



GUIDELINES ON EXCHANGE CERTIFICATE MANAGEMENT

Doc. Ref. No.: 600-30/3/0001274

Version 1.7

Proprietary Rights

The information contained in this document is proprietary and confidential to Payments Network Malaysia Sdn Bhd (PayNet) and its subsidiary companies (PayNet Group). All rights reserved. This material may not be duplicated, published, or disclosed, in whole or in part, without the prior written permission of PayNet.

Document Details

Document Owner	: IT Security Department
Effective Date	: 06 July 2020

Review & Approval

Payments Network Malaysia Sdn Bhd (PayNet)				
Task	Name	Designation/ Department	Date	Signature/ Remarks
Reviewed by	Shaheezul Mazhar Hj Abdul Razak	Head of Application Development (FPX)	02/07/2020	Reviewed V1.6
Approved by	Juliaty Abdul Rahman	Head of IT Security	03/07/2020	Approved V1.6
	Muhammad Azri Abu Samah	Head of Application Development	02/07/2020	Approved V1.6

Revision History

Version No.	Date of Update	Summary of Change	Updated By
1.0	02/2015	Initial Creation	Nora Azura
	23/03/2015	Approval by Muhammad Azri & Mohd Nasir on 16/03/2015 and 23/03/15 respectively.	
1.1	09/04/2015	To change the certificate management process for UAT.	Nora Azura
	17/04/2015	Approved by HOD of AD and ITS on 16/04/2015 and 17/04/2015 respectively.	
1.2	14/05/2015	Additional information to include the following: - To include SHA256 option during private key generation - To provide the guide on key & CSR generation for Linux & Windows platform.	Nora Azura
	28/05/2015	Approved by AD Manager and HOD of ITS on 27/05/2015 and 15/05/2015 respectively.	
1.3	04/06/2015	Minor Changes:- - Change of FPX Exchange Portal URL to include the port number. - Change of interface of the FPX Exchange Portal.	Nora Azura
1.4	28/10/2015	Minor Changes:- - To include OpenSSL command for certificate renewal - To include the naming convention for the FPX Certificate	Nora Azura
1.5	13/11/2018	- Updated template document - Updated MyClear to PayNet - Updated url to https://onsite.msctrustgate.com/services/PaymentsNetworkMalaysiaSdnBhdFPX/digitalidCenter.htm - Updated email address to certmgmt@paynet.my - Add **Leave the "extra" attributes blank → Challenge password and Company Name under each of diagram b. Information that will be incorporated into the certificate request	Norhayani
	18/01/2019	Approved by HOD of ITS and AD Manager on 17/01/2019 and 18/01/2019 respectively.	
1.6	16/6/2020	Minor Changes: - - Update Pre-Requisite description - Update OpenSSL Command to generate Key and CSR for Windows - Update Method for CSR Submission	Rozairol

Version No.	Date of Update	Summary of Change	Updated By
1.7		- Amend all Diagram flow by removing the phrase "Merchant receive the certificate and upload the certificate at their end"	
	03/07/2020	Approved by Head of ITS and Head of AD on 03/07/2020 and 02/07/2020 respectively	
	31/1/2023	Minor changes: - - Change MSC Trustgate URL Portal - Change email from certmgmt@paynet.my to sac_its@paynet.my - Change Exchange Portal URL	

Table of Content

1.0	Introduction	7
1.1	Objective.....	7
1.2	Definition	7
1.3	Scope.....	7
1.4	Pre - Requisite.....	7
2.0	Process Flow for Exchange Certificate Request (New).....	8
2.1	UAT Environment.....	8
2.2	PRODUCTION Environment	12
3.0	Process Flow for Exchange Certificate Request (Renewal)	20
3.1	UAT Environment (New Key)	20
3.2	Existing Key	23
3.3	PRODUCTION Environment	27
4.0	FPX Certificate	38
4.1	Download and install latest FPX Certificate.....	38
4.2	Renewal of FPX Certificate.....	38

List of Figures

Procedure for New Exchange Cert – Windows Platform (UAT)

Figure 1: Generate Private Key	8
Figure 2: Generate CSR File	9
Figure 3: Information in the certificate	9
Figure 4: Sample of Private Key	9

Procedure for New Exchange Cert – Linux Platform (UAT)

Figure 5: Sample of CSR File.....	10
Figure 6: Generate Private Key	10
Figure 7: Generate CSR File	10
Figure 8: Information in the certificate	11
Figure 9: Sample of Private Key	11
Figure 10: Sample of CSR File	11

Procedure for New Exchange Cert – Windows Platform (PROD)

Figure 11: Generate Private Key	13
Figure 12: Generate CSR File	13

Figure 13: Information in the certificate	13
Figure 14: Sample of Private Key	14
Figure 15: Sample of CSR File	14
Procedure for New Exchange Cert – Linux Platform (PROD)	
Figure 16: Generate Private Key	14
Figure 17: Generate CSR File	14
Figure 18: Information in the certificate	15
Figure 19: Sample of Private Key	15
Figure 20: Sample of CSR file	15
Figure 21: MSC Trustgate Portal Page	16
Figure 22: CSR Submission page	17
Figure 23: Online enrolment form	17
Figure 24: Confirmation on CSR submission	18
Figure 25: Merchant/TPA will received the signed certificate	18
Procedure for Renewal Exchange Cert: New Key – Windows Platform (UAT)	
Figure 26: Generate Private Key	20
Figure 27: Generate CSR File	21
Figure 28: Sample of Private Key	21
Figure 29: Sample of CSR file	21
Figure 30: Generate Private Key	22
Figure 31: Information in the certificate	22
Figure 32: Sample of private key	22
Figure 33: Sample of CSR file	23
Procedure for Renewal Exchange Cert: Existing Key – Windows Platform (UAT)	
Figure 34: Generate CSR using existing private key	24
Figure 35: Information in the certificate	24
Figure 36: Sample of Private Key	24
Figure 37: Sample of CSR file	25
Procedure for Renewal Exchange Cert: New Key – Linux Platform (UAT)	
Figure 38: Generate CSR file	25
Figure 39: Information in the certificate	25
Figure 40: Sample of Private Key	26
Figure 41: Sample of CSR File	26
Procedure for Renewal Exchange Cert: New Key – Windows Platform (PROD)	
Figure 42: Generate Private Key	27
Figure 43: Generate CSR File	28

Figure 44: Information in the certificate	28
Figure 45: Sample of Private Key	28
Figure 46: Sample of CSR file	29
Procedure for Renewal Exchange Cert: New Key – Linux Platform (PROD)	
Figure 47: Generate Private Key	29
Figure 48: Information in the certificate	29
Figure 49: Sample of Private Key	30
Figure 50: Sample of CSR file	30
Procedure for Renewal Exchange Cert: Existing Key – Windows Platform (PROD)	
Figure 51: Generate Private Key	31
Figure 52: Information in the certificate	32
Figure 53: Sample of CSR File	32
Procedure for Renewal Exchange Cert: Existing Key – Linux Platform (PROD)	
Figure 54: Generate Private Key	32
Figure 55: Information in the certificate	33
Figure 56: Sample of CSR File	33
Figure 57: MSC Trustgate Portal Page	33
Figure 58: CSR Submission page	34
Figure 59: Online enrolment form	34
Figure 60: Confirmation on CSR submission	35
Figure 61: Merchant/TPA will received the signed certificate	35
Figure 62: Merchant/TPA to download the latest FPX Certificate from the Portal	38

List of Table

Table 1: Definition	7
---------------------------	---

List of Diagram

Diagram 1: Process Flowchart for exchange certificate (new) of UAT Environment	8
Diagram 2: Process of Flowchart for exchange certificate (new) of PRODUCTION environment	12
Diagram 3: Process of Flowchart for exchange certificate (renewal) of UAT Environment	20
Diagram 4: Process of Flowchart for Exchange Certificate Request (renewal) of Existing Key	23
Diagram 5: Process Flowchart for Production Environment of New Key	27
Diagram 6: Process of Flowchart for Production Environment of Existing Key	31

1.0 Introduction

1.1 Objective

The purpose of this procedure is to define the process required for certificate maintenance for FPX – SMI (FPX – Simplified Merchant Interface). This will include the guide on initial setup and renewal process for the following:

- a) Exchange Certificate (Generated at Merchant's/TPA's end)
- b) FPX Certificate (Generated at PayNet)

1.2 Definition

This section described abbreviation used within this document.

Term	Definition
FPX	Financial Process Exchange
SMI	Simplified Merchant Interface
UAT	User Acceptance Test
PayNet	Payments Network Malaysia Sdn. Bhd.
CSR	Certificate Signing Request
TPA	Third Party Acquirer
PROD	Production

Table 1: Definition

1.3 Scope

This document is applicable for certificate maintenance at all environment (UAT and Prod).

1.4 Pre - Requisite

The certificate is renewable, whereby upon generation of new certificate it needs to be uploaded at PayNet. Merchant/TPA need to ensure they are using correct Private Key (EX0000XXXX.key).

****Please take note that Merchant do not need to upload the certificate received from sac_its@paynet.my at their end. The certificate receives just for the reference. Only PayNet will upload the Merchant's certificate.**

2.0 Process Flow for Exchange Certificate Request (New)

2.1 UAT Environment

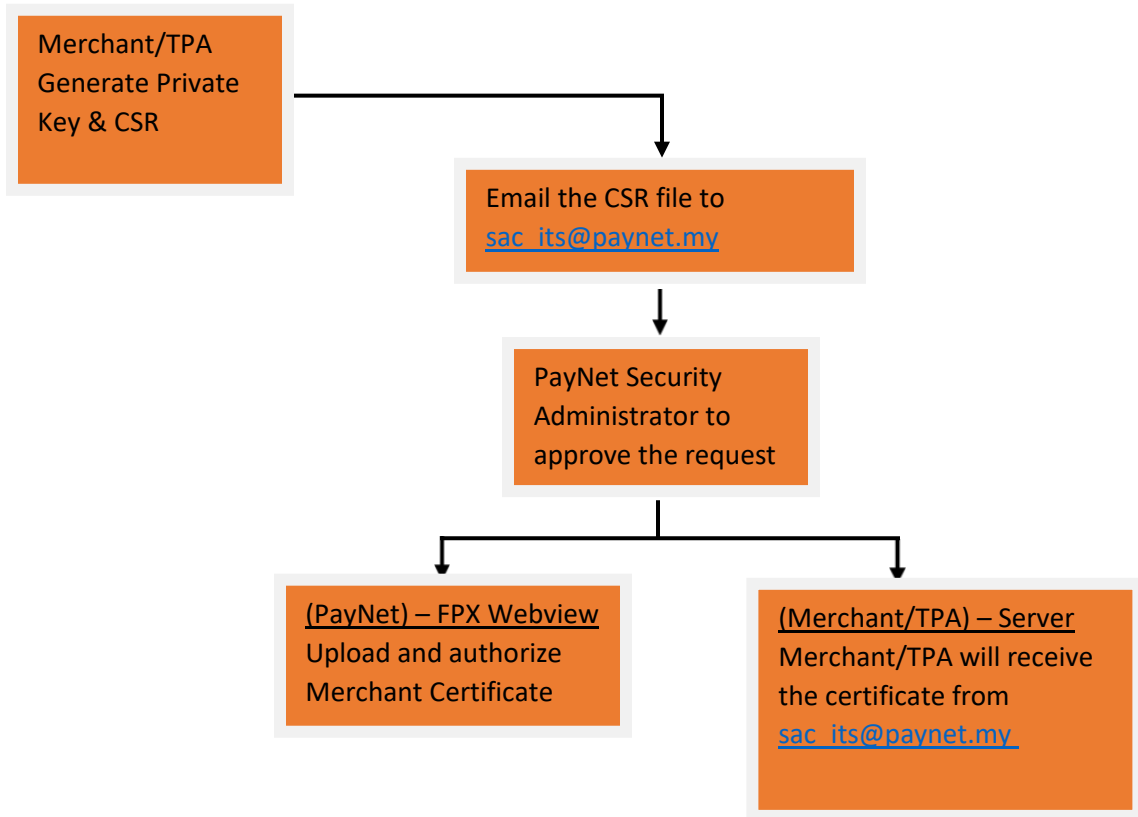


Diagram 1: Process Flowchart for exchange certificate (new) of UAT Environment

2.1.1 Procedure for Exchange Certificate Request

2.1.2 Windows Platform

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

a) Generate private key using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

