ETSI TS 119 495 V1.4.1 (2019-11)

Electronic Signatures and Infrastructures (ESI);
Sector Specific Requirements;
Qualified Certificate Profiles and TSP Policy Requirements
under the payment services Directive (EU) 2015/2366

Reference
RTS/ESI-0019495v141

Keywords
e-commerce, electronic signature, extended validation certificat, payment, public key, security, trust services

ETSI

650 Route des Lucioles
F-06921 Sophia Antipolis Cedex - FRANCE

Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in ETSI SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in ETSI SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Trademarks

The present document may include trademarks and/or tradenames which are asserted and/or registered by their owners. ETSI claims no ownership of these except for any which are indicated as being the property of ETSI, and conveys no right to use or reproduce any trademark and/or tradename. Mention of those trademarks in the present document does not constitute an endorsement by ETSI of products, services or organizations associated with those trademarks.

Foreword

This Technical Specification (TS) has been produced by ETSI Technical Committee Electronic Signatures and Infrastructures (ESI).

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"**must**" and "**must not**" are **NOT** allowed in ETSI deliverables except when used in direct citation.

Introduction

Regulation (EU) No 910/2014 [i.1] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (commonly called eIDAS) defines requirements on specific types of certificates named "qualified certificates".

Directive (EU) 2015/2366 [i.2] of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC (commonly called PSD2) defines requirements on communication among payment service providers and account servicing institutions.

The Commission Delegated Regulation (EU) 2018/389 [i.3] with regard to Regulatory Technical Standards for strong customer authentication and common and secure open standards of communication (RTS henceforth) is key to achieving the objective of the PSD2 (Directive (EU) 2015/2366 [i.2]) of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union. The RTS defines requirements on the use of qualified certificates (as defined in eIDAS) for website authentication and qualified certificates for electronic seal for communication among payment and bank account information institutions. Guidance on the use of eIDAS qualified certificates is included in the Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC [i.12].

The present document defines a standard for implementing the requirements of the RTS [i.3] for use of qualified certificates as defined in eIDAS (Regulation (EU) No 910/2014 [i.1]) to meet the regulatory requirements of PSD2 (Directive (EU) 2015/2366 [i.2]).

1 Scope

The present document:

1) Specifies profiles of qualified certificates for electronic seals and website authentication, to be used by payment service providers in order to meet the requirements of the PSD2 Regulatory Technical Standards (RTS) [i.3]. Certificates for electronic seals can be used for providing evidence with legal assumption of authenticity (including identification and authentication of the source) and integrity of a transaction. Certificates for website authentication can be used for identification and authentication of the communicating parties and securing communications. Communicating parties can be payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments or account servicing payment service providers. These profiles are based on ETSI EN 319 412-1 [1], ETSI TS 119 412-1 [2], ETSI EN 319 412-3 [3], ETSI EN 319 412-4 [4], IETF RFC 3739 [7] and ETSI EN 319 412-5 [i.6] (by indirect reference).

2) Specifies additional TSP policy requirements for the management (including verification and revocation) of additional certificate attributes as required by the above profiles. These policy requirements extend the requirements in ETSI EN 319 411-2 [5].

Whilst the present document identifies information that can be provided by NCAs and/or the EBA, such as by publishing through their national or European registers, as well as services provided by QTSP that can be used by NCAs, for example to request revocation, the present document places no requirements on the operation of NCAs nor on the EBA.

2 References

2.1 Normative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

Referenced documents which are not found to be publicly available in the expected location might be found at https://docbox.etsi.org/Reference/.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are necessary for the application of the present document.

[1] ETSI EN 319 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

[2] ETSI TS 119 412-1: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures".

NOTE: ETSI EN 319 412-1 [1] is extended in ETSI TS 119 412-1 [2] to include additional legal person identity type references which can be used in certificates based on the present document.

[3] ETSI EN 319 412-3: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons".

[4] ETSI EN 319 412-4: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 4: Certificate profile for web site certificates".

[5] ETSI EN 319 411-2: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates".

[6] Recommendation ITU-T X.680-X.693: "Information Technology - Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules".

[7] IETF RFC 3739: "Internet X.509 Public Key Infrastructure: Qualified Certificates Profile".

[8] ISO 3166-1: "Codes for the representation of names of countries and their subdivisions; Part 1: Country codes".

2.2 Informative references

References are either specific (identified by date of publication and/or edition number or version number) or non-specific. For specific references, only the cited version applies. For non-specific references, the latest version of the referenced document (including any amendments) applies.

NOTE: While any hyperlinks included in this clause were valid at the time of publication, ETSI cannot guarantee their long term validity.

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

[i.1] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

[i.2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.3] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance).

[i.4] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

[i.5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.6] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.8] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

[i.9] EBA/RTS/2017/10: "Final Report on Draft Regulatory Technical Standards setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2)".

[i.10] IETF RFC 8446: "The Transport Layer Security (TLS) Protocol Version 1.3".

[i.11] CA/Browser Forum: "Guidelines for The Issuance and Management of Extended Validation Certificates" v1.5.5.

[i.12] EBA-Op-2018-7: "Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC".

NOTE: Available at https://eba.europa.eu/file/58802/.

[i.13] EBA: "Type of identification numbers used in the EBA PSD2 Register and the EBA Credit Institutions Register".

NOTE: Available at https://eba.europa.eu/file/113309/.

[i.14] EBA: "List of email addresses of the national competent authorities that will follow the process for requesting revocation of eIDAS certificates as set out in the EBA Opinion on the use of eIDAS certificates (EBA-OP-2018-7)".

NOTE: Available at https://eba.europa.eu/file/113289/.

[i.15] EBA: "National identification codes to be used by qualified trust service providers for identification of competent authorities in an eIDAS certificate for PSD2 purposes".

