



OPEN BANKING

OpenSSL

***eIDAS PSD2 Certificate Signing Request
Profiles***

Date: 20th May 2020

Issue: 2.2

Classification: Public

REFERENCES

Number	Title	Link	Notes
1	Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366”	https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.02.01_60/ts_119495v010201p.pdf	ETSI specification for QWAC and QSEAL certificates.
2	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	https://www.ietf.org/rfc/rfc3739.txt	qcStatement specification RFC 3739

VERSION CONTROL

Version	Title	Notes
2.1	OpenSSL eIDAS PSD2 Certificate Signing Request Profiles Issue 2_1	First release.
2.2	Internet X.509 Public Key Infrastructure: Qualified Certificates Profile	<p>Section 2.5 <i>ASN.1 EDITOR</i> deleted. This illustrated a third party tool with example output.</p> <p>Section 3.2 <i>OBWAC OPENSSL .CNF FILE</i> - all text that must be modified by the client has been highlighted in red to reduce user error.</p> <p>Section 4.2 <i>OBSEAL OPENSSL CNF FILE FILE</i> - all text that must be modified by the client has been highlighted in red to reduce user error.</p> <p>qcStatement DER strings have been updated to ensure the correct nesting is used in sections:</p> <p>3.2 <i>OBWAC OPENSSL .CNF FILE</i></p> <p>3.3 <i>COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI + PSP_IC</i></p> <p>4.2 <i>OBSEAL OPENSSL CNF FILE</i></p> <p>4.3 <i>COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI + PSP_IC</i></p>

CONTENTS

1	PREFACE.....	4
1.1	PURPOSE OF THIS DOCUMENT.....	4
2	X.509 CERTIFICATE SIGNING REQUEST PROFILES.....	5
2.1	OBWAC AND OBSEAL.....	5
2.2	PSD2 STATEMENT.....	8
2.3	ORGANISATIONAL IDENTIFIER STATEMENT.....	8
2.4	CSR GENERATION - OPENSLL.....	9
3	OBWAC X509 CERTIFICATE SIGNING REQUEST PROFILE.....	10
3.1	INTRODUCTION.....	10
3.2	OBWAC OPENSLL .CNF FILE.....	10
	COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI.....	15
3.3	+ PSP_IC.....	15
3.4	EXAMPLE OBWAC CSR CREATION USING OPENSLL FOR ROLES PSP_AS, PSP_AI AND PSP_IC.....	17
4	OBSEAL X509 CERTIFICATE SIGNING REQUEST PROFILE.....	20
4.1	INTRODUCTION.....	20
4.2	OBSEAL OPENSLL CNF FILE.....	20
	COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI.....	25
4.3	+ PSP_IC.....	25
4.4	EXAMPLE OBSEAL CSR CREATION USING OPENSLL FOR ROLES PSP_AS, PSP_IC.....	27

1 PREFACE

1.1 PURPOSE OF THIS DOCUMENT

This document outlines the general procedure to generate Certificate Signing Requests (CSR) for Open Banking Public Key Infrastructure (PKI).

In particular, it focuses on the method required to generate a CSR compliant with ETSI specification "Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive (EU) 2015/2366" [REF 1].

2 X.509 CERTIFICATE SIGNING REQUEST PROFILES

2.1 OBWAC AND OBSEAL

The OBWAC and/or OBSEAL certificates are issued by the **Open Banking PKI** in return for a valid CSR.

The ETSI specification [REF 1] defines elements that must be present in an X.509 certificate to make it compliant with the standard. In particular:

- 1 The `organizationIdentifier` (oid: 2.5.4.97) element **MUST** be present in a valid CSR subject name and **MUST** conform to the pattern defined in [REF 1]. The value of `organizationIdentifier` should follow the syntax and the conventions found in section "5.2.1 PSD2 Authorization Number or other recognised identifier" on page 12 of [REF 1]. The NCA name, code, etc. rules are set out in section "5.2.3 Name and identifier of the competent authority" on page 14 of [REF 1]. The list of NCA Identifiers can be found on page 24 of [REF 1].
- 2 A `qcs-compatible` extension (oid: 1.3.6.1.5.5.7.1.3) **MUST** be present in a valid CSR. It **MUST** contain two elements: `qcs-QcType` (oid: 0.4.0.1862.1.6) and `etsi-psd2-qcStatement` (oid: 0.4.0.19495.2).
- 3 The value of the `qcs-QcType` element **MUST** be present in a valid certificate and **MUST** be either `id-etsi-qct-web` (oid: 0.4.0.1862.1.6.3) for OBWAC CSRs or `id-etsi-qct-eseal` (oid: 0.4.0.1862.1.6.2) for OBSEAL CSRs. The ASN.1 notation for the `qcs-QcType` element is shown below:

```
QcType ::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-
qct-eseal | id-etsi-qct-web, ...)
-- QC type identifiers
id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
-- Certificate for electronic signatures as defined in Regulation (EU)
No 910/2014
id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }
-- Certificate for electronic seals as defined in Regulation (EU)
No 910/2014
id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
-- Certificate for website authentication as defined in Regulation (EU)
No 910/2014
```

