Key Management

Exchange Certificate

Below are the steps required for Merchants to generate the private key and certificate.

Certificate Generation (Windows Platform)

Generation of Private Key and CSR at Merchant's/TPA's End.

- Generation of Private Key

```
openssl genrsa -out <file_name_pvt>.key 2048
```

INFO

Note: EX00000298 is used for the filename during key generation for illustration purpose only.

```
C:\openssl\bin>Openssl genrsa -out EX00000298.key 2048
WARNING: can't open config file: C:/OpenSSL/openssl.cnf
Generating RSA private key, 2048 bit long modulus
.....................+++
.....................+++
unable to write 'random state'
e is 65537 (0x10001)
```

- Generation of CSR

```
openssl req -out <file_name_csr>.csr -key <file_name_key>.key -new -sha256
```

```
C:\openssl\bin>openssl req -out EX00000298.csr -key EX00000298.key -new -sha256
```

- Information that will be incorporated into the certificate request. Please leave a challenge password and an optional company name blank.

```
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) [XX]:MY
State or Province Name (full name) []:Wilayah Persekutuan
Locality Name (eg, city) [Default City]:Kuala Lumpur
Organization Name (eg, company) [Default Company Ltd]:xxxx sdn bhd
Organizational Unit Name (eg, section) []:IT Security
Common Name (eg, your name or your server's hostname) []:EX000000
Email Address []:rozairol@paynet.my

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

- Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnl4+Sbhu5P/iXRqvtjn3lCysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZACIvdQ9PtzHsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsop
8ZxIfHa1S53R9XqaKB2zglBCP1W1KGz8K+qc+GRQQ+CqrkH3OiWPjPTAmkYZy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEqvgYPttmAmTPC9cn5rUWzObGIlS
PgR5D47tqpaw0wQSUYhzxbngnR8Rrqh/Ge0RKwIDAQABAoIBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHW4/czKQMicmic7/UtvXXOmQMeg6IWAjOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrlbgYSvacEc1te7/8Wl2saAbR77ilOSiVD2yy+Q76HGabQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozIqZ
SeIU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7Lt1pcJSlY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45IxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlnEXK9Pw+kNd8CgYEA56rp
eh3qyfj/0EC51iTJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVVqpiSQhFrN4GK+1D
D0rVmOrd2kneiue0ezYhjqkqsgOf3XiMSGXLVjUCgYEAhgw366L/OJkGTtdSfW+U
Xttv8i/QlWbhYaLpqW5ys6iiSnCp386tb0QN0Sqy/NYAVlhdhU8dH5RR3MGgxomf
zqnMGJgjJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAtNe3MEugV4/XaeLM7ryC5LjJfEB50O0IO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4IpEIwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPOrJpYiRDFRUT2OlqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1UhM8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOwTly8/cxc
V+QBWq0ijYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+lZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```


- Sample of CSR File


```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwezELMAkGA1UEBhMCTVkxCzAJBgNVBAgTAktMMQswCQYDVQQ
H
EwJXUDEQMA4GA1UEChMHTXIDbGVhcjELMAkGA1UECxMCQUQxDDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmlkenVhbkBteWNsZWFyLm9yZy5teTCCASIwDQYJ
KoZIhvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdghggUQwqp
4+egWTP/mcAXHlNtrvVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpfMWlvYB2yFRcN6Y7lZzBuYWm
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migds4JQQj9VtShs/CvqnPhkUEPgqq5B
9zolj4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESsCAwEAAaAx
MBYGCSqGSIb3DQEJAjEJEwdteWNsZWFyMBcGCSqGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAHeGqHm3ozCuu18gUWRjQhlG6i+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtgIA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyljhHiUl6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----
```

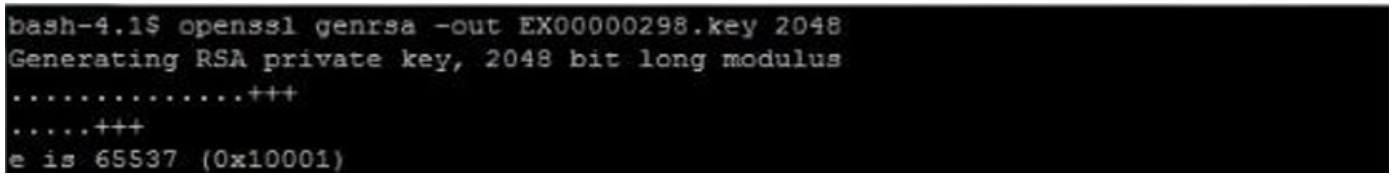
Certificate Generation (Linux Platform)

Generation of Private Key and CSR at Merchant's/TPA's End.

- Generation of Private Key

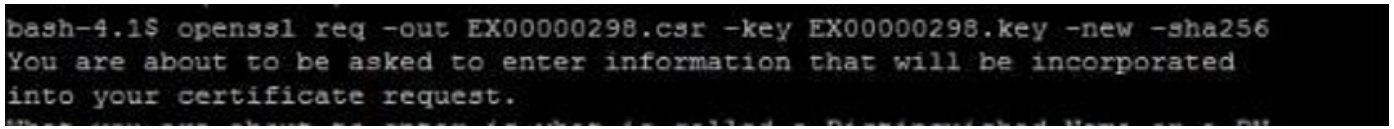
```
openssl genrsa -out <file_name_key>.key 2048
```

> **INFO**
> Note: EX00000298 file name is use for illustration purpose only.



- Generation of CSR

```
openssl req -out <file_name_csr>.csr -key <file_name_key>.key -new -sha256
```



- Information that will be incorporated into the certificate request. Please leave a challenge password and an optional company name blank.

