Simple Certificate Enrollment Protocol (SCEP)

Integration Guide

July 13, 2020

digicert®

Legal Notice

DigiCert, Inc.
2801 North Thanksgiving Way, Suite 500
Lehi, UT 84043
https://www.digicert.com/

Table of Contents

INTRODUCTION **4**

CREATE PROFILE IN DIGICERT PKI PLATFORM **4**
VERIFYING THE SCEP ENROLLMENT **7**
SCEP ENROLLMENT VIA DIGICERT SCEP CLIENT 7
SCEP RENEWAL 10
SCEP ENROLLMENT CODE (PASSCODE) ENHANCEMENTS **10**
SCEP SERVER ERROR CODES **12**

Introduction

The Simple Certificate Enrollment Protocol (SCEP) allows network administrators to easily enroll network devices for certificates in a scalable manner. It validates the authenticity through passcode and the SCEP protocol allows for the below authorization mechanisms for the initial enrollment:

- Default enrollment code: Default passcode set allows all the registered and not pre-registered devices to use the same default passcode. The pre-shared secret is established by the administrator of a DigiCert PKI Platform account against a certificate profile.

Note: Microsoft Intune integration via SCEP is also supported. Please refer to the Integration guide for Microsoft Intune for details.

An Enterprise PKI administrator retrieves the challenge password and gives it to a trusted network administrator to generate certificates for trusted network devices.

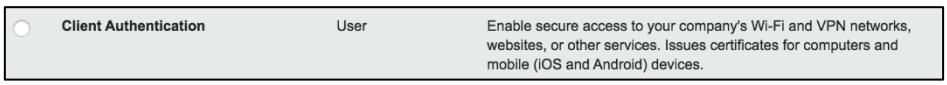
SCEP has also become an enrollment mechanism for end-user devices like mobile phones and laptops and is increasingly being used to deliver user authentication certificates for Wi-Fi and VPN access.

The DigiCert PKI Platform SCEP service supports the generation of a unique enrollment code for each certificate enrollment, or the use of a Default Enrollment Code that is shared by all devices enrolling for a certificate via SCEP.