- 4 The etsi-psd2-qcStatement (oid: 0.4.0.19495.2) element MUST be present in a valid CSR. One or more PSD2 roles MUST be present in a valid etsi-psd2-qcStatement. NCA name and NCA ID MUST be present in a valid etsi-psd2-qcStatement. The ASN.1 notation for the etsi-psd2-qcStatement element is shown below.

```
ETSIPSD2QcprofileMod { itu-t(0) identified-organization(4) etsi(0) id-
qc-statements(19495) idmod(0)
id-mod-psd2qcprofile(0) }

DEFINITIONS EXPLICIT TAGS ::=

BEGIN

-- EXPORTS All --

IMPORTS

QC-STATEMENT
  FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
  internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
  id-mod-qualified-cert-97(35)};

-- statements
etsi-psd2-qcStatement QC-STATEMENT ::= {SYNTAX PSD2QcType
IDENTIFIED BY id-etsi-psd2-qcStatement }
id-etsi-psd2-qcStatement OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495)
qcstatement(2) }

PSD2QcType ::= SEQUENCE{
  rolesOfPSP RolesOfPSP,
  nCAName NCAName,
  nCAId NCAId }

RolesOfPSP ::= SEQUENCE OF RoleOfPSP

RoleOfPSP ::= SEQUENCE{
  roleOfPspOid RoleOfPspOid,
  roleOfPspName RoleOfPspName}

RoleOfPspOid ::= OBJECT IDENTIFIER
-- Object Identifier arc for roles of payment service providers
-- defined in the present document

etsi-psd2-roles OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-
roles(1) }
```

```

-- Account Servicing Payment Service Provider (PSP_AS) role id-
psd2-role-asp-as OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-
roles(1) 1 }
-- Payment Initiation Service Provider (PSP_PI) role id-
psd2-role-asp-pi OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-
roles(1) 2 }
-- Account Information Service Provider (PSP_AI) role id-
psd2-role-asp-ai OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-
roles(1) 3 }
-- Payment Service Provider issuing card-based payment instruments
(PSP_IC) role
id-psd2-role-asp-ic OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-
roles(1) 4 }

-- Payment Service Provider role name corresponding with OID (i.e.
PSP_AS,
-- PSP_PI, PSP_AI, PSP_IC)
RoleOfPspName ::= UTF8String (SIZE(1..256))

NCAName ::= UTF8String (SIZE (1..256)) NCAId

::= UTF8String (SIZE (1..256))

END

```

NOTE: The `qcStatements` extension used in the CSRs for OBWAC and OBSEAL certificates MUST comply with the definition presented above and on page 17 of [REF 1]. The `qcStatements` extension used in the CSRs for OBWAC and OBSEAL certificates MAY contain other elements, but they are NOT mandatory and will not be discussed in this document.

- 5 **[OBWAC CSRs ONLY]** A valid OBWAC CSR MUST contain `extKeyUsage` (oid: 2.5.29.37) extension with `id-kp-serverAuth` (oid: 1.3.6.1.5.5.7.3.1) and `id-kp-clientAuth` (oid: 1.3.6.1.5.5.7.3.2) flags set [RFC5280].

2.2 PSD2 STATEMENT

As specified in [REF 1].

The PSD2 specific attributes shall be included in `etsi-psd2-qcStatement` within the `qcStatements` extension as specified in clause 3.2.6 of IETF RFC 3739 [7].

The QCStatement shall contain the following PSD2 specific certificate attributes as required by RTS [i.3] article 34:

1. The role of the payment service provider, which maybe one or more of the following:
 - account servicing (`PSP_AS`);
 - payment initiation (`PSP_PI`);
 - account information (`PSP_AI`);
 - issuing of card-based payment instruments (`PSP_IC`).
2. The name of the national competent authority where the payment service provider is registered. This is provided in two forms:
 - the full name string (`NCAName`) in English, and
 - an abbreviated unique identifier (`NCAId`).

Generally, to encode the above information into a CSR requires generating a valid ASN.1 representation. This is discussed later in the document.

2.3 ORGANISATIONAL IDENTIFIER STATEMENT

As specified in [REF 1].

The PSD2 Authorisation Number, or other identifier recognised by the NCA, shall be placed in the `organizationIdentifier` attribute of the Subject Distinguished Name field in the certificate.

The `organizationIdentifier` "PSDGB-OB-Unknown0015800001041ReAAI" means a certificate issued to a TPP where the authorisation number is `Unknown0015800001041ReAAI`, authorisation was granted by UK Open Banking (identifier `PSDGB-OB`). Other examples can include use of non-alphanumeric characters such as "PSDBE-NBB-1234.567.890", "PSDFI- FINFSA-1234567-8" and "PSDMT-MFSA-A 12345" (note space character after "A").

After consultations between European Banking Authority (EBA) and ETSI it was found that there are institutions which can request PSD2 certificates but have no authorisation number. If the authorisation number was not issued by the NCA, then another registration identifier recognised by the NCA is used from those defined in the standard ETSI EN/TS 319 412-1.

2.4 CSR GENERATION - OPENSLL

There are many utilities to generate CSR's to submit to a certificate authority. This document uses OpenSSL to demonstrate how a valid CSR is generated to submit to Open Banking to issue an OBWAC or OBSEAL x509 certificate that complies with ETSI certificate template.

OpenSSL does not offer an ASN.1 editor to natively generate PSD2 type statements out of the box although it does offer an ASN.1 parser. OpenSSL is supported on Windows and Unix platforms and the client is free to generate a CSR on the platform of their choice.

NOTE: The client is reminded to protect the private key according to their security policies.

OpenSSL does support embedding a valid DER encoded hexadecimal representation of a PSD2 statement in a CSR. Therefore, another tool is required to actually generate a valid PSD2 statement, which is DER encoded.

This document is not intended to be a tutorial on OpenSSL. However, general usage is based on installing OpenSSL on your target operating system and generating a CSR as follows:

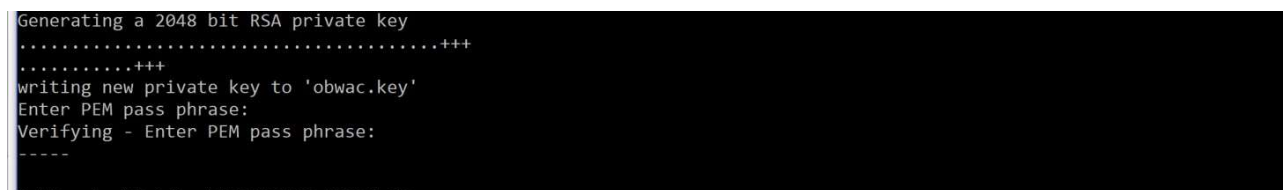
OBWAC CSR Generation

```
$ openssl req -new -config obwac.cnf -out obwac.csr -keyout obwac.key
```

OBSEAL CSR Generation

```
$ openssl req -new -config obseal.cnf -out obseal.csr -keyout obseal.key
```

Example:



```
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'obwac.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
```

The resulting `obwac.key` and/or `obseal.key` files must be protected by your security policies. The

`obwac.csr` and/or `obseal.csr` are submitted to Open Banking PKI for processing. If successful, a signed certificate is returned associated with the appropriate key file generated above.