NOTE: Available at https://eba.europa.eu/file/113255/.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in PSD2 [i.2], ETSI EN 319 412-1 [1], ETSI EN 319 411-2 [5] and the following apply:

EBA PSD2 Register: register of payment institutions and e-money institutions developed, operated and maintained by the EBA under Article 15 of Directive (EU) 2015/2366 [i.2]

NOTE 1: Register is available at https://euclid.eba.europa.eu/register/pir/search.

NOTE 2: This is separate from the register of credit institutions developed, operated and maintained by the EBA under Directive 2013/36/EU [i.4].

3.2 Symbols

Void.

3.3 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-1 [1], ETSI EN 319 411-2 [5] and the following apply:

CRL	Certificate Revocation List
EBA	European Banking Authority
NCA	National Competent Authority
OCSP	Online Certificate Status Protocol
PSD2	Payment Services Directive 2

NOTE: See Directive (EU) 2015/2366 [i.2].

PSP	Payment Service Provider
PSP_AI	Account Information Service Provider
PSP_AS	Account Servicing Payment Service Provider
PSP_IC	Payment Service Provider Issuing Card-based payment instruments
PSP_PI	Payment Initiation Service Provider
QSealC	Qualified electronic Seal Certificate
QWAC	Qualified Website Authentication Certificate
RTS	Regulatory Technical Standard for PSD2 strong customer authentication and common and secure open standards of communication

NOTE: See Commission Delegated Regulation (EU) 2018/389 [i.3].

4 General concepts

4.1 Use of Qualified Certificates

RTS [i.3] Article 34.1 requires that, for the purpose of identification, payment service providers rely on qualified certificates for electronic seals or qualified certificates for website authentication.

A website authentication certificate makes it possible to establish a Transport Layer Security (TLS, e.g. as specified in IETF RFC 5246 [i.5], IETF RFC 8446 [i.10] or later versions) channel with the subject of the certificate, which secures data transferred through the channel.

A certificate for electronic seals allows the relying party to validate the identity of the subject of the certificate, as well as the authenticity and integrity of the sealed data, and also prove it to third parties. The electronic seal provides strong evidence, capable of having legal effect, that given data is originated by the legal entity identified in the certificate.

NOTE: Regulation (EU) No 910/2014 [i.1] requires that TSPs issuing qualified certificates demonstrate that they meet the requirements for qualified trust service providers as per the regulation. ETSI standards referenced in the present document include those aimed at meeting these requirements. Granting a "qualified" status to a TSP is the decision of the national supervisory body.

4.2 Roles

According to RTS [i.3] the role of the payment service provider can be one or more of the following:

i) account servicing (PSP_AS);

ii) payment initiation (PSP_PI);

iii) account information (PSP_AI);

iv) issuing of card-based payment instruments (PSP_IC).

NOTE 1: A role "issuing of card-based payment instruments" (PSP_IC) is indicated in some public registers as "issuing of payment instruments".

NOTE 2: A PSP can be authorized by its national competent authority (NCA) to act in one or more PSD2 roles.

NOTE 3: A credit institution with a full license can act in its capacity as a third party provider, as specified in PSD2 [i.2], and be assigned all three roles under Article 34.3(a)(ii-iv) of the RTS [i.3], namely payment initiation (PSP_PI), account information (PSP_AI), issuing of card-based payment instruments (PSP_IC).

A credit institution can also act in an account servicing capacity and be assigned the account servicing (PSP_AS) role.

4.3 Payment Service Provider Authorizations and Services Passporting

According to PSD2 [i.2] and Capital Requirements Directive [i.4], the competent authority (NCA) responsible for payment services approves or rejects authorization of PSPs in their own country. If authorization is granted, the NCA lists the respective PSP in the national public register, together with an identification number, which could be, but is not necessarily, an authorization number. Subject to NCA approval PSPs can exercise the right of establishment and freedom to provide services in other Member States. This is called passporting. Information about passporting is published in the public register in the home country of the PSP or the EBA PSD2 Register.

Certificates issued according to the requirements laid down in the present document do not include any attributes regarding passporting.

4.4 PSD2 Authorization Number

For identification, the RTS [i.3] Article 34 requires the registration number used in a qualified certificate, as stated in the official records in accordance with Annex III item I of Regulation (EU) No 910/2014 [i.1], to be the authorization number of the payment service provider. This authorization number is required to be available in the National Competent Authority public register pursuant to Article 14 of PSD2 [i.2].

In case there is no PSD2 Authorization Number, other forms of registration number recognized by the NCA can be used in place of the PSD2 Authorization Number.

4.5 Registration and Certificate Issuance

Figure 1 presents the general concept of registration and certificate issuance. The qualified certificate compliant with the profile requirements given in the present document is issued only to payment service providers authorized by the NCA, confirmation of authorization is publicly available in that NCA public register. The list of credit institutions is publicly available in NCA credit institution registers. According to Article 20 of Directive 2013/36/EU [i.4] a list of the names of all credit institutions that have been granted authorization is published on the EBA Credit Institution Register.

According to Article 15 of PSD2 [i.2] the European Banking Authority (EBA) operates and maintains an electronic central register (EBA PSD2 Register) that contains the information as notified by the NCAs. This information will be updated regularly in a timely manner as envisaged under Article 15(2) of PSD2 [i.2] and Articles 7(5) and 8(5) and (8) of the Draft Regulatory Standards on the EBA Register under PSD2 [i.9]. According to the [i.9] the EBA PSD2 Register will contain relevant records of each NCA's register. The EBA PSD2 Register can be used instead of the NCA public register as a source of authorization information for payment institutions and electronic money institutions.