```
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) [XX]:MY
State or Province Name (full name) []:Wilayah Persekutuan
Locality Name (eg, city) [Default City]:Kuala Lumpur
Organization Name (eg, company) [Default Company Ltd]:xxxx sdn bhd
Organizational Unit Name (eg, section) []:IT Security
Common Name (eg, your name or your server's hostname) []:EX000000
Email Address []:rozairol@paynet.my

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
```

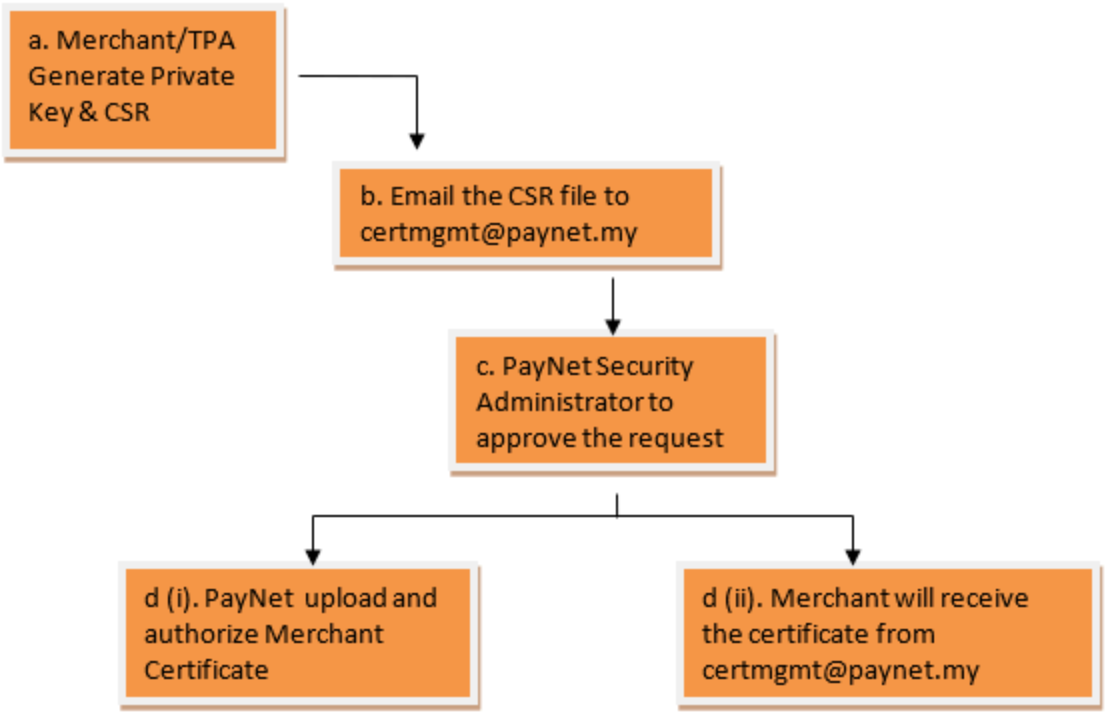
- Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtjn3ICysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZACIvdQ9PtzHsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsop
8ZxIfHa1S53R9XqaKB2zglBCP1W1KGz8K+qc+GRQQ+CqrkH3OiWPjPTAmkYZy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEqvgYPttmAmTPC9cn5rUWzObGIlS
PgR5D47tqpaw0wQSUYhzxbngnR8Rrqh/Ge0RKwIDAQABAoIBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHW4/czKQMicmic7/UtvXXOmQMeg6IWAjOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrlbgYSvacEc1te7/8Wl2saAbR77ilOSiVD2yy+Q76HGabQmdReFk720p1hyPtI
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdcIt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozIqZ
SeIU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7Lt1pcJSlY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45IxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlnEXK9Pw+kNd8CgYEA56rp
eh3qyfj/0EC51iTJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVVqpiSQhFrN4GK+1D
D0rVmOrd2kneiue0ezYhjqkqsgOf3XiMSGXLVjUCgYEAhgw366L/QJkGTtdSfW+U
Xttv8i/QlWbhYaLpqW5ys6iiSnCp386tb0QN0Sqy/NYAVlhdhU8dH5RR3MGgxomf
zqnMGJgjJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAtNe3MEugV4/XaeLM7ryC5LjJfEB50O0lO3Ml
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPOrJpYiRDFRUT2OlqJwVsD6FBrE8nwGVHmYxtc7lPZYlEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1UhM8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOwTly8/cxc
V+QBWq0ijYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+lZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```

- Sample of CSR File

Procedure for Merchant Certificate Request in UAT Environment

> **INFO**
>
> Note: We are acccepting a self-signed cert for testing environment and highly encourage to submit the cert via Paynet Developer Portal's Project section.