*****Note: EX00000298 will be the Exchange ID provided *****

```

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)
  
```

Figure 1: Generate Private Key

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

Figure 2: Generate CSR File

- b) 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 []:
```

Figure 3: Information in the certificate

- c) Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnK4+Sbhu5P/iXRqvtn3ICysNwBuPqW9L+DEfNkOVHctpQxbGe2dBa
ZAClvdQ9PtZhsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzeVkdsoq
8ZxlfHa1S53R9XqaKB2zgiBCP1W1KGz8K+gc+GRQQ+CqrKH3OiwPjPTAmKYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDIXEqvgYPTmAmTPC9cn5rUWzObGllS
PgR5D47tpaw0wQSUYhzxbngnR8Rqh/Ge0RKwIDAQABAolBAGqDe4smob/mCOb
b4rTi3wrthbXdFETVNHw4/czKQMicmic7/UtvXXOmQMeg6lWAjOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BUJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrbgYSvace1te7/8WI2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7Lt1pcJSIY1/Rks5w9XGxSWbxF+WiyrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyfi/0EC51iJJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lj47Tb7H82RYB8xARPg/mQEBcvT4wTGUG0HF+whVVqpiSQHFrN4GK+1D
D0rVmOrd2kneue0ezYhjkgsgOf3XiMSGXLVJUCgYEAhgw366L/OJkGIttSfW+U
Xttv8i/QIwBhYaLpQW5ys6iiSnCp386tb0QN0Sqy/NYAVIhdhU8dH5RR3MGgxomf
zqnMGJgjJm79xMYN3BbeLEAOJ4bgtAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAAtNe3MEugV4/XaeLM7ryC5LjJfEB50OIO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4IpElwVwjmmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPQrJpYiRDFRUT2OiqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZB
07wa0aOCgyBj8BFDNwEsCVfB9wrF+OPur44m+vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWWc1Uhm8P1bnThKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBWq0iYfEJpH+7hhPGmzaFiSwsejSziJR+KtyV5+IZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```

Figure 4: Sample of Private Key

d) Sample of CSR File.

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwezELMAkGA1UEBhMCTVkcCzAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnJELMAkGA1UEC3MCQUxQxDDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkBteWNsZWYyLm9yZy5teTCCASlwDQYJ
KoZihvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdghggUQwqp
4+egWTP/mcAXHINtrvVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpIMWlvYB2yFRcN6Y7IzZBuYWm
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPggq5B
9zolz4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsNMEEIGic8W54J0fEa6ofxntESsCAwEAAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyLm9yZy5teTCCASlwDQYJBJzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMoj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHiUI6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 5: Sample of CSR File

2.1.3 Linux Platform

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

a) Generation a private key and CSR using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

****Note: EX00000298 will be the Exchange ID provided ****

```

bash-4.1$ openssl genrsa -out EX00000298.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

```

Figure 6: Generate Private Key

```

bash-4.1$ openssl req -out EX00000298.csr -key EX00000298.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.

```

Figure 7: Generate CSR File

- b) 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 []:

```

Figure 8: Information in the certificate

2) Sample of Private Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0K2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtjn3lCysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZACiVdQ9PtZHSnVDz09h4Wl8xYi9gHblVFw3puVnMG5habS1AkmoR/dzoVkdsoP
8ZxIfHa1S53R9XqaKB2zgiBCP1W1KGz8K+qc+GRQQ+CqrkH3OiWPjPTAmkYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs8wKbD0vrDtXEvgYPTtmAmTPC9cn5rUwZObGllS
PgR5D47tqpaow0wQSUYhzbngnR8Rrgh/Ge0RKwIDAQABAolBAGqDe4smob//mCQb
b4rTi3wrthXdfEetVNHw4/czKQMicmic7/UtyXXOmQMeg6lWajOn9fnp27S22HEH
8G1T6SSEQQm65pLtv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrlbgYSvacEc1te7/8Wl2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1hyPtl
9/6TNRl7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EEycQuviAahp
0C6+7/63RiDxuTLUJmtEFZYfGUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SeIU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7Ltl1pcJSIY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxmug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyf/0EC51iITJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47TbH82RYB8xARPg/mQEBcvT4wTGUG0HF+whVvqpiSQhFrN4GK+1D
D0rVmOrd2kneiu0ezYhjqqsgOf3XiMSGXLVjUCgYEAhgw366L/QJkGtIdSfW+U
Xttv8/QIWbhYalPqW5ys6iiSnCp386tb0QN0Sqy/NYAVlhdhU8dH5RR3MGgxmof
zqnMGJgjJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAAtNe3MEugV4/XaeLM7ryC5LjJfEB50OIO3MI
TufY90h3k+CSDrgPprR3F9LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPQrJpYiRDFRUT2OiqJwVsD6FBR8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWWc1Uhm8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBWq0iYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+IZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----

```

Figure 9: Sample of Private Key

3) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVkcCZAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnJELMAkGA1UECjMCQUQxZDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcm1kenVhbkBteWNsZWYyLm9yZy5teTCCASlwdQYJ
KoZlHvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpMwlvYB2yFRcN6Y7IZzBuYWm
0tQJjQeF3cFZhbKKfGcSHx2tUud0fV6migds4JQqJ9VtShs/CvqnPhkUEPqq5B
9zoJ4z0wJpGGctGAg4/MeWFXdibU1RNa1e4Nyc8BbOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmXPZUj4EeQ+O7aqWsnMEEIGic8W54J0fEa6ofxntESsCAwEAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyMBCGCSqGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMoJ20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4Nl7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXHXGEOxd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zMO2oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHlU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 10: Sample of CSR File

2.1.4 Method for CSR submission

- Submit the CSR file to PayNet for Approval
 - a) Email the CSR file generate to sac_its@paynet.my
 - b) Kindly provide the following info:
 - Exchange Name
 - Exchange ID
 - Contact Person
 - c) New certificate will be emailed from Certificate Management
- Merchant to ensure to use correct Private Key and place the Private Key into correct Path.

2.2 PRODUCTION Environment

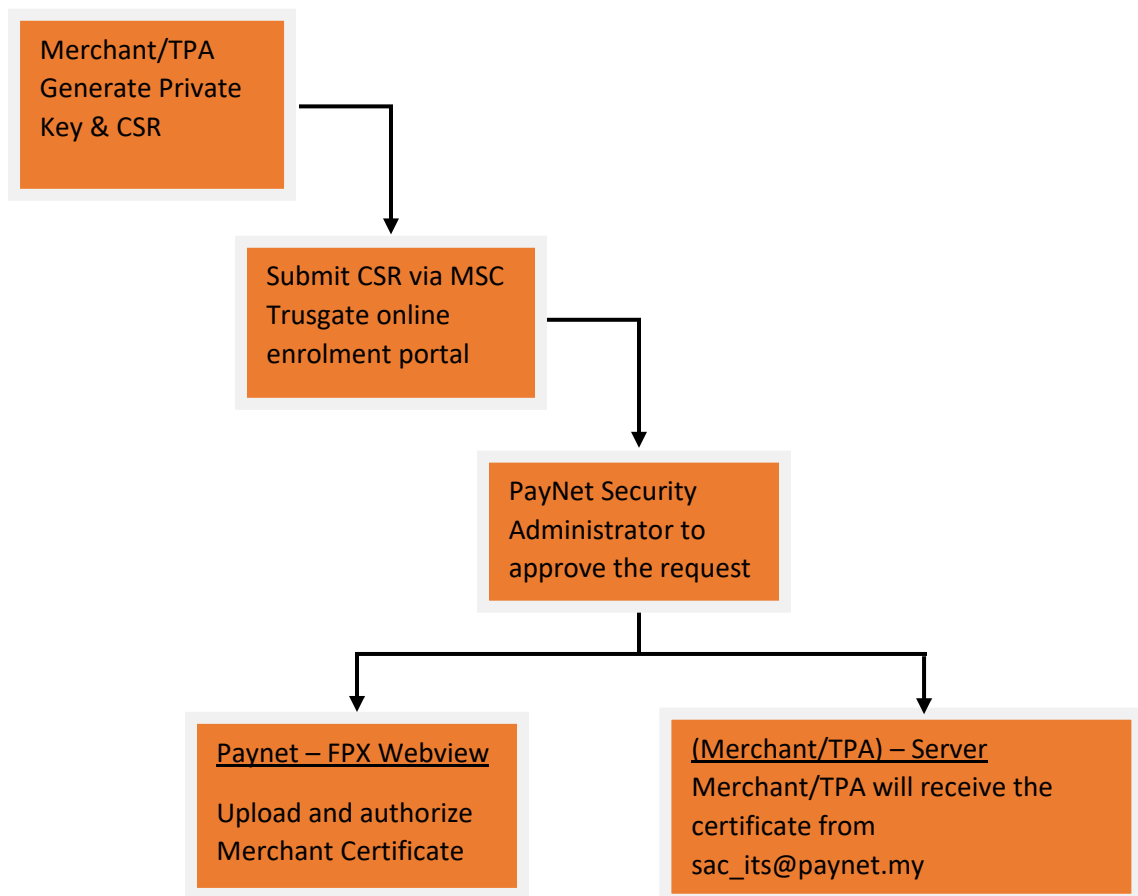


Diagram 2: Process of Flowchart for exchange certificate (new) of PRODUCTION environment

2.2.1 Procedure for Exchange Certificate Request

2.2.2 Windows Platform

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

a) Generate a private key using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

*****Note: EX00000298 will be the Exchange ID provided *****

```
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)
```

Figure 11: Generate Private Key

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

Figure 12: Generate CSR File

b) 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 []:
```