NOTE: The EBA Credit Institution Register and the EBA PSD2 Register are two separate registers.

The NCA can request to be informed about every certificate issued to payment service providers authorized by this NCA. The NCA requests this by an entry on the List of email addresses of the national competent authorities [i.14].

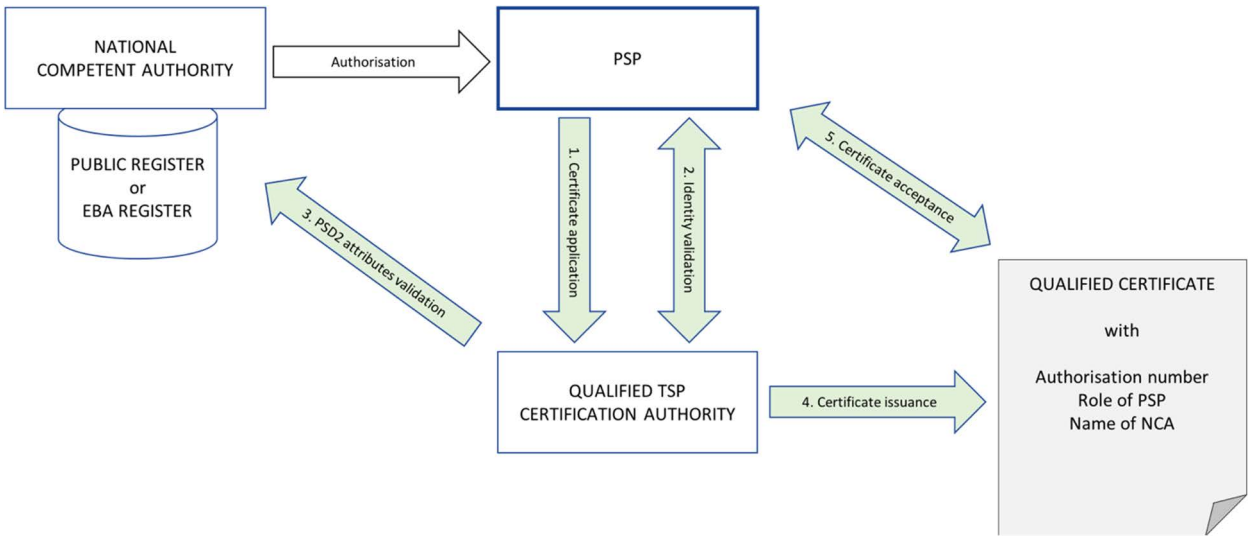


Figure 1: PSP Registration and certificate issuance

Before the issuance process can start, the PSP needs to be registered by an NCA and all relevant information needs to be available in a public register:

1) The PSP submits the certificate application and provides all necessary documentation containing PSD2 specific attributes to the Trust Service Provider (TSP) with granted qualified status according to eIDAS [i.1].

2) The TSP performs identity validation as required by its certificate policy.

3) The TSP validates PSD2 specific attributes using information provided by the NCA (e.g. national public registers, EBA PSD2 Register, EBA Credit Institution Register, authenticated letter).

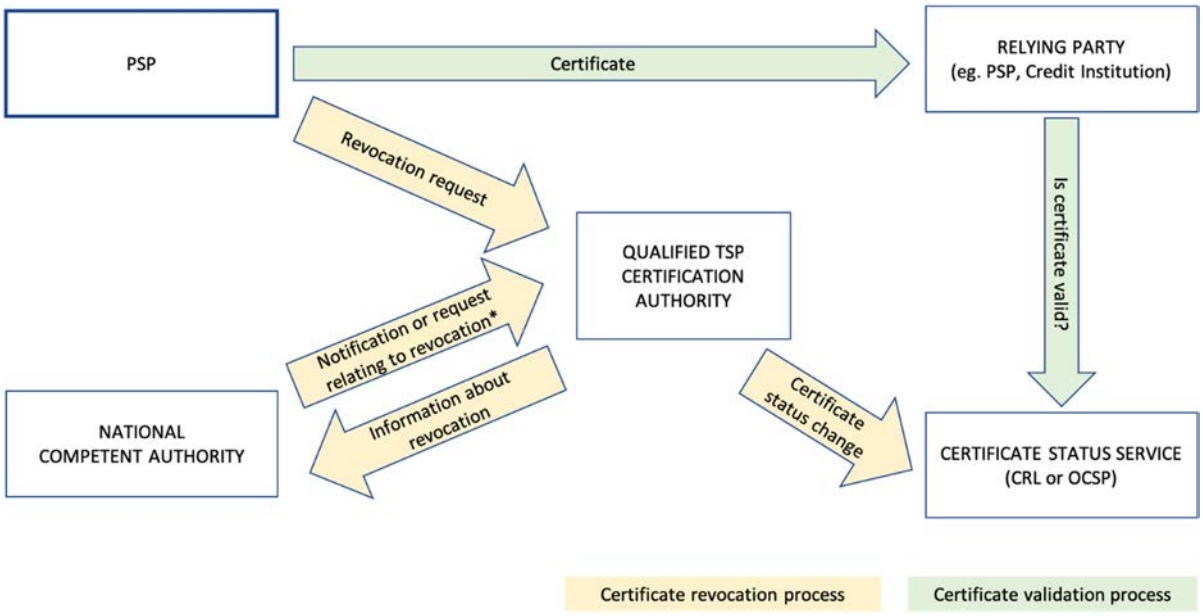
4) The TSP issues the qualified certificate in compliance with the profile requirements given in the present document.

5) The TSP emails information about the issued certificate to the NCA if that NCA has requested this notification.

6) The PSP accepts the certificate.