The contents of the `obwac.cnf` and `obseal.cnf` are dependent on what type of PSD2 service provider the client generating the CSR is, such as a `PSP_AS`.

Example OpenSSL `.cnf` files are supplied for clients in the next chapter.

3 OBWAC X509 CERTIFICATE SIGNING REQUEST PROFILE

3.1 INTRODUCTION

This chapter demonstrates how to generate a valid CSR by a client that requires an OBWAC X.509 certificate issued to them.

3.2 OBWAC OPENSSSL .CNF FILE

The following configuration file is used to generate a CSR for an OBWAC certificate using OpenSSL.

All text highlighted in **red** must be changed by the client to specific data pertinent to them.

NOTE: A client can use the OpenSSL .cnf file below to generate a CSR which is subsequently signed using their own certificate authority. However, such a certificate will not be trusted by Open Banking.

obwac.cnf file for OpenSSL CSR request

```
#
# OPENSSSL CSR REQUEST CONFIGURATION FILE
# =====
#
# OBWAC qualified client certificate request with PSD2 role: PSP_PI PSP_AI
#
# See latest specification: ETSI TS 119 495 V1.2.1 (2018-11)
#
https://www.etsi.org/deliver/etsi\_ts/119400\_119499/119495/01.02.01\_60/ts\_119495v010201p.pdf
#
oid_section = new_oids
[ new_oids ]
organizationIdentifier = 2.5.4.97
# OpenSSL may not recognise this OID so need to add.
[ req ]
default_bits = 2048
# RSA key size
encrypt_key = yes
# Protect private key: yes or no. yes recommended
default_md = sha256
# MD to use. sha256 recommended
utf8 = yes
# Input is UTF-8.
string_mask = utf8only
# Emit UTF-8 strings
prompt = no
# Prompt for DN. yes or no.
distinguished_name = client_dn
# DN template. Mandatory to include organizationIdentifier
req_extensions = client_reqext
# Desired extensions. Mandatory to include PSD2 QCStatements
#
# Subject Distinguished Name format in certificate
#
# EG: CN = 0015800001041ReAAI,
# 2.5.4.97 = PSDGB-OB-Unknown0015800001041ReAAI,
# O = Open Banking Limited (D), C = GB
#
#
[ client_dn ]
countryName = "GB"
```

```

# Country code - see doc above
organizationName = "Open Banking Limited (D)"
# Organizational name
#
# organizationIdentifier
#
# The organizationIdentifier shall be present in the Subject's
# Distinguished Name and encoded with legal person syntax
#
# EXAMPLE: The organizationIdentifier "PSDPL-PFSA-1234567890"
# means a certificate issued to a PSP where the authorization
# number is 1234567890, authorization was granted by the Polish
# Financial Supervision Authority (identifier after second
# hyphen-minus is decided by Polish numbering system). Other
# examples can include use of non-alphanumeric characters such
# as "PSDBE-NBB-1234.567.890" and "PSDFI-FINFSA-1234567-8" and
# "PSDMT-MFSA-A 12345" (note space character after "A")
#
organizationIdentifier = "PSDGB-OB-Unknown0015800001041ReAAI"
# Must be in format as shown above
commonName = "Unknown0015800001041ReAAI"
# Subject common name
#
# Required specific extensions in certificate
#
[ client_reqext ]
keyUsage = critical,digitalSignature
# Must be critical
#
# NOTE: As stated in section 7.1.2.3 item f of the CA/Browser
# Forum Baseline Requirements [i.8] (as referenced in ETSI EN
# 319 412-4 [4]) "id-kp-serverAuth or id-kp-clientAuth
# [RFC5280] or both values MUST be present". If the certificate
# is intended to be used as the client certificate in mutual
# authentication then both values of extKeyUsage certificate
# extension will need to be present. It is not intended that
# certificates issued under this profile are used just as
# client certificates.
#
extendedKeyUsage = clientAuth,serverAuth
# Must be defined as shown above
subjectKeyIdentifier = hash
# Hash value to calculate SKI
#
#
# QC-STATEMENT
#
# FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
# internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-qualified- cert-
97(35)};
# [OID = 1.3.6.1.5.5.7.1.3]
#
# Qualified Electronic Certificate Type Statement: QSIGN, QWAC, QSEAL
#
#
# QcType ::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-qct- esead
| id-etsi-qct-web, ...)
# oid: 0.4.0.1862.1.6
#
# -- QC type identifiers
# id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
# -- Certificate for electronic signatures as defined in Regulation (EU) No
910/2014

```

```

# -- oid: 0.4.0.1862.1.6.1
#
# id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }
# -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014
# -- oid: 0.4.0.1862.1.6.2
#
# id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
# -- Certificate for website authentication as defined in Regulation (EU) No
910/2014
# -- oid: 0.4.0.1862.1.6.3
#
# PSD2 Qualified Statement
#
#
# NOTE: The following ASN.1 notation is based on the ETSIPSD2Qc profile.
#
# ETSIPSD2QcprofileMod { itu-t(0) identified-organization(4) etsi(0)
# id-qc-statements(19495) idmod(0) id-mod-psd2qcprofile(0) }
# DEFINITIONS EXPLICIT TAGS ::=
#
# BEGIN
#
# -- EXPORTS All --
# IMPORTS
# QC-STATEMENT
# FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
# internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
# id-mod-qualified-cert-97(35)};
# -- statements
# etsi-psd2-qcStatement QC-STATEMENT ::= {SYNTAX PSD2QcType IDENTIFIED BY id-
etsi-psd2-qcStatement }
# id-etsi-psd2-qcStatement OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) qcstatement(2) }
# PSD2QcType ::= SEQUENCE{
#     rolesOfPSP RolesOfPSP,
#     nCAnName NCAnName,
#     nCAId NCAId }
#
# NCAnName ::= UTF8String (SIZE (1..256))
# NCAId ::= UTF8String (SIZE (1..256))
#
# RolesOfPSP ::= SEQUENCE OF RoleOfPSP
#
# RoleOfPSP ::= SEQUENCE{
#     roleOfPspOid RoleOfPspOid,
#     roleOfPspName RoleOfPspName}
#
# RoleOfPspOid ::= OBJECT IDENTIFIER
# -- Object Identifier arc for roles of payment service providers
# -- defined in the present document
# etsi-psd2-roles OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) }
#
# -- Account Servicing Payment Service Provider (PSP_AS) role
# id-psd2-role-psp-as OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 }
# -- Payment Initiation Service Provider (PSP_PI) role
# id-psd2-role-psp-pi OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 }
#
# -- Account Information Service Provider (PSP_AI) role
# id-psd2-role-psp-ai OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 }

