Draft ETSI TS 119 495 V0.0.3 (2018-01)

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

STABLE DRAFT FOR PUBLIC REVIEW UNTIL 23 MARCH 2018

Download the template for comments:

https://docbox.etsi.org/ESI/Open/Latest_Drafts/Template-for-comments.doc

Send comments ONLY to E-SIGNATURES_COMMENTS@list.etsi.org

Reference
DTS/ESI-0019495

Keywords
e-commerce, electronic signature, extended validation certificate, public key, security, trust services, payments

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

Important notice

The present document can be downloaded from:
http://www.etsi.org/standards-search

The present document may be made available in electronic versions and/or in print. The content of any electronic and/or print versions of the present document shall not be modified without the prior written authorization of ETSI. In case of any existing or perceived difference in contents between such versions and/or in print, the only prevailing document is the print of the Portable Document Format (PDF) version kept on a specific network drive within ETSI Secretariat.

Users of the present document should be aware that the document may be subject to revision or change of status.
Information on the current status of this and other ETSI documents is available at
https://portal.etsi.org/TB/ETSIDeliverableStatus.aspx

If you find errors in the present document, please send your comment to one of the following services:
https://portal.etsi.org/People/CommiteeSupportStaff.aspx

Copyright Notification

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to the present document 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 and bank account information institutions.

The Commission Delegated Regulation with regard to Regulatory Technical Standards on strong customer authentication and secure communication (RTS henceforth) [i.3] 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.

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 may 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 EN 319 412-3 [2], ETSI EN 319 412-4 [3], IETF RFC 3739 [6] 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 [4].

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

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

[4] 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".

[5] Recommendation ITU-T X.680-X.699: "Information technology - Abstract Syntax Notation One (ASN.1)".

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

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) No …/.. of XXX [Waiting for publication] supplementing Directive 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 (RTS).

[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".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of the present document, the terms and definitions given in PSD2 [i.2], in ETSI EN 319 412-1 [1] and in ETSI EN 319 411-2 [4] apply.

3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-1 [1], in ETSI EN 319 411-2 [4] and the following apply:

CRL	Certificate Revocation List
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 Standards

NOTE: See regulation …/.. of XXX [i.3].

TSP Trust Service Provider

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) channel with the subject of the certificate, which guarantees confidentiality, integrity and authenticity of all 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 [i.3] to RTS 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).

A PSP can be authorized by their NCA to act in one or more PSD2 roles.

4.3 Payment Service Provider Authorizations and Services Passporting

According to PSD2 [i.2] and Credit Institutions Directive [i.4], the competent authority (NCA) responsible for payment services approves or rejects authorization of PSPs in its own country. If authorization is granted, the NCA issues an authorization number and publishes that information in its public register(s). An NCA also approves or rejects the operation of PSPs in its own country, requesting access via other countries. The NCA approval to operate payment services in a new country, to a foreign PSP initially registered in another country, is called passporting. Information about passporting is published in the public registry in the home country of the PSP.

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

4.4 Authorization Number

For identification, the RTS [i.3] requires the registration number used in a qualified certificate, as stated in the official records in accordance with Annex III item (c) 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] or resulting from the notifications of every authorization granted under Article 8 of Directive 2013/36/EU [i.4] in accordance with Article 20 of that Directive.

4.5 Registration and Certificate Issuance

Figure 1 presents the general concept of registration and certificate issuance. The qualified certificate contains an authorization number of the PSP, which has been issued/specified by a National Competent Authority (NCA), and is publicly available in that NCA public register.

