# 憑證生成範例

### 建立憑證

https://goharbor.io/docs/main/install-config/configure-https/

#### 建立 CA 憑證

rootCA，行方應有現行的憑證，使用現行憑證即可。

目錄建立

```
mkdir cert
```

建立憑證鑰匙

```
openssl genrsa -out ca.key 4096
```

建立 root CA

```
openssl req -x509 -new -nodes -sha512 -days 3650 \
 -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=Brobridge
Root CA" \
 -key ca.key \
 -out ca.crt \
 -addext "subjectAltName=DNS:harbor.brobridge.lab"
```

#### 建立私服器憑證

建立私有鑰匙

- 私服器金鑰建立時，不要使用密碼。
- 依據資安要求給於長度即可，先前詢問涵宇是使用 4096。

```
openssl genrsa -out harbor.brobridge.lab.key 4096
```

建立 CSR

- 主體(subject)部分依照行方資訊填寫即可。

```
openssl req -sha512 -new \
    -subj "/C=TW/ST=Taipei/L=Taipei/O=Brobridge/OU=Personal/CN=harbor.
brobridge.lab" \
    -key harbor.brobridge.lab.key \
    -out harbor.brobridge.lab.csr
```

準備 v3 格式的設定檔

- 主要修改 alt_names，代入私服器 DNS 即可。

```
cat > v3.ext <<-EOF
authorityKeyIdentifier=keyid,issuer
basicConstraints=CA:FALSE
keyUsage = digitalSignature, nonRepudiation, keyEncipherment,
dataEncipherment
extendedKeyUsage = serverAuth
subjectAltName = @alt_names
[alt_names]
DNS.1=harbor.brobridge.lab
EOF
```

建立私服器憑證

- 根據資安要求，修改指定加密格式跟天數即可。

```
openssl x509 -req -sha512 -days 3650 \
    -CA ca.crt -CAkey ca.key -CAcreateserial \
    -in harbor.brobridge.lab.csr \
    -out harbor.brobridge.lab.crt \
    -extfile v3.ext
```

### 確認私服器憑證包含 SAN

檢查憑證內部資訊

```
openssl x509 -in harbor.brobridge.lab.crt -noout -text | grep -A 1
"Subject Alternative Name"
```

指定憑證瀏覽

```
curl -v https://harbor.brobridge.lab/v2/ --cacert ca.crt
```