PRETA Open Banking Europe: eIDAS Qualified Certificates Under PSD2 Frequently Asked Questions

Open Banking Europe - providing collaborative services to support PSD2 XS2A, in partnership with the financial industry

Contents

1. About Open Banking Europe

1.1 Purpose

The revised Payment Services Directive (PSD2) came into force in January 2018. At this point, all regulated entities (Payment Service Providers) had to ensure that they individually comply with PSD2 and the Regulatory Technical Standards (RTS) set out by the European Banking Authority (EBA).

Many experts believe that the financial industry is expected to organise itself to make sure that the implemented solutions for PSD2 are interoperable.

PRETA Open Banking Europe has been launched to support Payment Service Providers (PSPs) and Third Party Providers (TPPs) in meeting the Access to Account (XS2A) requirements of PSD2.

1.2 History

PRETA S.A.S. was created in 2013 to develop and innovate market competitive services in digital payment and identity solutions. The company is a wholly-owned subsidiary of EBA CLEARING, a provider of pan-European payment solutions currently owned by 52 shareholder banks.

Following a series of stakeholder consultations that started in 2016 to determine industry requirements, PRETA launched Open Banking Europe to build a PSD2 Directory solution to support PSPs and TPPs in meeting the PSD2 XS2A requirements. A project was launched in September 2017, with a series of funding banks, and later service providers, and this document has been developed through the first half of 2018.

1.3 Audience

Open Banking Europe is aimed at the following audiences:

- Competent Authorities
- Payment Service Providers (PSPs), including:
  - Account Servicing Payment Services Providers (ASPSPs)
  - Third Party Providers (TPPs)
- Qualified Trust Service Providers (QTSPs)
- Directory & Access Support Service Providers

1.4 Disclaimer

The PRETA Open Banking Europe documentation does not contain an in-depth legal analysis of PSD2 and its associated regulations and standards. They are an attempt to summarise the regulatory requirements of PSD2 in a clear and simple way.

Whilst care has been taken to ensure that the information contained in this document is true and correct at the time of publication, there are still clarifications needed around PSD2's scope and implementation and this may impact on the accuracy of the information contained within this document.

As such, Open Banking Europe cannot guarantee the accuracy or reliability of any information contained within this document at the time of reading, or that it is suitable for your intended use.

2. About This Document

2.1 Scope

This document provides the answers to common questions about the use of Qualified certificates to support secure communications between payment services under PSD2 and their related Regulatory Technical Standards (RTS). The aim of this document is **NOT** to define how security works, but rather to explain which types of certificates are used, how to procure and validate them and the various operational and commercial processes.

2.2 Audience

This document is aimed at the following audiences:

- Account Servicing Payment Services Providers (ASPSPs)
- National Competent Authorities (NCAs)
- Third Party Providers (TPPs)

2.3 References

This document cites a number of sources. For links to these sources, please see the Bibliography on page 17. The key documents are:

- The Revised Payment Services Directive (PSD2) - Directive (EU) 2015/2366)
- Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS)
- The RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2)

2.4 Terminology

Certificate
Public key certificate, as defined in ITU-T X.509.

eIDAS
Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market.

ETSI
The European Telecommunications Standards Institute.

CA/Browser Forum or CAB Forum
The Certification Authority & Browser Forum.

CRL
Certificate Revocation List, as defined in ITU-T X.509.

IETF
The Internet Engineering Task Force.

OCSP
Online Certificate Status Protocol, as defined in RFC 6960.

PSP
Payment Service Provider, as defined in PSD2.

PSD2
The Revised Payment Services Directive (EU) 2015/2366 on payment services in the internal market.

QSealC
Qualified Certificate for Electronic Seals, as defined in eIDAS.

QTSP
Qualified Trust Service Provider meeting the requirements at Qualified level, as defined in eIDAS.

Qualified Certificate
Public key certificate meeting the requirements at Qualified level, as defined in eIDAS.