4.6 Certificate Validation and Revocation

Figure 2 presents the general concept for certificate validation and revocation. Validation process is based on certificate status services provided by the TSP. In addition to handling revocation as specified in ETSI EN 319 411-2 [5] a revocation request can originate from the NCA which has authorized or registered the payment service provider. The list of NCAs following the procedure of revocation as proposed by EBA in (EBA-Op-2018-7) [i.12] is published by the European Banking Authority as a related document [i.14]. The TSP revokes the certificate based on a verifiably authentic revocation request.



NOTE: The present document does not place any specific requirements on the NCA regarding revocation.

Figure 2: Illustration of PSP Certificate validation and revocation

5 Certificate profile requirements

5.1 PSD2 QCStatement

GEN-5.1-1: The PSD2 specific attributes shall be included in a QCStatement within the qcStatements extension as specified in clause 3.2.6 of IETF RFC 3739 [7].

GEN-5.1-2: This QCStatement shall contain the following PSD2 specific certificate attributes as required by RTS [i.3] Article 34:

a) the role of the payment service provider, which maybe one or more of the following:

   i) account servicing (PSP_AS);

   ii) payment initiation (PSP_PI);

   iii) account information (PSP_AI);

iv) issuing of card-based payment instruments (PSP_IC).

b) the name of the 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). See clause 5.2.3 for further details.

GEN-5.1-3: The syntax of the defined statement shall comply with ASN.1 [6]. The complete ASN.1 module for all defined statements shall be as provided in Annex A; it takes precedence over the ASN.1 definitions provided in the body of the present document, in case of discrepancy.

NOTE: This extension is not processed as part of IETF RFC 5280 [i.7] path validation and there are no security implications with accepting a certificate in a system that cannot parse this extension.

Syntax:

```
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 }
```

5.2 Encoding PSD2 specific attributes

5.2.1 PSD2 Authorization Number or other recognized identifier

GEN-5.2.1-1: The PSD2 Authorization Number, or other identifier recognized by the NCA, shall be placed in organizationIdentifier attribute of the Subject Distinguished Name field in the certificate:

a) for QWACs: as defined in clause 5.3;

b) for QsealCs: as defined in clause 5.4.

GEN-5.2.1-2: If a PSD2 Authorization Number was issued by the NCA it shall be encoded using the syntax identified by the legal person semantics identifier as defined in ETSI EN 319 412-1 [1], clause 5.1.4 and as extended by ETSI TS 119 412-1 [2], clause 5.1.4, for PSD2 authorization identifier as follows.

GEN-5.2.1-3: If a PSD2 Authorization Number was issued by the NCA the organizationIdentifier attribute shall contain information using the following structure in the presented order:

- "PSD" as 3 character legal person identity type reference;
- 2 character ISO 3166-1 [8] country code representing the NCA country;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- 2-8 character NCA identifier without country code (A-Z uppercase only, no separator);
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- PSP identifier (authorization number as specified by the NCA. There are no restrictions on the characters used).

NOTE 1: Void.

NOTE 2: The current list of NCA Identifiers with country codes provided by EBA is referenced in Annex D. Other registries can use underscore ("_") instead of hyphen-minus ("-"), but in the context of the present document hyphen-minus is required when linking country code with an NCA identifier.

NOTE 3: Where other types of identification such as trade registration number or tax identification number are used as the authorisation number, in line Commission Delegated Regulation (EU) 2018/389 [i.3] Article 34.2, these are structured with "PSD" identity type reference as described in this clause.
For clarification see: https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4679.

NOTE 4: European Banking Authority published a list of types of identification numbers used in the EBA PSD2 Register and the EBA Credit Institutions Register [i.13].

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").

GEN-5.2.1-4: If the authorization number was not available in the NCA's public register, then another registration identifier recognized by the NCA shall be used as organizationIdentifier attribute as defined in ETSI EN 319 412-1 [1], clause 5.1.4 or in ETSI TS 119 412-1 [2], clause 5.1.4.

NOTE 5: For certificates issued under PSD2 it is generally expected that the identification number is to be treated as an authorisation number in line Commission Delegated Regulation (EU) 2018/389 [i.3] Article 34.2 as described in GEN-5.2.1-3.

5.2.2 Roles of payment service provider

GEN-5.2.2-1: `RolesOfPSP` shall contain one or more roles. The roles shall be as declared by an NCA via their public register for the subject PSP. Each role is represented by role object identifier and role name.

For the role of account servicing payment service provider, payment initiation service provider, account information service provider or payment service provider issuing card-based payment instruments as defined in the RTS [i.3]:

- **GEN-5.2.2-2:** the role object identifier shall be the appropriate one of the four OIDs defined in the ASN.1 snippet below; and
- **GEN-5.2.2-3:** the role name shall be the appropriate one of the abbreviated names defined in clause 5.1: `PSP_AS`, `PSP_PI`, `PSP_AI` or `PSP_IC`.

GEN-5.2.2-4: For any other role the role object identifier and the role name shall be defined and registered by an organization recognized at the European level.

NOTE: Using nationally recognized roles can have an adverse effect on interoperability at the European level. At the time of publication of the present document only the four roles mentioned in clause 4.2 are defined by the RTS [i.3].

REG-5.2.2-5: The TSP shall ensure that the name in `roleOfPspName` is the one associated with the role object identifier held in `roleOfPspOid`.

Syntax:

```
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))
```

5.2.3 Name and identifier of the competent authority

GEN-5.2.3-1: The `NCAName` shall be plain text name in English provided by the NCA itself for purpose of identification in certificates.

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

GEN-5.2.3-2: The `NCAId` shall contain information using the following structure in the presented order:

- 2 character ISO 3166-1 [8] country code representing the NCA country;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- 2-8 character NCA identifier without country code (A-Z uppercase only, no separator).

