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 describe 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	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.	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	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)	No external tool required. Very simple and fast to achieve.	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 below.
2. Deploy new Root on end user devices
3. Configure DPOP with BYOK. See the **BYOK** section below.

I want to use my existing Corporate PKI

Steps:

1. Configure DPOP with BYOK. See the **BYOK** section below.

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 below.

DPOP Operations

Introduction

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

- BYOK
- Netskope 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 with 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.

```
lab-dpop1(config)# run request certificate generate forward-proxy certificate-request common-name "DPOP1 Intermediate CA" email-address support@netskope.com

lab-dpop1(config)# show dataplane forward-proxy csr
"-----BEGIN CERTIFICATE REQUEST-----
MIICjjCCAXYCAQAwSTEgMB4GA1UEAwwXbGFiLWRwb3AxLmJvdXRob3JzLmluZm8x
JTAjBgkqhkiG9w0BCQEWFm1ib3V0aG9yc0BuZXRza29wZS5jb20wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDWnyor93Do44MEHlHgD6jj3Yz+pKjLxKu6
80GQaniq1Jp9ZMBPO9f3NdffgpmX5WEkEkXj1CXhoXneu/Wuu5ptkEdSefARwvbH
8ltsWUGNerxicFlwJWS6BwZW75xwWQeQtvZObIUsxlzFZ2DeNbBkD7AZyDsr5hyI
t4A8UjZh5/q4RQO/IL8jivRBfXWih8Y88/FKEVST/szt8sboUkWUn4rmuYz740A7
```

```
Kw+/5z5sqetnU+2C728RCZUIlwOKxO+f2D459nkhPXFo2bCweg++XZkRfOgraou8
0GazgKxqvXau/oW20mIgD465doM1PyToT03Qbo1ZLWVgP68fZEs5AgMBAAGgADAN
BgkqhkiG9w0BAQsFAAOCAQEAvd0IfnCnvZjHtNKBV9d0vK9Xr5P2lpLTPvQ+RNvT
BurMtQlpDCqdDieQ2Qm9iVlhWqtC1leSfG8XkLmdIUy1I2xLJrib0TcHT3tnVn+6
9UrIGQR40N8iGZJBVRILjATCs+uahqMwthTelPFpOIq2T4sC2b1XreXrLC0gpodd
MpU83Bg3IDwo+xTutIDYBnD9JJl9ApLQKTFOaTubbjL34IKcKk1yPAGwMlEyDKqM
Ee5oR59758T1xggrEq2Nb1/rDLx/SE5IkkNVVVtCxtwwZ1G3wucX63ixtRCdDcPg
llfvYF6DxpmOg43i0yJHGo1TfKazprFZGRSG0bx3ecLHDg==
-----END CERTIFICATE REQUEST-----
"

lab-dpop1(config)#
```

Option 2 - Use Openssl

Generate Key with 4k size.

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

Generate a CSR

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

Example:

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

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

Sign the CSR with the PKI

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

To sign the CSR with existing Corporate PKI, please follow the process of the PKI, the requirements are:

- Mandatory:
  - CA=True
- Optional:
  - `keyUsage =critical, digitalSignature, keyEncipherment, keyCertSign, cRLSign`
  - `extendedKeyUsage = critical, serverAuth, clientAuth`