- Merchant should generate their own PKI key pair and ensure that the PKI private key is store in a secure device. The PKI key pair can be generated using OpenSSL tool.

  OpenSSL is compatible for Windows, Linux and Unix-based OS and can be obtained from the following site of OpenSSL (http://www.openssl.org). Information on the “certificate generating utility” can be viewed at http://www.openssl.org/docs/apps/req.html. Refer to PKI Key Pair Generation Using Open SSL document for more details.

  The PKI certificate is in .cer format with 2048 bytes while the signing algorithm is in RSA.

  The signed value is in hexadecimal format.

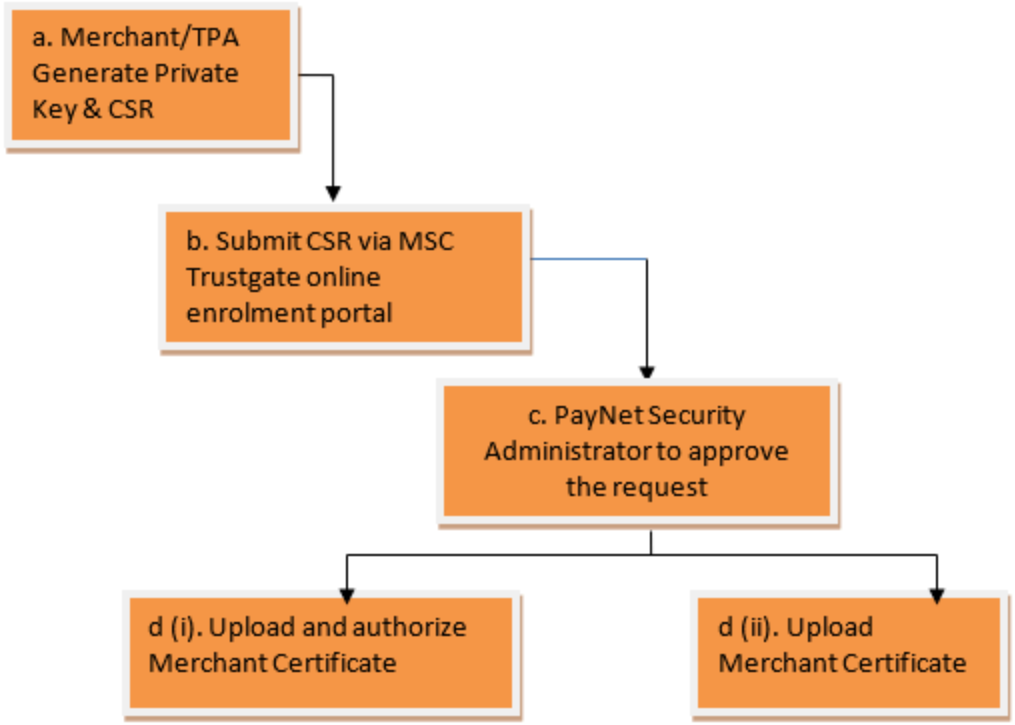
- Merchant to submit the CSR file to PayNet for approval.

- PayNet Security Administrator to approve the request.

- PayNet to upload and authorize Merchant Certificate in FPX Webview.

- Merchant will receive the new certificate from PayNet. Merchant to store the new exchange certificate in the server.

Procedure for Merchant Certificate Request in Production Environment



- Merchant should generate their own PKI key pair and ensure that the PKI private key is store in a secure device. The PKI key pair can be generated using OpenSSL tool.

OpenSSL is compatible for Windows, Linux and Unix-based OS and can be obtained from the following site of OpenSSL (http://www.openssl.org). Information on the “certificate generating utility” can be viewed at http://www.openssl.org/docs/apps/req.html. Refer to PKI Key Pair Generation Using Open SSL document for more details.

The PKI certificate is in .cer format with 2048 bytes while the signing algorithm is in RSA.

The signed value is in hexadecimal format.

- Merchant to Submit the CSR file to MSC Trustgate for approval via the following URL:

  https://onsite.msctrustgate.com/services/PaymentsNetworkMalaysiaSdnBhdFPX/digitalidCenter.htm

- PayNet Security Administrator to approve the request.

- PayNet to upload and authorize Merchant Certificate.

- Merchant will receive the new certificate from MSC Trustgate. Merchant to store the new exchange certificate in the server.

FPX Certificate

Download and install latest FPX Certificate

You may download latest FPX certificate under **resources** section.

Renewal of FPX Certificate

Below is the naming convention that has to be followed for renewal process:

- UAT → change from fpxuat.cer to fpxuat_current_cer