GEN-5.2.3-3: The `NCAId` shall be unique for purpose of identification in certificates and may be provided by the NCA itself.

GEN-5.2.3-4: NCA identifier shall be composed of the same values as in the equivalent fields of the authorization number defined in clause 5.2.1.

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

NOTE 1: The above allows additional buffer space for ASN.1 data encoding in an implementation. See GEN-5.2.3-2 for requirement on the content to be placed in this field.

NOTE 2: The current list of NCA Identifiers with country codes provided by EBA is referenced in Annex D. It is not expected that changes to an NCA identifier would affect the validity of certificates already issued.

5.3 Requirements for QWAC Profile

GEN-5.3-1: If the qualified certificate issued is for website authentication (QWAC) then the requirements of ETSI EN 319 412-4 [4] shall apply including requirements for qualified certificates, except where they conflict with the requirements specified in the present document.

NOTE 1: In particular, requirements stated in GEN-5.2.1-3 and GEN-5.2.1-4 take precedence over requirements stated in the CA/Browser Forum EV Guidelines [i.11], section 9.2 as referenced through ETSI EN 319 412-4 [4], clause 4.1.

In addition:

- **GEN-5.3-2:** The PSD2 QCStatement as identified in clause 5.1 shall be included in the certificate.
- **GEN-5.3-3:** The organizationIdentifier shall be present in the Subject's Distinguished Name and encoded with legal person syntax as specified in clause 5.2.1.

NOTE 2: 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*". It is not intended that certificates issued under this profile are used just as client certificates. Thus, if the certificate is intended to be used also as a client certificate in mutual authentication then both values id-kp-serverAuth and id-kp-clientAuth will be present in extKeyUsage certificate extension.

5.4 Requirements for QsealC Profile

GEN-5.4-1: If the qualified certificate issued is for electronic seal (QsealC) then the requirements of ETSI EN 319 412-3 [3] shall apply including requirements for qualified certificates.

In addition:

- **GEN-5.4-2:** The PSD2 QCStatement as identified in clause 5.1 shall be included in the certificate.
- **GEN-5.4-3:** The organizationIdentifier shall be present in the Subject's Distinguished Name and encoded with legal person syntax as specified in clause 5.2.1.

6 Policy requirements

6.1 General policy requirements

OVR-6.1-1: For TSPs issuing QsealCs all policy requirements defined for QCP-l shall be applied as specified in ETSI EN 319 411-2 [5].

OVR-6.1-2: For TSPs issuing QWACs all policy requirements defined for QCP-w shall be applied as specified in ETSI EN 319 411-2 [5] except where they conflict with the requirements specified in the present document.

OVR-6.1-3: The following policy identifier may be used to augment the policy requirements associated with policy identifier **QCP-w** as specified in ETSI EN 319 411-2 [5] giving precedence to the requirements defined in the present document.

Syntax:

```
-- QCP-w-psd2: certificate policy for PSD2 qualified website authentication certificates;
qcp-web-psd2 OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) policy-identifiers(3) 1}
```

NOTE: If there are no conflicts between the requirements in the present document and that in CA/Browser Forum EV Guidelines [i.11] then a QTSP following **QCP-w-psd2** can also be conformant to the CA/Browser Forum EV Guidelines [i.11].

6.2 Additional policy requirements

6.2.1 Certificate profile

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.6.1 the following shall apply:

- **OVR-6.2.1-1:** The profile requirements specified in clause 5 of the present document shall apply.

6.2.2 Initial identity validation

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.2.2 the following shall apply:

- **REG-6.2.2-1:** The TSP shall verify the PSD2 specific attributes (PSD2 Authorization Number or other recognized identifier, roles, name of the NCA) provided by the subject using authentic information from the NCA (e.g. a national public register, EBA PSD2 Register, EBA Credit Institution Register, authenticated letter).
- **REG-6.2.2-2:** If the NCA provides rules for validation of these attributes, the TSP shall apply the given rules.

6.2.3 Identification and authentication for revocation requests

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.2.4 the following shall apply:

- **REV-6.2.3-1:** The TSP shall document the procedure which can be used for submission of certificate revocation requests by NCAs in its certificate policy or practice statement. The TSP shall check the authenticity of certificate revocation requests submitted by NCAs.

- **REV-6.2.3-2:** In addition, the TSP shall provide an email address, or website in English or language understood by the NCAs served, for notifications from an NCA about changes of relevant PSD2 regulatory information of the PSP which can affect the validity of the certificate. The content and format of these notifications may be agreed between the NCA and TSP. However, the TSP shall investigate this notification regardless of its format.

- **REV-6.2.3-3:** The TSP shall recognize all of the following methods of authentication of the revocation request issued by the NCA:

  - a shared secret if it was provided by the TSP to the NCA for revocation purposes;

  - a digital signature supported by a certificate issued to the NCA by a TSP compliant with a QCP policy according to ETSI EN 319 411-2 [5].

  NOTE 1: The digital signature can be used to provide an advanced electronic seal from the NCA or an advanced electronic signature from a signatory acting on behalf of the NCA.

- **REV-6.2.3-4:** If the TSP is notified of an email address where it can contact the respective NCA then it should inform the NCA, using this email address, how the NCA can authenticate itself in revocation requests (see REV-6.2.3-3).

  NOTE 2: A list of NCA email addresses notified for this purpose is published by EBA [i.14].

6.2.4 Publication and repository responsibilities

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.1 the following shall apply:

- **DIS-6.2.4-1:** If the TSP is notified of an email address where it can inform the NCA identified in a newly issued certificate then the TSP shall send to that email address information on the content of the certificate in plain text including the certificate serial number in hexadecimal, the subject distinguished name, the issuer distinguished name, the certificate validity period, as well as contact information and instructions for revocation requests and a copy of the a certificate file.