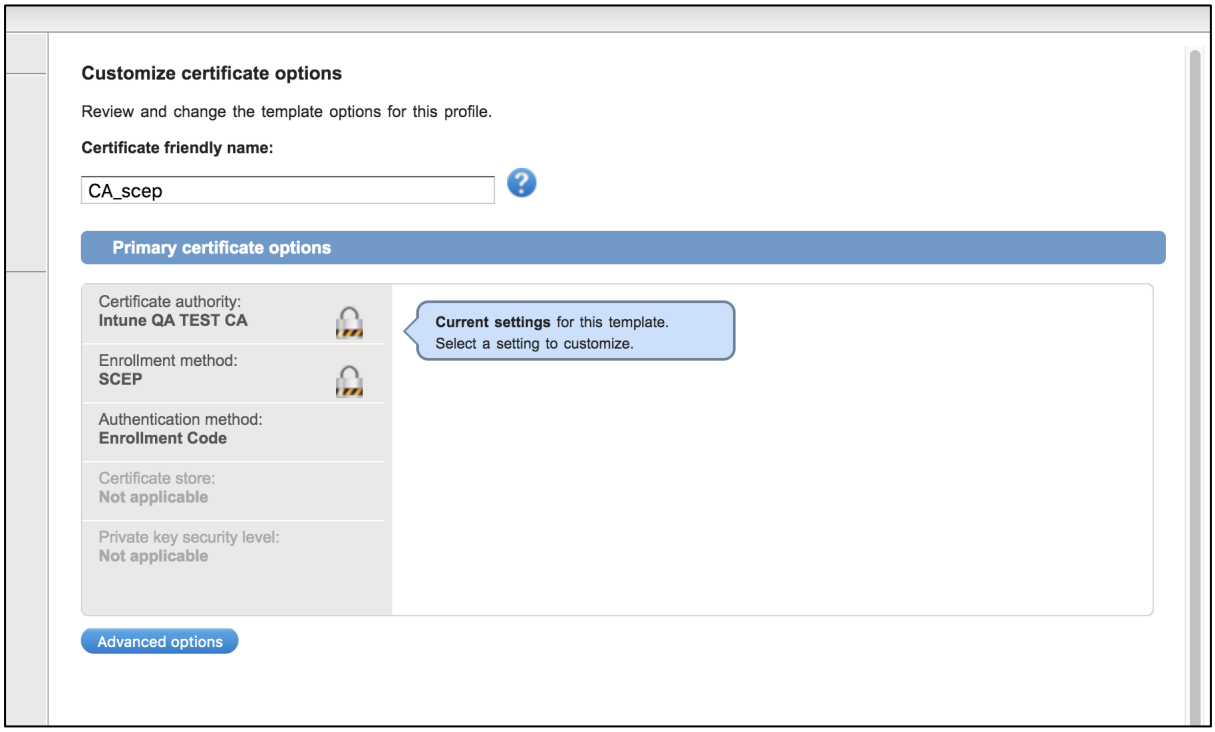
Create profile in DigiCert PKI Platform

To create a certificate profile in DigiCert PKI Platform for SCEP consumption, follow the below steps:

1. In the PKI Manager dashboard, click Manage certificate profiles.
2. Click Add certificate profiles.
3. Select the mode of the profile and click Continue.
4. Select the certificate template that you want to use (e.g. Client Authentication) and click Continue.