Figure 13: Information in the certificate

c) Sample of Private Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqni56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtjn3ICysNwBuPqW9L+DEfNkOVHctPQxbGc2dBa
ZACIvdQ9PtZhsnVDz09h4Wl8xYi9gHblVfW3pjuVnMG5habS1AkmoR/dzoVkdsoP
8ZxlfHhA1S53R9XqaKB2zglBCP1W1KGz8K+qc+GRQQ+QcrkH3OiwPjPTAmkYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEvgYpTtmAmTPC9cn5rUWzObGIIIS
PgR5D47tqapaw0wQSUyHxbngnR8Rrgh/Ge0RKwIDAQABAolBAGqDe4smob//mCOb
b4rTi3wrthbXdfEtVNHV4/czKQMicmic7/UtVXXOmQMeg6lWAjOn9fnp27S22HEH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrlbgYSvacEc1te7/8WI2saAbR77iIOSiVD2yy+Q76HGabQmdReFk720p1hyPtl
9/6TNRL7MVONdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EEYcQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrcvM6EZrgSCO1xSk6RtPIEAqyhphKMtizoZlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfINDYfoNE1
HKZ9cRMhvdFSduEqmaH7L1pcJSIY1/Rks5w9XGxSWbxF+WYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyf/0EC51ITJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj4Tb7H82RYB8xARPg/mQEBcvT4wTGUG0HF+whVVqpiSQhFrN4GK+1D
D0rVmOrd2kneue0ezYhjqqsgOf3XIMSGXLVJUCgYEAhgw366L/QJkGttdStfW+U
Xttv8i/QiWbhYal.pqW5ys6iiSnCp386tb0QN0Sgy/NYAVlhdhU8dH5RR3MGgxomf
zqnMGJgJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTUsCgYEAtNe3MEugV4/XaelM7ryC5LjFEB50O0IO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmmdhtAQ1Wqsm+6j9oQC6lvrOJ
RQq0EGP0rJpYiRDFRUT2OlqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1Uhm8P1bNThKf1Y4o+vmZGi2myn3Do3w7rKQOWtly8/cxc
V+QBWq0ijYEJpH+7hhPGmzaFiSwsejSzrJR+KtyV5+lZfKcV+T7IQ==
-----END RSA PRIVATE KEY-----

```

Figure 14: Sample of Private Key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVxkCzAJBgNVBAGTAktMMQswCQYDVQQQ
H
EwJXUDEQMA4GA1UEChMHXjXidBvGhVhYjELMAkGA1UECmMCQQUxQDAAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkbteWNsZWYyLm9yZy5teTCCASlwDQYJ
KoZlHvcNAQEBAQDggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrvVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAil3UPT7cx7J1Q89PYeFpFMWlvYB2yFRcN6Y7lZzBuYwM
0tQJjQef3c6FZHbKKfGcSHx2tUud0fV6migds4JQqj9VtShs/CvqnPhkUEPggq5B
9z0lj4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESCAwEAaAax
MBYGCsGSIb3DQEJAJEJEWdteWNsZWYyMBcGCSqGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAHeGqHm3ozCuu18gUWRjQhL6gi+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyljhHiU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 15: Sample of CSR File

2.2.3 Linux Platform

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

a) Generate a private key and CSR using OPENSSSL command

- openssl genrsa -out EX00000298.key 2048
- openssl req -out EX00000298.csr -key EX00000298.key -new -sha256

****Note:** EX00000298 will be the Exchange ID provided **

```

bash-4.1$ openssl genrsa -out EX00000298.key 2048
Generating RSA private key, 2048 bit long modulus
.....++++
.....++++
e is 65537 (0x10001)

```

Figure 16: Generate Private Key

```

bash-4.1$ openssl req -out EX00000298.csr -key EX00000298.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.

```

Figure 17: Generate CSR File

- b) 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 []:

```

Figure 18: Information in the certificate

- c) Sample of Private Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/xRqvtjn3iCysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZAClvdQ9PtZHSnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsoP
8ZxlfHhA1S53R9XqakB2zgiBCP1W1KGz8K+gc+GRQQ+CqrkH3OiWpJPTAmkYZy0YC
Dj8x5Yvd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEqvqYPTtmAmTPC9cn5rUWzObGllS
PgR5D47tqaw0wQSUyhzxbngnR8Rqh/Ge0RKwIDAQABAolBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHV4/czKQMicmic7/UtvXXOmQMeg6lWAjOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zArN8hr2M8yh
3LrbgYSvacEc1te7/8WI2saAbR77iIOSVD2yy+Q76HGAbQmdReFk720p1thyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi8gvdpAblsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrcvM6EZrgSCO1xSk6RtPIEAqyhphKMtuzozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFsdUeqmaH7L1tpcJSIY1/Rks5w9XGxSWbxF+WYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyfi/0EC51tJokWmfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVvqpiSQhFrN4GK+1D
D0rVmOrd2kneue0ezYhjqqsgOf3XiMSGXLVjUCgYEAHgw366L/OJkGTdSMV+U
Xttr8/QiWbhYalpqW5ys6iiSnCp386tb0QN0Sqy/NYAVlhdhU8dH5RR3MGxomf
zqnMGJgjJm79xMYN3BbeLEAOJ4bqfAUHG0Ahjy8AA9ITmrm1KS8+d3TYPKDaAbJfw
B+8LCc9f2TNVM4hWx0hTdUsCgYEAiNe3MEugV4/XaeLM7ryC5LjJfEB500lO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmDhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPQrJpYiRDFRUT20lqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBY8BFDNwEsCVfB9wrf+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1UhM8P1bNThKf1Y4o+vmZGi2myn3D03w7rqKOWtly8/cxc
V+QBWq0ijEJpH+7hhPGmzaFjSwsejSziJR+KtyV5+lZfKcV+T7iQ==
-----END RSA PRIVATE KEY-----

```

Figure 19: Sample of Private Key

- d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVxkCzAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGhVhcgJELMAkGA1UECgMCQUQxQDAKAgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkbteWNsZWYyLm9yZy5teTCCASlWdQYJ
KoZlHvcNAQEBAQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHIntrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAIL3UPT7cx7J1Q89PYeFpMwlvYB2yFRcN6Y7IZzBuYWm
0tQJjQEf3c6FZhbKKfGcSHx2tUud0fV6migdS4JQqJ9VtShs/CvqnPhkUEPggq5B
9zolz4z0wJpGgGctGAg4/MeWFXdibU1RNa1e4Nyc8BbOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJta1FszmXpZUj4EeQ+O7aqWsnMEEIGlc8W54J0fEa6ofxntESsCAwEAaAax
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyLm9yZy5teTCCASlWdQYJbZEkEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXD
99JcT3oT4n0Sihc2qB7pjrR9HyWGPeeUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zMO2oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHiU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 20: Sample of CSR file

2.2.4 Method for CSR submission

1) Submit CSR file to MSC Trustgate for Approval

a) Submit the CSR to the following URL:

<https://www.msctrustgate.com/mytrustid/enrollment?q=paynetfpx>

The screenshot displays the 'New Certificate Enrollment Request' page for Payments Network Malaysia Sdn Bhd (FPX). The page features a progress bar with five steps: 1. Instructions (active), 2. Package & Pricing, 3. Application Info, 4. Disclaimer, and 5. Complete. Below the progress bar, the 'Enrollment Instructions' section provides a list of steps: 'Select package' (Choose your desired digital certificate package), 'Application Info' (Upload your CSR and fill up your informations required for RA verification), and 'Complete' (Once complete, kindly wait for the verification and issuance of your certificate by our RA. You may check your request status by logging to MyTrustID Portal). A 'Next' button is located at the bottom right of the instructions section.

Figure 21: MSC Trustgate Portal Page

b) Click **Next** button

The screenshot shows the 'Select package' page, which is the second step in the enrollment process. The progress bar now shows step 1 as completed and step 2 as active. The 'Package' section contains a dropdown menu with 'Select Package' highlighted, and a list of available packages: 'New User - Digital Certificate - 1 Year - RMO'. The 'Description' section contains four input fields: 'Description', 'Validity (Years)', 'Delivery', and 'Email upon issuance'. A 'Back' button is located at the bottom left, and a 'Next' button is at the bottom right.

Figure 22: Select package page

d) Click **Next** button

e) Paste your CSR file into CSR information field

PAYMENTS NETWORK MALAYSIA SDN BHD (FPX)

TRUSTGATE
SECURE TRANSACTION. TRUSTED BUSINESS

New Certificate Enrollment Request

Enrollment for new client digital ID for Payments Network Malaysia Sdn Bhd

Instructions Package & Pricing Application Info Disclaimer Complete

CSR Information

Paste CSR information here *

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC/CCAeYCAQAwYExGZSABQgNVBAYTA1ZMOWwQYDQIDAAJXU
DEVMBMGAIUE
BwwMSVhhbG9jaThVbWVMSowKAYDQDCEQYX3ZW50cyBOZXB3
b3JkIE1hbG5E
gRUFNhbBCEGQxAgRgNVBAMMGWVhWb3R5Swcm84LmlydC5wYXNvZX
QubXVr
gqEMAGGCSGSlb3QCEBAQUAA4IBDnAwggEK4oBAQC8+mAdrWlt1
CMAMu6sw9
FPwU1YQmllgsOBcyK4ndDcaMq1Omm5uK3l2seFzAd2yDv7IA81G
-----
```

CSR Information	
C	MY
ST	WP
L	Kuala Lumpur
O	Payments Network Malaysia Sdn Bhd
CN	ebikko.prod.int.paynet.my

Figure 22: CSR Submission page

f) Fill in Application Information and Certificate Information then click **Next**

Application Information

Nationality *

Malaysian

Full Name *

Mohd Rozairul Azwan

MyKad No *

780923115783

Email *

test@paynet.my

Mobile No *

0133037627

Organization Name *

Payments Network Malaysia Sdn Bhd

Back

Certificate Information

CN *

ebikko.prod.int.paynet.my

Email *

test@paynet.my

Exchange ID *

EX00001234

Exchange Name *

TestMerchant Sdn Bhd

Next

Figure 23: Online enrolment form

PAYMENTS NETWORK MALAYSIA SDN BHD
(FPX)



New Certificate Enrollment Request

Enrollment for new client digital ID for Payments Network Malaysia Sdn Bhd

✓

Instructions

✓

Package & Pricing

✓

Application Info

4

Disclaimer

5

Complete

Digital ID Subscriber Agreement

SUBSCRIBER AGREEMENT

PLEASE READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING A MSC TRUSTGATE.COM's CERTIFICATE OR DIGITAL ID ("CERTIFICATE" OR "MYTRUST ID"). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE.

1. Certificate Application and Description of Certificates. This Section details the terms and conditions regarding your application ("Certificate Application") for a Certificate and, if MSC Trustgate.com ("MSCTG") accepts your Certificate Application, the terms and conditions regarding the use of the Certificate to be issued by MSCTG to you as a "Subscriber" of that Certificate. A Certificate is a digitally

☒ I hereby confirm that all the information given for this application is true and accurate and have not withheld any information that would affect the acceptance of my application. By signing this application form, I also agree to be bound by the terms and conditions as stipulated in Client ID Digital Certificate Subscriber Agreement, and any amendments made thereto from time to time.

Back

Submit

Figure 24: Confirmation on CSR submission

PAYMENTS NETWORK MALAYSIA SDN BHD
(FPX)



New Certificate Enrollment Request

Enrollment for new client digital ID for Payments Network Malaysia Sdn Bhd

✓

Instructions

✓

Package & Pricing

✓

Application Info

✓

Disclaimer

✓

Complete

✓

Congratulations!

Your request has completed.

Your application will be review and will only be processed and emailed within the next business day.

For assistance please email to support@msctrustgate.com or call our support team at +603- 8318 1800

An email has been sent to you with the access code to login to MyTrustID portal to check your request and do certificate management.

Login to MyTrustID Portal

Figure 26: Confirmation page

Your Digital ID is ready



noreply@msctrustgate.com <noreply@msctrustgate.c...>

Friday, 27 January 2023 at 11:23 AM

To: Mohd Rozairol Azwan Hassan

=====

This is an Incoming external email. Please put EXTRA CAUTION before opening.

=====

Dear MOHD ROZAIROL AZWAN BIN HASSAN,

Our Administrator has approved your Digital ID request and ready to be used.