```

```

# -- Payment Service Provider issuing card-based payment instruments (PSP_IC)
role
# id-psd2-role-psp-ic OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4 }
# -- Payment Service Provider role name corresponding with OID (i.e. PSP_AS,
# -- PSP_PI, PSP_AI, PSP_IC)
# RoleOfPspName ::= UTF8String (SIZE(1..256))
#
# END
#
#
# qcStatements DER strings
# =====
#
# NOTE 1: Uncomment only one qcStatements line, that
# matches the set of PSD2 roles relevant to your
# organisation. See Open Banking documentation for
# more information.
#
# NOTE 2: Each qcStatements line in the section below
# embeds NCAName of "Financial Conduct Authority" and
# NCAId of "GB-FCA". Please modify them to match the
# NCA relevant to your organisation. See Open Banking
# documentation for more information.
#
# PSP_AS
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982
702303a301330110607040081982701010c065053505f41530c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_PI
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982
702303a301330110607040081982701020c065053505f50490c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_AI
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982
702303a301330110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_IC
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982
702303a301330110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_AS,PSP_PI
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701020c06505350
5f50490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AS,PSP_AI
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701030c06505350
5f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AS,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701040c06505350
5f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_PI,PSP_AI
qcStatements=DER:306e3013060604008e4601063009060704008e46010602305706060400819827
02304d302630110607040081982701020c065053505f504930110607040081982701030c065053505
f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_PI,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982
702304d302630110607040081982701020c065053505f504930110607040081982701040c06505350
5f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AI,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982

```

702304d302630110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
PSP_AS,PSP_PI,PSP_AI
#qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
PSP_AS,PSP_PI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
PSP_AS,PSP_AI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
PSP_PI,PSP_AI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
PSP_AS,PSP_PI,PSP_AI,PSP_IC
#qcStatements=DER:3081943013060604008e4601063009060704008e46010602307d06060400819827023073304c30110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

3.3 COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI + PSP_IC

NOTE: Each `qcStatements` line in the section below embeds NCAName of "Financial Conduct Authority" and NCAIdof "GB-FCA". Please modify them to match the NCA relevant to your organisation.

PSP_AS

```
qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081
982702303a301330110607040081982701010c065053505f41530c1b46696e616e6369616c204
36f6e6475637420417574686f726974790c0647422d464341
```

PSP_PI

```
qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081
982702303a301330110607040081982701020c065053505f50490c1b46696e616e6369616c204
36f6e6475637420417574686f726974790c0647422d464341
```

PSP_AI

```
qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081
982702303a301330110607040081982701030c065053505f41490c1b46696e616e6369616c204
36f6e6475637420417574686f726974790c0647422d464341
```

PSP_IC

```
qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081
982702303a301330110607040081982701040c065053505f49430c1b46696e616e6369616c204
36f6e6475637420417574686f726974790c0647422d464341
```

PSP_AS, PSP_PI

```
qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081
982702304d302630110607040081982701010c065053505f415330110607040081982701020c0
65053505f50490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647
422d464341
```

PSP_AS, PSP_AI

```
qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081
982702304d302630110607040081982701010c065053505f415330110607040081982701030c0
65053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647
422d464341
```

PSP_AS, PSP_IC

```
qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081
982702304d302630110607040081982701010c065053505f415330110607040081982701040c0
65053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647
422d464341
```

PSP_PI, PSP_AI

```
qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081
982702304d302630110607040081982701020c065053505f504930110607040081982701030c0
65053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647
422d464341
```

PSP_PI, PSP_IC

qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982702304d302630110607040081982701020c065053505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AI, PSP_IC

qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982702304d302630110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS, PSP_PS, PSP_AI

qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS, PSP_PI, PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS, PSP_AI, PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_PI, PSP_AI, PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819827023060303930110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS, PSP_PI, PSP_AI, PSP_IC

qcStatements=DER:3081943013060604008e4601063009060704008e46010603307d06060400819827023073304c30110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

3.4 EXAMPLE OBWAC CSR CREATION USING OPENSSSL FOR ROLES PSP_AS, PSP_AI AND PSP_IC

1. Comment out the PSP_PI, PSP_AI qcStatements=DER line in obwac.cnf
2. Uncomment the PSP_AS, PSP_AI, PSP_IC qcStatements=DER line in obwac.cnf
3. Make sure the PSP_AS, PSP_AI, PSP_IC qcStatements=DER line in obwac.cnf contains correct NCAName and NCAId values, edit if necessary.
4. Run the following command:

```
openssl req -new -config obwac.cnf -out obwac.csr -keyout obwac.key
```