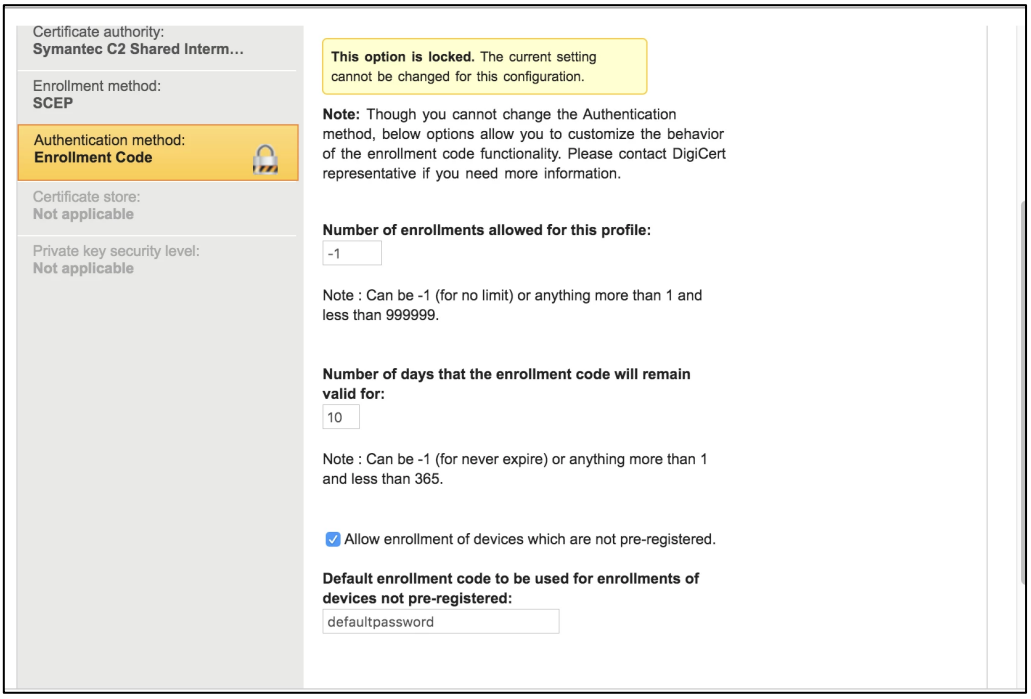


5. Provide a **friendly name** for the profile.



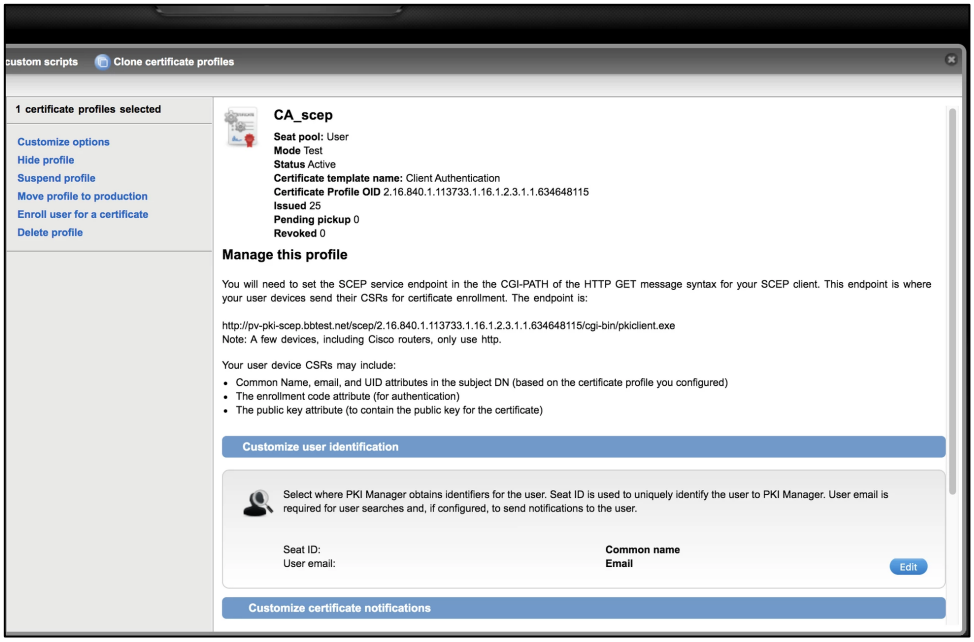
6. Select the enrollment method as "SCEP".

7. Authentication method is defaulted to "Enrollment Code". Configure the enrollment code options as required. More details on the enrollment code configuration can be found at: SCEP Enrollment Code (passcode) enhancements



8. Under **Advanced Options** and select Subject DN, SAN fields as required. The values for these fields can be read from the SCEP request if the "Scep Request" source is selected.

9. Save the profile after completing the configuration. If successful, a confirmation message is displayed, together with the SCEP Server end-point URL.



Note: You can use http or https to submit requests against the SCEP Server URL.

Verifying the SCEP enrollment

Summary of steps:

A. Create a certificate profile with SCEP as the enrollment method as mentioned in the above section.

B. Choose your Subject DN / SAN options appropriately.

C. Create a Seat for your entity (User/Device/Server) if not already created via PKI Manager (manually or by uploading a CSV file), or via Web Services. If using a Default enrollment code for authentication, then devices can be enrolled directly without need to create a Seat, i.e. no pre-enrollment/registration.

D. Enroll for a device certificate via the DigiCert SCEP Client. Contact your DigiCert Representative to gain access to the client.

SCEP Enrollment via DigiCert SCEP Client

This section details how to enroll for a device certificate making use of the DigiCert SCEP Client.

Note: The SCEP protocol only supports RSA keys and CSRs - ECC-based keys are NOT supported (EST protocol can be used instead).

---

1. Create an RSA key pair using the below OpenSSL command:

```
openssl genrsa -out private_key.pem 2048
```

2. Convert private key to der format:

```
openssl pkcs8 -topk8 -inform PEM -outform DER -in private_key.pem -out
private_key.der -nocrypt
```

3. Write out the public key:

```
openssl rsa -in private_key.pem -pubout -outform DER -out public_key.der
```

4. Generate an RSA-based CSR and convert it to DER format:

```
openssl req -new -sha256 -key private_key.pem -out csr.pem
```

A sample template is shown below:

```
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a
DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [AU]:
State or Province Name (full name) [Some-State]:
Locality Name (eg, city) []:
Organization Name (eg, company) [Internet Widgits Pty Ltd]:
Organizational Unit Name (eg, section) []:
Common Name (e.g. server FQDN or YOUR name) []:
Email Address []:Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

NOTE: This challenge password should be the enrollment passcode which was set in the SCEP profile.