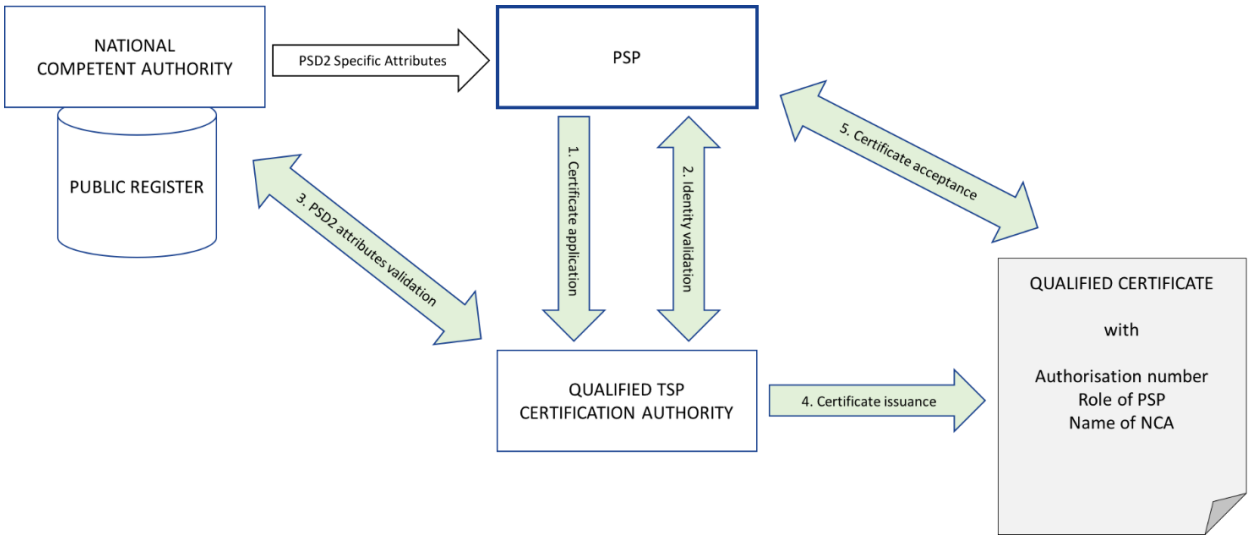

Figure 1: PSP Registration and certificate issuance

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

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

3) TSP validates PSD2 specific attributes using information provided the NCA (e.g. public registry, authenticated letter).

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

5) 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 service provided by the TSP. Revocation request can originate from the certificate subject (PSP) or from the NCA which has issued the PSP authorization number contained in the certificate. TSP revokes the certificate based on a verifiably authentic revocation request.

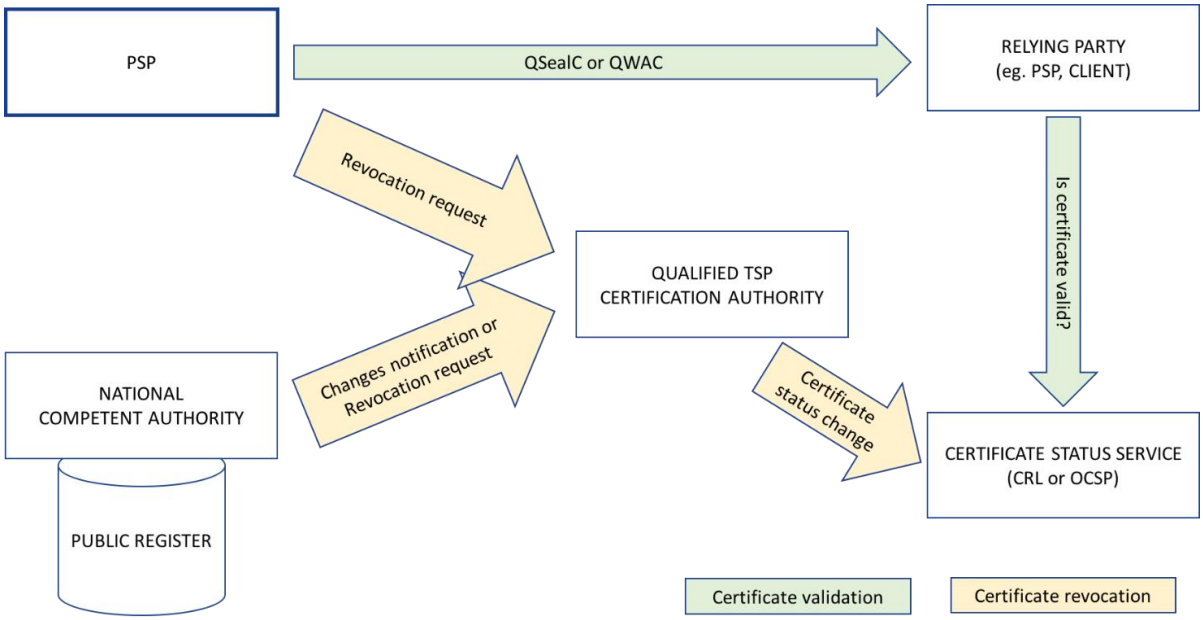

Figure 2: PSP Certificate validation and revocation

5 Certificate profile requirements

5.1 PSD2 QCStatement

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 [6].

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.

The syntax of the defined statement shall comply with ASN.1 [5]. 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 Authorization number

The authorization number 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.

The authorization number 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 extended for PSD2 authorization identifier as follows.

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 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)
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- PSP identifier (authorization number as specified by NCA).

EXAMPLE: The organizationIdentifier "PSDES-BDE-3DFD21" means a certificate issued to a PSP where the authorization number is 3DFD21, authorization was granted by the Spanish NCA Banco de España (identifier after second hyphen-minus is decided by Spanish numbering system)

Any separator in NCA identifier shall be removed.

