PKI SCEP Integration Guide

Introduction

Simple Certificate Enrollment Protocol, is a protocol originating from Cisco, and standardized by the IETF.
Its latest version is available at: https://tools.ietf.org/html/draft-nourse-scep-23

While abandoned nowadays by the IETF, SCEP is still very popular among vendors (Juniper, Checkpoint, etc.) because of its simplicity, compared to IETF-pushed alternatives. This is the reason why the PKI offers a SCEP connector, that has the following specifications:

- only CA mode is supported, but its implementation circumvents the security issues associated with this mode
- only challenge mode is supported for initial requests, the challenge changing every day to mitigate security issues
- renewal using authentication from previous certificate is supported
- operations GetCA, GetCACaps and PKCSReq are supported

Setup

The SCEP connector is automatically setup by the PKI during it installation.
To integrate with devices, the following parameters are needed:

- URL: http://<pki_ip_address>/scep
- Challenge: see under "SCEP" > "SCEP Challenge"

Some devices require the following information:

- Full URL: http://<pki_ip_address>/scep/pkiclient.exe
- SCEP CA Certificate: see under "SCEP" > "SCEP CA Certificate" (its fingerprint is there as well)

Finally, please note that the SCEP connector will be unavailable if you deactivate the "Server" certificate profile.

SCEP Setup for Cisco Devices

Cisco IOS devices can be enrolled by typing the following commands:

```
enable
configure terminal
```

```
crypto key generate rsa general-keys modulus 2048
crypto pki trustpoint nspki
enrollment url http://<pki_ip_address>/scep
exit
crypto pki authenticate nspki


Certificate has the following attributes:
Fingerprint MD5: XXXXXXXXXXX
Fingerprint SHA1: XXXXXXXXXXXXXXX


% Do you accept this certificate? [yes/no]: yes


crypto pki enroll nspki


%
% Start certificate enrollment ..
% Create a challenge password. You will need to verbally provide this
password to the CA Administrator in order to revoke your certificate.
For security reasons your password will not be saved in the configuration.
Please make a note of it.


Password: <scep_challenge>
Re-enter password: <scep_challenge>


% The subject name in the certificate will include: XXXXXXXXXXX
% Include the router serial number in the subject name? [yes/no]: no
% Include an IP address in the subject name? [no]: no
Request certificate from CA? [yes/no]: yes
% Certificate request sent to Certificate Authority
% The 'show crypto pki certificate verbose nspki' command will show the fingerp
```

Please note that this doesn't cover the PKI CA Certificate import, that should be performed separately, if necessary.