

DPOP Interception Certificate Best Practices

- [Introduction](#)
- [Comparing PKI options for DPOP](#)
- [Identifying the right configuration](#)
 - [I want to use a Dedicated PKI](#)
 - [I want to use my existing Corporate PKI](#)
 - [I want to use Netskope PKI](#)
- [DPOP Operations](#)
 - [Introduction](#)
 - [BYOK](#)
 - [Generate a CSR](#)
 - [Option 1 - Generate the CSR and export with the DPOP CLI](#)
 - [Option 2 - Use Openssl](#)
 - [Sign the CSR with the PKI](#)
 - [Import the signed Certificate on DPOP](#)
 - [Netskope Cloud CA](#)
 - [Self signed certificate](#)
 - [Backup/rollback](#)
- [Dedicated PKI Operations](#)
 - [Requirements](#)
 - [Setup a Dedicated PKI with openssl](#)
 - [Prepare CA structure](#)
 - [Generate the private key](#)
 - [Generate Root certificate](#)
 - [Check the Root CA details](#)
 - [Export the Root CA certificate to deploy on end user devices](#)
 - [Generate a new CSR directly in the PKI directory](#)
 - [Sign a CSR with the Dedicated PKI](#)

Introduction

This guide is designed to present the options supported by DPOP (DataPlane On-Premises) to perform SSL interception, and provide best practices.

In addition, the "Dedicated PKI Operations" section describes how to create a new PKI if needed.

Comparing PKI options for DPOP

To perform SSL interception, DPOP needs to generate server certificates that are trusted by end user devices.

DPOP supports 4 different types of PKI Root for SSL interception:

- [Dedicated PKI for SSL interception \(Recommended option\)](#)
- [Leveraging an existing Corporate PKI](#)
- [Using Netskope Cloud PKI \(not recommended, incompatible with ECA\)](#)
- [Generating a new Root directly on the appliance.](#)

In all cases the Root of the PKI must be deployed on end user devices, this can be performed by GPO, SCCM, MDM or similar solution.

	Pros	Cons
Dedicated PKI with OpenSSL	<ul style="list-style-type: none"> Independent of existing PKI No revocation management needed No risk on existing PKI 	Needs to be deployed on managed devices
Existing Corporate PKI	Already deployed on managed devices.	<ul style="list-style-type: none"> DPOP will generate valid certificate without any validation. It is best practice to not mix manually validated PKI and interception PKI. Even if DPOP Sub CA is revoked, SSL clients may continue to trust it.
Netskope Cloud PKI	Automatically deployed with NS Client	<ul style="list-style-type: none"> This feature is not compatible with Ephemeral CA. DPOP with Netskope Cloud PKI will block activation of Ephemeral CA feature.
new Root on the appliance (self signed certificate CLI)	<ul style="list-style-type: none"> No external tool required. Very simple and fast to achieve. 	<ul style="list-style-type: none"> Private key of the root is not exportable in clear text for other purposes Import/export is the only way to synchronize the key with other DPOP

The Root is limited to DPOP use cases, it's not possible to use it for BYOK in cloud proxy on other use cases.

The appliance should not be in production since the new Root will be immediately active.

Identifying the right configuration

I want to use a Dedicated PKI

Steps:

1. Setup the Dedicated PKI. See the "Dedicated PKI Operations" section.
2. Deploy new Root on end user devices
3. Configure DPOP with BYOK. See the "BYOK" section.

I want to use my existing Corporate PKI

Steps:

1. Configure DPOP with BYOK. See the "BYOK" section.

I want to use Netskope PKI

 This feature is not compatible with Ephemeral CA feature.

Steps:


1. Deploy Netskope Root CA on managed devices (The Root CA can be downloaded from the management console in Settings > Manage > Certificates > Signing CA)
2. Configure DPOP with Netskope CA. See the "Netskope Cloud CA" section.

