SafeNet Authentication Client
Integration Guide

Using SAC CBA for Blue Coat ProxySG
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 N.V. 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:** 007-013411-001, Rev. A

**Release Date:** February 2016
Contents

Third-Party Software Acknowledgement .................................................................................................................. 4
Description .................................................................................................................................................................. 4
Applicability ............................................................................................................................................................ 5
Environment ............................................................................................................................................................. 5
Audience .................................................................................................................................................................... 5
CBA Flow using SAC .............................................................................................................................................. 5
Prerequisites ........................................................................................................................................................... 6
Supported Tokens in SAC ....................................................................................................................................... 6
Configuring BlueCoat ProxySG .................................................................................................................................. 7
  Configuring a CA Certificate List ........................................................................................................................... 7
  Configuring a Certificate Realm .......................................................................................................................... 15
  Configuring the HTTPS Reverse Proxy Service .................................................................................................... 18
  Configuring an Authentication Policy ................................................................................................................ 20
Running the Solution .............................................................................................................................................. 28
Support Contacts ..................................................................................................................................................... 29
Third-Party Software Acknowledgement

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

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.

The Blue Coat ProxySG appliances provide complete control over all of your web traffic, delivering world-class threat protection. Robust features include user authentication, web filtering, data loss prevention, inspection, and visibility of SSL-encrypted traffic (including the ability to stream decrypted content to an external server with an Encrypted Tap license), content caching, bandwidth management, stream-splitting, and more.

The Blue Coat Secure Web Gateway Virtual Appliance (SWG VA) combines the market-leading security capabilities of Blue Coat ProxySG with the flexibility of virtualization to provide a cost-effective enterprise branch
office solution. With the Blue Coat SWG VA, businesses can support web security and other critical remote office infrastructure on a common platform, reducing costs and IT resource requirements.

This document provides guidelines for deploying certificate-based authentication (CBA) for user authentication to Blue Coat ProxySG using SafeNet tokens.

It is assumed that the Blue Coat ProxySG environment is already configured and working with static passwords prior to implementing SafeNet multi-factor authentication.

Blue Coat ProxySG 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.
- **Blue Coat ProxySG (Virtual Appliance)**

**Environment**

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

- **SafeNet Authentication Client (SAC)**—Version 9.0 GA
- **Blue Coat ProxySG (Software)**—Version SGOS 6.5.6.4 SWG Edition
- **Blue Coat ProxySG (Virtual Appliance)**—Model No. VA-100

**Audience**

This document is targeted to system administrators who are familiar with Blue Coat ProxySG, and are interested in adding multi-factor authentication capabilities using SafeNet tokens.

**CBA Flow using SAC**

The diagram below illustrates the flow of certificate-based authentication:
1. A user attempts to connect to the Blue Coat ProxySG server using the Blue Coat ProxySG client application. The user inserts the SafeNet token on which his/her certificate resides, and, when prompted, enters the token password.

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

### Prerequisites

Before implementing certificate-based authentication for Blue Coat ProxySG using SafeNet tokens, ensure the following:

- To use CBA, Microsoft Enterprise Certificate Authority must be installed and configured. In general, any certificate authority (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 (9.0) should be installed on all client machines.
- Client and Web Server Appliance certificates of type X.509 (issued from the same certificate authority) are required for testing purpose.
- Reverse proxy setup must be up and running.

### Supported Tokens in SAC

SAC supports a number of tokens that can be used as a second authentication factor for users who authenticate to Blue Coat ProxySG.

SafeNet Authentication Client 9.0 (GA) supports the following tokens:

**Certificate-based USB tokens**
- SafeNet eToken PRO Java 72K
- SafeNet eToken PRO Anywhere
- SafeNet eToken 5100/5105
- SafeNet eToken 5200/5205
- SafeNet eToken 5200/5205 HID and VSR

**Smart Cards**
- SafeNet eToken PRO Smartcard 72K
- SafeNet eToken 4100

**Certificate-based Hybrid USB Tokens**
- SafeNet eToken 7300
- SafeNet eToken 7300-HID
- SafeNet eToken 7000 (SafeNet eToken NG-OTP)
Software Tokens