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.

```
lab-dpop1(config)# set dataplane forward-proxy server-cert
Copy and paste just your single PEM-formatted server CA certificate (no keys).
Enter one or more lines of input. When done, press Ctrl-D
-----BEGIN CERTIFICATE-----
MIIEtjCCAp6gAwIBAgIJAP3vkTz2S2bQMA0GCSqGSIb3DQEBCwUAMGgxCzAJBgNV
BAYTAlVTMRMwEQYDVQQIDApDYWxpZm9ybmlhMRQwEgYDVQQHDAtTYW50YSBDbGFy
YTERMA8GA1UECgwITmV0c2tvcGUxGzAZBgNVBAMMEk5ldHNrb3BlIERQT1AgUm9v
dDAeFw0yMzEyMDgxMjI5MjBaFw0zMzEyMDUxMjI5MjBaMCAxHjAcBgNVBAMMFURQ
T1AxIEludGVybWVkaWF0ZSBDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBAMo8znKgrbhOiUE1bxsgwK0G8RS/4BhP1J5C51Mxgt5qhRD1657ci7W/5Cng
BI2IkMZbCXk6UH5jXNnSmOmuAWIupnzvhAnJYunmQP21WYc55BKEOlOt/IHm2O6+
dBwT2mLfnwCQodjM49tV5qxCvJvDKxpmTGunMtXUnf1QhorYYAjpDxFlHTz8yEzM
lX110swuzeae1yWkCvkBVfP8kDQbbs79zQwJ+KMaVd8+Njvqz8AqcURCYy9XBtdc
jK1Sm95BJg8Rghr2zjjywYtubK+twdghkUdzM3gKO5c2qG23HbJNravq4zqz8NLa
D48oCfmPCp3MlHtEt6bs7vO/vb0CAwEAAaOBqjCBpzASBgNVHRMBAf8ECDAGAQH/
AgEAMA4GA1UdDwEB/wQEAwIBpjAgBgNVHSUBAf8EFjAUBggrBgEFBQcDAQYIKwYB
BQUHAwIwHQYDVR0OBBYEFEMju6Q8f23APyTiwKPzAbb/omBrMB8GA1UdIwQYMBaA
FK6zqrw/xFLz4B9go1FZo4oovxWaMB8GA1UdEQQYMBaBFHN1cHBvcnRAbmV0c2tv
cGUuY29tMA0GCSqGSIb3DQEBCwUAA4ICAQCZSyEKcVVj3t+C1tKtUROoWIyU+dL3
```

```
KRN+pO9Qs2jjEgV1N/chwBdzToyrcbH1MvTGrHLSCqtE/vTuS+noKg8cIl212Uwl
sE7vSmkEFAXYFzgo2Cx8cbIIQKVITg7C9/VBQNhzeL5poc/j50fY9EtsHKkH9xvp
iIl3ibLE2HSDb5rAP6HMGC1PFnLsSEAki7SPL2gZhuQhL+b2MXEob9wlySla34Qx
8loWbj9S1I/OCYZjw+5k/5ixpGUVMPuWrCjkgCqKQTeFmOrwENSHUL5goMRUgYHH
QkZfDdOFq8AUqMjE4Dj2EtphkAzH0CpW0bduai9BL8RpmqzdAB8z6lH6FcLRzrE7
1+R5EJSQjYUSP06RPC7xqkMa4PN8KD2kD45Bfo/SgH0AM80TjrQO68yEKZu6QIT8
5flkW/pexwW5AkK31UR9oVAYryz3W/I2K7zFL+ZtEn6d7Wp7APRkwK/TWkrfDSVY
rFY2wU5QSifyKV7DeJcjQ+fPkmRv1zhev18XG01YYJkDw+XU0Jb4ItrPLTlXXiUq
oTGBJAR+zGyRu3r9Yq9EiS/2ak3ZNsHh+SZZhoiqqjjQp2kEntXy3kjMhxkdZk0O
6++oT2Vi6pBUCxjI0o6hpRl+LdOBKjP/CpEm6GI8mp+bJPkqhw8ox6XWpNaEoCWR
bkgDYD2GSr4AXg==
-----END CERTIFICATE-----


Certificate Issuer:
    Country: US
    State: California
    Issuer Field: Santa Clara
    Organization: Netskope
    Common Name: Netskope DPOP Root
Subject:
    Common Name: DPOP1 Intermediate CA
Valid On:   Dec  8 12:29:20 2023 GMT
Expires On: Dec 05 12:29:20 2033

lab-dpop1(config)# save
This may take few seconds to few minutes depending on the configuration changes.
Restarting lcforwardproxy container
Configuration saved

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.

```
lab-dpop1(config)# delete dataplane forward-proxy server-key
lab-dpop1(config)# delete dataplane forward-proxy server-cert
lab-dpop1(config)# save
This may take few seconds to few minutes depending on the configuration changes.
Restarting lcforwardproxy container
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.

```
lab-dpop1(config)# run request certificate generate forward-proxy self-signed common-name "DPOP Root" email-address support@netskope.com
successfully generated self signed ca


lab-dpop1(config)# save
This may take few seconds to few minutes depending on the configuration changes.
Restarting lcforwardproxy container
Configuration saved

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:

```
% openssl version
LibreSSL 3.3.6
```

- Linux:

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

To install openssl on Windows, Win32/Win64 OpenSSL Installer for Windows - Shining Light Productions

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

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

```
mkdir "SampleCA"
cd "SampleCA"
mkdir {certsdb,certreqs,private}
chmod 700 private
touch index.txt

```

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:

```
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:

```
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:

```
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.

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

Generate CSR

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

Example:

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

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) [US]:
State or Province Name (full name) [California]:
Locality Name (eg, city) [Santa Clara]:
Organization Name (eg, company) [Netskope]:
Organizational Unit Name (eg, section) []:
Common Name (eg, YOUR name) [Netskope DPOP Root]:DPOP CA
Email Address [support@netskope.com]:
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:

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

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

```
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:

```
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.