QWAC
Qualified Certificate for Website Authentication, as defined in eIDAS.

RTS
Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

TLS
Transport Layer Security, as defined in IETF RFC 5246 (v1.2) or IETF RFC 8446 (v1.3).

XS2A
Access to Account.

3. Certificates

3.1 What are certificates?

Certificates are widely used as a means for identifying persons, systems, or organisations and are an important part of securing modern day communications. A certificate binds an identity to a cryptographic key which can be used to secure communications.

Certificates are issued by an organisation trusted to assure the identity of the owner of a key. This trusted organisation is commonly called a Certification Authority, or under European Union (EU) legislation it is called a Trust Service Provider (TSP).

The security of certificates is based on a special type of cryptography, called Public Key Cryptography, and the infrastructure used by a TSP to manage certificates is called a Public Key Infrastructure (PKI).

Certificates are based around a common set of recognised standards which are adapted to meet the requirements of a community of users.

3.2 What are Qualified Certificates?

Qualified Certificates are certificates aimed at enhancing trust in electronic transactions across the EU, regulated through Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS). eIDAS defines requirements on Qualified Certificates, and the Qualified Trust Service Providers (QTSP) that issue them, which ensure their trustworthiness. The operation of QTSPs is supervised by a national supervisory body to assure that these requirements are met.

The 'Qualified' status gives a certificate a legal and trust mark which indicates that it meets specific technical and security requirements.

Most of the requirements of the eIDAS regulation are aligned with generally accepted standards and practices. However, these are enhanced to include technical features specific to Qualified Certificate such as being automatically identifiable as Qualified.

A list of QTSPs recognised by a supervisory body as meeting the requirements of eIDAS is issued by each nation. Each national list is referenced through a list of lists issued by the European Commission. All the lists can be viewed through a Trusted List Browser or automatically processed through the List of Trusted Lists.

3.3 Why are eIDAS Certificates relevant to PSD2?

> *Article 34*
>
> **Certificates**
>
> 1. For the purpose of identification, as referred to in Article 30(1)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 or for website authentication as referred to in Article 3(39) of that Regulation.

Article 34 of the RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2) says that eIDAS certificates will be used for the identification of Payment Service Providers (PSPs), and specifically references two of the existing types of Qualified Certificate as follows:

- Qualified Certificate for Electronic Seals (QSealC)
- Qualified Certificate for Website Authentication (QWAC)

Article 34 of the RTS also places additional requirements on the content of a PSD2 Qualified Certificate. In particular:

- Article 34.2 requires that the certificate contains the PSP Authorisation Number issued by the National Competent Authority (NCA),
- Article 34.3 requires that the certificate includes the role(s) of the PSP,
- and the name of the Competent Authority where the PSP is registered.

Certificates and related infrastructures are a key part of securing modern day communications and it is assumed that they will be used for securing the PSP interfaces, i.e. Application Programming Interfaces (APIs), in PSD2.

Having said that, while the interface must be secure and based on international standards, there is no explicit legal requirement that certificates or Qualified Certificates are used for securing communications where identification is not a concern.

3.4 Is there a Standard for the new PSD2 data fields?

ETSI has specified a recommended Standard - ETSI TS 119 495 - for Qualified Certificates to meet the requirements of the RTS. This standard builds on other ETSI Standards for QTSPs and Qualified Certificates, in particular ETSI EN 319 411-2 on policy requirements for TSPs issuing qualified Certificates and ETSI TS 119 412-1, ETSI EN 319 412-3, ETSI EN 319 412-4 and ETSI EN 319 412-5 on certificate profiles.

3.5 When is it appropriate to use QSealCs or QWACs?

Article 34 of the RTS has generated some questions, as it allows QSealCs or QWACs to be used for identification, leading some to believe there is a choice. In fact, QSealCs and QWACs are designed to be used with different security protocols which have different features.