- SafeNet eToken Virtual
- SafeNet eToken Rescue

Configuring Blue Coat ProxySG

Configuring Blue Coat ProxySG for CBA requires the following:

- Configuring a CA Certificate List, page 7
- Configuring a Certificate Realm, page 15
- Configuring the HTTPS Reverse Proxy Service, page 18
- Configuring an Authentication Policy, page 20

Configuring a CA Certificate List

Configuring a CA certificate list requires:

- Creating a Keyring, page 7
- Importing the Web Server Appliance Certificate, page 9
- Importing the Client CA Certificate, page 11
- Creating a CA Certificate List, page 13

Creating a Keyring

1. In a web browser, open the following URL, and then log in as an administrator:

   https://<ProxySG_IP_Address>:8082

   Where, <ProxySG_IP_Address> is the IP address of the ProxySG virtual appliance, and 8082 is the default management port.

2. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click SSL > Keyrings.

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

3. In the right pane, on the Keyrings tab, click Create.
4. On the **Create Keyring** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Keyring name</th>
<th>Enter a name for the keyring (for example, Test).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Private key visibility</td>
<td>Select <strong>Show key pair</strong>.</td>
</tr>
</tbody>
</table>

(See screen image above from Blue Coat® software. Trademarks are the property of their respective owners.)

On the **Blue Coat ProxySG Management Console** window, in the right pane, the newly created keyring is listed.

(See screen image above from Blue Coat® software. Trademarks are the property of their respective owners.)
**Importing the Web Server Appliance Certificate**

1. Copy the text of the Web Server Appliance certificate (including the Begin Certificate and End Certificate statements) to the system clipboard.

2. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click SSL > Keyrings.

3. In the right pane, on the **Keyrings** tab, select the keyring (for example, **Test**) that you created earlier in step 4 of “Creating a Keyring” on page 7, and then click **Edit**.

4. On the “Edit Keyring” window, under **Certificate**, click **Import**.

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

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. On the **Import Certificate** window, click **Paste From Clipboard**, and then click **OK**.

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

6. Click **Close**.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
7. On the Blue Coat ProxySG Management Console window, click **Apply**.

![Blue Coat ProxySG Management Console](image)

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

8. A successful message is displayed. Click **OK**.

![Changes Done Successfully](image)

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

### Importing the Client CA Certificate

A CA certificate verifies the identity of a Certificate Authority. It is used by the Blue Coat ProxySG to verify Web Server and Client certificates.

1. Copy the text of the CA certificate to the system Clipboard.
2. On the Blue Coat ProxySG Management Console window, click the **Configuration** tab, and then in the left pane, click **SSL > CA Certificates**.

![Blue Coat ProxySG Configuration](image)

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

3. In the right pane, on the **CA Certificates** tab, click **Import**.
4. On the **Import CA Certificate** window, perform the following steps:
   a. In the **CA Cert Name** field, enter the name of the CA certificate (for example, **ProxySGCA**).
   b. Click **Paste From Clipboard**.
   c. Click **OK**.

   ![Image](image1.png)

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

5. On the **Blue Coat ProxySG Management Console** window, in the right pane, the CA certificate is listed. Click **Apply**.

   ![Image](image2.png)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
6. A successful message is displayed. Click **OK**.

![Changes Done Successfully](image)

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

**Creating a CA Certificate List**

1. On the **Blue Coat ProxySG Management Console window**, click the **Configuration** tab, and then in the left pane, click **SSL > CA Certificates**.

![Configuration Tab](image)

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

2. In the right pane, on the **CA Certificate Lists** tab, click **New**.
3. On the Create CA Certificate List window, perform the following steps:
   a. In the CA Cert List Name field, enter a name for the certificate list (for example, ReverseProxyCCL).
   b. In the list box on the left, select the imported CA certificate (for example, ProxySGCA) that you imported earlier in step 4 of “Importing the Client CA Certificate” on page 11.
   c. Click Add >> to move the selected certificate to the list box on the right.
   d. Click OK.

   ![Create CA Certificate List window](image)

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

4. On the Blue Coat ProxySG Management Console window, in the right pane, the CA certificate list is listed. Click Apply.

   ![Blue Coat ProxySG Management Console](image)

   (The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. A successful message is displayed. Click OK.