```
openssl req -in csr.pem -out csr.der -outform DER
```

5. Enroll for a certificate via SCEP making use of the "enroll" operation and the keys/CSR generated in the above operations:

```
java -jar DigicertScepClient.jar -url http://pki-
scep.symauth.com/scep/2.16.840.1.113733.1.16.1.3.1.4.1.634903267/cgi-
bin/pkiclient.exe -operation enroll -key passed -privkeyfile
private_key.der -pubkeyfile public_key.der -csr csr.der
```

Command line Usage:

```
SCEPClient -url <url> -operation [enroll|renew] -key
[<passed|generate>] -privkeyfile <private-key-file> -pubkeyfile
<public-key-file> -csr <file|filepath> [...optional args...]
...where the required argugments are:
   -url <url>           The URL of the SCEP server
   -name <name>         The dnsName of the passcode you're enrolling
for
   -passcode <code>     The passcode you're enrolling for
   -subject <subj>      A subject name for the CSR
   -operation <enroll|renew specifying the operation being invoked
   -key <passed|generate>  A pre-generated RSA key is being passed as
-privkeyfile |-pubkeyfile
   -privkeyfile <filepath> specifying the private key path to be used
for the operation
   -pubkeyfile <filepath>  specifying the public  key path to be used
for the operation
...and the optional args are:
   -debug <true|false>       Whether to output the debug logs to the
console
   -outpath <path>       Path to write the temp outputs from the client
   -passcode <code>      Challenge
   -subject <subj>       Subject in the form of CN=<something>
   -dnsName <dnsName>    DNS name
   -upn <upn>            UPN name
   -uri <uri>            URI
   -rfc822Name <rfc822name>   rfc822Name
   -keysize <keysize>     RSA Key Size
   -keyPassword <pwd>     The password for the above key (if needed)
   -csr <file>|<filepath> A pre-generated CSR in der format or a folder
containing csr files in der format
   -cert <file>           Certificate to be used for the renew
operation
```

Note: If you are submitting a CSR containing an enrollment code within the Challenge Password attribute of the CSR, then you do not need to provide the -passcode option.

Example output:

```
$ java -jar DigicertScepClient.jar -url http://pki-
scep.symauth.com/scep/2.16.840.1.113733.1.16.1.3.1.4.1.634903267/cgi-
bin/pkiclient.exe -operation enroll -key passed -privkeyfile
private_key.der -pubkeyfile public_key.der -csr csr.der
Util:log>Reading from keypair file individually
Util:log>Generating temporary self-signed cert...
Util:log>Using SCEP URL 'http://pki-
scep.symauth.com/scep/2.16.840.1.113733.1.16.1.3.1.4.1.634903267/cgi-
bin/pkiclient.exe'
Util:log>Using CA Instance 'null'
Util:log>Using subject = 'CN=test-device-01@digicert.com'
Util:log>Using passcode 'null'
Util:log>Using dnsName 'null'
Util:log>Using upnName 'null'
Util:log>Using uri 'null'
Util:log>Using rfc822Name 'null'
Util:log>Writing temporary self-signed cert to out.cer...
Util:log>Constructing client...
Util:log>Reading CSR from csr.der...
```

```
Util:log>Creating enrollment transaction...
log4j:WARN No appenders could be found for logger
(org.jscep.client.Client).
log4j:WARN Please initialize the log4j system properly.
log4j:WARN
See http://logging.apache.org/log4j/1.2/faq.html#noconfig for more
info.
Util:log>Sending the transaction...
Util:log>Transaction result:false
Util:log>Certificate was issued!
Store=java.security.cert.CertStore@65c7a252
Util:log>Got certificate:C=US, O=LTE STD Full, CN=stest-device-
01@yopmail.om/3fe7abf5b0b764c29b3102e49de21e2b; writing to ./csr.cer
```

SCEP Renewal

If the certificate (csr.cer generated above) is within the renewal window set by the Administrator for the target certificate profile, use the below command to renew the certificate:

