SafeNet Authentication Client
Integration Guide

Using SafeNet Authentication Client CBA for IBM Security Access Manager 9.0
All information herein is either public information or is the property of and owned solely by Gemalto NV. 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.

© 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 Part Number:** 007-013729-001 Rev. A  
**Release Date:** February 2017
Contents

Third-Party Software Acknowledgement ........................................................................................................... 4
Description .......................................................................................................................................................... 4
Applicability ...................................................................................................................................................... 5
Environment ....................................................................................................................................................... 5
Audience ............................................................................................................................................................ 5
CBA Flow using SafeNet Authentication Client ................................................................................................. 6
Prerequisites ....................................................................................................................................................... 6
Tokens Supported by SafeNet Authentication Client .......................................................................................... 7
Configuring IBM Security Access Manager 9.0 ................................................................................................. 8
   Basic Configuration ........................................................................................................................................ 8
   Configuring Reverse Proxy for CBA .............................................................................................................. 11
   Configuring the Client Certificate Mapping File ............................................................................................ 13
   Configuring SSL Certificates ....................................................................................................................... 16
Running the Solution ......................................................................................................................................... 18
Support Contacts ............................................................................................................................................... 19
Third-Party Software Acknowledgement

This document is intended to help users of Gemalto products when working with third-party software, such as IBM Security Access Manager 9.0.

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

Remote access poses both a security and a compliance challenge to IT organizations. The ability to positively identify users (often remote users) requesting access to resources is a critical consideration in achieving a secure remote access solution. Deploying a remote access solution without strong authentication is like putting your sensitive data in a vault (the datacenter), and leaving the key (user password) under the door mat.

A robust user authentication solution is required to screen access and provide proof-positive assurance that only authorized users are allowed access.

Public Key Infrastructure (PKI) provides an effective strong authentication solution for the functional, security, and compliance requirements.

SafeNet Authentication Client (SAC) is a PKI middleware application that provides a secure method for exchanging information based on public-key cryptography, enabling trusted third-party verification of user identities. SafeNet’s certificate-based tokens provide secure remote access, as well as other advanced functions, in a single token, including digital signing, password management, network logon, and combined physical/logical access.

The tokens come in different form factors, including USB tokens, smart cards, and software tokens. All of these form factors are interfaced using a single middleware client, SAC. 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 secure web access, secure network logon, PC and data security, and secure email. PKI keys and certificates can be created, stored, and used securely with the hardware or software tokens.

SafeNet Authentication Manager (SAM) provides your organization with a comprehensive platform to manage all of your authentication requirements, across the enterprise and the cloud, in a single, integrated system. SAM enables management of the complete user authentication life-cycle. SAM links tokens with users, organizational rules, and security applications to allow streamlined handling of your organization’s authentication infrastructure with a flexible, extensible, and scalable management platform.

SAM is a comprehensive token management system. It is an out-of-the-box solution for Public Certificate Authorities (CA) and enterprises to ease the administration of SafeNet’s hardware or software tokens devices. SAM is designed and developed to support the best practices of managing PKI devices in common PKI implementations. It offers a robust yet easy to customize framework that supports different organizations’ PKI devices management workflows and policies. Using SAM to manage tokens is not mandatory, but it is recommended for enterprise organizations.

For more information, refer to the SafeNet Authentication Manager Administrator Guide.

IBM® Security Access Manager for Web provides an integrated security management platform for authentication services, access control, authorization services, identity mapping, web single sign-on, entitlements, and audit services across enterprise resources. The solution also provides integrated, policy-based security management for the extended enterprise that enables customers, business partners, employees, suppliers, and distributors to securely access enterprise resources in a trusted manner. The Information Center maintains data on the Security Access Manager for Web components.
This document describes the deployment of certificate-based authentication (CBA) for user authentication to IBM Security Access Manager 9.0 using SafeNet tokens.

It is assumed that the IBM Security Access Manager 9.0 environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

IBM Security Access Manager 9.0 can be configured to support multi-factor authentication in several modes. CBA will be used for the purpose of working with SafeNet 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, using Microsoft Smart Card Base Cryptographic Provider to manage Gemalto IDPrime MD smart cards. For more details about different SAC installation modes, refer to the *SafeNet Authentication Client Administration Guide*.

- **IBM Security Access Manager 9.0**

**Environment**

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

- **SafeNet Authentication Client (SAC) - Version 10.2**
- **IBM Security Access Manager 9.0**

**Audience**

This document is intended for use by system administrators who are familiar with IBM Security Access Manager 9.0, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.
CBA Flow using SafeNet Authentication Client

1. The user attempts to connect to the IBM Security Access Manager 9.0 server using the IBM Security Access Manager 9.0 client application. The user inserts the SafeNet token on which his certificate resides, and, when prompted, enters the token password.

2. After successful authentication, the user is allowed access to internal resources.

Prerequisites

This following must be installed and configured before implementing certificate-based authentication for IBM Security Access Manager 9.0 using SafeNet tokens:

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

- If SAM is used to manage the tokens, Token Policy Object (TPO) must be configured with an MS CA Connector. For further details, refer to the in the SafeNet Authentication Manager Administrator’s Guide.

- Users must have a SafeNet token with an appropriate certificate enrolled on it.

- SafeNet Authentication Client (SAC version 10.2) should be installed on all client machines.
Tokens Supported by SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of authenticators that can be used as a second authentication factor for users who authenticate to IBM Security Access Manager 9.0.

