To configure the Authentication Server:

1. In the left pane, click Authentication > Auth. Servers.

2. In the New field, select Certificate Server, and then click New Server.
3. In the **Name** field, enter a rule name

4. In the **User Name Template** field, leave the default value.

5. Click **Save Changes**.

### Attaching Authentication Servers to User Realms

To use CBA, you must attach the authentication server’s policy created in the previous section to a user realm.

#### Create User realm

1. In the left pane, click **Users > User Realms**.
2. Under **User Authentication Realms**, click **New**.

3. In the **Name** field enter a name (in this example: **DomainUsers** is used)

4. Under **Servers**, in the **Authentication** field, select the authentication server you created in the previous section (**Demo CA**).

5. Click **Save Changes**.
6. In the left pane, click **Users > User Realms**, then click the user realm to be edited (in this Example **Domain Users**).

7. In the right pane, select the **Authentication Policy** tab.
8. In the Authentication Policy tab, click Certificate, and then select Only allow users with a client-side certificate signed by trusted client CAs to sign in.

9. Click Save Changes.

10. In the Role Mapping tab, select New Rule.
11. In **Role Mapping Rule** fill in the Below:
   
a. **Rule Based on.** In this example **Username** is demonstrated
b. **Name:** Enter rule name. In this example **Users** is demonstrated
c. **Under Rules:** if **username** is add user name. In this example **User Bob** is demonstrated
d. **Under then assign these roles** in this example user role **Users** (System created Users role) is demonstrated.

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
12. Click **Save Changes**.

The role was added successfully.

---

**Sign-in Policies**

Sign-in policy is a system rule that in this example specifies sign-in URL.

To configure a sign-in policy:

1. Select **Authentication > Signing In > Sign-In Policies**.
2. In the **Sign-In Policies** tab, click **New URL**.

![Sign-In Policies](image)

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
3. Complete the configuration as follows:
   a. **User type**: Select Users
   b. **Sign-in URL**: Enter a URL Format: `<host>/<path>/`  
      Use * as wildcard at the beginning of the host name. In this example: `*/DomainUsers/`
   c. **Sign-In Page**: leave default
   d. **Meeting URL**: leave default
   e. Under **Authentication Realm**, select **User picks from a list of authentication realms**.
   f. Under **Selected realms**, add the user realm created previously (in this example: **DomainUsers**).

![Screen Image](image.png)

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)

4. **Click Save Changes**.
A new user URL, **DomainUsers**, was added.

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
Configuring Pulse Connect Secure Client

In this example **Pulse Secure Installer** (Win x64) is demonstrated:

**Add Connection:**

1. Open pulse Secure and Click **Add connection**

![Pulse Secure Add Connection](image)

* (The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
2. Enter the fields as follows:
   **Type**: Leave default
   **Name**: Enter connection name (in this example CBA).
   **Server URL**: Use the format **Error! Hyperlink reference not valid.** For example: https://juniper.juniperdemo.com/DomainUsers/

3. Click **Add**.

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
Running the Solution

Prerequisite: Connected Token/Smartcard with Smart Card User certificate

1. On the new connection, in this example CBA, click Connect

2. In the SAC Token Logon window, enter Token Name and Token Password, and click OK.
The user is authenticated and a VPN connection is established

(The screen image above is from Pulse Connect Secure® software. Trademarks are the property of their respective owners.)
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></td>
<td>(Subject to change. An up-to-date list is maintained on the Customer Support Portal)</td>
</tr>
<tr>
<td>Global</td>
<td>+1-410-931-7520</td>
</tr>
<tr>
<td>Australia</td>
<td>1800.020.183</td>
</tr>
<tr>
<td>China</td>
<td>North: 10800-713-1971</td>
</tr>
<tr>
<td></td>
<td>South: 10800-1301-932</td>
</tr>
<tr>
<td>France</td>
<td>0800-912-857</td>
</tr>
<tr>
<td>Germany</td>
<td>0800-181-6374</td>
</tr>
<tr>
<td>India</td>
<td>000.800.100.4290</td>
</tr>
<tr>
<td>Israel</td>
<td>180-931-5798</td>
</tr>
<tr>
<td>Region</td>
<td>Telephone number</td>
</tr>
<tr>
<td>------------</td>
<td>------------------</td>
</tr>
<tr>
<td>Italy</td>
<td>800-786-421</td>
</tr>
<tr>
<td>Japan</td>
<td>0066 3382 1699</td>
</tr>
<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>