ETSI TS 119 495 V1.6.1 (2022-11)

Electronic Signatures and Infrastructures (ESI);
Sector Specific Requirements;
Certificate Profiles and TSP Policy Requirements
for Open Banking

Reference
RTS/ESI-0019495v1.6.1

Keywords
e-commerce, electronic signature, extended validation certificate, 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 - APE 7112B
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° w061004871

Contents

Intellectual Property Rights

Essential patents

IPRs essential or potentially essential to normative deliverables may have been declared to ETSI. The declarations pertaining to these essential IPRs, if any, are 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 Directives including the ETSI IPR Policy, no investigation regarding the essentiality of IPRs, 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.

DECT™, **PLUGTESTS™**, **UMTS™** and the ETSI logo are trademarks of ETSI registered for the benefit of its Members. **3GPP™** and **LTE™** are trademarks of ETSI registered for the benefit of its Members and of the 3GPP Organizational Partners. **oneM2M™** logo is a trademark of ETSI registered for the benefit of its Members and of the oneM2M Partners. **GSM**® and the GSM logo are trademarks registered and owned by the GSM Association.

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

Open Banking enables third parties to provide additional payment services through an open interface to financial institutions, such as banks. Earlier versions of the present document were specifically aimed at the following European regulatory environment.

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].

Countries outside the EU are also establishing similar regulatory environments for Open Banking. Hence the later versions of the present document have internationalised the requirements to enable it to be applicable to other non-EU regulatory environments for open banking.

The present document defines requirements to apply the RTS [i.3] requirement to use qualified certificates as defined in eIDAS (Regulation (EU) No 910/2014 [i.1]) for EU PSD2 [i.2], but also enables the use of other forms of regulated certificates to be adopted for other similar regulatory regimes outside the EU.

The EU commission has recently issued a document on plans to extend the current EU PSD2 related regulations in COM(2020) 592 [i.16]. The provisions of the present document might be applicable to such Open Finance services.

1 Scope

The present document:

1) Specifies requirements for qualified certificates, or other non-EU schemes which provide equivalent assurance based ETSI best practices, for electronic seals and website authentication, to be used by payment service providers in order to meet needs of Open Banking including the EU PSD2. 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].

3) Specifies specific requirements for EU use of the qualified certificates for electronic seals and website authentication, to meet the requirements of the EU 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. The identifier for the Competent Authority and its country (see clause 5.2.3) can be used to identify the applicable legislation. It can be determined whether a country's' national legislation follows the EU PSD2 Directive (Directive (EU) 2015/2366 [i.2]), and hence whether the RTS [i.3] applies, using the EBA list of NCA identifiers as identified in Annex D.

The requirements in clauses 5 and 6 for the certificate profile and policy are common to both EU PSD2 and non-EU Open Banking certificates.

The present document identifies information for Open Banking that is provided by a regulatory authority recognized through regulations as competent for providing such information. In the case of EU PSD2 this information is provided through a national register operated by the NCA or a register operated by the European Banking Authority. In addition, the TSP may provide services to the Competent Authority to enable revocation of certificates based on information provided by competent authority. The present document places no requirements on the operation of Competent Authorities providing information for Open Banking.

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".

[9] ETSI EN 319 411-1: "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements".

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 (EU 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/.

[i.16] Communication from the commission to the European parliament, the council, the European economic and social committee and the committee of the regions on a Retail Payments Strategy for the EU (COM(2020) 592 final).

[i.17] OBE: "Global National Competent Authority Codes List".

NOTE: Available at https://www.openbanking.exchange/obe/global-national-competent-authority-codes-list/.

3 Definition of terms, symbols and abbreviations

3.1 Terms

For the purposes of the present document, the terms given in EU PSD2 [i.2], ETSI EN 319 412-1 [1], ETSI EN 319 411-1 [9], ETSI EN 319 411-2 [5] and the following apply:

competent authority: authority recognized under the applicable regulations as competent for providing authorization information for open banking

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].

open banking: regulatory and technical environment for payment and other financial services

NOTE 1: In Europe, the regulated environment for Open Banking covers payment is Directive (EU) 2015/2366 [i.2] and associated regulations.

NOTE 2: Within the present document Open Banking can include other financial services such as planned for the European Open Finance framework (see COM(2020) 592 [i.16]).