5.2.2 Roles of payment service provider

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]:

- the role object identifier shall be the appropriate one of the four OIDs defined in the ASN.1 snippet below; and
- 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`.

For any other role the role object identifier and the role name shall be defined and registered by an organization recognized by the NCA or 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].

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(256))
```

5.2.3 Name and identifier of the competent authority

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

```
NCAName ::= utf8String (SIZE (256))
```

The `NCAId` shall contain information using the following structure in the presented order:

- 2 character ISO 3166 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).

The `NCAId` shall be unique and provided by NCA itself for purpose of identification in certificates.

NCAId 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 (256))
```

5.3 Requirements for QWAC Profile

If the qualified certificate issued is for website authentication (QWAC) then the requirements of ETSI EN 319 412-4 [3] shall apply including requirements for qualified certificates.

In addition:

a) The PSD2 QCStatement as identified in clause 5.1 shall be included in the certificate.

b) 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: 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) "*id-kp-serverAuth [RFC5280] 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 will need to be present. It is not intended that certificates issued under this profile are used just as client certificates.

5.4 Requirements for QSealC Profile

If the qualified certificate issued is for electronic seal (QSealC) then the requirements of ETSI EN 319 412-3 [2] shall apply including requirements for qualified certificates.

In addition:

a) The PSD2 QCStatement as identified in clause 5.1 shall be included in the certificate.

b) 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

For TSPs issuing QSealCs (QCP-l) policy requirements shall be applied as specified in ETSI EN 319 411-2 [4].

For TSPs issuing QWACs (QCP-w) policy requirements shall be applied as specified in ETSI EN 319 411-2 [4].

6.2 Additional policy requirements

6.2.1 Certificate profile

Requirements specified in ETSI EN 319 411-2 [4], clause 6.6.1 shall apply.

The profile requirements specified in clause 5 of the present document shall apply.

6.2.2 Initial identity validation

Requirements specified in ETSI EN 319 411-2 [4], clause 6.2.2 shall apply.

The TSP shall verify the PSD2 specific attributes (authorization number, roles, name of NCA) provided by the subject using authentic information from the NCA (e.g. the official registry). If the NCA provides rules for validation of these attributes, the TSP shall apply the given rules.

NOTE: Guidance for NCAs to support Qualified TSP validation of PSD2 specific attributes is given in Annex C. In particular it should be clear what information is used to validate an authorization number.

6.2.3 Identification and authentication for revocation requests

The requirements specified in ETSI EN 319 411-2 [4], clause 6.2.4 shall apply.

In addition the following requirements apply:

The TSP shall document the procedure for submission of certificate revocation requests by NCAs in its certificate policy or practice statement. The TSP may specify the content, format and the communication channels to be used to submit the certificate revocation requests. The TSP shall check the authenticity of certificate revocation requests submitted by NCAs.

In addition, the TSP shall provide an email address for notifications from 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.

NOTE: Guidance for NCAs to support revocation of PSD2 certificates due to changes in PSD2 specific attributes is given in Annex C.

6.2.4 Publication and repository responsibilities

The requirements specified in ETSI EN 319 411-2 [4], clause 6.1 shall apply.

In addition the following requirements apply:

An NCA can request information from a TSP about certificates containing a PSP authorization number assigned by the NCA. If such a request is made, the TSP shall inform the NCA about issued certificates as stated in the TSP policy.

NOTE: Guidance for NCAs for maintaining PSD2 certificate information so that Qualified TSPs can be made aware of changes in PSD2 specific attributes is given in Annex C.

6.2.5 Certificate renewal

The requirements specified in ETSI EN 319 411-2 [4], clause 6.3.6 shall apply.

In addition the following requirements apply:

Before certificate renewal the TSP shall repeat the verification of the PSD2 specific attributes to be included in the certificate. If the NCA provides rules for validation of these attributes, the TSP shall apply the given rules.

6.2.6 Certificate revocation and suspension

The requirements identified in ETSI EN 319 411-2 [4], clause 6.3.9 apply.

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 for the revocation.

The TSP shall process such requests, and shall validate their authenticity. If no reason is provided 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, the TSP shall revoke the certificate if any of the following conditions holds:

- the authorization of the PSP has been revoked;
- the authorization number of the PSP has changed;
- the NCA name or identifier has changed;
- any PSP role included in the certificate has been revoked;
- revocation is required by law;
- any other condition stated in the certificate policy of the TSP.