Please find your digital certificate below:

-----BEGIN CERTIFICATE-----

```
MIIEJjCCAw6gAwIBAgIQE0HjUGaefe6B2lcFefPIEDANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQG
EwJNNWTEgMcGGA1UEChMHUGF5bWVudHMgTmV0d29yayBNYXhheXNpYSBTZG4gQmhmMRIwEAYDVQDD
EwIQYXl0ZXQgQ0EwHhcNMjMMDAwMDAwWhcNMjMMDAwMDAwMTU5WjBhMQswCQYDVQQGEwJN
WTEVMBMGALUECBQMS3VhbGEgTHVtcHVyMRUwEwYDVQQHFAxLdWFSYSBMdWlwdXlxJDAiBgNVBAMT
G2FwaS5jb2N0bWVudHMgTmV0d29yayBNYXhheXNpYSBTZG4gQmhmMRIwEAYDVQDD
ggEBANDnVZND9FG8SKuepc1iFhoyA6bSxkv1EOWs050gsuxPc5KyIa1IwWKT8XVRv0wkvy2q7z
/wb9t4rNyVM7Ata1/VH9jOzS2Es49N+uRmZflrxqTRjzsesKehHjXm5NrGGAKpSmJwI15LXS64oS
nZiLw/0Vc2leM6VXkwUOToS5w/HidhaE+AODijsgI13ZlpwCTRbyqXgZeUdHy/e4GIBcNqCAWt5D
ySyP9XWG6hWMQZ2AUE0ZJqENTj7Kkbz9jzeIEe8FzBJ6loHY08hOvW1ST3sK0VPgcr+//I0zScFO
KeM5RreDy0fcPwa8mCYG3GyeivgAHcmc9GTBJUFlSp8CAwEAAaOB7TCB6jAMBGNVHRMBAf8EAjAA
MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwQwYDVROfBDww
OjA4oDagNIYyYHR0cDovL2Nybc5tc2N0cnVzdGdhGduY29tL1BheU5ldENBL0xhdGVzdENSTC5j
cmwwHQYDVDR0OBByEFNjhGjJpNtZDiRaDA42s8W7vemHPMB8GA1UdIwQYMBaAFMRhnlDqWKS6oDw5
va2a6omf1/RyMCYGA1UdEQQfMB2CG2FwaS5jb2N0bWVudHMgTmV0d29yayBNYXhheXNpYSBTZG4g
QmhmMRIwEAYDVQDD
9w0BAQsFAAOCAQEARNpSPeX6Zu8ovaRfK2cXPX98uceV2GcY+bLicX17zcchMQFP6T71/7wq0721
j1jC/svu6rJptGs jPFW7uUK547BpStqyrcwuFgtxF5q3j6ui4ermlI/iOK5PlsvtZMavX6biNNFo
SO4U3baCYCePGMyOUw8f0E9/Ffltzsy9piKqz9Gr/OEpgma44QyYbzdDGKQq4G0PrliV9w8RMxkA
HQYW6pnB/hRTrN299s0JIY4DDvvnDyScLrpS0Sza7U5fudv8JRawYFyNnHkh7O1YLCW9kwcxNXq7
2WJ/cRQWYqHLEnBzrQKKjd1JjdgTzkhiL0I7WrX4zRF3cw8EptJnmQ==
```

-----END CERTIFICATE-----

Please do not reply to this email. If you need further clarification, please do not hesitate to contact us by email to support@msctrustgate.com

Figure 27: Certificate will send via email from noreply@playnet.my

- 2) Keep the new exchange certificate for your reference
 - Merchant to ensure to use correct Private Key and place the Private Key into correct Path.

3.0 Process Flow for Exchange Certificate Request (Renewal)

3.1 UAT Environment (New Key)

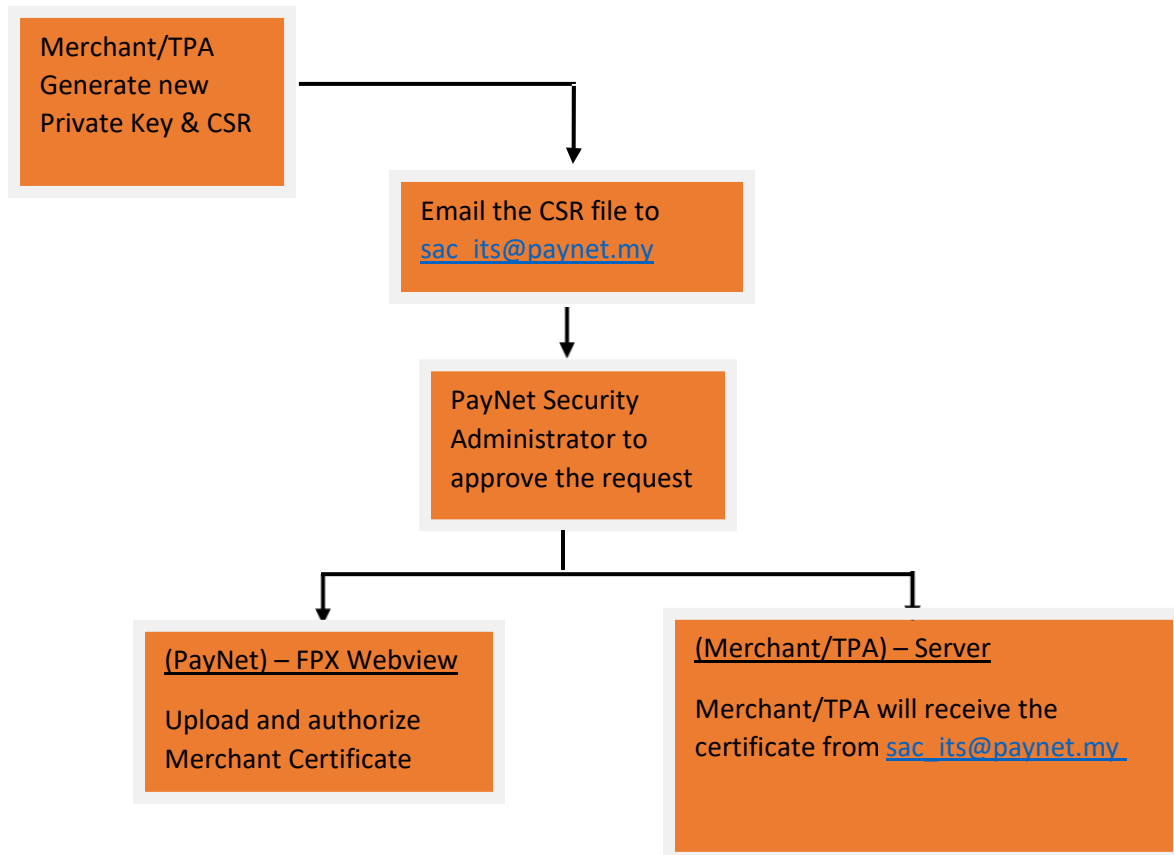


Diagram 3: Process of Flowchart for exchange certificate (renewal) of UAT Environment

3.1.1 Procedure for Exchange Certificate Request

3.1.1.1 Windows Platform

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

a) Generate a private key using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

*****Note: EX00000298 will be the Exchange ID provided *****

```

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)
  
```

Figure 25: Generate Private Key

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

Figure29: Generate CSR File

b) Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtjn3ICysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZACIvdQ9PtZhsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoYkdsop
8ZxlfHa1S53R9XqaKB2zgiBCP1W1KGz8K+gc+GRQQ+CqrkH3OiWPjPTAmkYZy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEvgYPTtmAmTPC9cn5rUWzObGII5
PgR5D47tpaw0wQSUYhzxbngnR8Rrgh/Ge0RKwIDAQABAoIBAGqDe4smob//mCOb
b4rTi3wrthXdFEtVNHV4/czKQMicmic7/UtyXXOmQMeg6lWajOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zArN8hr2M8yh
3LribgYSvacEc1te7/8WI2saAbR77iO5VD2yy+Q76HGabQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKZ9cRMhvdFSduEqmaH7Lt1pcJSIY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyfy/0EC51ITJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whV/VqpiSQhFrN4GK+1D
D0VrmOrd2kneiu0ezYhjqkqsgOf3XiMSGXLVJUcGyEAhgw366L/QJkGttdSfW+U
Xttv8/QWbhyA1pQW5ys6iiSnCp386tb0QN0Sq/NYAVIhdhU8dH5RR3MGgxomf
zqnMGJggJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9f2TNVM4hWx0hTdUsCgYEAAtNe3MEugV4/XaelM7ryC5LjJfEB50O0IO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmhdhAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPQrJpYiRDFRUT2OiqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1Uhm8P1bNthKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBWq0iyYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+lZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```

Figure30: Sample of Private Key

c) Sample of CSR File

```
-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwesELMAkGA1UEBhMCTVlcZAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHXIDbGVhcnRlcjELMAkGA1UECmMCQXUxODAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkbteWNsZWYyLm9yZy5teTCCASlWdQYJ
KoZihvcNAQEBAQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpMWlvYB2yFRcN6Y7IZzBuYWM
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPggq5B
9z0lj4z0wJpGGetGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmzpZUj4EeQ+O7aqWsnMEEIGlc8W54J0fEa6ofxntESsCAwEAAaAx
MBYGCsGSIb3DQEJAJEJewdteWNsZWYyMBcGCsGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zMO2oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyljhHiU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----
```

Figure31: Sample of CSR file

3.1.1.2 Linux Platform

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

a) Generate a private key and CSR using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

****Note: EX00000298 will be the Exchange ID provided ****

```
bash-4.1$ openssl genrsa -out EX00000298.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)
```