The obwac.csr will contain the CSR that can be submitted to the Open Banking Directory for signing. It will look like the CSR shown below:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDVjCCAqYCAQAwwYExCzAJBgNVBAYTAkdCMSEwHwYDVQQKDBhPcGVuIEJhbmtp
bmcgTGltZXRLZCAoRCkxKzApBgNVBGMElBTREdCLU9CLVVua25vd24wMDE1ODAw
MDAxMDQxUmVBQUkxIjAgBgNVBAMMGVVua25vd24wMDE1ODAwMDAxMDQxUmVBQUkw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQBBrFVBalOkREQZQpDQDz
Ngj6xk6nWwRQWwcb6m5Yv7n0aidoOC23SsGR8M7MLoYFHRi9RNOmrvfoyevkZa2q
m8zcQeuPHcLHO/z7iTU7NdMiK/AcVUMmOC9Q2ws8VXj38A0Guf8G5FFFSAVSzentC
VqxswwWF6nNHBUbTP7J3NscnR1sw6Tn7/nXwgRzimFiF0MgPp1stZuPqi70DY0WdT
shIH0JvPJQ8ABG/8UE+3whgW85h26aEg2IY0yYDUGk5a3KQXddHyF4Ji/zSK2FAf
NxjsQ4P+BxWY2bkND/1D5KIhqFh6xqf34EgTByOm2R7vSIWZDZHoLZv74VNPdSH
AgMBAAGggfYwgfMGCSqGSIb3DQEJdJGB5TCB4jAObgNVHQ8BAf8EBAMCB4AwHQYD
VR01BBYwFAYIKwYBBQUHAWIGCCsGAQUFBwMBMB0GA1UdDgQWBBC5Ra7Bvfk3ML
TosGc+cRYyFhsTCBkQYIKwYBBQUHAQMEgYQwgYEwEwYGBACORgEGMAkGBwQAjkYB
BgMwagYGBACBmCcCMGAwOTARBgCEAIGYJwEBDAZQU1BfQVMwEQYHBACBmCcBAwwG
UFNQX0FJMBEGBwQAgZgnAQQMB1BTUF9JQwwbRmluYW5jaWFsIENvbmR1Y3QgQXV0
aG9yaXR5DAZHQi1GQ0EwDQYJKoZIhvcNAQELBQADggEBAIfs7JywpN0eLVPo03J2
Qh2xsMX9J9f5qghzzEtFSW+Zuk/1nyBT4QbRcKUC/IkAkVB6tYJ94arHXuevO6Ya
R0rgsucRNVYP/dgiLEqtGIuSeqKSBxOjhtkP58tKcA8ZCCuYN1YbzmPxL71Z1fZW
zV8q80g1ZHRhYhdIY2ANPT3rDhBTtzK0f8KMtnoOzeuKkkcpMYN3ifvVrieMrUum
o2hzxV5rIq5qZuNls2Li2tZDX3KQ0E0ZU3Si6Q3QQ89paR85DMIN2OqW4mZ8ify3
ON2rnUquarjkdOpxMUeyul1g3mbLFDXaAfhZbqo9fwqiXWlidNA2WU8GdQ2MOesx
zGY=
-----END CERTIFICATE REQUEST-----
```

The CSR structure (but not the internal structure of extensions) can be examined using openssl:

```
$ openssl asn1parse -in obvac.csr -inform PEM
```

```
  0:d=0  hl=4  l= 958   cons: SEQUENCE
  4:d=1  hl=4  l= 678   cons: SEQUENCE
  8:d=2  hl=2  l=   1   prim: INTEGER           :00
 11:d=2  hl=3  l= 129   cons: SEQUENCE
 14:d=3  hl=2  l=  11   cons: SET
 16:d=4  hl=2  l=   9   cons: SEQUENCE
 18:d=5  hl=2  l=   3   prim: OBJECT             :countryName
 23:d=5  hl=2  l=   2   prim: PRINTABLESTRING   :GB
 27:d=3  hl=2  l=  33   cons: SET
 29:d=4  hl=2  l=  31   cons: SEQUENCE
 31:d=5  hl=2  l=   3   prim: OBJECT             :organizationName
 36:d=5  hl=2  l=  24   prim: UTF8STRING        :Open Banking Limited (D)
 62:d=3  hl=2  l=  43   cons: SET
 64:d=4  hl=2  l=  41   cons: SEQUENCE
 66:d=5  hl=2  l=   3   prim: OBJECT             :2.5.4.97
 71:d=5  hl=2  l=  34   prim: UTF8STRING        :PSDGB-OB-Unknown001580001041ReAAI
107:d=3  hl=2  l=  34   cons: SET
109:d=4  hl=2  l=  32   cons: SEQUENCE
111:d=5  hl=2  l=   3   prim: OBJECT             :commonName
116:d=5  hl=2  l=  25   prim: UTF8STRING        :Unknown001580001041ReAAI
143:d=2  hl=4  l= 290   cons: SEQUENCE
147:d=3  hl=2  l=  13   cons: SEQUENCE
149:d=4  hl=2  l=   9   prim: OBJECT             :rsaEncryption
160:d=4  hl=2  l=   0   prim: NULL
162:d=3  hl=4  l= 271   prim: BIT STRING
437:d=2  hl=3  l= 246   cons: cont [ 0 ]
440:d=3  hl=3  l= 243   cons: SEQUENCE
443:d=4  hl=2  l=   9   prim: OBJECT             :Extension Request
```

```

454:d=4 hl=3 l= 229 cons: SET
457:d=5 hl=3 l= 226 cons: SEQUENCE
460:d=6 hl=2 l= 14 cons: SEQUENCE
462:d=7 hl=2 l= 3 prim: OBJECT :X509v3 Key Usage
467:d=7 hl=2 l= 1 prim: BOOLEAN :255
470:d=7 hl=2 l= 4 prim: OCTET [HEX DUMP]:03020780
STRING
476:d=6 hl=2 l= 29 cons: SEQUENCE
478:d=7 hl=2 l= 3 prim: OBJECT :X509v3 Extended Key Usage
483:d=7 hl=2 l= 22 prim: OCTET [HEX
STRING DUMP]:301406082B0601050507030206082
B0601050507030

507:d=6 hl=2 l= 29 cons: SEQUENCE

509:d=7 hl=2 l= 3 prim: OBJECT :X509v3 Subject Key Identifier
514:d=7 hl=2 l= 22 prim: OCTET [HEX
STRING DUMP]:04141CE516BB06F7E493730B4E8B0
673E711632161B1

538:d=6 hl=3 l= 145 cons: SEQUENCE
541:d=7 hl=2 l= 8 prim: OBJECT :qcStatements
551:d=7 hl=3 l= 132 prim: OCTET [HEX
STRING DUMP]:3081813013060604008E46010630
09060704008E46010603306A0606040081
982702306
0303930110607040081982701010C06505
3505F415330110607040081982701030C0
65053505F4149301106070400819827010
40C065053505F49430C1B46696E616E636
9616C20436F6E6475637420417574686F7
26974790C0647422D464341

686:d=1 hl=2 l= 13 cons: SEQUENCE :sha256WithRSAEncryption
688:d=2 hl=2 l= 9 prim: OBJECT
9:d=2 hl=2 l= 0 prim: NULL
701:d=1 hl=4 l= 257 prim: BIT STRING

```

The CSR may be uploaded to Open Banking PKI to issue an OBWAC public certificate associated with your private key.

4 OBSEAL X509 CERTIFICATE SIGNING REQUEST PROFILE

4.1 INTRODUCTION

This chapter demonstrates how to generate a valid CSR by a client that requires an OBSEAL x509 certificate issued to them.

4.2 OBSEAL OPENSLL CNF FILE

The following configuration file is used to generate a CSR for an OBSEAL certificate using OpenSSL.

All text highlighted in **red** must be changed by the client to specific data pertinent to them.

NOTE: A client can use the OpenSSL .cnf file below to generate a CSR which is subsequently signed using their own certificate authority. However, such a certificate will not be trusted by Open Banking.