If the NCA as the owner of the PSD2 specific information notifies the TSP, that relevant information has changed which can affect the validity of the certificate, 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: Revocation can be considered necessary if the investigation of the TSP confirms based on authentic information that any of the conditions listed above holds.

Annex A (normative): ASN.1 Declaration

```
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 (256))

NCAId ::= utf8String (SIZE (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(256))

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 may 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).

An electronic seal is a digital signature of 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 may be applied to requests and responses between PSPs.

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 CA 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): Guidance for PSD2 National Competent Authorities

C.1 What information is in a qualified certificate

RTS [i.3] requires that payment service providers (PSPs) identify themselves when communicating and ensure the confidentiality and the integrity of the personalized security credentials of the payment service user.

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, including a PSD2 specific identifier, 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 home NCA;
- 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 is protected by the digital signature of the issuing CA and provides a level of legal assumption under eIDAS Regulation [i.1].

C.2 PSD2 specific attributes in qualified certificates

Qualified certificates contain PSD2 specific attributes which are:

- authorization number;
- role or roles of PSP;
- NCA name (NCAName) and unique identifier (NCAId).

C.3 NCA Own Naming Conventions

NCA provides the following which will be included in the certificate:

- NCA Long Name (English Language) Registered name - name registered in appropriate source for PSD2 NCAs (see note).
- NCA Identifier containing:
  - NCA Country;
  - 2-8 character NCA identifier (A-Z uppercase only, no separator) unique within the country.

NOTE: It is expected that official NCA reference information will be published by the European Commission.

C.4 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 PSD2 specific attributes in public registry of the Home NCA. NCA provides information on PSD2 specific attributes validation procedures related to their own public register or processes, if any.

It is expected that NCA provides rules for Qualified TSPs so that there is a clear definition of how to access authorization and roles in the NCA registry (e.g. contact information or online web site) and use this information to verify those attributes (e.g. how the information provided may be related to the information to be placed in the certificate, any additional checks the Qualified TSP should make directly with the NCA).

C.5 Validation of the Authorization Status of the PSP, if Qualified TSP relies solely on the NCA Public Register

If no additional rules of validation are provided by the NCA, then Qualified TSPs rely on the NCA Public Register information with no direct confirmation from the NCA. In this case, the status of authorization will be shown clearly and unambiguously in the Public Register, in order to provide assurance for the Qualified TSP that the PSP has a valid Authorization at the point of issuance.

C.6 Provision of PSD2 Regulatory information about the PSP, if Qualified TSP relies solely on the NCA Public Register

As per PSD2 Article 14, the NCA is expected to provide an online Public Register containing a clear record of the PSP and associated Regulatory information (as in clause C.2).

In order for Qualified TSPs to accurately verify, embed the information about the PSP in a Qualified Certificate as required by the RTS, the NCA is expected to provide:

- A clear definition of the sole Authorization Number to be used by the Qualified TSP to represent the PSP, and how it might be identified within the registry.
- 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 referencing table for the NCA and their Public Register, is expected to be shown for the Payment Services Authorized for that PSP, showing a clear mapping between the Services 1-8 as shown in Annex I of PSD2 [i.2], and how the NCA expects unambiguous translation to the following roles:
  - i) account servicing (PSP_AS);
  - ii) payment initiation (PSP_PI);
  - iii) account information (PSP_AI);

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

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 may be made available by Qualified TSPs to NCAs:

- In the case of direct interaction between Qualified TSP and NCA about the issuance of each certificate, then it is suggested that the NCA holds records on which Qualified TSP issued which certificates to which PSPs.
- NCAs could require information about issued certificate, after certificate issuance and acceptance. This information could be provided by Qualified TSPs or PSPs, depending on the certificate policy or certificate practice statement of the Qualified TSP.

C.8 How NCA can request a TSP to revoke issued certificate

An NCA may request a Qualified TSP to perform a revocation of certificate(s) issued to a given PSP by that Qualified TSP. This could include the following scenarios:

- information in the Public Registry 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 the reason for revocation.) The Qualified TSP will revoke the certificate based on a valid certificate revocation request from the NCA within 24 hours.

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 registry has changed and it could affect the validity of the certificate. The content and format of these notifications may be agreed between the NCA and 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 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 violates the validity of PSD2 specific attributes in the certificate. The processing of this notification could take longer than the 24 hours required for revocation requests.

History

Document history		
V0.0.0	October 2017	Early draft for PSD2 Workshop
V0.0.1	December 2017	Stable draft
V0.0.2	January 2018	Stable draft for public review - output of ESI#61
V0.0.3	January 2018	Clean-up done by ***editHelp!*** E-mail: mailto:edithelp@etsi.org