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.

© 2016 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: 007-013523-001, Rev. A
Release Date: June 2016
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Third-Party Software Acknowledgement</td>
<td>4</td>
</tr>
<tr>
<td>Description</td>
<td>4</td>
</tr>
<tr>
<td>Applicability</td>
<td>5</td>
</tr>
<tr>
<td>Environment</td>
<td>5</td>
</tr>
<tr>
<td>Audience</td>
<td>5</td>
</tr>
<tr>
<td>CBA Flow using SafeNet Authentication Client</td>
<td>5</td>
</tr>
<tr>
<td>Prerequisites</td>
<td>6</td>
</tr>
<tr>
<td>Supported Tokens in SafeNet Authentication Client</td>
<td>6</td>
</tr>
<tr>
<td>Configuring IBM WebSphere Application Server</td>
<td>7</td>
</tr>
<tr>
<td>Configuring an LDAP Repository</td>
<td>7</td>
</tr>
<tr>
<td>Adding a CA Root Certificate</td>
<td>14</td>
</tr>
<tr>
<td>Setting up the Application to Use the Client Certificate Authentication</td>
<td>17</td>
</tr>
<tr>
<td>Running the Solution</td>
<td>25</td>
</tr>
<tr>
<td>Support Contacts</td>
<td>27</td>
</tr>
</tbody>
</table>
Third-Party Software Acknowledgement

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

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 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.

PKI is an effective strong authentication solution to the functional, security, and compliance requirements.

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. 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, SafeNet Authentication 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 based on the best practices of managing PKI devices in common PKI implementations. It offers robust yet easy to customize frameworks that meets 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 WebSphere Application Server provides the ability to deploy and run applications with flexible, secure, and Java EE-certified runtime environments – from lightweight production environments to large enterprise deployments.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to IBM WebSphere Application Server using SafeNet tokens.
It is assumed that the IBM WebSphere Application Server environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

IBM WebSphere Application Server 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)** - SafeNet Authentication Client is the middleware that manages SafeNet's tokens.
- **IBM WebSphere Application Server**

**Environment**

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

- **SafeNet Authentication Client (SAC)**—Version 10.0
- **IBM WebSphere Application Server**—Version 8.5
- **Windows Server 2008r2 Active Directory and CA server**
- **Windows 7 x32 as Client**

**Audience**

This document is targeted to system administrators who are familiar with IBM WebSphere Application Server, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

**CBA Flow using SafeNet Authentication Client**

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

1. A user attempts to connect to the IBM WebSphere Application Server using the IBM WebSphere Application Server client application URL. The user inserts the SafeNet token on which his or her certificate resides, and, when prompted, enters the token password.
2. After successful authentication, the user is allowed access to IBM WebSphere Application.

Prerequisites

This section describes the prerequisites that must be installed and configured before implementing certificate-based authentication for IBM WebSphere Application Server using SafeNet tokens:

- 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.
- If SAM is used to manage the tokens, Token Policy Object (TPO) should 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 must have a SafeNet token with an appropriate certificate enrolled on it.
- SafeNet Authentication Client 10.0 should be installed on all client machines.
- SafeNet Authentication Client should be installed on the certificate authority from where a certificate will be enrolled on the token.
- Active Directory, LDAP server, IBM WebSphere Application Server, and client are up and running and should communicate with each other.

Supported Tokens in SafeNet Authentication Client

SafeNet Authentication Client (SAC) supports a number of tokens that can be used as a second authentication factor for users who authenticate to IBM WebSphere Application Server.

SafeNet Authentication Client 10.0 (GA) supports the following tokens:

Certificate-based USB tokens
- SafeNet eToken 5110/5105

Smart Cards
- IDPrime MD 830-FIPS
- IDPrime MD 830-ICP
- IDPrime MD 3810
- IDPrime MD 3810 MIFARE 1K

Software Tokens
- SafeNet eToken Virtual
Configuring IBM WebSphere Application Server

Configuring IBM WebSphere Application server requires:

- Configuring an LDAP Repository, page 7
- Adding a CA Root Certificate, page 14
- Setting up the Application to Use the Client Certificate Authentication, page 17

Configuring an LDAP Repository

1. In a web browser, open the following url:
   
   `http://<WebSphere Application Server IP address or name>:<port number>/ibm/console`

   Or
   
   `https://<WebSphere Application Server IP address or name>:<port number>/ibm/console`

   **NOTE:** The port number will be according to the created installation profile.

2. On the WebSphere Application Server login window, enter the administrator user ID and password, and then click Log in.

   *(The screen image above is from IBM®. Trademarks are the property of their respective owners.)*
After successful login, the WebSphere Application Server Administrator console is displayed.

3. On the WebSphere Application Server Administrator console, in the left pane, click Security > Global security, and then in the center pane, under Application security, select Enable application security.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. Under **User account repository**, perform the following steps:
   a. In the **Available realm definitions** field, select **Standalone LDAP registry**.
   b. Click **Set as current**.
   c. Click **Configure**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
5. Under **General Properties**, complete the following fields, and then click **OK**:

| **Primary administrative user name** | Enter the user name of the primary administrative user. The user is defined with administrative privileges in the user registry. |
| **Type of LDAP server** | Select **Microsoft Active Directory**. |
| **Host** | Enter the LDAP server host name or IP address. |
| **Base distinguished name (DN)** | Enter the base distinguished name of the directory. |
| **Bind distinguished name (DN)** | Enter the full distinguished name of the administrator. |
| **Bind password** | Enter the administrator password. |

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

NOTE: Click Test connection to ensure that the connection with the LDAP server is successfully established.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
7. In the left pane, click **Security > Global security**, and then in the center pane, under **User account repository**, click **Configure**.