```
java -jar DigicertScepClient.jar -url http://pki-
scep.symauth.com/scep/2.16.840.1.113733.1.16.1.3.1.4.1.634903267/cgi-
bin/pkiclient.exe  -operation renew -key passed -privkeyfile
private_key.der -pubkeyfile public_key.der -csr csr.der -cert csr.cer
```

All options remain as they are for "enroll" operation except the operation value will be "**renew**" and you would need to pass the previously obtained certificate in the "**-cert**" option.

This original certificate & private key will be used to sign the CSR passed and a new renewed certificate will be issued.

Note: The CSR can be the same one that was used during the enrollment, or it can be a new CSR with the exact same Subject DN, created using the same keypair during the original CSR generation.

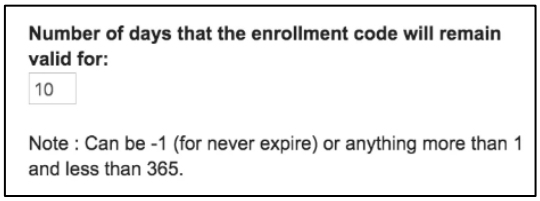
The older certificate will still be valid for the remaining validity period, and the renewed certificate will have a validity period based on the certificate profile, plus the addition of any days before the expiry date of the certificate.

SCEP Enrollment Code (passcode) enhancements

The basic authentication of SCEP envelope includes a challenge password (i.e. an enrollment code or a passcode). This section includes enhancements which allows the PKI administrator to manage SCEP, specifically for IoT Manufacturing use-cases.

a. **An increased validity period:** The enrollment code validity has been increased to 365 days. For SCEP enrollments, by default the validity period is 10 days. However, the administrator can update this value while creating the certificate profile.

b. **Never-Expire Enrollment Code:** In the enrollment code validity text box, if the value is set to **-1**, the enrollment code will never expire.



c. Re-use of Enrollment Codes: For SCEP profiles, an administrator can select an option for multiple usage of enrollment codes for all devices enrolling for a certificate against a given certificate profile. Selecting this option will keep the enrollment code value the same for all the enrollments submitted against that profile.
For setting the default passcode, please select the checkbox "Allow enrollment of device which are not pre-registered".

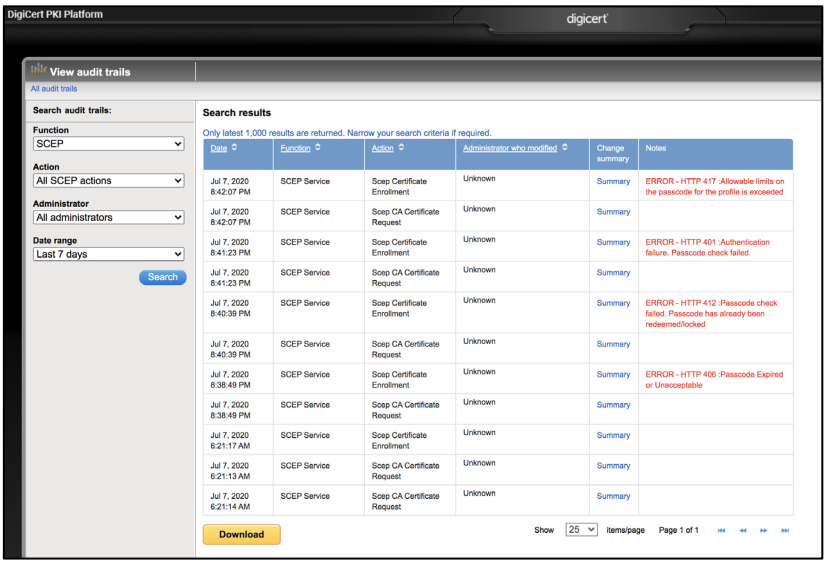