NOTE 3: Within the present document, PSD2 on its own is used to denote any regulation for Open Banking. The abbreviation EU PSD2 is used to identify Directive (EU) 2015/2366 and other associated directives or regulations.

open banking attributes: attributes representing Open Banking specific information about payment and financial institutions

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
EU PSD2	EUropean Payment Services Directive

NOTE: See Directive (EU) 2015/2366 [i.2] and national legislation recognized as implementing this directive such as nations in European Economic Area.

NCA	National Competent Authority

NOTE: Under EU PSD2 [i.2].

OCSP	Online Certificate Status Protocol
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
QTSP	Qualified TSP

NOTE: See Regulation (EU) No 910/2014 [i.1].

QWAC	Qualified Website Authentication Certificate
RTS	Regulatory Technical Standard

NOTE: For EU PSD2 strong customer authentication and common and secure open standards of communication. See Commission Delegated Regulation (EU) 2018/389 [i.3].

TLS	Transport Layer Security

NOTE: For example, see IETF RFC 8446 [i.10].

TSP	Trust Service Provider

4 General concepts

4.1 Use of Certificates for Open Banking

The present document identifies two classes of certificates used for Open Banking:

- A website authentication certificate which 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 digital signatures used as electronic seals which allows the relying party to validate the identity of the subject of the certificate, as well as the authenticity and integrity of the signed data. The digital signature provides strong evidence, capable of having legal effect, that given data is originated by the legal entity identified in the certificate.

The certificates used for Open Banking are also required to be issued by TSPs which meet any regulatory requirements to ensure their reliability as specified under the applicable regulation.

NOTE: Under EU PSD2 the RTS [i.3] Article 34.1 requires that, for the purpose of identification, payment service providers rely on EU qualified certificates for electronic seals or EU qualified certificates for website authentication. The criteria for recognition of EU qualified certificates are stated in Regulation (EU) No 910/2014 [i.1] which requires that TSPs issuing EU qualified certificates demonstrate that they meet the requirements for EU qualified trust service providers as per the regulation.

4.2 Roles

Roles are attributes which can be used to indicate the specific roles that a payment service provider is authorized to operate under as by the competent authority. Every role is uniquely identified by an ASN.1 [6] object identifier. The roles authorized by the competent authority for the PSP can be unspecified within the certificate and made available, for example, through an open banking directory service.

For certificates issued under EU PSD2 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 Competent Authority to act in one or more roles.

NOTE 3: Under EU PSD2 credit institution with a full license can act in its capacity as a third party provider, as specified in EU 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.

NOTE 4: Non-EU PSD2 environments with semantically equivalent roles may use the roles listed above.

NOTE 5: If the role is "unspecified" within the certificate then it is expected that information on the activities authorized are made available by other means.

NOTE 6: Object identifiers for further roles can be defined outside the scope of the present document.

4.3 Payment Service Provider Authorizations and Services Passporting

According to EU 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 Competent Authority 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 the Competent Authority 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 granted by countries other than country of the Competent Authority.

NOTE: Under EU PSD2 [i.2], certificates do not include any attributes regarding passporting.

4.4 Authorization Number

Certificates issued according to the requirements laid down in the present document include an identifier called Authorization Number which can be used by the Competent Authority to uniquely identify a payment service provider.

NOTE: Under EU PSD2 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 Competent Authority public register pursuant to Article 14 of EU PSD2 [i.2].
For clarification, see https://eba.europa.eu/single-rule-book-qa/-/qna/view/publicId/2019_4679.

4.5 Registration and Certificate Issuance

Figure 1 presents the general concept of registration and certificate issuance. The certificate compliant with the profile requirements given in the present document is issued only to payment service providers and related financial institutions authorized by the Competent Authority, confirmation of authorization is publicly available.

The Competent Authority can request to be informed about every certificate issued using information it provides.