```
#
# OPENSLL CSR REQUEST CONFIGURATION FILE
# =====
#
# OBSEAL qualified client certificate request with PSD2 role: PSP_PI PSP_AI
#
# See latest specification: ETSI TS 119 495 V1.2.1 (2018-11)
#
https://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.02.01_60/ts_119495v0
10201p.pdf
#
oid_section = new_oids
[ new_oids ]
organizationIdentifier = 2.5.4.97
# OpenSSL may not recognize this OID so need to add.
[ req ]
default_bits = 2048
# RSA key size
encrypt_key = yes
# Protect private key: yes or no. yes recommended
default_md = sha256
# MD to use. sha256 recommended
utf8 = yes
# Input is UTF-8.
string_mask = utf8only
# Emit UTF-8 strings
prompt = no
# Prompt for DN. yes or no.
distinguished_name = client_dn
# DN template. Mandatory to include organizationIdentifier
req_extensions = client_reqext
# Desired extensions. Mandatory to include PSD2 QCStatements
#
# Subject Distinguished Name format in certificate
#
# EG: CN = 0015800001041ReAAI,
# 2.5.4.97 = PSDGB-OB-Unknown0015800001041ReAAI,
# O = Open Banking Limited (D), C = GB
#
#
[ client_dn ]
countryName = "GB"
# Country code - see doc above
organizationName = "Open Banking Limited (D)"
# Organizational name
```

```

#
# organizationIdentifier
#
# The organizationIdentifier shall be present in the Subject's
# Distinguished Name and encoded with legal person syntax
#
# EXAMPLE: The organizationIdentifier "PSDPL-PFSA-1234567890"
# means a certificate issued to a PSP where the authorization
# number is 1234567890, authorization was granted by the Polish
# Financial Supervision Authority (identifier after second
# hyphen-minus is decided by Polish numbering system). Other
# examples can include use of non-alphanumeric characters such
# as "PSDBE-NBB-1234.567.890" and "PSDFI-FINFSA-1234567-8" and
# "PSDMT-MFSA-A 12345" (note space character after "A")
#
organizationIdentifier = "PSDGB-OB-Unknown0015800001041ReAAI"
# Must be in format as shown above
commonName = "Unknown0015800001041ReAAI"
# Subject common name
#
# Required specific extensions in certificate
#
[ client_reqext ]
keyUsage = critical,digitalSignature,nonRepudiation
# Must be critical
#
subjectKeyIdentifier = hash
# Hash value to calculate SKI
#
#
# QC-STATEMENT
#
# FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
# internet(1) security(5) mechanisms(5) pkix(7) id-mod(0) id-mod-qualified-cert-
97(35)};
# [OID = 1.3.6.1.5.5.7.1.3]
#
# Qualified Electronic Certificate Type Statement: QSIGN, QWAC, QSEAL
#
#
# QcType ::= SEQUENCE OF OBJECT IDENTIFIER (id-etsi-qct-esign | id-etsi-qct-eseal
| id-etsi-qct-web, ...)
# oid: 0.4.0.1862.1.6
#
# -- QC type identifiers
# id-etsi-qct-esign OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 1 }
# -- Certificate for electronic signatures as defined in Regulation (EU) No
910/2014
# -- oid: 0.4.0.1862.1.6.1
#
# id-etsi-qct-eseal OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 2 }
# -- Certificate for electronic seals as defined in Regulation (EU) No 910/2014
# -- oid: 0.4.0.1862.1.6.2
#
# id-etsi-qct-web OBJECT IDENTIFIER ::= { id-etsi-qcs-QcType 3 }
# -- Certificate for website authentication as defined in Regulation (EU) No
910/2014
# -- oid: 0.4.0.1862.1.6.3
#
# PSD2 Qualified Statement
#
#
# NOTE: The following ASN.1 notation is based on the ETSIPSD2Qc profile.

```

```

#
# ETSIPSD2QcprofileMod { itu-t(0) identified-organization(4) etsi(0)
# id-qc-statements(19495) idmod(0) id-mod-psd2qcprofile(0) }
# DEFINITIONS EXPLICIT TAGS ::=
#
# BEGIN
#
# -- EXPORTS All --
# IMPORTS
# QC-STATEMENT
#   FROM PKIXqualified97 {iso(1) identified-organization(3) dod(6)
#   internet(1) security(5) mechanisms(5) pkix(7) id-mod(0)
#   id-mod-qualified-cert-97(35)};
# -- statements
# etsi-psd2-qcStatement QC-STATEMENT ::= {SYNTAX PSD2QcType IDENTIFIED BY id-
etsi-psd2-qcStatement }
# id-etsi-psd2-qcStatement OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) qcstatement(2) }
# PSD2QcType ::= SEQUENCE{
#   rolesOfPSP RolesOfPSP,
#   nCAName NCAName,
#   nCAId NCAId }
#
# NCAName ::= UTF8String (SIZE (1..256))
# NCAId ::= UTF8String (SIZE (1..256))
#
# RolesOfPSP ::= SEQUENCE OF RoleOfPSP
#
# RoleOfPSP ::= SEQUENCE{
#   roleOfPspOid RoleOfPspOid,
#   roleOfPspName RoleOfPspName}
#
# RoleOfPspOid ::= OBJECT IDENTIFIER
# -- Object Identifier arc for roles of payment service providers
# -- defined in the present document
# etsi-psd2-roles OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) }
#
# -- Account Servicing Payment Service Provider (PSP_AS) role
# id-psd2-role-psp-as OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 }
# -- Payment Initiation Service Provider (PSP_PI) role
# id-psd2-role-psp-pi OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 }
#
# -- Account Information Service Provider (PSP_AI) role
# id-psd2-role-psp-ai OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 }
# -- Payment Service Provider issuing card-based payment instruments (PSP_IC)
role
# id-psd2-role-psp-ic OBJECT IDENTIFIER ::=
# { itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4 }
# -- Payment Service Provider role name corresponding with OID (i.e. PSP_AS,
# -- PSP_PI, PSP_AI, PSP_IC)
# RoleOfPspName ::= UTF8String (SIZE(1..256))
#
# END
#
#
# qcStatements DER strings
# =====
#
# NOTE 1: Uncomment only one qcStatements line, that

```