Note: The Default enrollment code must be at least 9 characters long and up to 64 characters, which can be alpha-numeric. You must securely store this enrollment code value and not share it with unintended devices.

d. Restricting the number of enrollments from a profile: From a SCEP profile, the number of enrollments can be restricted. A text box is provided for entering the maximum number of enrollments to be allowed against a certificate profile. Once set by the administrator, the maximum number of enrollment codes that can be created, will be monitored, and limited to the value set within the profile.

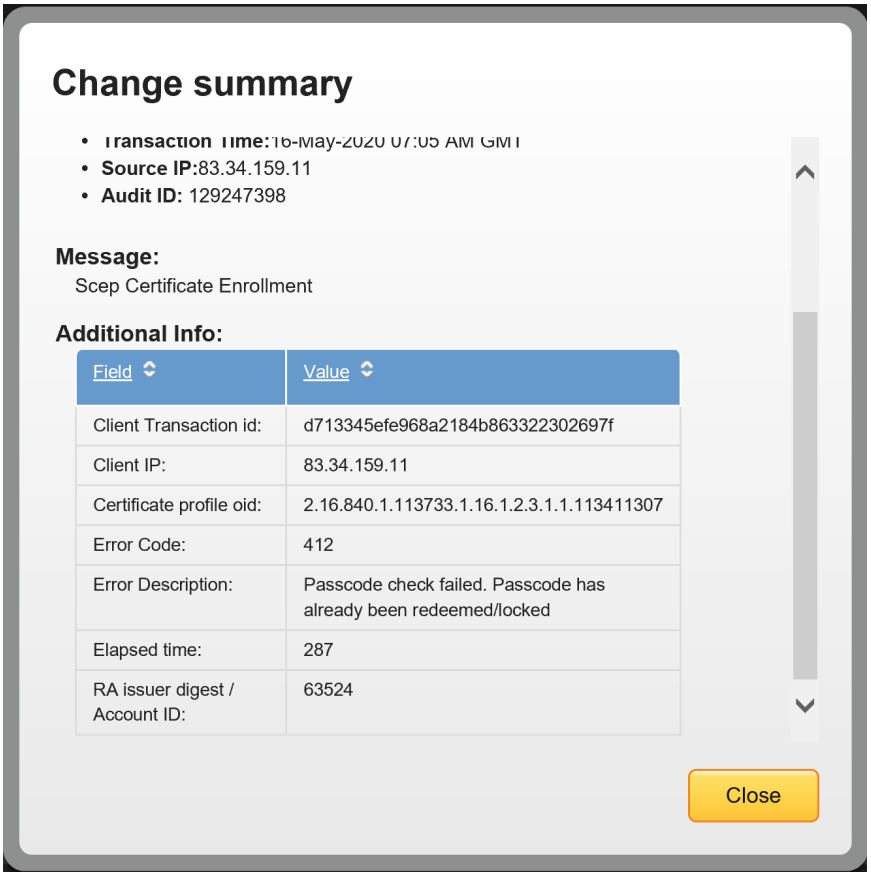
Note: It can be -1 (for no limit) or a value greater than 1 and less than 999999.

SCEP Server Error Codes

The SCEP Server error codes and messages can be tracked under the **View audit trials** page within PKI Manager, by selecting SCEP under the Function search filter, and the appropriate Action to search for a specific SCEP operation.



When clicking on the **Summary** link, additional audit trail information can be obtained for every SCEP operation, e.g. transaction id and time, source IP address, etc.



The below table captures the standard based HTTP error codes used by the DigiCert PKI Platform SCEP Server, to deliver more meaningful error codes and messages to clients interacting with DigiCert's SCEP Server.

HTTP error code	HTTP error message	DigiCert error message	Description
400	BAD REQUEST	Passcode verification failed.	**Bad enrollment request**. Typically, a miss-match of name-value pairs contained within the CSR and those configured by the Administrator for the matching certificate profile, e.g. missing attribute within the Subject DN and/or Subject Alternative Name (SAN).
401	UNAUTHORIZED	Passcode Authentication failed.	Enrollment code is **invalid** - does not match the value configured by the Administrator
406	NOT ACCEPTABLE	Passcode has expired.	Enrollment code has **expired**
412	PRECONDITION FAILED	Passcode is either redeemed or locked Number of bad password attempt exceed	Enrollment code has already been **redeemed/locked**
417	ERROR OCCURRED	Allowable limits on the passcode for the profile is exceeded	The number of enrollments allowed in the profile configuration has been exceeded