MyID

SCEP Device Identities

Integration Guide

Lutterworth Hall, St Mary's Road, Lutterworth, Leicestershire, LE17 4PS, UK
www.intercede.com | info@intercede.com | @intercedemyid | +44 (0)1455 558111

Document reference: INT1804-06

May 2017

Copyright

Whilst Intercede Limited has made every effort in the preparation of this manual to ensure the accuracy of the information, the information contained in this manual is delivered without warranty, either express or implied. Intercede Limited will not be held liable for any damages caused, or alleged to be caused, either directly or indirectly by this manual.

Licenses and Trademarks

Conventions Used in this Document

- Lists:
  - Numbered lists are used to show the steps involved in completing a task when the order is important
  - Bulleted lists are used when the order is unimportant or to show alternatives

- **Bold** is used for menu items and for labels.

  For example:

  - "Record a valid email address in **'From' email address**"
  - Select **Save** from the **File** menu

- *Italic* is used for emphasis and to indicate references to other sections within the current document:

  For example:

  - "Copy the file *before* starting the installation"
  - "See *Issuing a Card* for further information"

- ***Bold and italic*** are used to identify the titles of other documents.

  For example: "See the ***Release Notes*** for further information."

  Unless otherwise explicitly stated, all referenced documentation is available on the product CD.

- A `fixed width` font is used where the identification of spaces is important, including filenames, example SQL queries and any entries made directly into configuration files or the database.

- **Notes** are used to provide further information, including any prerequisites or configuration additional to the standard specifications.

  For example:

  Note: This issue only occurs if updating from a previous version.

- Warnings are used to indicate where failure to follow a particular instruction may result in either loss of data or the need to manually configure elements of the system.

  For example:

Warning:	You must take a backup of your database before making any changes to it.

Contents

1 Introduction

MyID supports issuing device identities using the Simple Certificate Enrollment Protocol (SCEP).

1.1 Change history

Version	Description
`INT1804-01`	First release
`INT1804-02`	Rebranding.
`INT1804-03`	Update with known issues.
`INT1804-04`	Update to remove fixed issues.
`INT1804-05`	Update to remove fixed issues.
`INT1804-06`	Update to path of certificates.

1.2 Overview

MyID allows you to issue device identities to devices that support SCEP; for example, you can issue a certificate to a router. The MyID support for SCEP extends the standard device identities feature; for general information on MyID device identities, see the ***Administration Guide***.

The procedure is as follows:

1. Add a device to MyID.
2. Create a credential profile for a SCEP device identity.
3. Request a device identity for the device.
4. Optionally, validate the device identity request.
5. On the SCEP client (for example, a router) request the device identity from the MyID SCEP server.
6. MyID issues a device identity to the device containing one or more certificates.

2 Installation and Configuration

See the readme provided with the SCEP module for information on installing SCEP support for MyID.

The SCEP module installs the following:

- An update to the MyID database to support SCEP device types.
- An update to the MyID website to add SCEP Management Information Reports.
- A new website containing the SCEP server.

2.1 Setting up the SCEP server on a separate machine

You can install the SCEP web service server on the MyID application server, or on a separate machine.

Note: As the SCEP service is a web service, you must have the IIS Role on the server onto which you install the SCEP software. By default, the MyID application server does not require this role; you must add it if you intend to use the application server as the SCEP server.

If you install the SCEP web service on a separate machine to the application server, you must transfer the COM proxy to allow communication between the SCEP web service server and the application server.

You must export the COM Proxies from the application server to the SCEP server.

To do this, you must generate a proxy installer for the MyIDSCEPHandler COM+ application.

1. On the SCEP application server, open the Component Services and navigate to the MyIDSCEPHandler COM+ application.
2. Right click and select **Export**.
3. Click **Next**.
4. Select **Export as: Application proxy** and then select an appropriate location to generate the proxy installer.
5. Click **Next**.
6. Copy the `.msi` files to the SCEP web service server and run the installers from there.

2.2 Certificates

The SCEP application server requires a signing certificate and an encryption certificate.

2.2.1 Signing certificate

The signing certificate must have the following properties:

- Application policy: `Certificate Request Agent`.
- Request Handling Purpose: `Signature`.
- Key Usage: `Digital Signature`.

2.2.2 Encryption certificate

The encryption certificate must have the following properties:

- Application policy: `Certificate Request Agent`.
- Request Handling Purpose: `Encryption`.
- Key Usage: `Key Encipherment`.

2.3 Registry entries

To configure the SCEP registry:

1. On the SCEP application server, log in using the MyID COM+ account.
2. Request the previously-created SCEP signing and encryption certificates that will be placed in the CAPI store.

   Note: Do not enable strong private key protection on the certificates, as this will prevent processing of the request by the MyID account.
3. Once the certificates have been generated, install and save them as `.cer` files in Base64/PEM format.

   You must save them in a location accessible to the MyID application; for example, the MyID installation folder. By default, this is:

   ```
   C:\Program Files (x86)\Intercede\MyID\
   ```
4. Enter the filenames of the certificates in the system registry:

   Note: You must log in as a user with sufficient privileges to edit the registry.

   a) Run the Windows `regedit` utility.

   b) Navigate to:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Intercede\Edefice
   ```

   c) If not already present, create the key `SCEP`.

   d) Create or set the following string values to the full path of the related certificate:

   - `SigningCertificate`
   - `EncryptionCertificate`

3 Working with SCEP Device Identities

Note: If you are using SCEP purely for iOS OTA provisioning, you do not need to carry out any of the instructions in this section. See the *Setting up iOS OTA provisioning* section in the ***Mobile Identity Management Installation and Configuration Guide*** instead.

3.1 Setting up and requesting SCEP device identities

See the *Managing Devices* section of the ***Administration Guide*** for details of working with device identities.

You must carry out the following:

1. Set up a credential profile as described in the *Managing Devices* section of the ***Administration Guide***.

   You can optionally specify the **Require Challenge** option – for SCEP device identities, you can choose whether to display the one-time challenge code on screen or send an email message containing the challenge code.

   Note: You must not select any certificates policies that are marked as archived; you cannot issue device identities with archived certificates. If you attempt to collect a device identity using a credential profile that has an archived certificate, the collection will fail.

2. Add a device using the **Add Device** workflow or the Device Management API.

   When you add a device, make sure that the **Device Name** field will match one of the following in the SCEP request:

   - The DNSName in the Subject Alternative Name
   - The CN of the device's DN.

3. Request a device using the **Request Device Identity** workflow or the Device Management API.

   If you specified an owner for the device when you added it, the owner must be within your scope as an operator.

   You can choose to require a challenge code – you can display this code on screen, or send an email message containing the code to the device owner.

4. Optionally, validate the device identity request using the **Validate Device Request** workflow.

3.2 Collecting SCEP device identities

To collect a SCEP device identity, you must send a request from your SCEP-compliant device; for example, your router.

The SCEP device creates a PKCS#10 certificate request within a PKCS#7 container.

Note: The PKCS#10 request must meet the minimum key size requirements of the credential profile you have set up for the SCEP device identity.

This request can also contain the challenge code, which was either displayed on screen when you requested the device identity, or sent in an email message to the device owner.

The request is sent to the MyID SCEP server. The URL is:

```
http://<SCEPserver>/MyIDSCEP/MyIDSCEP.ashx
```

where:

- `<SCEPserver>` is the name of the machine on which you installed the MyID SCEP server; for example:

  `http://myserver.example.com/MyIDSCEP/MyIDSCEP.ashx`