  NOTE: A list of NCA email addresses notified for this purpose is published by EBA [i.14].

6.2.5 Certificate renewal

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.3.6 the following shall apply:

- **REG-6.2.5-1:** Before certificate renewal the TSP shall repeat the verification of the PSD2 specific attributes to be included in the certificate.

6.2.6 Certificate revocation

In addition to the applicable requirements specified in ETSI EN 319 411-2 [5], clause 6.3.9 the following shall apply:

- **REV-6.2.6-1:** The TSP shall allow the NCA, as the owner of the PSD2 specific information, to request certificate revocation following the procedure defined in the TSP's certificate policy or certificate practice statement. The procedure shall allow the NCA to specify a reason, which can be descriptive rather than in a standard form, for the revocation.

- **REV-6.2.6-2:** The TSP shall process such requests, and shall validate their authenticity. If it is not clearly indicated or implied why the revocation is requested or the reason is not in the area of responsibility of the NCA then the TSP may decide to not take action. Based on an authentic request from an NCA, the TSP shall revoke the certificate in a timely manner (see note 2 below) if any of the following conditions holds (in addition to any general requirements of ETSI EN 319 411-2 [5]):

  - the authorization of the PSP has been revoked;

  - any PSP role included in the certificate has been revoked.

NOTE 1: This does not imply any obligations on the NCA to notify the TSP in such situations.

- **REV-6.2.6-3:** The TSP shall provide an email address, or website in English or language understood by the NCAs served, where an NCA can submit authenticated revocation requests and other notifications relating to revocation.

- **REV-6.2.6-4:** If the NCA as the owner of the PSD2 specific information notifies the TSP, that information has changed which can affect the validity of the certificate, but without a properly authenticated request with an acceptable reason for why the certificate should be revoked, the TSP shall investigate this notification regardless of its content and format, and shall revoke the affected certificate(s) if necessary. This notification need not be processed within 24 hours.

NOTE 2: Regulation (EU) No 910/2014 [i.1] requires that TSPs issuing qualified certificates publish the revocation status of the revoked certificate in a timely manner, and in any event within 24 hours after the receipt of the acceptable revocation request.

NOTE 3: Revocation can be considered necessary if the investigation of the TSP confirms based on authentic information that any of the conditions listed above holds.

NOTE 4: Granting new PSP roles by the NCA does not necessarily affect the validity of the existing certificate.

- **REV-6.2.6-5:** If the TSP is notified of an email address where it can inform the NCA identified in a revoked certificate then the TSP shall send to that email address information about the certificate revocation.

NOTE 5: A list of NCA email addresses notified for this purpose is published by EBA [i.14].

Annex A (normative): ASN.1 Declaration

```
ETSIPSD2QcprofileMod { itu-t(0) identified-organization(4) etsi(0) psd2(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))

-- Policy Identifiers
etsi-psd2-policy OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) policy-identifiers(3)}
```

```
-- QCP-w-psd2 certificate policy for PSD2 qualified website authentication certificates
qcp-web-psd2 OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) policy-identifiers(3) 1}

END
```

Annex B (informative): Certificates supporting PSD2 - clarification of the context

The main purpose of a digital certificate is to bind the identity of the owner of a public key to the public key. Using the certificate, it is possible to communicate securely with its owner (the subject). What "securely" means exactly depends on the type of certificate.

A website authentication certificate makes it possible to establish a Transport Layer Security (TLS) [i.5] channel with the subject of the certificate, which guarantees confidentiality, integrity and authenticity of all data transferred through the channel. This means that the person or system connecting to the website presenting the certificate can be sure who "owns" the end point of the communication channel (the owner of the certificate), that the data was not changed between the end points, and that nobody else could have read the data along the way. However, the communicated data is only protected while it is travelling through the TLS channel. The data is produced in plain (unencrypted) form by the sender system, and the data will appear in plain (unencrypted) form in the receiver system. Therefore, once the TLS channel is closed, the data loses the protection of its authenticity, integrity and confidentiality, unless it is protected by other means.

A website authentication certificate can also be used to identify the calling party (client) when using TLS as described above. This means that the called party (server) can authenticate who "owns" the calling end of the communication channel (the owner of the certificate). Thereby, if both communicating parties have website authentication certificates, they can use them to set up a secure TLS channel providing mutual authentication (MATLS). Qualified website authentication certificates supporting PSD2 are issued only to legal persons and TLS communication between calling party and called party is established between servers. The present document does not directly support natural persons, however, it is suggested that natural persons may represent themselves as legal persons (see below).

Under the eIDAS regulation [i.1] an electronic seal is defined in a way which implies that it is created by a legal person. A certificate for electronic seals makes it possible for the owner of the certificate to create electronic seals on any data. The digital signature technology guarantees the integrity and authenticity of the signed/sealed data. This means that the persons receiving digitally signed data can be sure who signed the data (the owner of the certificate), that the data was not changed since it was signed, and they can also present this signed data to third parties as an evidence of the same (who signed it, and that it was not changed since). Therefore, digitally signed data can keep its authenticity and integrity over time when appropriately maintained, regardless of how it is stored or transferred. (An electronic seal can be validated by anyone, at any time, to check whether the integrity and authenticity of the data still holds.) The electronic seal provides strong evidence that given data is originated by the legal entity identified in the certificate. An electronic seal can also protect the authenticity and integrity of data when relayed through a third party, although on its own does not protect against replay attacks. Electronic seals can be applied to requests and responses between PSPs.