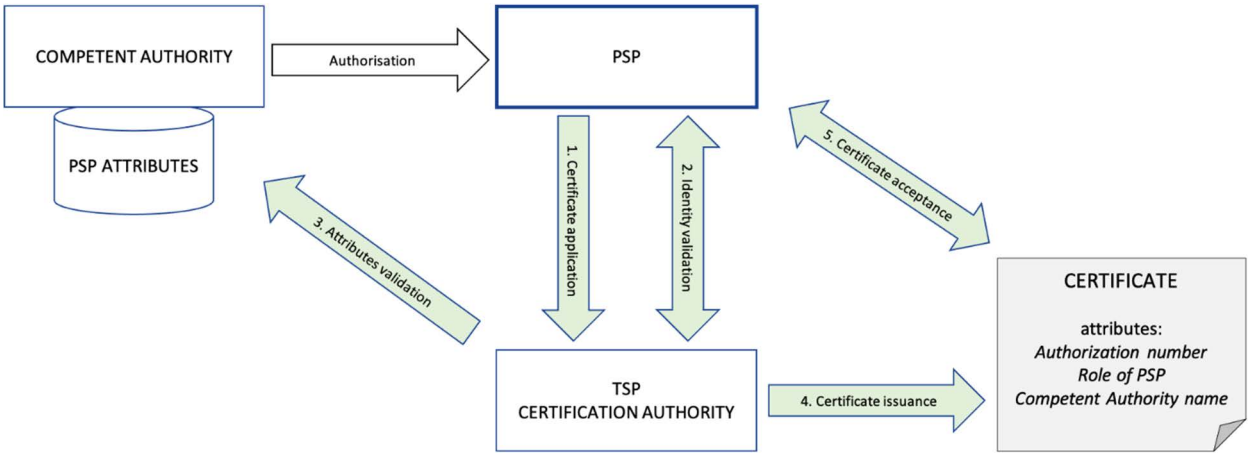


Figure 1: Registration and certificate issuance

Before the issuance process can start, the PSP needs to be registered by a Competent Authority and all relevant information needs to be available to TSP for validation:

1) The PSP submits the certificate application and provides all necessary documentation containing Open Banking Attributes to the regulated Trust Service Provider (TSP).

NOTE 1: Under EU PSD2 regulated Trust Service Provider (TSP) means granted qualified status according to eIDAS [i.1].

2) The TSP performs identity validation as described in its certificate policy, which itself shall be compliant with the applicable Open Banking regulatory requirements.

3) The TSP validates Open Banking Attributes using information provided by the Competent Authority.

NOTE 2: Under EU PSD2 this includes national public registers, EBA PSD2 Register, EBA Credit Institution Register, other information authenticated by Competent Authority.

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

5) The TSP sends (e.g. via email) information about the issued certificate to the Competent Authority if that Competent Authority has requested this notification.

6) The PSP uses the certificate.

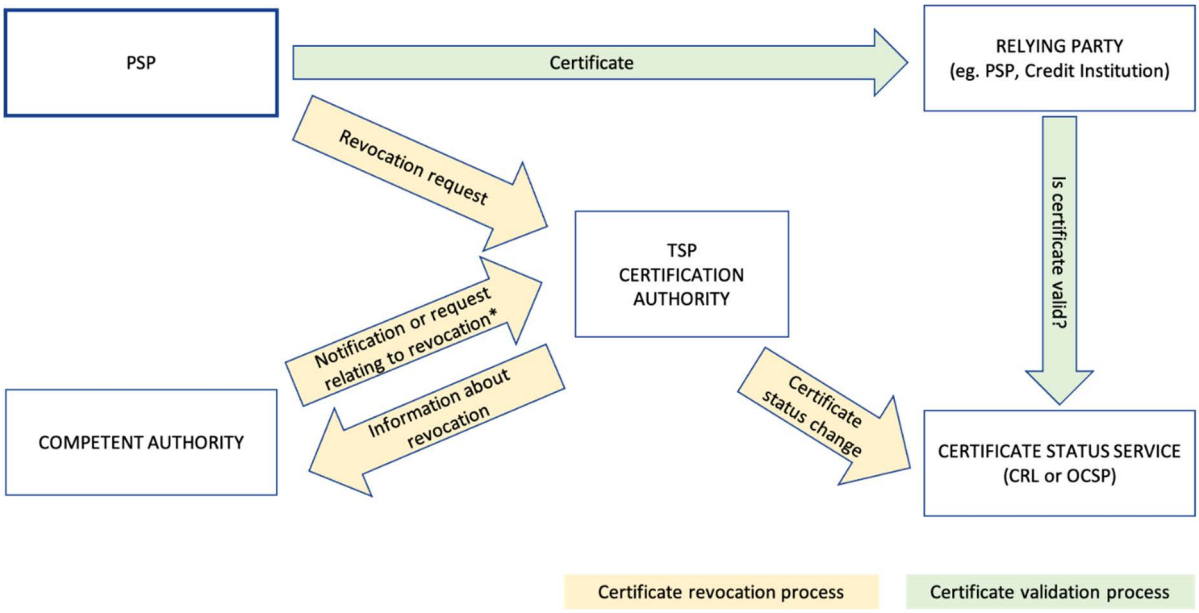
The Competent Authority is the authoritative source of Open Banking Attributes.