DPOP Operations

Introduction

On the DPOP, the CLI allows to configure one of the following mode:

- BYOK
- Netskope Cloud CA
- Self signed certificate


 DPOP supports only one configured certificate. It is not possible to have several certificates imported and switch between them.

BYOK

To use a custom key/certificate, 2 options are supported:

- Generate the key and csr directly on the DPOP. See the "Option 1 - Generate the CSR and export the DPOP CLI" section.
- Generate a key and csr separately and import the key/certificate on the DPOP. See the "Option 2 - Use Openssl" section.


CSR is the most secure method and generally the recommended option.

 Private keys are encrypted and can be restored but are not exportable in clear text. If you need access to keys, it's better to use OpenSSL to generate the CSR.

 The same key/certificate can be used on multiple DPOP but having a dedicated key/cert per DPOP is considered as best practice.

Generate a CSR

Option 1 - Generate the CSR and export with the DPOP CLI

 When using CSR, please be aware Private key is stored on disk only after certificate is imported. The DPOP must not be rebooted between CSR and certificate import, otherwise the private key is lost and a new CSR will be required.

```
1 lab-dpop1(config)# run request certificate generate forward-proxy certificate-request common-name "DPOP1 Intermediate CA" email-address support@netskope.com
2
3 lab-dpop1(config)# show dataplane forward-proxy csr
4 "-----BEGIN CERTIFICATE REQUEST-----
5 MIICjCCAXYCAQAwSTEGMB4GA1UEAwVxbGFiLWVudXR0b3JzLm1uZm8x
6 JTAjBgkqhkiG9w0BCQEFM1ib3V0aG9yc0BuZXRza29wZS5jb20wggEiMA0GCSqG
7 SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDwmyor93Do44MEH1Hgd6jj3Yz+pkjLxKu6
8 80GQaniq1Jp9ZMBP09f3NdfgpmX5WEkEkXj1CXhoXneu/Wuu5ptkEdSefARwvbH
9 81tswUGNerxicFlwJWS6BwZw75xwWQeQtvZ0bIUxLzFZ2DeNBkD7AZyDsr5hyI
10 t4A8UjZh5/q4RQ0/IL8jivRfXwih8Y88/FKEVST/szt8sboUkUn4rmuYz740A7
```

```

11 Kw+/5z5sqetnU+2C728RCZUIlW0Kx0+f2D459nkhPFo2bCweg++XZkRF0graou8
12 0GazgKxqvXau/ow20mIgd465doM1PyToT03Qbo1ZLWvgP68fZEs5AgMBAAGgADAN
13 BgkqhkiG9w0BAQsFAA0CAQEAvd0IfnCvZjHtNKBV9d0vK9Xr5P21pLTPVQ+RNVt
14 BurMtQlPDCqdDieQ2Qm9iVlhWqtC1eSf68XkLmdIuy1I2xLJrib0TcHT3tnVn+6
15 9UrIGQR40N8iGZJBVRILjATCs+uahqMwthTe1PFp0Iq2T4sC2b1XreXrLC0gpodd
16 Mpu83Bq3IDwo+xTutIDYBnD9JJl9ApLQKTF0aTubbjL34IKcKk1yPAGwMLEyDKqM
17 Ee5oR59758T1xggrEq2Nb1/rDLx/SE5IkknVVVtCxtwWZ1G3wucX63ixtRCdCpG
18 llfvYF6Dxm0g43i0yJHG01TfKazprFZGRS60bx3ecLHDg==
19 -----END CERTIFICATE REQUEST-----
20 "
21
22 lab-dpop1(config)#

```

Option 2 - Use Openssl

Generate Key with 4k size.

```
1 openssl genrsa -out private/dpop_key.pem 4096
```

Generate a CSR

```
1 openssl req -config openssl.cnf -new -key private/dpop_key.pem -out certreqs/dpop_csr.pem
```

