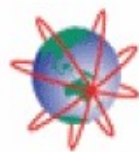


AusCERT CA

Certificate Services Manager

Software Version 2.8.24

Simple Certificate
Enrollment Protocol
Guide Version 2.8.012412



AusCERT

Simple Certificate Enrollment Protocol

Introduction

The Simple Certificate Enrollment Protocol (SCEP) is a mechanism for automating the requests of digital certificates. An administrator, by using SCEP, can automatically re-enroll and retrieve new digital certificates for the ones that are due to expire or expired. It was developed originally by Cisco Systems for use in network devices such as routers, but its use has expanded to other hardware and software devices.

A recent example of a SCEP-capable system would be Apple's iOS platform and the devices that run it (iPhone, iPad, iPod Touch).

AusCERT CSM supports SCEP and is integrated with a fully-compliant SCEP server. This document describes the settings required to access and use CSM as a SCEP server to enroll certificates.

Settings

1. Enabling Self-Enrollment and Setting Access Code

Users can download certificates through SCEP only if Self-Enrollment is enabled and access code set in AusCERT CSM. This can be done while adding a new organization/department or editing organization/department by the Master Administrator or the RAO Administrator.

To enable self-enrollment and set access code for organizations:

- In the 'Organizations' screen, click the 'Add' button or the 'Edit' button beside an existing organization.
- In the 'Add New Organization' or 'Edit Organization' dialog, click the 'Client cert' tab.

The screenshot shows a dialog box titled "Edit Organization: Test Organization" with five tabs: "General", "Client cert", "SSL", "Code Signing Certificate", and "E-mail Template". The "Client cert" tab is selected. The form contains the following fields and controls:

- Self Enrollment:** A checkbox that is checked (indicated by a green checkmark).
- Access Code:*** A text input field containing the value "654321".
- Web API:** A checkbox that is unchecked.
- Allow Key Recovery by Master Administrators:** A checkbox that is unchecked.
- Allow Key Recovery by Organization Administrators:** A checkbox that is checked (indicated by a green checkmark).
- Allow Principal Name:** A checkbox that is checked (indicated by a green checkmark).
- Allow Principal Name Customization:** A checkbox that is unchecked.
- Client Cert Types:** A button labeled "Customize".
- Key Usage Template:** A button labeled "KUT".

At the bottom of the dialog are "OK" and "Cancel" buttons.

- Select the Self Enrollment checkbox.

The Access Code field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

To enable self-enrollment and set access code for departments:

- In the 'Organizations' screen, click the respective 'Department' button beside an Organization for which you want to enable self-enrollment and set access code.
- In the 'Departments' dialog, click the 'Add' button or the 'Edit' button beside an existing department.
- In the 'Add New Department' or 'Edit Department' dialog, click the 'Client cert' tab.

The screenshot shows the 'Add New Department' dialog box with the 'Client cert' tab selected. The 'Self Enrollment' checkbox is checked. The 'Access Code' field contains the text 'a2b1c4'. Below this, there are five checkboxes for key recovery permissions, all of which are checked: 'Allow Key Recovery by Master Administrators', 'Allow Key Recovery by Organization Administrators', 'Allow Key Recovery by Department Administrators', 'Allow Principal Name', and 'Allow Principal Name Customization'. At the bottom, there is a 'Client Cert Types' section with a 'Customize' button. The dialog has 'OK' and 'Cancel' buttons at the bottom left.

- Select the Self Enrollment checkbox.

The Access Code field will appear.

- Enter the access code in the field. This should be a mixture of alpha and numeric characters that cannot easily be guessed.
- Click 'OK'.

To view the access code that is already set for organizations/departments, click the 'Edit' button beside the respective organization/department. You can view the access code under the 'Client cert' tab. DRAO administrator cannot set and view access codes and must consult RAO administrator to find access code.

Note: The same access code should be entered in the 'challengePassword' field during the process of creating Certificate Signing Request. See section [Certificate Signing Request](#) for more details.

2. URL of the SCEP server

`http://cert-manager.com/customer/AusCERT/scep/smime/pkiclient.exe`

The URL of the SCEP server must be entered into the user's SCEP client software – not typed into a browser. It tells the client software where to send the SCEP requests. Properly formatted SCEP requests are sent to this URL. The individual configuration of these clients lies outside of the scope of this document. However, we have provided a list of SCEP capable-clients below. Each client has its own accompanying support documentation which will assist with SCEP configuration.

SCEP Clients

The following software provides support for SCEP:

- [cryptlib \(C\)](#)
- [Network Device Enrollment Service \(Windows Server 2008\)](#)
- [OpenCA \(Perl\)](#)
- [OpenSCEP \(Perl\)](#)
- [jscep \(Java\)](#)
- [EJBCA \(Java Enterprise Edition\)](#)

Note 1: The URI protocol should be 'http' and not 'https', since the SCEP protocol relies on signed messages during a transaction and so operates over 'http'.

Note 2: Private keys for certificates obtained using SCEP cannot be escrowed as the private key is never sent to CSM.

3. Certificate Signing Request

The Certificate Signing Request (CSR) requires the following:

- Key size - A minimum of 2048 bit.
- Subject information - Client certs need a minimum of CN and emailAddress.
- The subject CN must be an allowed domain, or the emailAddress (client certificates) must lie in an allowed domain for that organisation or department.
- The CSR **requires** a 'challengePassword' to be set. This should be set to the 'Access Code' from within AusCERT CSM for the organisation or department the certificate is being enrolled into. See section [Enabling Self-Enrollment and Setting Access Code](#) for more details on setting access code.

Tips for using SCEP in AusCERT CSM for iOS devices:

On some older versions of iOS (4.x), setting the RSA Key Size in the mobileconfig file at 4096 may be required, as it appears iOS will sometimes generate 2047 bit keys (when 2048 bit is chosen), which will not be accepted by AusCERT CSM or the CA.

In the nested-arrays for the Subject information in the mobileconfig, it may be necessary to use the OID for the 'emailAddress' field - 1.2.840.113549.1.9.1.

The 'challengePassword' can be set using the 'Challenge' key/value pair in the mobileconfig.