NOTE 3: According to Article 15 of EU 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 Competent Authorities. This information will be updated regularly in a timely manner as envisaged under Article 15(2) of EU PSD2 [i.2] and Articles 7(5) and 8(5) and (8) of the Regulatory Standards on the EBA Register under EU PSD2 [i.9]. According to the [i.9] the EBA PSD2 Register will contain copies of relevant records of each Competent Authorities' registers. The EBA PSD2 Register can be used instead of the Competent Authority public register as a source of authorization information for payment institutions and electronic money institutions. The EBA Credit Institution Register and the EBA PSD2 Register are two separate registers.

NOTE 4: It is suggested that Competent Authorities implement disclosure mechanisms to make registers available to facilitate the verification process of Open Banking entities by TSPs.

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 Competent Authority which has authorized or registered the payment service provider.



NOTE 1: Under EU PSD2 the list of Competent Authorities 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 2: The present document does not place any specific requirements on the Competent Authority regarding revocation.

Figure 2: Illustration of PSP Certificate validation and revocation

5 Certificate profile requirements

5.1 QCStatement for Open Banking

GEN-5.1-1: The Open Banking 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 Open Banking Attributes:

a) the role of the payment service provider as identified in clause 4.2;

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.

NOTE 1: Under EU PSD2 specific requirements are laid out in RTS [i.3] Article 34.

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 definition provided in the body of the present document, in case of discrepancy.

NOTE 2: 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 specific attributes for Open Banking

5.2.1 Authorization Number or other recognized identifier for Open Banking

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

a) for website authentication certificate: as defined in clause 5.3;

b) for digital signatures: as defined in clause 5.4.

GEN-5.2.1-2: Void.

GEN-5.2.1-3: If an Authorization Number was issued by a Competent Authority the subject organizationIdentifier attribute should contain the Authorization Number encoded 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 Competent Authority country;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8));
- 2-8 character Competent Authority identifier without country code (A-Z uppercase only, no separator);
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- identifier (authorization number as specified by the Competent Authority. There are no restrictions on the characters used).

NOTE 1: Void.

NOTE 2: Under EU PSD2 the current list of Competent Authorities 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 a Competent Authority identifier (NCAId).

NOTE 3: Other types of identification such as trade registration number or tax identification number can be used instead of the authorization number.

NOTE 4: Under EU PSD2 - 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").

NOTE 5: In case of conflict with requirements in ETSI EN 319 412-1 [1], the semantics identifier "id-etsi-qcs-SemanticsId-Legal" specified in clause 5.1.4 of ETSI EN 319 412-1 [1] is not used outside the scope of EU PSD2.

GEN-5.2.1-4: If the encoding is not as defined in GEN 5.2.1-3 above another form of identity type shall be carried in organizationIdentifier encoded using the syntax identified by the legal person semantics identifier as defined in ETSI EN 319 412-1 [1], clause 5.1.4.

5.2.2 Roles of payment service provider

GEN-5.2.2-1: `RolesOfPSP` shall contain one or more roles or contain a single entry indicating that the role is unspecified. The roles shall be as declared by a Competent Authority via its public records for the subject PSP. Each role is represented by a role ASN.1 Object Identifier [6] and a name string.

GEN-5.2.2-2: If the certificate is issued for EU PSD2 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: If the certificate is issued for EU PSD2 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 5.2.2-3A: If the role is unspecified the role name shall be "Unspecified".