Example:

```

1 openssl req -config openssl.cnf -new -key private/dpop_key.pem -out dpop_csr.pem
2
3 You are about to be asked to enter information that will be incorporated
4 into your certificate request.
5 What you are about to enter is what is called a Distinguished Name or a DN.
6 There are quite a few fields but you can leave some blank
7 For some fields there will be a default value,
8 If you enter '.', the field will be left blank.
9 -----
10 Country Name (2 letter code) [US]:
11 State or Province Name (full name) [California]:
12 Locality Name (eg, city) [Santa Clara]:
13 Organization Name (eg, company) [Netskope]:
14 Organizational Unit Name (eg, section) []:
15 Common Name (eg, YOUR name) [Netskope DPOP Root]:DPOP CA
16 Email Address [support@netskope.com]:
17 mbouthors@mac-10g sample_pki %

```

Sign the CSR with the PKI

To sign the CSR with dedicated PKI included in this guide, see the "Sign the CSR with the Dedicated PKI" section.

To sign the CSR with existing Corporate PKI, follow the process of the PKI.

Import the signed Certificate on DPOP

⚠ The new certificate is active at the "save" action, please make sure it is trusted by end user devices before importing it

Once the certificate as been signed but the PKI, import it with DPOP CLI:

⚠ If you generated the private key externally, please use " set dataplane forward-proxy server-key" to import it.

```

1 lab-dpop1(config)# set dataplane forward-proxy server-cert
2 Copy and paste just your single PEM-formatted server CA certificate (no keys).
3 Enter one or more lines of input. When done, press Ctrl+D
4 -----BEGIN CERTIFICATE-----
5 MIIETjCCAp6GawIBAgIJAP3vkTz2S2bQMA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNV
6 BAYTA1VTMRMwEQYDVQIDApDYWxwZm9ybm1hMRQwEgYDVQQHDATYw50ySBD6GFy
7 YTERMA8GA1UECgwITmV0c2tvcGUxGzAZBgNVBAMMEK5ldHNrb3B1IERQT1AgUm9v
8 dAeFw0yMzEyMDgxMjI5MjBjBjF0ZmZlYm9uZm9uZm9uZm9uZm9uZm9uZm9uZm9u
9 T1AxIEludGVybWkkaWw0ZSB0QCCASiWdQYJKoZIhvcNAQEBBQADggEPADCCAQoC
10 ggEBAAMo8znKgrbh0iUE1bxsqW0G8RS/4BhP1J5C51Mxgt5qhRD1657ci7w/5Cng
11 BI2IkMzBcXk6UH5jXNnSm0muAWIupnzvhAnJYunmQP21wYc55BKE010t/1Hm206+
12 dBwT2mLfnwCQodjM49tV5qxQvJvDKxpmTGunMtxUnf1QhorYYAjpDxFLHtZ8yEzM
13 lX110swuzeae1yWkCvkBVFp8kDQbbs79zQw+KMaVd8+Njvqz8AqCURCY9XBtdc
14 jK1Sm95Bjg8Rghr2zjyYwtubK+twdghkUdzM3gK05c2qG23HbJNrvag4zqz8NLa
15 D48oCfmpCp3M1HtEt6bs7v0/vb0CAwEAooBqjCBpzASBGNVHRMBAF8ECCDAGAQH/
16 AgEAMA4GA1UdDwEB/wQEAWIbPjAgBGNVHSubA8EFjAUBggrBgEFBQcDAQYIKwYB
17 BQUhAwIwHQYDVR0BBYEFEMju6Q8f23APyTiWkPzAbb/ombRMB8GA1UdIwQYMBAA
18 FK6zqrw/xFLz4B9go1FZo4oovxWamb8GA1UdEQYMBaBFH1cHBvcnRAbmV0c2tvc
19 cGUuY29tMA0GCSqGSIb3DQEBCwUAA4ICAQCZSyEKcVvJ3t+C1tKtUR0owIyU+dL3
20 KRN+p09qs2jjEgV1N/chwBdzToyrCbH1MvTgrHLSCqtE/vTus+noKg8cI1212Uw1
21 sE7vSmkEFAXYFzgo2Cx8cbIIQKVITg7C9/VBQNhzeL5poc/j50f99EtSHkKHX9xp
22 iI13iBlE2HSDb5rAP6HMGc1PFnLsSEAKi7SPL2gZhuQhL+b2MXEob9wLyS1a34Qx
23 81owbj9S1I/OCYZjw+5k/5ixpGUVMPuwrCjkgCqKQTeFmOrWENSHUL5goMRUGYHH
24 QkZfd0Fq8AUmJE4Dj2EtpkAzH0CpW0bduai9BL8RpmqzdAB8z6LH6FCLRzrE7
25 1+R5EJSQjYUSP06RPC7xqkMa4PN8K2kD45Bf0/SgH0AM0TjRQ068yEKZu6QIT8

