SafeNet Authentication Client
Integration Guide

Using SafeNet Authentication Client CBA for Wi-Fi Network
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:** 007-014051-001, Rev. A

**Release Date:** January 2018
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, in this case, Wi-Fi Network, Authenticated with an NPS Radius Server Role which is a Microsoft Windows component. 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.

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 Wi-Fi Network, 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 Wi-Fi Network.

Gemalto’s X.509 certificate-based USB tokens and smart cards have been integrated with Wi-Fi Network, 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 Wi-Fi Network 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 Wi-Fi Network 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 Wi-Fi Network using Gemalto tokens or smart cards.

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

Wi-Fi Network 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.

For more details about different SAC installation modes, please refer to the Customization section in *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)** - SAC 10.4 Post GA
- **TP-LINK 931F3E Wireless N router**
- **Windows Server 2008R2** installed with Active Directory, Certificate Authority, NPS Radius
- **Win 10 1703** - Installed on Laptop PC Domain Joined.

Audience

This document is targeted at system administrators who are familiar with Wi-Fi Network, 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 To Wi-Fi Network:

1. User connects a SafeNet Token containing the certificate.

2. User connects to the Wi-Fi network.

3. User enters the token password. The certificate on the token is validated.

4. On successful Authentication, the user can log in to the Wi-Fi network.

Prerequisites

To enable users to perform authentication to Wi-Fi Network using Gemalto tokens and smart cards, ensure the following:

- Users can authenticate to the Wi-Fi Network environment with a static password before configuring 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 a valid certificate enrolled.

- To use CBA, the Microsoft Enterprise Certificate Authority must be installed and configured. Any CA can be used. In this guide, integration is demonstrated using Microsoft CA.

- SafeNet Authentication Client (SAC 10.4 Post GA) must be installed on all client machines.
Supported Tokens and Smart Cards in SafeNet Authentication Client

SafeNet Authentication Client (SAC 10.4 Post GA) 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 all supported devices please refer to SafeNet Authentication Client Customer Release Notes.

Configuring NPS RADIUS Server

Complete the procedures in this section to configure CBA Authentication for two-factor authentication. Following configuration, users will be able to authenticate using certificates on their smart cards or tokens.

In this example: Network Policy Server in Windows Server is demonstrated as a RADIUS server.

Configure the Wi-Fi Device as RADIUS Client

1. Open the Network Policy Server Console. Under **Policies > Expand RADIUS Clients and Servers**, right-click **RADIUS Clients**, and click **New**.

   ![Screen image](image)

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

2. Enter the details of the Wi-Fi Device (In This Example: **TP-LINK**) and enter the following under **Settings**:
   - **Select Enable Radius Client**
   - **Friendly Name**: enter device name
   - **Address**: enter device IP
   - **Shared secret**: Choose generation method (in this example, Manual)
   - **Under shared secret**: enter the shared secret that will be defined on Wi-Fi device.
Configuring NPS Policies for Wireless - IEEE 802.11

1. Open the Network Policy Server console
2. Select Policies > Connection Request Policies and ensure that Use Windows authentication for all users is enabled.
3. Under **Policies**, right-click **Network Policies** and select **New**.

![Network Policy Server]

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

4. Under **Policy Name**, enter the required name.

5. Under **Type of network access server**, select **Unspecified**, and click **Next**.

![Specify Network Policy Name and Connection Type]

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
6. In the **Specify Conditions** window, click **Add**.

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

7. Choose **User Groups** and click **Add**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. Click **Add Groups**

9. Add **Domain Users**, and Click **OK Twice**
10. Click **Add Again**

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)
11. Choose **NAS Port Type**, and click **Add**.

12. Select **Wireless – IEEE 802.11** and **Wireless – Other** and click **OK**.
3. Ensure that **NAS Port Type Condition** was added, and click **Next**.

![Specify Conditions](image1)

*Condition description:*
The NAS Port Type condition specifies the type of media used by the access client, such as analog phone lines, ISDN, tunnels or virtual private networks, IEEE 802.11 wireless, and Ethernet switches.

![Specify Access Permission](image2)

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

4. Select **Access Granted**, and click **Next**.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
5. In the **Configure Authentication Methods** screen, click **Add**.