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

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) }

-- authorised role(s) is Unspecified within the certificate
id-psd2-role-psp-unspecified OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 0 }

-- 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 using Latin alphabet provided by the Competent Authority itself for purpose of identification in certificates.

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

NOTE 1: Under EU PSD2 the current list of Competent Authority Names in English provided by EBA is referenced in Annex D.

NOTE 2: A list of competent authority names collected from competent authorities around the world is referenced in Annex E.

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 Competent Authority country;
- hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
- 2-8 character Competent Authority 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 Competent Authority itself.

GEN-5.2.3-4: Competent Authority 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 3: 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 4: Under EU PSD2 the current list of Competent Authority Identifiers with country codes provided by EBA is referenced in Annex D. It is not expected that changes to a Competent Authority identifier would affect the validity of certificates already issued.

NOTE 5: If the certificate is issued for EU PSD2, NCAId represents the Competent Authority acting under EU PSD2.

NOTE 6: A list of competent authority names collected from competent authorities around the world is referenced in Annex E.

5.3 Profile Requirements for Certificate for TLS Authentication

GEN-5.3-1: If the certificate issued is for client/server TLS authentication then the requirements of ETSI EN 319 412-4 [4] shall apply, 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.

NOTE 2: Certificates issued for EU PSD2 are required to be Qualified Website Authentication Certificates (QWAC), hence the requirements in ETSI EN 319 412-5 [i.6] for qualified certificates also apply.

In addition:

GEN-5.3-2: The QCStatement for Open Banking 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 3: 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 bepresent*". 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 Profile Requirements for Certificates for Digital Signatures

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

NOTE 1: Certificates issued for EU PSD2 are required to be Qualified electronic Seal Certificates (QSealC) hence the requirements in ETSI EN 319 412-5 [i.6] for qualified certificates also apply.

NOTE 2: Certificate for electronic seal can be recognized as a certificate issued for legal persons.

In addition:

GEN-5.4-2: The QCStatement for Open Banking 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 for EU PSD2: 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 applicable to qualified website certificates 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: TSPs issuing certificates for EU PSD2 may use the following policy identifier to augment the policy requirements associated with policy identifier **QEVCP-w** or **QNCP-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 EU 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 1: 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].

NOTE 2: Prior to ETSI EN 319 411-2 [5] v1.5.1 QEVCP-w was referred to as QCP-w.

OVR-6.1-4: For TSPs issuing certificates for digital signatures not for EU PSD2: policy requirements relevant to certificates issued to legal persons defined for NCP shall be applied as specified in ETSI EN 319 411-1 [9].

NOTE 3: This requirement can be met by issuing QSealCs as defined in OVR-6.1-1 above.

OVR-6.1-5: For TSPs issuing certificates for website authentication not for EU PSD2 all policy requirements defined for NCP, OVCP or EVCP shall be applied as specified in ETSI EN 319 411-1 [9], including requirements for certificates issued to legal persons.

NOTE 4: This requirement can be met by issuing QWACs as defined in OVR-6.1-2 above.

OVR-6.1-6: The certificates used for Open Banking should be issued by TSPs which are audited by an auditor accredited to carry out audits against ETSI EN 319 411-1 [9] or ETSI EN 319 411-2 [5].

OVR-6.1-7: The requirements specified in CA/Browser Forum Baseline Requirements [i.8], clause 6.3.2 regarding certificate lifetime need not to be applied.

6.2 Additional policy requirements

6.2.1 Certificate profile

In addition to the applicable requirements specified in ETSI EN 319 411-1 [9] clause 6.1, the following shall apply:

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

NOTE: As required for EU PSD2 qualified certificates need also to conform to ETSI EN 319 411-2 [5].

6.2.2 Initial identity validation

In addition to the applicable requirements specified in ETSI EN 319 411-1 [9], clause 6.1 the following shall apply:

- **REG-6.2.2-1:** The TSP shall verify the Open Banking Attributes (see clauses 5.1 and 5.2) provided by the subject using authentic information from the Competent Authority (e.g. a national public register, EBA PSD2 Register, EBA Credit Institution Register, authenticated letter).