Figure 32: Generate Private Key

b) 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 []:
```

Figure33: Information in the certificate

c) Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqj56BZM/+ZwBceU22u
9VDew3MpRGn4+Sbhu5P/iXRqvtjn3CysNwBuPqW9L+DEInkOVHctpQxbGc2dBa
ZACIvdQ9PztHsnVDz09h4W8xYigHbVfW3pjuVnMG5habS1AkmoR/dzoV/kdsop
8ZxifHa1S53R9XqaKB2zgBCP1W1KGz8K+gc+GRQQ+CqrkH3OiwPjPTAmkyZy0YC
Dj8x5Yvd2JtVE1rV7g3JwLxs6wkBd0vrDtXEqvgYPTmAmTPC9cn5rUWzObGIIIS
PgR5D471qpaaw0wQSUYhzbngnR8Rrgh/Ge0RKwIDAQABAolBAGqDe4smob//mCQob
b4rTi3wrthbXdfEtVNHw4/czKQMicmic7/UtvXXOmQMeg6lWjOn9fnp27S22HFI
8G1T6SSEQQm65pL/tv0BM1vXeP4BTJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LribgYsvacEc1te7/8Wl2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EEYcQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKZ9cRMhvdFSDuEqmaH7L1pcJSiY1/Rks5w9XGxSWbxF+WwYrMGaDVTN7hFhuMc
mY45IxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyfi/0EC51TJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj4Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVvqpiSQhFrN4GK+1D
DorVmOrd2kneieue0ezYhjqqsgOf3XiMSGXLVJUCgYEAhgw366L/OJkGItDStW+U
Xttv8i/QIwbbYalpqW5ys6iiSnCp386tb0QN0Sqy/NYAVIhdhU8dH5RR3MGgxomf
zqnMGJgJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LC9fZTNVM4hWx0hTdUsCgYEAiNe3MEugV4/XaelM7ryC5LJfEB50O0IO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQqOEGPQrJpYiRDFRUT2OlgJwVsD6FBRE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0aCgYEBj8BFDNwEsCVfB9wrf+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MwVc1Uhm8P1bNThKf1Y4o+vmZGi2myn3D03w7rqKOWTly8/cxc
V+QBWq0jYEJpH+7hhPGmzaFiSwsejSznJR+KtyV5+IZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```

Figure 34: Sample of private key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVlxCzAJBgNVBAGTAktIMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnRlMAkGA1UECmMCQUQxODAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcm1kenVhbkBteWNsZWYyLm9yZy5teTCCASlwdQYJ
KoZihvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgHggUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpFMWlvYB2yFRcN6Y7IZZBuYWm
0tQJjQEf3c6FZHbKKfGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPggq5B
9z0lj4z0wJpGGctGag4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsnMEEIGlc8W54J0fEa6ofxntESsCAwEAAaAx
MBYGCsGCSqGSIb3DQEJAJEJEwdteWNsZWYyMBcGCsGCSqGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAEHegHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEERUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyljhHiUI6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 35: Sample of CSR file

3.2 Existing Key

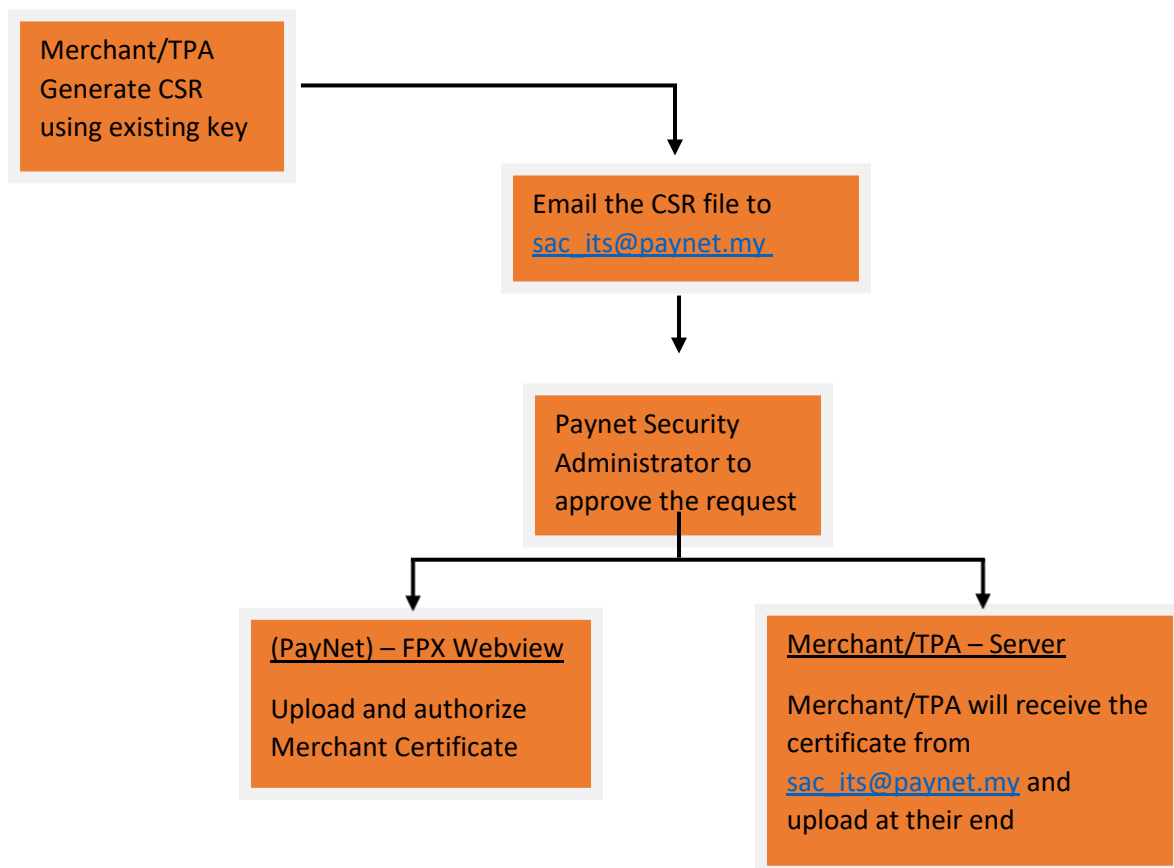


Diagram 4: Process of Flowchart for Exchange Certificate Request (renewal) of Existing Key

3.2.1 Procedure for Exchange Certificate Request

3.2.1.1 Windows Platform

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

a) Generate CSR using existing private key

- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

***** Note: EX12345678 will be the Exchange ID provided *****

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

Figure 36: Generate CSR using existing private key

b) 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 []:
```

Figure 37: Information in the certificate

c) Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCCqj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtn3ICysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZAClvdQ9PtZhsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsoq
8ZxlfHa1S53R9XqaKB2zgiBCP1W1KGz8K+gc+GRQQ+CqrkH3OiWPjPTAmkYzy0YC
Dj8x5Yvd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEvgYpTtmAmTPC9cn5rUWzObGILS
PgR5D477qpaw0wQSUyHxzbngrR8Rrgh/Ge0RKwIDAQABAolBAGqDe4smob/mCOb
b4rTi3wrthbXdEetVNHw4/czKQMicmic7/UtvXXOmQMeg6lWajQn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrlbgYSvacEc1te7/8Wl2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1thyPtI
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEIZYFgUrCvM6EZrgSCO1xSk6RfPIEAqyhphKMtizozlqZ
SelU9NkCgYEAEAGQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7L1pcJSIY1/Rks5w9XGxSWbxF+WYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxmug90EBhd7lc+dlEXK9Pw+kNd8CgYEAS6rp
eh3qfy/0EC51iJJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVvqpiSQhFrN4GK+1D
D0rVmOrd2kneiu0ezYhjgkqsgOf3XiMSGXLVjUCgYEAhgw366L/OJkGTtdSfW+U
Xttv8i/QWbhYalPqW5ys6iiSnCp386tb0QN0Sqy/NYAVIhdhU8dH5RR3MGgxmof
zqnMGJgjJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAtNe3MEugV4/XaelM7ryC5LjJfEB50OIO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPQrJpYiRDFRUT2OiqJwVsD6FBR8nwGVHmYxtc7IPZYIEuCuZFXFPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczy3MWWVc1UhM8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBWq0ijYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+IZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----
```

Figure 38: Sample of Private Key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwczELMAkGA1UEBhMCTVlxCzAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnRlMAkGA1UECjxMCQUxMCQDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmlikenVhbkBteWNsZWYyLm9yZy5teTCCASlwDQYJ
KoZihvcNAQEBAQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpIMWivYB2yFRcN6Y7IZzBuYWm
0tQJjQEf3c6FZHbKKIGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPgq5B
9zolz4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESsCAwEAaAaX
MBYGCsQGSIb3DQEJAJEJEwdteWNsZWYyMBcGCsQGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4Ni7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGPeeUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zm02oHC6FU3oe5CPwcjGeqQibT0tTLYeifsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHiUI6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 39: Sample of CSR file

3.2.1.2 Linux Platform

1) Generation of CSR using existing private key at Merchant's/ TPA's End

a) Generate a private key and CSR using OPENSSSL command

- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

***** Note: EX00000298 will be the Exchange ID provided *****

```

bash-4.1$ openssl req -out EX00000298.csr -key EX00000298.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.

```

Figure 40: Generate CSR file

b) 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 []:

```

Figure 41: Information in the certificate

c) Sample of Private Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqnj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtn3lCysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZAClvdQ9PtZhsnVDz09h4Wl8xYr9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsoP
8ZxlfHa1S53R9XqaKB2zglBCP1W1KGz8K+gc+GRQQ+CqrK3OiwPJPtAmkYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEvgYpTtmAmTPC9cn5rUWzObGIIIS
PgR5D47tpaw0wQSUYhzbngnR8Rqh/Ge0RKwIDAQABAolBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHw4/czKQMicmic7/UtvXXOmQMeg6lWAjOn9fnp27S22HEH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LribgYSvaceE1te7/8Wl2saAbR77iIOSND2yy+Q76HGAbQmdRefK720p1hyPtI
9/6TNRL7MVoNdHdIPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EEycQuviAahp
0C6+7/63RiDxuTLUJmtE1ZYFgUrcvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfnNDYfoNE1
HKZ9cRMhvdFSduEqmaH7L1pcJSIY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY451xbZky8Qu1euaORfyb4dOsYxMug90EBhd7lc+dlEXK9Pw+kNd8CgYEA56rp
eh3qyfj0EC51TJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj4Tb7H82RYB8xARPg/mQEBcvT4wTGUG0HF+whVvqpiSqHFrN4GK+1D
D0rVmOGDpJpYrDFRUT2OlqJwVsD6FBrE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrF+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GTPQvAM3jczgy3MWVc1Uhm8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBV0qjYEJpH+7hhPGmzaFiSwsejSzriJR+KtyV5+lZfKcV+T7IQ==
-----END RSA PRIVATE KEY-----

```

Figure 42: Sample of Private Key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwesELMAkGA1UEBhMCTVkcCzAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIdBGVhcjELMAkGA1UECjMCQUQxQDAKAgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkBteWNsZWYyLm9yZy5teTCCASlwdQYJ
KoZihvcNAQEBAQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHlNtrvVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAil3UPT7cx7J1Q89PYeFpFMWlvYB2yFRcN6Y7IzZBuYWm
0tQJjQeF3c6FZHBKKfGcSHx2tUud0V6migs4JQQj9VtShs/CvqnPhkUEPggq5B
9zolz4z0wJpGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmXPZUj4EeQ+O7aqWsnMEEIGic8W54J0fEa6ofxntESsCAwEAaAx
MBYGCsGSIb3DQEJAJEJewdteWNsZWYyMBcGCSqGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfppqbBuGWekv5mMoj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3Q3zMO2oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHiU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 43: Sample of CSR File

3.2.1.3 Method for CSR submission

- 1) Submit the CSR file to PayNet for approval.
 - a) Email the CSR file generated to sac_its@paynet.my
 - b) Kindly provide the following info:
 - Exchange Name
 - Exchange ID
 - Contact Person
 - c) New certificate will be emailed from Certificate Management.
 - Merchant to ensure to use correct Private Key and place the Private Key into correct Path.
- 2) Keep the new exchange certificate for Merchant reference

3.3 PRODUCTION Environment

3.3.1 New Key

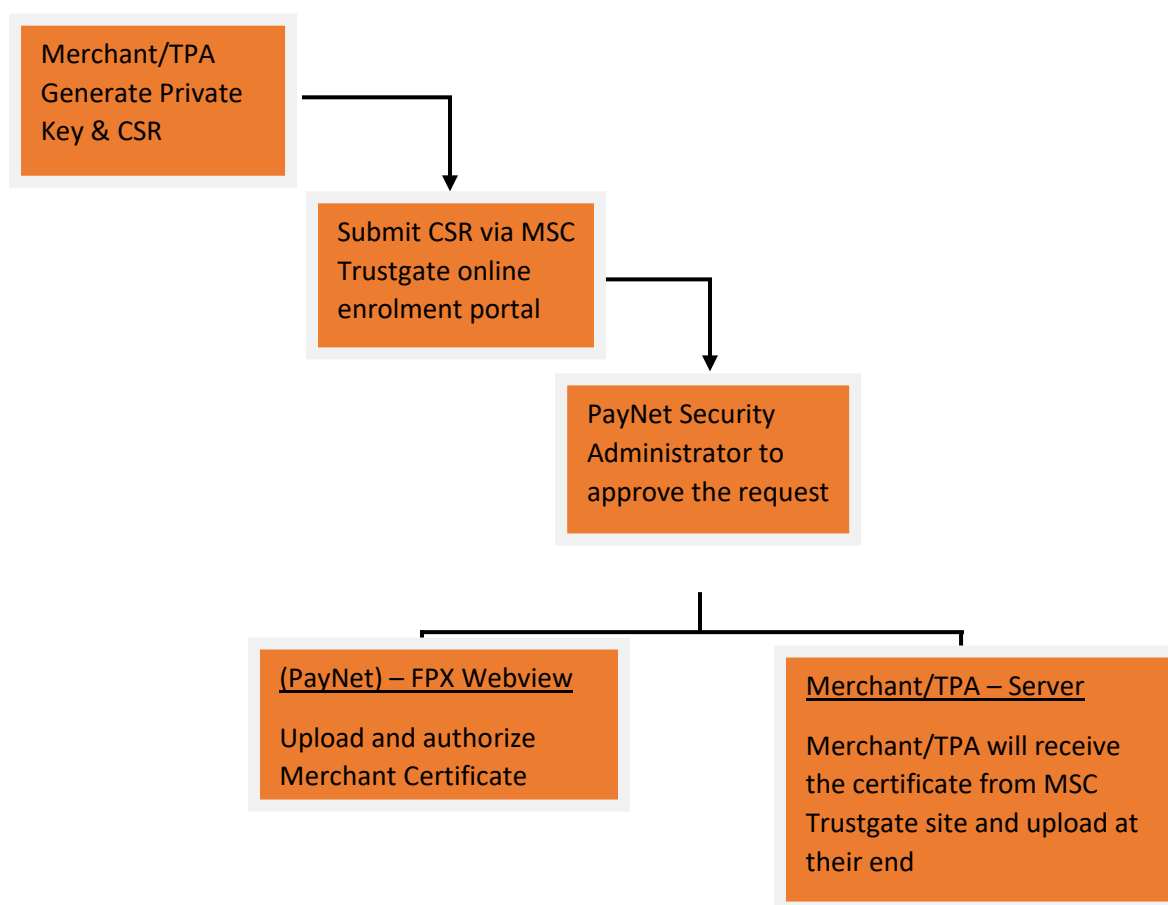


Diagram 5: Process Flowchart for Production Environment of New Key

3.3.1.1 Procedure for Exchange Certificate Request

3.3.1.1.1 Windows Platform

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

a) Generate a private key using OPENSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

*****Note: EX00000298 will be the Exchange ID provided *****