6. In the **Add EAP** window, choose **Microsoft: Smart Card or other certificate**, and click **OK**.

![Configure Authentication Methods](image)

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

7. In the **Add EAP** window, choose **Microsoft Protected EAP (PEAP)**, and click **OK**.

![Configure Authentication Methods](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
8. After Added Both, Select **Microsoft Protected EAP (PEAP)**, and click **Edit**.

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

9. In the **Edit Protected EAP Properties** window, click **Add**

(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)
10. Select **Smart Card or other certificate** and click **OK**.

![Image of Smart Card or other certificate selection](image)

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

11. Move up or remove the unwanted methods (in this example only **Smart Card or other certificate** was configured) and click **OK**.

![Image of method removal](image)

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
12. Click **Next** (without changing the default values), and then click **Finish**.

![Completing New Network Policy](image1)

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

13. Move the new policy to the top of the **Network Policies** list.

![Network Policy Server](image2)

*(The screen image above is from Microsoft© software. Trademarks are the property of their respective owners.)*
Configuring Wi-Fi Device

The steps demonstrated below are for a **TP-LINK 931F3E** device.

1. Connect and login to **TP-LINK Device > Under Wireless > Wireless Security**, and fill in the fields as follows:
   - Select **WPA/WPA2-Enterprise**
   - In **Version**, choose **Automatic**.
   - In **Encryption**, choose **Automatic**
   - In **Radius Server IP**, enter the Radius IP
   - In **Radius Password**, enter the shared secret as configured previously

   ![Screen Image](image-url)

   *(The screen image above is from tp-link® software. Trademarks are the property of their respective owners.)*

2. Click **Save**.
Configuring Wi-Fi Connection Client Side

**Prerequisites:** The steps Demonstrated below are for a Wi-Fi Connection that is already successfully connected to the Wi-Fi Device, and where the authentication method has been changed to Certificate Based Authentication.

1. Open **Network and Sharing Center** and click on the Wi-Fi Connection.

   ![Network and Sharing Center](image1)

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

2. Click **Wireless Properties**.

   ![Wi-Fi Status](image2)

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


3. In the **Wireless Network Properties** window, click the **Security** tab, then click **Advanced Settings**.

4. In the **Advanced Settings** window, select the **Specify authentication mode**, then select **User Authentication**.

5. Click **OK** to return to **Wireless Network Properties, Security tab**.
6. In the **Wireless Network Properties** window, click the **Security** tab, then configure as follows:
   - **Security Type**: select **WPA2-Enterprise**.
   - **Encryption Type**: select **AES**.
   - **Choose a network authentication method**: select **Microsoft: Smart Card or other certificate**

7. Click **Settings** (placed to the right of the Microsoft: Smart Card or other certificate).

8. In the **Smart Card or other Certificate Properties** window, under **When Connecting**, do the following:
   - Select **Use My Smart Card**
   - Select **Use Simple certificate selection**
   - Select **Verify the server’s identity by validating the certificate**
   - Under **Trusted Root Certification Authorities**, select the trusted domain root CA
9. Click **Advanced**.

![Image of Smart Card or other Certificate Properties]

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

10. In the **Configure Certificate Selection** window, select **Certificate Issuer** and select the trusted domain root CA.

![Image of Configure Certificate Selection]

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

11. Click **OK** repeatedly until all the screens are closed.
Running the Solution

Enroll a Smartcard User certificate on the smart card/token.
1. Connect token.
2. From the Windows Taskbar menu, select Network > Wi-Fi.

(The screen image above is from Microsoft® software. Trademarks are the property of their respective owners.)
3. Select the Wi-Fi network and click **Connect**.

4. In the **Windows Security Sign in** window, enter the credentials in the **Smart card credential** field, and click **OK**.
The Wi-Fi is now connected.

(The screen image above is from Microsoft® 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>Italy</td>
<td>800-786-421</td>
</tr>
<tr>
<td>Japan</td>
<td>0066 3382 1699</td>
</tr>
<tr>
<td>Region</td>
<td>Telephone number</td>
</tr>
<tr>
<td>--------------</td>
<td>------------------</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>

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