![Changes Done Successfully](image)

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

Configuring a Certificate Realm

Configuring a Certificate Realm requires:

- Creating a Certificate Realm, page 15
- Configuring the Certificate Realm Main Properties, page 16
- Configuring the Certificate Realm General Properties, page 17

Creating a Certificate Realm

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Authentication > Certificate.

![Certificate Realms](image)

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

2. In the right pane, on the Certificate Realms tab, click New.

3. On the Add Certificate Realm window, in the Realm name field, enter a name for certificate realm (for example, SAC_CBA), and then click OK.

![Add Certificate Realm](image)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
4. On the **Blue Coat ProxySG Management Console** window, in the right pane, the newly created certificate realm is listed. Click **Apply**.

5. A successful message is displayed. Click **OK**.

**Configuring the Certificate Realm Main Properties**

1. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **Authentication > Certificate**.

2. In the right pane, on the **Certificate Main** tab, in the **Realm name** field, select the certificate realm (for example **SAC_CBA**) that your created earlier in step 3 of “Creating a Certificate Realm”, on page 15, and then click **Add**.
3. On the **Add OID** window, enter the OID value, and then click **OK**.

   ![Add OID window](image)

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

   **NOTE:** The OID value is available in the **Enhanced Key Usage** field of the client certificate.

4. On the **Blue Coat ProxySG Management Console** window, in the right pane, under **Extended Key Usage**, the OID value is listed. Click **Apply**.

   ![Blue Coat ProxySG Management Console](image)

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

**Configuring the Certificate Realm General Properties**

1. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **Authentication > Certificate**.
2. In the right pane, on the **Certificate General** tab, complete the following fields, and then click **Apply**.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Realm name</strong></td>
<td>Select the certificate realm (for example <strong>SAC_CBA</strong>) that you created in step 3 of &quot;Creating a Certificate Realm&quot; on page 15.</td>
</tr>
<tr>
<td><strong>Virtual URL</strong></td>
<td>Enter the virtual URL configured for reverse proxy setup.</td>
</tr>
</tbody>
</table>

3. A successful message is displayed. Click **OK**.

![Screen image of Blue Coat software](image-url)

(THE SCREEN IMAGE ABOVE IS FROM BLUE COAT® SOFTWARE. TRADEMARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.)

### Configuring the HTTPS Reverse Proxy Service

Ensure that your reverse proxy setup is up and running before configuring the HTTP reverse proxy service.

1. On the **Blue Coat ProxySG Management Console** window, click the **Configuration** tab, and then in the left pane, click **Services > Proxy Services**.

![Screen image of Blue Coat software](image-url)

(THE SCREEN IMAGE ABOVE IS FROM BLUE COAT® SOFTWARE. TRADEMARKS ARE THE PROPERTY OF THEIR RESPECTIVE OWNERS.)
2. In the right pane, on the **Proxy Services** tab, expand **Reverse_proxy**, select the HTTPS service (for example, **HTTPS-Rev** that you created at the time of creating the reverse proxy setup), and then click **Edit Service**.

   ![Proxy Services Screen](image1)

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

3. On the **Edit Service** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th><strong>Keyring</strong></th>
<th>Select the keyring (for example, <strong>Text</strong>) that you created earlier in step 4 of “Creating a Keyring” on page 7.</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>CCL</strong></td>
<td>Select the CA Certificate List (for example, <strong>ReverseProxyCCL</strong>) that you created earlier in step 3 of “Creating a CA Certificate List” on page 13.</td>
</tr>
</tbody>
</table>

   ![Edit Service Window](image2)

   *(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
Configuring an Authentication Policy

With an authentication realm configured, now configure a policy on the ProxySG appliance to authenticate, log, and control user access to the web server.

The sections below explain about setting up rules to authenticate users, restrict access for specific users and groups, and deny all other access to the web server.

Creating the Web Authentication Layer

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and in the left pane, click Policy > Visual Policy Manager.

2. In the right pane, click Launch.


4. On the Add New Layer window, enter a name for the web authentication layer, and then click OK.
5. On the **Blue Coat Visual Policy Manager** window, on the newly created authentication layer (for example, **Web Authentication Layer**), right-click in the **Action** column of the default rule, and then click **Set**.