Whilst electronic seals can only be applied by a legal person, as stated in eIDAS regulation [i.1] recital 68: *"The concept of 'legal persons' … leaves operators free to choose the legal form which they deem suitable for carrying out their activity. Accordingly, 'legal persons', within the meaning of the TFEU [Treaty on the Functioning of the European Union], means all entities constituted under, or governed by, the law of a Member State, irrespective of their legal form."*. Thus, any legally recognized entity can, depending on the applicable legislation, apply an electronic seal including individual persons. Currently, the website certificate profiled in the present document is aimed at legal persons with the same applicability.

Certificates for both website authentication and electronic seals can be qualified or non-qualified. The requirements on the issuance of a qualified certificate are more stringent, so using a qualified certificate provides a stronger association of the protected data with the identity of the owner of the certificate. As an example, before issuing a qualified certificate the issuer trust service provider will verify the identity of the owner in a face-to-face meeting and based on government-issued photo ID documents, or by equivalently secure procedures. Hence, qualified certificates can have a stronger legal assumption of the evidential value than non-qualified ones.

Both qualified website authentication certificates (QWACs) and qualified electronic seal certificates (QsealCs) are based on widely implemented technology. QWACs are derived from website certificates supported by all the modern web browsers and commonly used to provide system-to-system secure channels. QsealCs are derived from certificates used with digital signature technology widely employed e.g. for document security, business to business communication and in modern banking networks.

In consequence:

- A qualified website authentication certificate (QWAC) should be used to establish a secure TLS channel to protect the communication (in the transport layer) from potential attackers on the network. The person or system connecting to the website can be sure who they are communicating with, but cannot prove this to third parties. Using QWAC does not give legally assumed evidence of a transaction.
- A qualified certificate for electronic seals (QsealC) should be used to protect the data or messages (in the application layer) from potential attackers during or after the communication. The electronic seal does not provide confidentiality (i.e. there is no encryption of application data). The person receiving the sealed data can be sure who sealed the data, and can also prove this to third parties even after the communication has ended. QsealC provides evidence of a transaction with legal assumption and can protect the authenticity and integrity of data when relayed through third parties.
- A certificate can be either for website authentication or electronic seals, but not both. Therefore, these two types of certificates are not interchangeable.

Annex C (informative): Additional information on QTSP and NCA/EBA interactions

C.1 Introduction

Whilst the main body of the present document identifies information that can be provided by NCAs and/or the EBA, such as by publishing through their national or European registers, as well as services provided by QTSP that can be used by NCAs, for example to request revocation, the present document places no requirements on the operation of NCAs nor on the EBA.

The following text is for information only.

C.2 What information is in a qualified certificate

RTS [i.3] requires that payment service providers (PSPs) identify themselves.

For this purpose, payment service providers are required to rely on:

- qualified certificates for electronic seals; or
- qualified certificates for website authentication;

as defined in the eIDAS Regulation [i.1].

Qualified certificates are issued by Qualified Trust Service Providers (qualified TSPs) on request from payment service provider (PSP). It is aimed that certificates issued by qualified TSPs for PSPs are compliant with the requirements described in the present document.

The qualified certificate contains:

- identity information about the PSP, such as a PSD2 Authorization Number which makes it possible to unambiguously identify the PSP;
- PSD2 specific attributes, which can be used by relying parties communicating with the PSP to ascertain its role(s) as authorized by the NCA in the country of registration of the PSP;
- the public key of the PSP, which can be used to (depending on the type of certificate) validate the electronic seal or authenticate the website of the PSP.

The qualified certificate is a verifiable electronic document, whose integrity and authenticity are protected by the digital signature of the issuing TSP and provides a level of legal assumption under eIDAS Regulation [i.1].

Even when credit institutions are acting only in an account servicing capacity and need not use certificates conforming to the present document, it is highly recommended for them to use qualified certificates for electronic seal and/or qualified certificates for website authentication to secure the communication and documents when communicating with other PSPs.

If a payment service provider, including credit institutions, act in its capacity as an account servicing payment service provider, and has decided to use qualified certificates for electronic seal and/or qualified certificates for website authentication to secure the communication and documents when communicating with other PSPs, it is expected to be assigned the role 'account servicing (PSP_AS)' under Article 34(3)(a)(i) of the RTS [i.3].

C.3 PSD2 specific attributes in qualified certificates

Qualified certificates contain PSD2 specific attributes which are:

- authorization number if it is issued by the NCA, or registration number recognized on national or European level or Legal Entity Identifier included in the register of credit institutions. The standard requires the registration number to be one recognized under ETSI EN 319 412-1 [1] or ETSI TS 119 412-1 [2];
- role or roles of PSP;
- NCA name (NCAName) and unique identifier (NCAId).

C.4 NCA's naming conventions

The name of the NCA will be included in the certificate as follows:

- NCA Long Name (English Language) Registered name - name registered in appropriate source for PSD2 NCAs.
- NCA Identifier containing:
  - 2 character ISO 3166-1 [8] country code representing the NCA Country;
  - hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
  - 2-8 character NCA identifier (A-Z uppercase only, no separator) without country code, unique within the country.

A list of NCA Identifiers including country codes provided by EBA is referenced in Annex D. NCAs can sometimes use underscore ("_") instead of hyphen-minus ("-") but in the context of the present document hyphen-minus is required when linking country code with an NCA identifier. It is not expected that changes to an NCA identifier would affect the validity of certificates already issued.

C.5 Validation of Regulatory information about a requesting PSP

Before the issuance of any PSD2 certificate, the qualified TSP validates the identity of the requesting PSP and then validates PSD2 specific attributes in the public register of the Home NCA (NCA in the country of authorization/registration of the PSP) or the EBA PSD2 Register, which contains updated copy of information from NCA registers, or the EBA Credit Institutions Register. Validation by qualified TSP is based on information and procedure for validation provided by the NCA where available (e.g. a national public register, EBA PSD2 Register, authenticated letter, EBA Credit Institutions Register).