```

```

26 5f1Kw/pexwW5AKK31UR9oVAYryz3W/I2K7zFL+ZtEn6d7Wp7APRkwK/TwkrfDSVY
27 rFY2wU5QSifyKV7DeJcjq+fPkmRv1zhev18XG01YYJkDw+XU0Jb4ItrPLTLXXiUq
28 oTGBJAR+zGyRu3r9Y9EiS/2ak3ZNsHH+SZZhoiqqjJQp2kEntXy3kjMhXkdZk00
29 6++oT2Vi6pBUCxjI0o6hpRl+Ld0BKjP/CpEm6GI8mp+bJPkqhW8ox6XWpNaEoCwR
30 bkgDYD2GSr4AXg==
31 -----END CERTIFICATE-----
32
33
34 Certificate Issuer:
35   Country: US
36   State: California
37   Issuer Field: Santa Clara
38   Organization: Netskope
39   Common Name: Netskope DPOP Root
40 Subject:
41   Common Name: DPOP1 Intermediate CA
42 Valid On: Dec 8 12:29:20 2023 GMT
43 Expires On: Dec 05 12:29:20 2033
44
45 lab-dpop1(config)# save
46 This may take few seconds to few minutes depending on the configuration changes.
47 Restarting lcfowardproxy container
48 Configuration saved
49
50 lab-dpop1(config)#

```

Netskope Cloud CA

⚠ This feature is not compatible with Ephemeral CA feature. If ECA is enable, this configuration will fail.

When no custom certificate is configured on the DPOP, the Netskope Cloud CA is automatically used.

If you installed a custom certificate already, you can switched to Netskope Cloud CA by deleting the custom certificate.

⚠ The Root CA must be downloaded from the management console (Settings > Manage > Certificates > Signing CA) and deployed on end user devices.

```

1 lab-dpop1(config)# delete dataplane forward-proxy server-key
2 lab-dpop1(config)# delete dataplane forward-proxy server-cert
3 lab-dpop1(config)# save
4 This may take few seconds to few minutes depending on the configuration changes.
5 Restarting lcfowardproxy container
6 Configuration saved

```

Self signed certificate

Alternatively, it is possible to generate a new Root CA on the DPOP directly.

⚠ If the DPOP is already in production, this action is likely to generate an outage since the new certificate will be applied at the "save" step. It is required to deploy the new certificate before sending traffic to the DPOP.

```

1 lab-dpop1(config)# run request certificate generate forward-proxy self-signed common-name "DPOP Root" email-address support@netskope.com
2 successfully generated self signed ca
3
4
5 lab-dpop1(config)# save
6 This may take few seconds to few minutes depending on the configuration changes.
7 Restarting lcfowardproxy container
8 Configuration saved
9
10 lab-dpop1(config)#

```

Backup/rollback

Before changing configuration, it is recommended to backup existing DPOP configuration.

[Exporting Configurations - Netskope Knowledge Portal](#)

[Importing Configurations - Netskope Knowledge Portal](#)

Dedicated PKI Operations

Requirements

openssl or LibreSSL must be installed on a device to generate the PKI.