```

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)
  
```

Figure 44: Generate Private Key

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

Figure 45: Generate CSR File

- b) 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 []:
```

Figure 46: Information in the certificate

- c) Sample of Private Key

```
-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCqj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/iXRqvtn3iCysNwBuPqW9L+DEfNkOVHctpQxbGc2dBa
ZACIvdQ9PtZhsnVDz09h4Wl8xYi9gHblVFw3pjuVnMG5habS1AkmoR/dzoVkdsoP
8ZxIfHa1S53R9XqaKB2zglBCP1W1KGz8K+gc+GRQQ+CqrkH3OiWPjPTAmkYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEqvGYPTtmAmTPC9cn5rUWzObGllS
PgR5D47tqpaW0QSUYhzbngnR8Rrgh/Ge0RKwIDAQABAoIBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHw4/czKQMicmic7/UtvXXOmQMeg6lWajOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LribgYsvacEc1te7/8Wl2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi6gvdpaAbLsfyPdclt2/EFycQuviAahp
0C6+7/63RiDxuTLUJmtEfZYFgUrcvM6EZrgSCO1xSk6RtPIEAqyhphKMtizozlqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJRJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7Lt1pcJSiY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlhEXK9Pw+kNd8CgYEA56rp
eh3qyfi/0EC51iJJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVVqpiSQhFrN4GK+1D
D0tVmOrd2kneue0ezYhjqkqsgOf3XiMSGXLVjUCgYEAhgw366L/OJkG.TtdSfW+U
Xttv8i/QIwBhYalPqW5ys6iiSnCp386tb0QN0SqY/NYAVIhdhU8dH5RR3MGgxomf
zqnMGJggJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNV4hWvX0hTdUsCgYEAtnE3MEugV4/XaeLM7ryC5LjJfEB50O0IO3MI
TufY90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQq0EGPOrJpYiRDFRUT2OlqJwVsD6FbRE8nwGVHmYxtc7IPZYIEuCuZFXPb1WXZb
07wa0a0CgYBj8BFDNwEsCVfB9wrf+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVaM3jczgy3MWVc1Uhm8P1bNThKf1Y4o+vmZGi2myn3Do3w7rqKOWTly8/exc
V+QBWq0ijYEjPH+7hhPGmzaFiSwsejSzriJR+KtyV5+IZFkCv+T7IQ==
-----END RSA PRIVATE KEY-----
```

Figure 47: Sample of Private Key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVlrczAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnRlMAkGA1UECjMCQUQxQDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmlikenVhbkBteWNsZWZyLm9yZy5teTCCASlwDQYJ
KoZihvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrvVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpfMWlvYB2yFRcN6Y7IZzBuYWm
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migds4JQQj9VtShs/CvqnPhkUEPggq5B
9z0lj4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwyXJ+a1FszmzpZUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESsCAwEAAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWZyMBcGCsGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYejfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyljHiU6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 48: Sample of CSR file

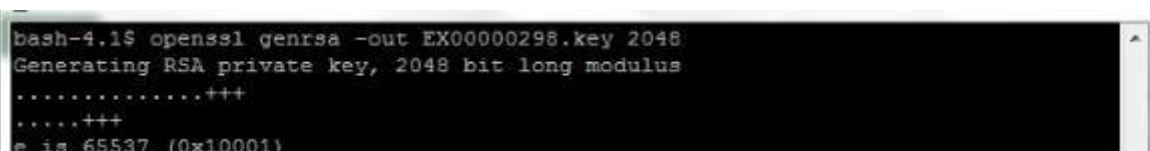
3.3.1.1.2 Linux Platform

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

a) Generate a private key and CSR using OPENSSSL command

- Command to generate Private Key → ***Openssl genrsa -out EX00000298.key 2048***
- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

***** Note: EX00000298 will be the Exchange ID provided *****



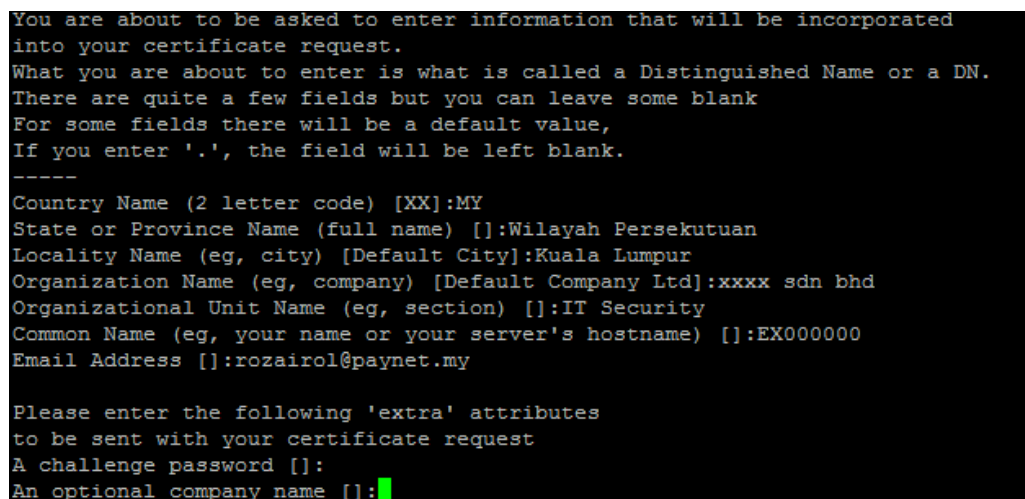
```

bash-4.1$ openssl genrsa -out EX00000298.key 2048
Generating RSA private key, 2048 bit long modulus
.....+++
.....+++
e is 65537 (0x10001)

```

Figure 49: Generate Private Key

b) 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 []:

```

Figure 50: Information in the certificate

c) Sample of Private Key

