Grant Permission to Use Signing Certificate Private Key

Introduction

Use this guide to enable "Authenticated Users" to use the private certificate key stored on the IIS server to sign messages, which is necessary to sign and encrypt outgoing messages (i.e. SAML and WS-Federation Assertions).

Prerequisites

1. Have access to the Certificates Console of the SecureAuth IdP appliance

<table>
<thead>
<tr>
<th>SecureAuth IdP Version</th>
<th>OS Version</th>
</tr>
</thead>
<tbody>
<tr>
<td>7.x+</td>
<td>Windows Server 2008</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2008 R2</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012</td>
</tr>
<tr>
<td></td>
<td>Windows Server 2012 R2</td>
</tr>
</tbody>
</table>

2. Have a certificate to be used by SecureAuth IdP

This certificate must have these **Key Usage** capabilities: Digital Signature, Non-Repudiation, Key Encipherment, and Data Encipherment
If the certificate is being imported, the **Network Service** must have Read access.
1. Open the **Certificates Console** on the appliance (Start --> All Programs --> SecureAuth --> Certificates Console)

2. In the **Certificates** folder (under **Certificates --> Properties**), right-click the **Signing Certificate** (typically issued by SecureAuth G3 Intermediate, SecureAuth Intermediate, or MFClient)

3. Select **All Tasks**, and then click **Manage Private Keys ...**
4. In the new window, click Add, which opens the Select Users, Computers, Service Accounts, or Groups window

5. Type Authenticated Users in the Object Names field, and click Check Names

   Authenticated Users now appears in the window

6. Click OK

7. In the previous window, click Apply, and then OK to close the window