- **REG-6.2.2-2:** If the Competent Authority 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 319 411-1 [9], 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 Competent Authorities 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 Competent Authority served, for notifications from the Competent Authority about changes of relevant 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 Competent Authority and the 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 Competent Authority:

  - a shared secret if it was provided by the TSP to the Competent Authority for revocation;

  - a digital signature supported by a certificate issued to the Competent Authority by a TSP compliant with a policy according to ETSI EN 319 411-1 [9], ETSI EN 319 411-2 [5] or another certificate policy as accepted by the TSP.

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

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

NOTE 2: Under EU PSD2 a list of Competent Authorities 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 319 411-1 [9], 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 Competent Authority 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 certificate file.

NOTE: Under EU PSD2 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 319 411-1 [9], clause 6.3.6 the following shall apply:

- **REG-6.2.5-1:** Before certificate renewal the TSP shall repeat the verification of the Open Banking Attributes to be included in the certificate.

6.2.6 Certificate revocation

In addition to the applicable requirements specified in ETSI EN 319 411-1 [9], clause 6.3.9 the following shall apply:

- **REV-6.2.6-1:** The TSP shall allow the Competent Authority, as the owner of the Open Banking Attributes, to request certificate revocation following the procedure defined in the TSP's certificate policy or certificate practice statement. The procedure shall allow the Competent Authority 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 Competent Authority, then the TSP may decide to not take action. Based on an authentic request from a Competent Authority, 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 319 411-1 [9]):

  - 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 Competent Authority 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 Competent Authorities served, where a Competent Authority can submit authenticated revocation requests and other notifications relating to revocation.

- **REV-6.2.6-4:** If the Competent Authority as the owner of the Open Banking Attributes 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.

NOTE 2: As the notification is not specifically requesting revocation the certificate need not be revoke within 24 hours.

NOTE 3: 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 4: 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 5: Granting new PSP roles by the Competent Authority 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 Competent Authority identified in a revoked certificate then the TSP shall send to that email address information about the certificate revocation.

NOTE 6: Under EU PSD2 a list of Competent Authority 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) }

-- authorised role(s) is Unspecified within the certificate
id-psd2-role-psp-unspecified OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 0 }

-- 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 EU 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 electronic Seal Certificate (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): EU PSD2 specific 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;
- Open Banking 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 Open Banking Attributes in qualified certificates

Qualified certificates contain Open Banking 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 Open Banking 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 Open Banking 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 Open Banking 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 mentioned 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 Open Banking 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): EU PSD2 specific 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.

Annex E (informative): Global list of NCA Identifiers provided by Open Banking Europe

A list of NCA abbreviations collected from competent authorities around the world is published [i.17] on the Open Banking Europe website at: https://www.openbanking.exchange/obe/global-national-competent-authority-codes-list/.

Annex F (informative): Change History

Date	Version	Information about changes
May 2018	V1.1.1	Publication.
July 2018	V1.1.2	Correction to ASN.1 errors.
November 2018	V1.2.1	Added guidance on the interface between QTSPs and PSD2 National Competent Authorities for validating PSD2 specific certificate attributes and supporting revocation.
March 2019	V1.3.1	Removed dependency of requirement of CA/B Forum guidelines where this conflicts with ETSI standards. Updated wording.
June 2019	V1.3.2	Changed identifier of the Competent Authority HR-CNB to HR-HNB in Annex D.
November 2019	V1.4.1	Document contains following changes: • Annex D related to the latest publication by EBA of the list of NCA's identifiers and names. • Procedure for handling future minor and major changes in documents published by EBA, according to QTSP responsibilities and validity of certificates with old identifiers and names in transition period. • Clarifications relating to recent information published by EBA.
March 2021	V1.5.1	Making document applicable to open banking outside the EU but based on national regulatory environments equivalent to PSD2. • New definitions of Competent Authority and Open Banking. • Competent Authority identifier defines regulatory environment. • Authorization Number can be used for institutions outside of EU PSD2. • Outside EU PSD2 certificates need not to be qualified.
September 2022	V1.6.1	Added Annex E global list of NCA Identifiers provided by Open Banking Europe Update to OVR-6.1-3 to clarify that QCP-w-psd2 policy may be used to augment policies: QEVCP-w (was previously referred to as QCP-w) or the new EN 319 41-1-2 defined policy QNCP-w.

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
V1.5.1	April 2021	Publication
V1.6.1	November 2022	Publication