```

-----BEGIN RSA PRIVATE KEY-----
MIIEpAIBAAKCAQEA0k2GtAKo+Dp+D9aP4sczN2CGCBRDCCqj56BZM/+ZwBceU22u
9VDew3MpRGnI4+Sbhu5P/XRqvtn3ICysNwBuPqW9L+DEfNkOVHctPQxbGc2dBa
ZACIvdQ9PtZhsnVDz09h4Wl8xYi9gHblVFw3puVnMG5habS1AkmoR/dzoVkdsoP
8ZxlfHa1S53R9XqaKB2zgiBCP1W1KGz8K+qc+GRQQ+CqrkH3OiWPjPTAmkYzy0YC
Dj8x5YVd2JtTVE1rV7g3JwLxs6wKbD0vrDtXEvgYPTtmAmTPC9cn5rUWzObGllS
PgR5D47tqpaW0wQSUyHxzxbngnR8Rrgh/Ge0RKwIDAQABAolBAGqDe4smob//mCOb
b4rTi3wrthbXdFEtVNHV4/czKQMicmic7/UtvXXOmQMeg6lWAjOn9fnp27S22HFH
8G1T6SSEQQm65pL/tv0BM1vXePt4BtJG9dEaeCd1HIP/PGGFhQ+1zARn8hr2M8yh
3LrIbgySVacEc1te7/8Wl2saAbR77iIOSiVD2yy+Q76HGAbQmdReFk720p1hyPtl
9/6TNRL7MVoNdhDiPbGzq0dY+Q1PQGcXi8gvdpaAbLsfyPdclt2/EEycQuviAahp
0C6+7/63RiDxuTLUJmtEIZYFgUrCvM6EZrgSCO1xSk6RtPIEAqyhphKMtizoIqZ
SelU9NkCgYEA6GQoK5Ox/AGXPK5RqUrc0ps38MZo594vqhtJrJ7zvJnfNDYfoNE1
HKz9cRMhvdFSduEqmaH7L1tpcJSIY1/Rks5w9XGxSWbxF+WiYrMGaDVTN7hFhuMc
mY45lxbZky8Qu1eua0Rfyb4dOsYxMug90EBhd7lc+dlnEXK9Pw+kNd8CgYEA56rp
eh3qyfj/0EC51tJoKwMfsV1XbG7rX2mP5Yx01dmN/Se3Rj/Mrx4TEunzXN42S86
A06Kd41Lrj47Tb7H82RYB8xARPg/mQEBcvT4wTGuG0HF+whVvqpiSQhFrN4GK+1D
D0rVmOrd2kneue0ezYhjqqsgOf3XiMSGXLVjUCGyEAhgw366L/QJkGTtdSfW+U
Xttv8i/QWbhyALpqW5ys6iiSnCp386tb0QN0Sqy/NYAVlhdhU8dH5RR3MGgxmof
zqnMGJgjJm79xMYN3BbeLEAOJ4bgfAUHG0Ahjy8AA9ITMm1KS8+d3TYPkDaAbJfw
B+8LCc9fZTNVM4hWx0hTdUsCgYEAAtNe3MEugV4/XaelM7ryC5LjJfEB50OIO3MI
Tufy90h3k+CSDrgPprR3F9/LGtc0FB4lpElwVwjmdhtAQf1Wqsm+6j9oQC6lvrOJ
RQqQEGPQrJpYiRDFRUT2OiqJwVsD6FBR8nwGVHmYxtc7IPZYIEuCuZFXFPb1WXZb
07wa0aOCyVfB9wrf+OPur44m/vSBtV61U/JJvxl3Q6Wz4r4BwEPC
GtPOVAM3jczgy3MWVc1Uhm8P1bnThKf1Y4o+vmZGi2myn3Do3w7rqKOWtly8/cxc
V+QBWq0ijYEjPH+7hhPGmzaFiSwsejSzriJR+KtyV5+IZFkCv+T7iQ==
-----END RSA PRIVATE KEY-----

```

Figure 51: Sample of Private Key

d) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBhMCTVkcCzAJBgNVBAGTAktMMQswCQYDVQQH
EwJXUDEQMA4GA1UEChMHMTXIDBgVhcgELMAkGA1UECjMCQUxQxQDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkBteWNsZWYyLm9yZy5teTCCASlwdQYJ
KoZlHvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHlNtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpIMWlvYB2yFRcN6Y7IZzBuYWm
0tQJjQEf3c6FZHbKKfGcSHx2tUud0fV6migds4JQQj9VtShs/CvqnPhkUEPgq5B
9z0lj4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESsCAwEAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyMBcGCsGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfpqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjr9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYeJfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHiU16g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 52: Sample of CSR file

3.3.2 Existing Key

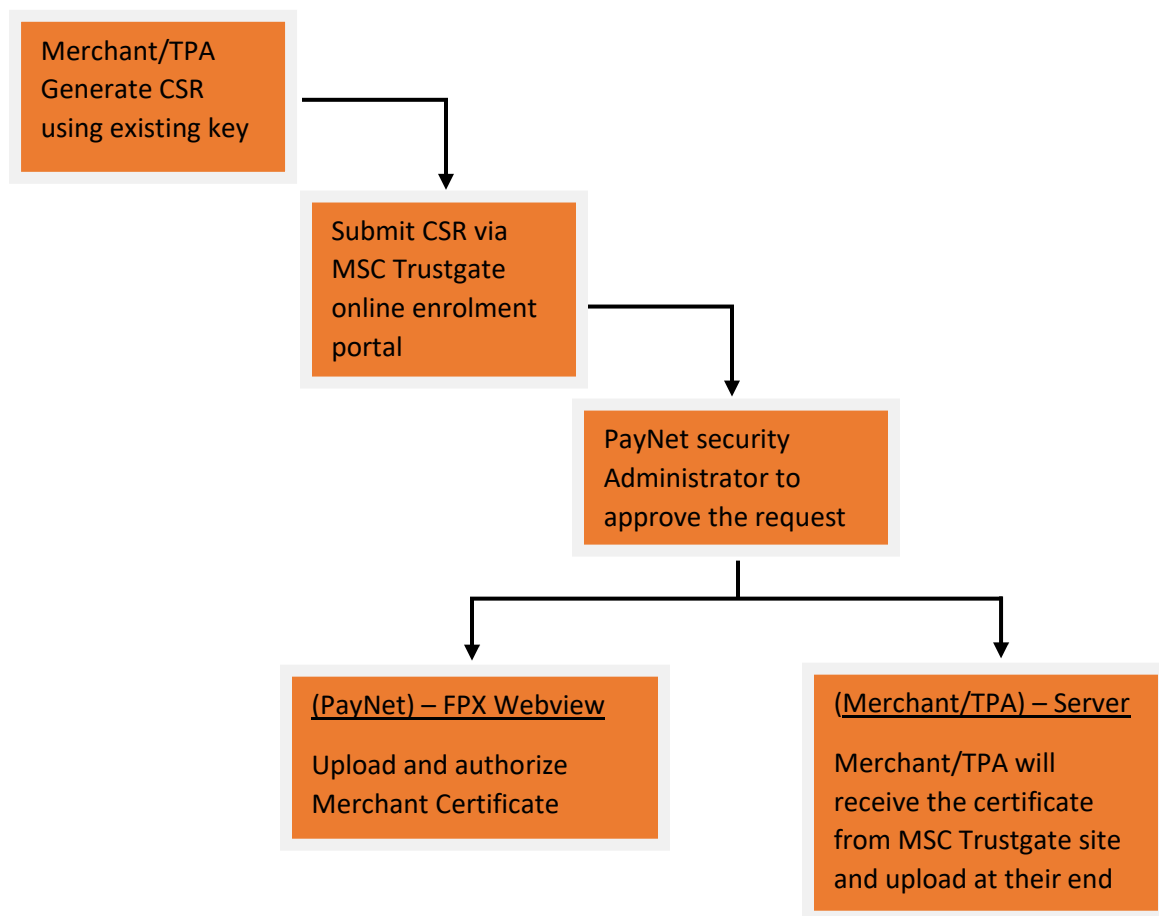


Diagram 6: Process of Flowchart for Production Environment of Existing Key

3.3.2.1 Procedure for Exchange Certificate Request

3.3.2.1.1 Windows Platform

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

a) Generate CSR using existing private key

- Command to generate CSR → ***openssl req -out EX00000298.csr -key EX00000298.key -new -sha256***

***** Note: EX00000298 will be the Exchange ID provided *****

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

Figure 53: Generate Private Key

- b) 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 []:

```

Figure 54: Information in the certificate

- c) Sample of CSR File

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwEzELMAkGA1UEBnMCTVksCzAJBgNVBAGTAktMMQswCQYDVQQH
HwEwJXUdEQMA4GA1UEChMHMTXIDbGVhcnJELMAkGA1UECjMCQUxQxDDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkBteWNsZWYyLm9yZy5teTCCASlwdQYJ
KoZihvcNAQEBAQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpIMWlvYB2yFRcN6Y7IZzBuYWm
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPgqq5B
9zolz4z0wJpGGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsNMEEIGlc8W54J0fEa6ofxntESsCAwEAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyMBcGCsGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAEHcGqHm3ozCuu18gUWRjQhlg6i+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGPeeUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYeJfsPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyijhHil6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 55: Sample of CSR File

3.3.2.1.2 Linux Platform

Generation of CSR using existing private key at Merchant's/TPA's end

- a) Generate Private Key and CSR using OPENSSL command

- 4 Command to generate Private Key → **Openssl genrsa -out EX00000298.key 2048**
- 5 Command to generate CSR → **openssl req -out EX00000298.csr -key EX00000298.key -new -sha256**

**** Note: EX00000298 will be the Exchange ID provided ****

```

bash-4.1$ openssl req -out EX00000298.csr -key EX00000298.key -new -sha256
You are about to be asked to enter information that will be incorporated
into your certificate request.

```

Figure 56: Generate Private Key

- b) 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 []:

```

Figure 57: Information in the certificate

- c) Sample of CSR file

```

-----BEGIN CERTIFICATE REQUEST-----
MIIC8TCCAdkCAQAwezELMAkGA1UEBhMCTVlxZAJBgNVBAgTAktMMQswCQYDVQQQ
H
EwJXUDEQMA4GA1UEChMHMTXIDbGVhcnJELMAkGA1UEC3MCQUxQxDDAKBgNVBAMTA0
9u
ZTEIMCMGCSqGSIb3DQEJARYWcmllkenVhbkBteWNsZWYyLm9yZy5teTCCASlwDQYJ
KoZihvcNAQEBBQADggEPADCCAQoCggEBANJNhrQCqPg6fg/Wj+LHMzdgghgUQwqp
4+egWTP/mcAXHINtrVQ3sNzKURp5ePkm4buT/4l0ar7Y595QsrDcAbj6lvS/gxH
zZDIR3LaUMWxnNnQWmQAiL3UPT7cx7J1Q89PYeFpfMWlvYB2yFRcN6Y7IZzBuYWm
0tQJJqEf3c6FZHbKKfGcSHx2tUud0fV6migs4JQQj9VtShs/CvqnPhkUEPgq5B
9z0lj4z0wJpGgGctGAg4/MeWFXdibU1RNa1e4NycC8bOsCmw9L6w7VxKr4GD7bZgJ
kzwvXJ+a1FszmxpZUj4EeQ+O7aqWsnMEEIGlc8W54J0fEa6ofxntESsCAwEAaAx
MBYGCsGSIb3DQEJAJEJEwdteWNsZWYyMBcGCsGSIb3DQEJBzEKEwhwYXNzd29y
ZDANBgkqhkiG9w0BAQUFAAOCAQEAAHeGqHm3ozCuu18gUWRjQhIG6i+2frdx3h9ou
qWpfppqbBuGWekv5mMOj20YAtglA+O34bsBD8Wkbp8qyBM0lb2mlvg0f8T4c/akj
rVp6cqt4NI7SL1pP5GgQQGmKvSvjGTB+6CFTqBWymkQ6fydyF5Zm+WkVXhXGEOXd
99JcT3oT4n0Sihc2qB7pjrR9HyWGpEErUA28XH/Yq3gvqnQrAnZ9cHVEFLhde/pt
0hYk6DEuvup4pGFHqRp3QQ3zM02oHC6FtU3oe5CPwcjGeqQibT0tTLYeifjPKkb7
EMde03OM5bOwT8G1/p0EQFqu8RjUyIjhHiUI6g2VAZv3pBNfvA==
-----END CERTIFICATE REQUEST-----

```

Figure 58: Sample of CSR File

3.3.3 Method for CSR submission

3.3.3.1 Submit CSR file to MSC Trustgate for Approval

a) Submit the CSR to the following URL:

<https://www.msctrustgate.com/mytrustid/enrollment?q=paynetfpx>

The screenshot displays the 'New Certificate Enrollment Request' page for Payments Network Malaysia Sdn Bhd (FPX). The page features a progress bar with five steps: 1. Instructions (active), 2. Package & Pricing, 3. Application Info, 4. Disclaimer, and 5. Complete. Below the progress bar, the 'Enrollment Instructions' section provides a list of steps: 'Select package' (Choose your desired digital certificate package), 'Application Info' (Upload your CSR and fill up your informations required for RA verification), and 'Complete' (Once complete, kindly wait for the verification and issuance of your certificate by our RA. You may check your request status by logging to MyTrustID Portal). A 'Next' button is located at the bottom right of the instructions section.

Figure 59: MSC Trustgate Portal Page

b) Click **Next** button

The screenshot shows the 'Select package' page. The progress bar indicates that step 1 (Instructions) is completed, and step 2 (Package & Pricing) is the current step. The 'Package' section shows a dropdown menu with 'Select Package' highlighted, and a list of available packages: 'New User - Digital Certificate - 1 Year - RM0'. The 'Description' section contains input fields for 'Description', 'Validity (Years)', 'Validity', 'Delivery', and 'Email upon issuance'. 'Back' and 'Next' buttons are located at the bottom of the page.

Figure 60: Select package page

d) Click **Next** button

e) Paste your CSR file into CSR information field

PAYMENTS NETWORK MALAYSIA SDN BHD
(FPX)

TRUSTGATE

SECURE TRANSACTION. TRUSTED BUSINESS.

New Certificate Enrollment Request

Breadcrumb for new client digital ID for Payments Network Malaysia Sdn Bhd

Instructions

Package & Pricing

Application Info

Disclaimer

Complete

CSR Information

Paste CSR information here *

-----BEGIN CERTIFICATE REQUEST-----
MIIC/CCAeYCAQAwYExCQAIBqNBAYTAk1ZMQswCQYDVQQIDAJXU
DEVBMGA1UE
BwwMS3VnbGEgTHVhcHVMSoxKAYDVKQKDCEFYXIzW50cyBOZXR3
b3JlIE1hbGE5
c2ltIFNpbCaGQxiAgBoNVBAMMGVjaWhwbySwcm9kLmldCScyYXo/ZX
QubXor
ggEIMAGCGSgGSib3dQEBAQUAAIIBDnAwppEKAnIQACQ+mAdYWml
CMXmv6kar9
FP4wJ1YQwalgsOBvyc/k4ySDoeMq1Onmj5vK3j2ns9E+AdzPd7IAoB1G

CSR Information

C	MY
ST	WP
L	Kuala Lumpur
O	Payments Network Malaysia Sdn Bhd
CN	ebikko.prod.int.paynet.my

Figure 61: CSR Submission page

f) Fill in Application Information and Certificate Information then click **Next**

Application Information

Nationality *

Malaysian

Full Name *

Mohd Rozainol Azwan

MyKad No *

780923115783

Email *

test@paynet.my

Mobile No *

0133037627

Organization Name *

Payments Network Malaysia Sdn Bhd

Back

Certificate Information

CN *

ebikko.prod.int.paynet.my

Email *

test@paynet.my

Exchange ID *

EX00001234

Exchange Name *

TestMerchant Sdn Bhd

Next

Figure 62: Online enrolment form

PAYMENTS NETWORK MALAYSIA SDN BHD
(FPX)

TRUSTGATE

SECURE TRANSACTION. TRUSTED BUSINESS

New Certificate Enrollment Request

Enrollment for new client digital ID for Payments Network Malaysia Sdn Bhd

✓

Instructions

✓

Package & Pricing

✓

Application Info

4

Disclaimer

5

Complete

Digital ID Subscriber Agreement

SUBSCRIBER AGREEMENT

PLEASE READ THIS SUBSCRIBER AGREEMENT ("SUBSCRIBER AGREEMENT") BEFORE APPLYING FOR, ACCEPTING, OR USING A MSC TRUSTGATE.COM's CERTIFICATE OR DIGITAL ID ("CERTIFICATE" OR "MYTRUST ID"). IF YOU DO NOT AGREE TO THE TERMS AND CONDITIONS OF THIS SUBSCRIBER AGREEMENT, DO NOT APPLY FOR, ACCEPT, OR USE THE CERTIFICATE.

1. Certificate Application and Description of Certificates. This Section details the terms and conditions regarding your application ("Certificate Application") for a Certificate and, if MSC Trustgate.com ("MSCTG") accepts your Certificate Application, the terms and conditions regarding the use of the Certificate to be issued by MSCTG to you as a "Subscriber" of that Certificate. A Certificate is a digitally

☒ I hereby confirm that all the information given for this application is true and accurate and have not withheld any information that would affect the acceptance of my application. By signing this application form, I also agree to be bound by the terms and conditions as stipulated in Client ID Digital Certificate Subscriber Agreement, and any amendments made thereto from time to time.

Back

Submit

Figure 63: Confirmation on CSR submission

PAYMENTS NETWORK MALAYSIA SDN BHD
(FPX)

TRUSTGATE

SECURE TRANSACTION. TRUSTED BUSINESS

New Certificate Enrollment Request

Enrollment for new client digital ID for Payments Network Malaysia Sdn Bhd

✓

Instructions

✓

Package & Pricing

✓

Application Info

✓

Disclaimer

✓

Complete

✓

Congratulations!

Your request has completed.

Your application will be review and will only be processed and emailed within the next business day.

For assistance please email to support@msctrustgate.com or call our support team at +603- 8318 1800

An email has been sent to you with the access code to login to MyTrustID portal to check your request and do certificate management.

Login to MyTrustID Portal

Figure 64: Confirmation page

© 2020 PayNet. Internal Use Only

Page 36 of 36

Your Digital ID is ready



noreply@msctrustgate.com <noreply@msctrustgate.c...>

Friday, 27 January 2023 at 11:23 AM

To: Mohd Rozairol Azwan Hassan

=====

This is an Incoming external email. Please put EXTRA CAUTION before opening.

=====

Dear MOHD ROZAIROL AZWAN BIN HASSAN,

Our Administrator has approved your Digital ID request and ready to be used.

Please find your digital certificate below:

-----BEGIN CERTIFICATE-----