```
# matches the set of PSD2 roles relevant to your
# organisation. See Open Banking documentation for
# more information.
#
# NOTE 2: Each qcStatements line in the section below
# embeds NCAName of "Financial Conduct Authority" and
# NCAid of "GB-FCA". Please modify them to match the
# NCA relevant to your organisation. See Open Banking
# documentation for more information.
#
# PSP_AS
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081982
702303a301330110607040081982701010c065053505f41530c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_PI
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081982
702303a301330110607040081982701020c065053505f50490c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_AI
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081982
702303a301330110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_IC
#qcStatements=DER:305b3013060604008e4601063009060704008e4601060330440606040081982
702303a301330110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e64
75637420417574686f726974790c0647422d464341
# PSP_AS,PSP_PI
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701020c06505350
5f50490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AS,PSP_AI
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701030c06505350
5f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AS,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982
702304d302630110607040081982701010c065053505f415330110607040081982701040c06505350
5f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_PI,PSP_AI
#qcStatements=DER:306e3013060604008e4601063009060704008e46010603305706060400819827
02304d302630110607040081982701020c065053505f504930110607040081982701030c065053505
f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_PI,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982
702304d302630110607040081982701020c065053505f504930110607040081982701040c06505350
5f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AI,PSP_IC
#qcStatements=DER:306e3013060604008e4601063009060704008e4601060330570606040081982
702304d302630110607040081982701030c065053505f414930110607040081982701040c06505350
5f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341
# PSP_AS,PSP_PI,PSP_AI
#qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819
827023060303930110607040081982701010c065053505f415330110607040081982701020c065053
505f504930110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e64756
37420417574686f726974790c0647422d464341
# PSP_AS,PSP_PI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819
827023060303930110607040081982701010c065053505f415330110607040081982701020c065053
505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e64756
37420417574686f726974790c0647422d464341
# PSP_AS,PSP_AI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819
827023060303930110607040081982701010c065053505f415330110607040081982701030c065053
```

505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e64756
37420417574686f726974790c0647422d464341
PSP_PI,PSP_AI,PSP_IC
#qcStatements=DER:3081813013060604008e4601063009060704008e46010603306a06060400819
827023060303930110607040081982701020c065053505f504930110607040081982701030c065053
505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e64756
37420417574686f726974790c0647422d464341
PSP_AS,PSP_PI,PSP_AI,PSP_IC
#qcStatements=DER:3081943013060604008e4601063009060704008e46010603307d06060400819
827023073304c30110607040081982701010c065053505f415330110607040081982701020c065053
505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f4
9430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

4.3 COMBINATIONS OF ALL 4 PSP_XX ROLES: PSP_AS + PSP_PI + PSP_AI + PSP_IC

PSP_AS

qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982702303a301330110607040081982701010c065053505f41530c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_PI

qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982702303a301330110607040081982701020c065053505f50490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AI

qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982702303a301330110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_IC

qcStatements=DER:305b3013060604008e4601063009060704008e4601060230440606040081982702303a301330110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS, PSP_PI

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701010c065053505f415330110607040081982701020c065053505f50490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_AI

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701010c065053505f415330110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_IC

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701010c065053505f415330110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_PI,PSP_AI

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701020c065053505f504930110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_PI,PSP_IC

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701020c065053505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AI,PSP_IC

qcStatements=DER:306e3013060604008e4601063009060704008e4601060230570606040081982702304d302630110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_PI,PSP_AI

qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f41490c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_PI,PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_AI,PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701010c065053505f415330110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_PI,PSP_AI,PSP_IC

qcStatements=DER:3081813013060604008e4601063009060704008e46010602306a06060400819827023060303930110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

PSP_AS,PSP_PI,PSP_AI,PSP_IC

qcStatements=DER:3081943013060604008e4601063009060704008e46010602307d06060400819827023073304c30110607040081982701010c065053505f415330110607040081982701020c065053505f504930110607040081982701030c065053505f414930110607040081982701040c065053505f49430c1b46696e616e6369616c20436f6e6475637420417574686f726974790c0647422d464341

4.4 EXAMPLE OBSEAL CSR CREATION USING OPENSRL FOR ROLES PSP_AS, PSP_IC

1. Comment out the PSP_PI, PSP_AI qcStatements=DER line in obseal.cnf
2. Uncomment the PSP_AS, PSP_AI, PSP_IC qcStatements=DER line in obseal.cnf
3. Make sure the PSP_AS, PSP_AI, PSP_IC qcStatements=DER line in obseal.cnf contains correct NCAName and NCAId values, edit if necessary.
4. Run the following command:

```
openssl req -new -config obseal.cnf -out obseal.csr -keyout obseal.key
```

5. The obseal.csr will contain the CSR that can be submitted to the Open Banking Directory for signing. It will look like the CSR shown below:

