Windows Digital Certificate Management

Introduction

This article discusses basic management of digital certificates (a.k.a. public key certificates) for SecureAuth IdP appliances running on Microsoft Windows Server 2008 R2, 2012, and 2012 R2.

SecureAuth IdP uses digital certificates throughout the system to verify an end-user's identity and provide secure communications with other systems.

Certificates must be kept current in order to ensure secure and valid connections between devices.

See SecureAuth IdP Digital Certificate Overview for additional background information about how digital certificates used with SecureAuth IdP

Applies to

<table>
<thead>
<tr>
<th>SecureAuth IdP Version</th>
<th>OS Version</th>
</tr>
</thead>
</table>

Discussion

Certificate Stores

What is a Certificate Store?

A Certificate Store can be regarded as a logical container in Windows that holds one or more certificates.

Certificate Stores used in a SecureAuth IdP Environment

The table below provides a description of the most commonly used Certificate Stores in a SecureAuth IdP environment
<table>
<thead>
<tr>
<th>Store</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Personal</td>
<td>Certificates associated with private keys to which the user has access&lt;br&gt;These certificates have been issued to the user or computer, or the service for which certificates are managed</td>
</tr>
<tr>
<td>Trusted Root Certification Authorities</td>
<td>Implicitly trusted certification authorities (CAs)&lt;br&gt;Includes all of the certificates in the Third-Party Root Certification Authorities store, plus root certificates from customer organizations and Microsoft</td>
</tr>
<tr>
<td>Intermediate Certification Authorities</td>
<td>Certificates issued to subordinate CAs</td>
</tr>
</tbody>
</table>

**How to Access Certificates in a Certificate Store**

The most common way to view certificates in a certificate store is to use the **Certificates Manager MMC snap-in**

The **Certificate Manager MMC snap-in** can be used to view details about certificates, modify or delete certificates, or request new certificates

**Access the Certificate Manager**

To access the Certificate Manager

1. Click **Start**, type `mmc.exe`, and then press **Enter**
2. From the **File** menu, click **Add/Remove Snap In**
3. Under **Available snap-ins**, double-click **Certificates**
4. Select **Computer Account**, and then click **Next**
5. In the **Select Computer** dialog, click **Finish**
6. In the **Add or Remove Snap-ins** window, click **OK**

**View Certificate Information**
To view information about a certificate

1. Start the Certificate Manager
2. Select the Certificate Store from the left pane
3. In the middle pane, double-click the certificate
4. The **Certificate** window appears, showing various attributes of the certificate

View detailed descriptions of digital certificate attributes
### Supported uses of the certificate
Summary information, such as the applications, signing, encryption, or authentication, for which the certificate can be used
This section also explains if a certificate has expired or is invalid

### Entity to which the certificate was issued
The name of recipient of the certificate
Recipients can include end users, computers, or entities such as certification authorities (CAs)

### The issuer of the certificate
The name of the CA that issued the certificate

### Validity period of the certificate
This includes the date the certificate becomes valid and the date the certificate expires

### Issuer statement
Clicking the Issuer Statement button opens a separate window that contains additional information about the certificate or a URL where additional information can be obtained

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Version</td>
<td>The X.509 version number</td>
</tr>
<tr>
<td>Serial Number</td>
<td>The unique serial number that the issuing certification authority (CA) assigns to the certificate</td>
</tr>
<tr>
<td>Signature Algorithm</td>
<td>The hash algorithm that the CA uses to digitally sign the certificate</td>
</tr>
<tr>
<td>Issuer</td>
<td>Information regarding the CA that issued the certificate</td>
</tr>
<tr>
<td>Valid from</td>
<td>The beginning date for the period in which the certificate is valid</td>
</tr>
<tr>
<td>Valid to</td>
<td>The final date for the period in which the certificate is valid</td>
</tr>
<tr>
<td>Subject</td>
<td>The name of the individual, computer, device, or CA to whom the certificate is issued</td>
</tr>
<tr>
<td>Public key</td>
<td>The public key type and length associated with the certificate</td>
</tr>
<tr>
<td>Thumbprint algorithm</td>
<td>The hash algorithm that generates a digest of data (or thumbprint) for digital signatures</td>
</tr>
<tr>
<td>Thumbprint</td>
<td>The digest (or thumbprint) of the certificate data</td>
</tr>
<tr>
<td>Friendly name</td>
<td>A display name to use instead of the name in the Subject field</td>
</tr>
<tr>
<td>Enhanced Key Usage</td>
<td>The purposes for which this certificate can be used</td>
</tr>
</tbody>
</table>

Before a certificate is trusted, Windows must verify that the certificate comes from a trusted source – this verification process is called **path validation**

---

### Import or Export Certificates

#### Import Certificate
When a computer receives a certificate, or transfers a certificate from one computer to another, the certificate and private key must be imported before they can be used.
The import process places the certificate in the correct certificate folder

Do not import a certificate by double-clicking it from Windows Explorer – always use the Certificate Manager to perform an import as described below

1. Start the Certificate Manager
2. Select the Certificate Store (folder) in which to import the certificate
3. From the Action menu, point to All Tasks, and then click Import
4. Click Next and follow the instructions provided
Export Certificate

1. To create a backup copy of the certificate or use the certificate on another computer, first export the certificate and private key

   Exporting the certificate places it in a file that can be transferred to another computer or be placed in a safe place.
When exporting a certificate with its private key, always protect the certificate and private key with a strong password.

2. Start the **Certificate Manager**

3. Right-click the certificate to export, point to **All Tasks**, and then click **Export**

4. In the **Certificate Export Wizard**, click **Next**
5. If available, choose **Yes, export the private key**; otherwise, click **No, do not export the private key**, then click **Next**

The latter option appears only if the private key is marked as exportable and the user has access to it
6. Select the format to use, and then click Next
7. If the private key is being exported (step 4), type a **strong password** to use to encrypt the key, confirm the password, and then click **Next**.
8. The export process creates a file in which to store the certificate.

Enter a name for the file and the location (include the entire path), or click **Browse**, navigate to the location, and then enter the file name.
9. Click Finish
Completing the Certificate Export Wizard

You have successfully completed the Certificate Export wizard.

You have specified the following settings:

- **File Name**: C:\Users\Administrator\Downloads\cert
- **Export Keys**: Yes
- **Include all certificates in the certification path**: Yes
- **File Format**: Personal Information Exchange (*.pfx)
Private Key Privileges

When a certificate is imported, its corresponding private key must be configured to allow access from SecureAuth IdP.

If this step is not completed, the dependent functions in the product will fail.

Reference the documents below to properly configure certificates:

<table>
<thead>
<tr>
<th>Certificate</th>
<th>Document</th>
</tr>
</thead>
<tbody>
<tr>
<td>SAML Signing Certificate</td>
<td>Grant Permission to Use Signing Certificate Private Key</td>
</tr>
<tr>
<td>WS Federation Certificate</td>
<td>Grant Permission to Use Signing Certificate Private Key</td>
</tr>
<tr>
<td>WSE 3.0 / WCF Client Certificate</td>
<td>Digital Certificate Private Key Management</td>
</tr>
<tr>
<td>License Info Certificate</td>
<td>Digital Certificate Private Key Management</td>
</tr>
</tbody>
</table>

Related Topics:
- Digital Certificate Private Key Management
- How SecureAuth IdP Services Use Certificates for Secure Authentication
- SecureAuth IdP Digital Certificate Overview
- Grant Permission to Use Signing Certificate Private Key
- Locate the Digital Certificate in Supported Browsers
- How to Submit a Certificate Revocation Request for a SecureAuth IdP-issued X.509 Certificate