```
MIIEJjCCAw6gAwIBAgIQE0HjUGaefe6B2lcFefPIEDANBgkqhkiG9w0BAQsFADBNMQswCQYDVQQG
EwJNNWTEgMCgGA1UEChMhUGF5bWVudHMgTmV0d29yayBNYXheXNpYSBTZG4gQmhmMRIWEAYDVQOD
EwLQYXLOZQXGgQ0EWHhcNMjMwMTI3MDAwMDAwWhcNMjMwMTI3MjM1OTU5WjBhMQswCQYDVQGEwJN
WTEVMBMGAlUECBQMS3VhbGEgTHVtcHVyMRUwEwYDVQHFAXLdWFSYSBMDWlwdXlxJDAiBgNVBAMT
G2FwaS5jbjAucHJvZC5pbmV0LnBheW5ldC5teTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoC
ggEBANDnVZND9FG8SKuepc1iFhoyA6bSxkv1EOWs050gsuxPc5KyIa1IwWrKTN8XVRv0wkvy2q7z
/wb9t4rNyVM7Ata1/VH9jOzS2Es49N+uRmZflrxqTRjzsesKehHjXm5NrGGAKpSmJwI15LXS64oS
nZiLw/0Vc2leM6VXkwUOToS5w/HiDhaE+AODijsgI13ZlpwCTRbyqXgZeUdHy/e4GIBcNqCAWt5D
ySyP9XWG6hWMQZ2AUE0ZJqENTj7Kkbz9jzeIEe8FzBJ6loHY08hOvW1ST3sK0VPgcr+//I0zScFO
KeM5RreDy0fcPwa8mCYG3GYeiVgAHcmc9GTBJUFlSp8CAwEAAaOB7TCB6jAMBGNVHRMBAf8EAjAA
MA4GA1UdDwEB/wQEAwIFoDAdBgNVHSUEFjAUBgggrBgEFBQcDAQYIKwYBBQUHAWIwQwYDVROfBDWw
OjA4oDagNIYyaHR0cDovL2Nybc5tc2N0cnVzdGdhGduY29tL1BheU5ldENBL0xhdGVzdENSTC5j
cmwwHQYDVRO0BBYEFNjhgJjPntzDiRaDA42s8W7vemHPMB8GA1UdIwQYMBaAFMRhnlDqWKS6oDw5
va2a6omf1/RyMCYGA1UdEQQfMB2CG2FwaS5jbjAucHJvZC5pbmV0LnBheW5ldC5teTANBgkqhkiG
9w0BAQsFAAOCAQEARNpSPeX6zu8ovaRfK2cXPX98uceV2GcY+bLicX17zcchMQFP6T71/7wq0721
j1jC/svu6rJptGs jPFw7uUK547BpStqyrcwuFgtxF5q3j6ui4ermlI/iOK5PlsvtzMavX6biNNFo
SO4U3baCYCePGMYOUw8f0E9/Ff1tZsy9piKqz9Gr/OEpgma44QyYbzdDGKQq4G0PrliV9w8RMxkA
HQYW6pnB/hRTrN299s0JIY4DDvvnDyScLrpS0Sza7U5fudv8JRawYFyNnHkh7O1YLCW9kwcxNXq7
2WJ/cRQWYqHLEnBzrQKKjd1JjdgTzkhiL0I7WrX4zRF3cw8EptJnmQ==
```

-----END CERTIFICATE-----

Please do not reply to this email. If you need further clarification, please do not hesitate to contact us by email to support@msctrustgate.com

Figure 65: Certificate will send via email from noreply@playnet.my

3.3.3.2 Keep the new exchange certificate for your reference

- Merchant to ensure to use correct Private Key and place the Private Key into correct Path.

4.0 FPX Certificate

4.1 Download and install latest FPX Certificate

- Go to <https://exchange.fpx.prod.inet.paynet.my/>
- Go to Certificate
- FPX UAT Cert (fpxuat.cer) – UAT environment
- FPX Production Cert (fpxprod.cer) – Production Environment

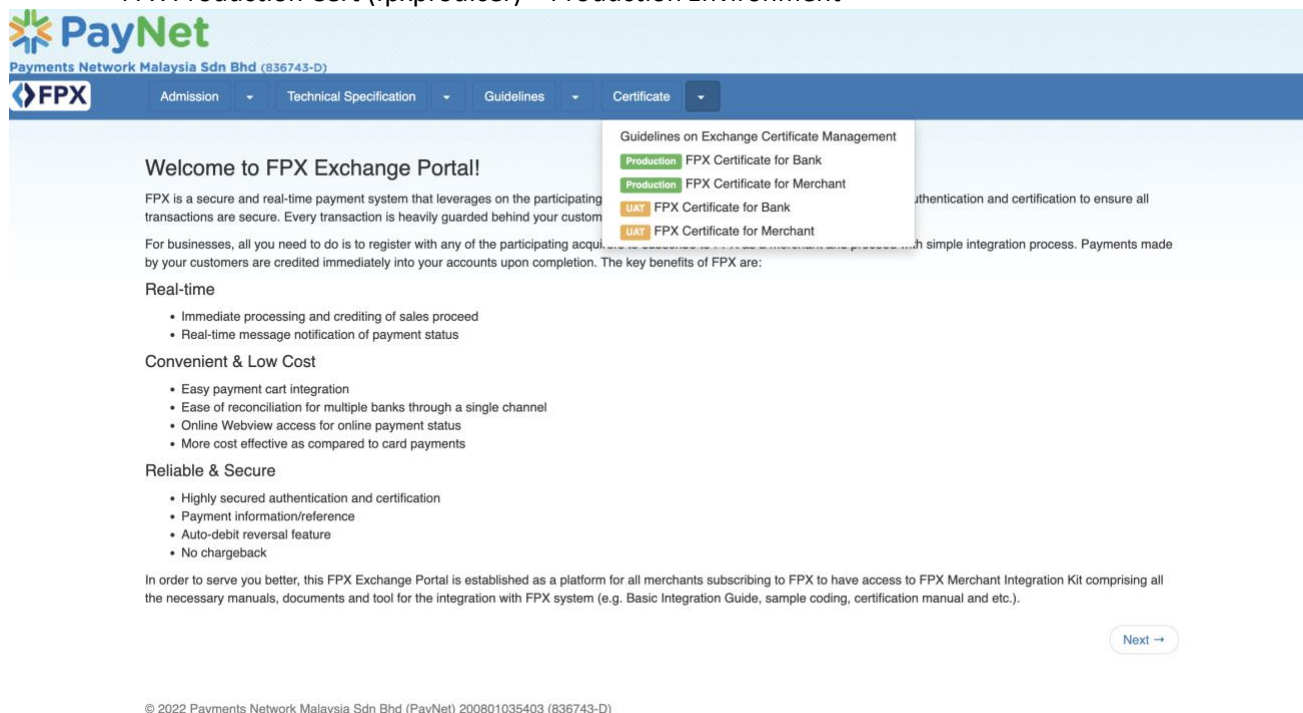


Figure 26: Merchant/TPA and Bank to download the latest FPX Certificate from the Portal

4.2 Renewal of FPX Certificate

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

- UAT → change from fpxuat.cer to fpxuat_current.cer
- Production → change from fpxprod.cer to fpxprod_current.cer

Note: Refer to **Sample Source Codes for FPX** document on how to incorporate the renewal of FPX Certificate function into Merchant's existing system.