---

**NOTE:** Ensure that **Standalone LDAP registry** is selected in the **Available realm definitions** field.

---

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

![Screenshot of Additional Properties with Advanced Lightweight Directory Access Protocol (LDAP) selected](image)

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

9. Under **General Properties**, ensure that in the **Certificate map mode** field, **Exact_DN** is selected.

![Screenshot of General Properties with Exact_DN selected](image)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
Adding a CA Root Certificate

Add a CA root certificate to the default trust store on the IBM WebSphere Application server.

1. On the WebSphere Application Server Administrator console, in the left pane, click **Security > SSL certificate and key management**, and then in the center pane, under **Related Items**, click **Key stores and certificates**.

![WebSphere Administrator Console](image1.png)

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

2. Click **NodeDefaultTrustStore**.

![WebSphere Administrator Console](image2.png)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
3. Under **Additional Properties**, click **Signer certificates**.

4. Click **Add**.
5. Under **General Properties**, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Alias</strong></th>
<th>Enter an alias for the signer certificate (for example, Root_CA). The alias is used to refer the signer certificate in the key store.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>File name</strong></td>
<td>Enter the full path to the signer certificate file.</td>
</tr>
</tbody>
</table>

![Image of General Properties](image1.png)

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

6. The CA root certificate is added. Click **Save**.

![Image of CA root certificate added](image2.png)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
Setting up the Application to Use the Client Certificate Authentication

Performing client certificate authentication with the .ear application requires:

- Defining Quality of Protection (QoP) Settings for the SSL Client Authentication, page 17
- Updating the Application to Support the Client Certificate Authentication, page 20
- Installing the Enterprise Application, page 21
- Starting the Enterprise Application, page 24

NOTE: In this solution, the IBM WebSphere DefaultApplication.ear application is used.

Defining Quality of Protection (QoP) Settings for the SSL Client Authentication

1. On the WebSphere Application Server Administrator console, in the left pane click Security > SSL certificate and key management, and then, in the center pane, under Related Items, click SSL configurations.

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

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

3. Under Additional Properties, click **Quality of protection (QoP) settings** to define Quality of protection (QoP) settings for SSL.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. Under **General Properties**, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Client authentication</th>
<th>Select Required.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Protocol</td>
<td>Select SSL_TLS</td>
</tr>
</tbody>
</table>

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

5. Click **Save**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
Updating the Application to Support the Client Certificate Authentication

NOTE: It is assumed that DefaultApplication.ear is exported and edited.

1. Open the web.xml file that is located at the following path:
   `<path where the .ear directory is exported>/DefaultWebApplication.war/WEB-INF/web.xml`

NOTE: The web.xml file is located in the directory where the DefaultApplication.ear file is exported.

2. Edit the web.xml file.

3. In the web.xml file, add or replace the `<login-config>` tag with the following content to add the client certificate authentication method.

   ```xml
   <login-config>
   <auth-method>CLIENT-CERT</auth-method>
   </login-config>
   ```

4. Locate the `<transport-guarantee>` tag and replace it with the following content to change the transport guarantee setting to CONFIDENTIAL.

   ```xml
   <transport-guarantee>CONFIDENTIAL</transport-guarantee>
   ```

5. Save and close the web.xml file.
Installing the Enterprise Application

Install the Enterprise application after the `web.xml` is edited.

1. Log in to the WebSphere Application Server Administrator console.

2. On the WebSphere Application Server Administrator console, in the left pane, click Applications > New Application, and then in the right pane, click New Enterprise Application.

3. Under Path to the new application, select Local file system, click Browse to select a path to the enterprise application file, and then click Next.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
4. Under **How do you want to install the application?**, select **Fast Path**, and then click **Next**.

5. Under **Select installation options**, click **next**.
6. Under **Map modules to servers**, click **Next**.

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

7. Under **Summary**, click **Finish**.

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
8. After successful installation, click **Save**

![Image](image-url)

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

**Starting the Enterprise Application**

1. On the WebSphere Application Server Administrator console, in the left pane, click **Applications > Application Types > WebSphere enterprise applications**, and then in the center pane, select the installed application (for example, **DefaultApplication.ear**).

![Image](image-url)

(The screen image above is from IBM®. Trademarks are the property of their respective owners.)
2. Click **Start**. The application is started successfully and the application status is changed to ![](The screen image above is from IBM®. Trademarks are the property of their respective owners.)

### Running the Solution

Before running the solution, ensure that a Smart card user certificate must be present on the SafeNet USB token.

1. Insert the SafeNet USB token into the client machine.
2. In a web browser, open the following url:

   https://<Server IP or Name>:<SSL Port>/<Application>

   Where, `<Server IP or Name>` is the IP address or name of the IBM WebSphere Application server, `<SSL Port>` is the SSL port number based on the created installation profile, and `<Application>` is the application path (for example, `/snoop`) in Default App.Ear.

3. You will be redirected to the **Confirm Certificate** window. Click **OK**.
4. On the **SafeNet Authentication Client** login window, enter the token password, and then click **OK**.

After successful authentication, the requested information is displayed.
### 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>
</table>
| **Address**            | Gemalto  
4690 Millennium Drive  
Belcamp, Maryland  21017 USA                                               |
| **Phone**              | United States  
1-800-545-6608  
International  
1-410-931-7520                                                   |
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. |