![Blue Coat Visual Policy Manager window](image)

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

6. On the **Set Action Object** window, click **New > Authenticate**.

![Set Action Object window](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
7. On the **Add Authenticate Object** window, complete the following fields, and then click **OK**.

<table>
<thead>
<tr>
<th>Name</th>
<th>Enter a name for the authenticate object (for example, <strong>Authenticate</strong>).</th>
</tr>
</thead>
<tbody>
<tr>
<td>Realm</td>
<td>Select the certificate realm (for example, <strong>SAC_CBA</strong>) that you created earlier in step 3 of “Creating a Certificate Realm” on page 15.</td>
</tr>
<tr>
<td>Mode</td>
<td>Select <strong>Auto</strong>.</td>
</tr>
</tbody>
</table>

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

8. On the **Set Action Object** window, click **OK**.

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
Creating a Web Access Layer

Create a policy rule that enables the ProxySG appliance to grant users access to the network.

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and in the left pane, click Policy > Visual Policy Manager.

![Configuration tab](image1)

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

2. In the right pane, click Launch.


![Add Web Access Layer](image2)

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

4. On the Add New Layer window, enter a name for the web access layer, and then click OK.

![Add New Layer](image3)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
5. On the Blue Coat Visual Policy Manager window, on the newly created web access layer (for example, Web Access Layer), right-click in the Source column of the default rule, and then click Set.

![Image](image1.png)

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

6. On the Set Source Object window, select Authenticated User, and then click OK.

![Image](image2.png)

(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
7. On the **Blue Coat Visual Policy Manager** window, on the newly created web access layer (for example, **Web Access Layer**), right-click in the **Action** column of the default rule, and then click **Allow**.

![Blue Coat Visual Policy Manager](image)

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

8. The icon in the **Action** column changes from red to green. Click **Install policy**.

![Blue Coat Visual Policy Manager](image)

*(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)*
9. A successful message is displayed. Click OK.

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

Creating a CPL Layer

1. On the Blue Coat ProxySG Management Console window, click the Configuration tab, and then in the left pane, click Policy > Visual Policy Manager.

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

2. In the right pane, click Launch.


(The screen image above is from Blue Coat® software. Trademarks are the property of their respective owners.)
4. On the **Add New Layer** window, enter a name for the CPL layer, and then click **OK**

![Add New Layer Window](image)

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

5. On the **Blue Coat Visual Policy Manager** window, on the **CP Layer** tab, enter the following code:

   `<Proxy> ssl.proxy_mode = https-reverse-proxy
   authenticate(<certificate realm>)

Where, `<certificate realm>` is the certificate realm (for example **SAC_CBA**) that you created earlier in step 3 of “Creating a Certificate Realm” on page 15.

![Blue Coat Visual Policy Manager](image)

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

6. Click **Install policy**.

7. A successful message is displayed. Click **OK**.

![Policy Installed](image)

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

Before running the solution, ensure that the Blue Coat ProxySG virtual appliance is configured as a reverse proxy with HTTPS service. Also, a user certificate must be present on the SafeNet USB token.

1. In a web browser, open the following URL:
   
   `https://<Virtual IP of BlueCoat>`

   Where, `<Virtual IP of Bluecoat>` is an IP address that is configured on the BlueCoat ProxySG appliance.

2. The browser displays all the certificates available on the machine. Select the end user certificate that is added on the SafeNet USB token.

3. You will be redirected to the **Confirm Certificate** window. Click **OK**.

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

4. On the **SafeNet Authentication Client** login window, enter the token password, and then click **OK**.

   ![SafeNet Authentication Client login window](image-url)
After successful authentication, you are redirected to access the web page.

### 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><strong>Address</strong></td>
<td>Gemalto, Inc.</td>
</tr>
<tr>
<td></td>
<td>4690 Millennium Drive</td>
</tr>
<tr>
<td></td>
<td>Belcamp, Maryland 21017 USA</td>
</tr>
<tr>
<td><strong>Phone</strong></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><strong>Technical Support</strong></td>
<td><a href="https://serviceportal.safenet-inc.com">https://serviceportal.safenet-inc.com</a></td>
</tr>
<tr>
<td><strong>Customer Portal</strong></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>