SafeNet Authentication Client 10.2 (GA) supports the following tokens:

**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 complete list of supported authenticators, refer to *SafeNet Authentication Client Customer Release Notes*
Configuring IBM Security Access Manager 9.0

This section describes configuration of IBM ISAM 9, enabling the user to log on to the protected web application using a smart card.

Basic Configuration

IBM ISAM 9 is configured with default options. This section describes the initial configuration steps required to create a basic environment.

To set up basic configuration:

1. Log in to the Security Web Gateway Appliance console.

2. Go to Secure Web Settings > Reverse Proxy and ensure that you have a reverse proxy instance.
3. Select the required Reverse Proxy and click **Manage > Junction Management**.

![Image of IBM Security Access Manager interface](image1)

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

4. Ensure that a Junction is configured (the web application to be protected by WebSEAL).

   In the following example, the gemalto.com website is configured as the protected web application.

![Image of IBM Security Access Manager junction configuration](image2)

*(The screen image above is from IBM. Trademarks are the property of their respective owners.)*
5. Log in to the junction under the Reverse Proxy you created and make certain you have a username and password to access WebSEAL.

(The screen image above is from IBM. Trademarks are the property of their respective owners.)
Configuring Reverse Proxy for CBA

To use CBA with IBM ISAM 9:

1. Log in to the **Security Web Gateway Appliance** console.

![Screenshot of Security Web Gateway Appliance console](image1.png)

*The screen image above is from IBM. Trademarks are the property of their respective owners.*

2. Select **Secure Web Settings > Reverse Proxy**.

![Screenshot of Secure Web Settings](image2.png)

*The screen image above is from IBM. Trademarks are the property of their respective owners.*

3. Select the Reverse Proxy you created and click **Edit**.
4. On the **Server** tab, under **Client Connection**, verify that the **HTTPS** check box is selected.

   ![Server tab with HTTPS check box selected](image)

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

5. Click on the **Authentication** tab, and under **Client Certificates**, in the **Accept Client Certificates** field, select **Required** from the drop-down list.

   ![Authentication tab with required certificate](image)

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

6. Click **Save**.

7. When prompted, click the link to deploy and restart the reverse proxy.
Configuring the Client Certificate Mapping File

WebSEAL uses the Cross Domain Authentication Service (CDAS) to authenticate a user, using the details of a client certificate to determine the corresponding Security Access Manager user identity. The rules that govern the mapping of the client certificate are defined in XSL style notation.

The CDAS supports all user registries supported by Security Access Manager.

The rule evaluation can return an LDAP search string. This string representation of the LDAP search filter must be in accordance with the format described in RFC 2254.

For more information on user mapping rules, refer to the following link:

To configure the client certificate mapping file:


2. Enter a name for the mapping file and then click Save.
3. Select the CDAS filename that you created and click **Edit** on the top menu bar. The CDAS file content is displayed.

4. Scroll to the end of the file and change “SubjectDN” to “SubjectCN”.

   In this example, the xslt rule will extract the **CN** data field from the certificate and compare it to the **CN** data field in the ISAM user store.

5. Click **Save** to deploy the file.

6. Click **Secure Web Settings** > **Reverse proxy**.

7. Select the reverse proxy server and click **Manage** > **Configuration** > **Edit Configuration File**.
8. Verify that in the [cert-map-authn] stanza, the rules-file key is set to the certificate mapping file you created.

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

9. Click **Save**.

10. When prompted, click the link to deploy and restart the reverse proxy.
Configuring SSL Certificates

For ISAM to use a certificate that was created with an external Root CA, it must include the Root CA signer certificate in its database. By default, an SSL certificate database, `pdsrv`, is created when installing ISAM 9.0. The database contains known signer certificates (for example, Verisign).

For more information on managing signer certificates in a certificate database, refer to the following link:

To add your local Root CA signer certificate:

1. Log in to the **Security Web Gateway Appliance** console.

2. Click **Manage System Settings > SSL Certificates**.

3. Select the file `pdsrv` and click **Manage > Edit SSL Certificate Database**.
4. To import the Root CA signer certificate to the database, on the **Signer Certificates** tab, click **Manage > Import**.

![Image of IBM Security Access Manager](image1.png)

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

5. The **Import Signer Certificate** window opens. Press **Browse** and select the CA certificate. Enter a label for the certificate and click **Import**.

![Image of IBM Security Access Manager](image2.png)

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

6. Click **Save**.
Running the Solution

After configuration is completed, the user can browse to the configured WebSEAL junction and authenticate using a certificate.

To authenticate to a protected web application:

1. Log in to the WebSEAL junction using SSL protocol. The Token Logon window opens.

2. Enter the token password. The user will be authenticated to the protected web application.
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.

<table>
<thead>
<tr>
<th>Contact Method</th>
<th>Contact Information</th>
</tr>
</thead>
<tbody>
<tr>
<td>Address</td>
<td>Gemalto</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td>Phone</td>
<td>United States</td>
</tr>
<tr>
<td></td>
<td>1-800-545-6608</td>
</tr>
<tr>
<td></td>
<td>International</td>
</tr>
<tr>
<td></td>
<td>1-410-931-7520</td>
</tr>
<tr>
<td></td>
<td>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.</td>
</tr>
</tbody>
</table>