When the TSP uses the EBA PSD2 Register for validation of PSD2 specific attributes, it will need to check the authenticity of the register. It is suggested that this is done by relying on website authentication certificates.

If the information in the EBA PSD2 Register is not sufficient to validate all PSD2 specific attributes, the TSP can contact the NCA in the country of registration of the PSP for clarifications.

C.6 Provision of PSD2 Regulatory information about the PSP

As per PSD2 [i.2] Article 14, the NCA can provide an online Public Register containing a clear record of the PSP and associated Regulatory information (as in clause C.3). Article 15 of PSD2 [i.2] defines the EBA PSD2 Register which contains accurate presentation of information originated from NCAs.

If the NCA provides the following in a public register this can be used by qualified TSPs to accurately verify the information about the PSP and embed it in a Qualified Certificate as required by the RTS:

- A clear definition of the sole Authorization Number to be used by the qualified TSP to represent the PSP, and how it can be identified within the register.
- Clear and unambiguous Roles of the PSP, related to a unique Authorization Number, in the context of PSD2, shown in the form:
  - i) account servicing (PSP_AS);
  - ii) payment initiation (PSP_PI);
  - iii) account information (PSP_AI);
  - iv) issuing of card-based payment instruments (PSP_IC).
- If not clearly stating the Role of the PSP, in the context of PSD2, then a clear mapping to the Services 1-8 as shown in Annex I of PSD2 [i.2], and how the NCA expects unambiguous translation of those to the following roles:
  - i) account servicing (PSP_AS);
  - ii) payment initiation (PSP_PI) as corresponding to payment initiation service as referred to in point (7) of Annex I to PSD2 [i.2];
  - iii) account information (PSP_AI) as corresponding to account information service as referred to in point (8) of Annex I to PSD2 [i.2];
  - iv) issuing of card-based payment instruments (PSP_IC) as corresponding to issuing of payment instruments and/or acquiring of payment transactions as referred to in point (5) of the Annex I to PSD2 [i.2].

A credit institution can act in its capacity as a third party provider and therefore is expected to use certificates conforming to the present document, this credit institution is assigned all three roles under Article 34.3(a)(ii-iv) of the RTS [i.3], namely payment initiation (PSP_PI), account information (PSP_AI); issuing of card-based payment instruments (PSP_IC).

In case there is no PSD2 Authorization Number, other forms of registration recognized by the NCA can be used in place of a PSD2 Authorization Number. If necessary to ensure uniqueness the authorization number can contain a prefix including the type of institution, as listed in PSD2 [i.2] Article 1.1: Credit institution - CI, Payment institution - PI, Electronic money institution (or e-money institution) - EMI, Account information service provider exempted under Article 33 of PSD2 [i.2] (they have only the AIS role) - RAISP.

In other case the unique identification number presented in the certificate is e.g. Legal Entity Identifier, VAT number or National Trade Register number. The identification number is required to be one recognized under ETSI EN 319 412-1 [1]/ETSI TS 119 412-1 [2].

C.7 How NCAs can get information about issued Certificate(s) for PSPs

For the purpose of reporting and management of authorizations by the NCA, involving PSD2 Qualified Certificates, the following can be available to NCAs:

- In the case of direct interaction between a qualified TSP and an NCA about the issuance of each certificate, then it is suggested that the NCA notifies a contact email address, that TSPs are required to use in order to notify the respective NCA about the issued and/or revoked certificates.
- The NCAs can require information about issued certificate to be provided by the qualified TSP, after certificate issuance and acceptance.

C.8 How NCAs can request a TSP to revoke issued certificates

An NCA can request a qualified TSP to revoke a PSD2 certificate. This can be in the form of an authenticated request which the TSP is required to act upon if valid or a notification which it will investigate. Valid reasons for revocation can include the following scenarios:

- information in the Public Register has changed to substantially affect the validity of the PSD2 attributes in the certificate;
- the authorization status granted by that NCA has changed (e.g. that PSP is no longer authorized).

The qualified TSP will specify the content, format and the communication channels to be used to submit certificate revocation requests in its certificate policy (e.g. a certificate revocation request typically identifies the certificate in question, the submitter of the request and a reason for revocation). It is noted that there is a concern that there is not a common standard for the submission of revocation requests. This could be a matter for future standardization. The qualified TSP will revoke the certificate based on a valid certificate revocation request from the NCA as soon as possible but at least within 24 hours. The request is required to have some form of authentication of the NCA making the request.

As an alternative to certificate revocation requests, the NCA as the owner of the information can notify the qualified TSP that relevant information in its public register has changed and it could affect the validity of the certificate. The content and format of these notifications can be agreed between the NCA and the qualified TSP. The qualified TSP will investigate this notification regardless of its format. The notifications can be submitted to the qualified TSP using an agreed communication channel, however, an email address or website will be provided by the qualified TSP as a default means of submission. The qualified TSP revokes the certificate if it finds authentic information which confirms that the PSD2 specific attributes in the certificate are no longer valid. The processing of this notification can take longer than the 24 hours required for revocation requests.

Annex D (informative): List of NCA Identifiers provided by European Banking Authority

The current list of NCA abbreviations [i.15] is published on the European Banking Authority website at https://eba.europa.eu/file/113255/.

NCAs can sometimes use underscore ("_") instead of hyphen-minus ("-"), but in the context of the present document hyphen-minus is required when linking country code with an NCA identifier.

History

Document history		
V1.1.1	May 2018	Publication (Withdrawn)
V1.1.2	July 2018	Publication
V1.2.1	November 2018	Publication
V1.3.1	March 2019	Publication
V1.3.2	June 2019	Publication
V1.4.1	November 2019	Publication