```
-----BEGIN CERTIFICATE REQUEST-----
MIIDI TCCAnECAQAwgYExCzAJBgNVBAYTAkdCMSEwHwYDVQQKDBhPcGVuIEJhbmtp
bmcgTGltaxRlZCAoRCKxKzApBgNVBGMElBTREdCLU9CLVVua25vd24wMDE1ODAw
MDAxMDQxUmVBQUkxIjAgBgNVBAMMGVVua25vd24wMDE1ODAwMDAxMDQxUmVBQUkw
ggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDeLPwiCRmC2IywVvOtkUz6
iZwj13wY75B+7GoauzLC61o+KaB6uaun9i1BU2szOT8DW+0ew1vOYt/gebFN5q1J
NLgyg7xyl4bYq60lCoAFbHxaG2OrL+3z2RFN6BCBkWWvhu/NfVqkzPGNVpt8dpys
BqJ0g08XMO6e6i29YMD6TcfCczQc8tL/RsHjmwS1I3A1Ni1F8IGU+8CB2+mpxfvv
Psu5tA6hlWtPuvGfjdacfHb3ANaBPxZx5PgBmWocRVLlCRZ8e8JoFoEQ6SkYAJJ/
nW4iEJwHhhU16X5Y+71navrNzghJgw9dnJtBJk3YttyJkwc5zGhcc+3WRHwzLw
AgMBAAGggcEwgb4GCSqGSIb3DQEJDjGBsDCBrTAOBgNVHQ8BAf8EBAMCBsAwHQYD
VR0OBBYEFNIMhxNVxLeS07Zz/iFEyS6Lmz5uMHwGCCsGAQUFBwEDBHAwbjATBgYE
AI5GAQYwCQYHBACORgEGAjBxBgYEAIGYJwIwTTAmMBEGBwQAgZgnAQEMBlBTUF9B
UzARBgcEAIGYJwEEDAZQU1BfSUMMG0ZpbmFuY21hbCBDb25kdWN0IEF1dGhvcml0
eQwGR0ItRkNBMA0GCSqGSIb3DQEBCwUAA4IBAQA/20Gwj7SbICcytxYuYwngb9JC
b8AoAqJOf4+rNzrs/zW5QRh79t9TXFYmQypIvqSrymk3of4Aw2oFEAe6+Z31po6S
OXEOVT6GkYQo98Y6/N5zapdqNxK51HjMRBJUS34DzFPj3bYCjs3oEa6WRk3ATvr8
Iq3QQ6p/DWPEx12pR4N0Bgoce7+QD5qEX6jEPrTB1J1SSWMCIDCn8D05IM8IcNGA
sZlunQFCxlrAK7+/wmXknbnBbslfINvLMUet+CZgiYSWhK1WpsKM1uJexefegiUd
aXMOWvvnwKjQO6EIJb+QF8LWpwc/FqbMc/X5r/vkIbOsc6ytH3qaRu6Cszcus
-----END CERTIFICATE REQUEST-----
```

The CSR structure (but not the internal structure of extensions) can be examined using openssl:

```
$ openssl asn1parse -in obseal.csr -inform PEM
```

```

    0:d=0  hl=4  l= 905   cons: SEQUENCE
    4:d=1  hl=4  l= 625   cons: SEQUENCE
    8:d=2  hl=2  l=   1   prim: INTEGER           :00
   11:d=2  hl=3  l= 129   cons: SEQUENCE
   14:d=3  hl=2  l=  11   cons: SET
   16:d=4  hl=2  l=   9   cons: SEQUENCE
   18:d=5  hl=2  l=   3   prim: OBJECT           :countryName
   23:d=5  hl=2  l=   2   prim: PRINTABLESTRIN
                        NG           :GB
   27:d=3  hl=2  l=  33   cons: SET
   29:d=4  hl=2  l=  31   cons: SEQUENCE
   31:d=5  hl=2  l=   3   prim: OBJECT           :organizationName
   36:d=5  hl=2  l=  24   prim: UTF8STRING       :Open Banking Limited (D)
   62:d=3  hl=2  l=  43   cons: SET
   64:d=4  hl=2  l=  41   cons: SEQUENCE
   66:d=5  hl=2  l=   3   prim: OBJECT           :2.5.4.97
   71:d=5  hl=2  l=  34   prim: UTF8STRING       :PSDGB-OB-Unknown0015800001041ReAAI
  107:d=3  hl=2  l=  34   cons: SET

  109:d=4  hl=2  l=  32   cons: SEQUENCE
  111:d=5  hl=2  l=   3   prim: OBJECT           :commonName
  116:d=5  hl=2  l=  25   prim: UTF8STRING       :Unknown0015800001041ReAAI
  143:d=2  hl=4  l= 290   cons: SEQUENCE
  147:d=3  hl=2  l=  13   cons: SEQUENCE
  149:d=4  hl=2  l=   9   prim: OBJECT           :rsaEncryption
  160:d=4  hl=2  l=   0   prim: NULL
  162:d=3  hl=4  l= 271   prim: BIT STRING
  437:d=2  hl=3  l= 193   cons: cont [ 0 ]
  440:d=3  hl=3  l= 190   cons: SEQUENCE
  443:d=4  hl=2  l=   9   prim: OBJECT           :Extension Request
  454:d=4  hl=3  l= 176   cons: SET
  457:d=5  hl=3  l= 173   cons: SEQUENCE
  460:d=6  hl=2  l=  14   cons: SEQUENCE
  462:d=7  hl=2  l=   3   prim: OBJECT           :X509v3 Key Usage
  467:d=7  hl=2  l=   1   prim: BOOLEAN           :255
  470:d=7  hl=2  l=   4   prim: OCTET STRING       [HEX DUMP]:030206C0
  476:d=6  hl=2  l=  29   cons: SEQUENCE
  478:d=7  hl=2  l=   3   prim: OBJECT           :X509v3 Subject Key Identifier
  483:d=7  hl=2  l=  22   prim: OCTET STRING       [HEX
                        DUMP]:0414D20C1F1355C4B792D3B673FE2144C
                        92E8B9B3E6E

  507:d=6  hl=2  l= 124   cons: SEQUENCE
  509:d=7  hl=2  l=   8   prim: OBJECT           :qcStatements
  519:d=7  hl=2  l= 112   prim: OCTET STRING       [HEX
                        DUMP]:306E3013060604008E46010630090607
                        04008E4601060230570606040081982702304D
                        302630110607040081982701010C065053505F
                        415330110607040081982701040C065053505F
                        49430C1B46696E616E6369616C20436F6E6475
                        637420417574686F726974790C0647422D4643
                        41

  633:d=1  hl=2  l=  13   cons: SEQUENCE
  635:d=2  hl=2  l=   9   prim: OBJECT           :sha256WithRSAEncryption
  646:d=2  hl=2  l=   0   prim: NULL
  648:d=1  hl=4  l= 257   prim: BIT STRING

```

The CSR may be uploaded to Open Banking PKI to issue an OBSEAL public certificate associated with your private key.