To check openssl version:

- MacOS:

```
1 % openssl version
2 LibreSSL 3.3.6
```

• Linux:

```
1 $ openssl version
2 OpenSSL 1.1.1w 11 Sep 2023
```

To install openssl on Windows, [Win32/Win64 OpenSSL Installer for Windows - Shining Light Productions](#)

```
1 C:\Program Files\OpenSSL-Win64\bin>openssl.exe version
2 OpenSSL 3.2.0 23 Nov 2023 (Library: OpenSSL 3.2.0 23 Nov 2023)
3
4 C:\Program Files\OpenSSL-Win64\bin>
```

Setup a Dedicated PKI with openssl

Note: this guide exclude CRL and certificate revocation because it's not useful for SSL interception and it would require to publish the CRL on a web server.

Note2: Key of the CA is very sensitive, it is only needed to sign new sub CA and should be stored secured (in a vault or offline) when not used.

Prepare CA structure

```
1 mkdir "SampleCA"
2 cd "SampleCA"
3 mkdir {certsdb,certreqs,private}
4 chmod 700 private
5 touch index.txt
6
```

Import openssl.cnf from: [openssl.cnf](#)

You can also use the following archive which provide the folders and openssl configuration [SampleCA.zip](#)

Generate the private key

The following command will generate a new 4k RSA private key:

```
1 openssl genrsa -out private/root_key.pem 4096
```

Generate Root certificate

The following command will generate a new Root certificate valid for 10 years using best practice extensions:

```
1 openssl req -config openssl.cnf -new -x509 -days 3650 -key private/root_key.pem -out root_cert.pem -extensions extensions_root
```

Check the Root CA details

The following command will display the details of the new Root certificate:

```
1 openssl x509 -in root_cert.pem -text -noout
```

Export the Root CA certificate to deploy on end user devices

`root_cert.pem` is the Root certificate that needs to be deployed on all managed devices.

Once the Root is trusted on end user devices, it can be used to issue intermediate CA for DPOP appliances.

Generate a new CSR directly in the PKI directory

Generate Key with 4k size.

```
1 openssl genrsa -out private/dpop_key.pem 4096
```

Generate CSR

```
1 openssl req -config openssl.cnf -new -key private/dpop_key.pem -out certreqs/dpop_csr.pem
```

Example:

```
1 openssl req -config openssl.cnf -new -key private/dpop_key.pem -out dpop_csr.pem
2
3 You are about to be asked to enter information that will be incorporated
4 into your certificate request.
5 What you are about to enter is what is called a Distinguished Name or a DN.
6 There are quite a few fields but you can leave some blank
7 For some fields there will be a default value,
8 If you enter '.', the field will be left blank.
9 -----
```

```
10 Country Name (2 letter code) [US]:
11 State or Province Name (full name) [California]:
12 Locality Name (eg, city) [Santa Clara]:
13 Organization Name (eg, company) [Netskope]:
14 Organizational Unit Name (eg, section) []:
15 Common Name (eg, YOUR name) [Netskope DPOP Root]:DPOP CA
16 Email Address [support@netskope.com]:
17 mbouthors@mac-10g sample_pki %
```

Sign a CSR with the Dedicated PKI

To sign a CSR with the Dedicated PKI:


- import the csr in "certreqs" directory
- use the following command to generate the certificate

1. To display a cert request details:

```
1 openssl req -in certreqs/dpop_csr.pem -text -noout
```

2. To sign the CSR with the Dedicated PKI on with OpenSSL:

```
1 openssl ca -config openssl.cnf -rand_serial -days 3650 -extensions extensions_intermediate_ca -in certreqs/dpop_csr.pem
```

 If using MacOS LibreSSL (-rand_serial not supported), use the following command instead:

```
1 openssl ca -config openssl.cnf -create_serial -days 3650 -extensions extensions_intermediate_ca -in certreqs/dpop_csr.pem
```

 Note: the PKI only accept one certificate per DN, it's not allowed to sign twice the same CSR.