QSealCs are used with Advanced (or Qualified) Electronic Seals, based on using Public Key cryptography (commonly called Digital Signatures), such as is defined in ETSI PAdES, CAdES or XAdES standards[1] to protect application data blocks. QWACs are used with a Transport Layer Security Protocol such as is defined in IETF RFC 5246 or IETF RFC 8446 to protect data in peer-to peer communications.

In particular, the following features of the protection may be provided using the certificates with Electronic Seals or Transport Layer Security:

Feature	QSealC with Electronic Seal	QWAC with Transport Layer Security
Where is protection applied?	During communication and in storage	Just during communication
Is data protected when passed through intermediary?	Protection applies end-to-end, even if passed through intermediary	Only applied to direct peer-to-peer communications
What data is protected?	Specific data block	All data passing through channel
Evidential value?	Advanced or Qualified Electronic Seals are specifically recognised under eIDAS	No specific recognition
Type of protection?	Authentication and integrity	Authentication, integrity and confidentiality

In general, there are advantages with the type of protection that may be afforded with either type of certificate. Paragraph 14 of the Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC identifies three basic choices:

1. Parallel use of QWACs and QSealCs: this will allow PSPs to identify themselves to each other and

[1] Currently, no specific standard exists for use of JSON Web Signatures as eIDAS Advanced Electronic Signatures, although IETF RFC 7515 provides a general structure for such signatures.

communicate securely using QWACs with a Transport Layer Security Protocol and ensure that the application data submitted originates from the PSP identified in the QSealC using Advanced or Qualified Electronic Seals.

2. Use of QWACs only: this will allow PSPs to identify themselves and communicate securely using QWACs with a Transport Layer Security Protocol but cannot provide evidence that the data submitted originates from the PSP identified.
3. Use of QSealCs with an additional element that ensures secure communication: this will allow PSPs to identify themselves to each other but cannot ensure confidentiality during the communication session. Therefore, an additional element that ensures secure communication should be used in order to comply with the requirements of Article 35(1) of the RTS, such as a Transport Layer Security Protocol using general commercially available (i.e. not Qualified) certificates.

In summary, whether a QSealC or QWAC is used is not an arbitrary choice but depends on the way the Certificates are used within the design of the interface.

3.6 Where can I get further guidance on the link between eIDAS & PSD2?

Further guidance on the use of eIDAS Qualified Certificates for PSD2 is given in:

- Annex B of ETSI TS 119 495
- PRETA Open Banking Europe: Understanding Internet Security & eIDAS Certificates
- The Euro Retail Payments Board (ERPB): Final Report of the ERPB Working Group on Payment Initiation Services
- Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC

A resource page can also be found at the link below, including a list of QTSPs that are offering PSD2 certificates.

4. Certificate Validation

4.1 What do we mean by certificate validation?

When a party uses a PSD2 Qualified Certificate to identify another party, they will want to check that the certificate is 'valid'. This check generally involves checks on the following aspects of a certificate:

What to Check	How to Check it
That the Trust Service Provider (TSP) is Qualified	EU Trusted Lists
That the certificate is technically correct and has not expired	A raft of standards and practices in current use today
That the certificate is Qualified	*QCStatement* marking certificate as Qualified, etc.
That the certificate contains the required PSD2 information	Checking against ETSI TS 119 495
That the certificate has not been revoked since it was issued	Certificate Revocation List (CRL) / Online Certificate Status Protocol (OCSP) checks

Note these checks confirm the validity of the certificate and the identity authentication supported by the certificate. However, it does not necessarily confirm that the authorisations for the PSP are up-to-date (please see 5.4 Are PSP Authorisation & Roles updates synchronised with certificates? on page 14).

4.2 Where do I get the QTSP root certificates for certificate validation?

Before validating a certificate, it is necessary to have a list of trusted QTSPs and their 'root certificates' which will be used as the basis for validation checks.

Major software platforms often come with a pre-configured 'root certificate store' but this generally does **not** include those root certificates which are recognised as trusted QTSPs under the eIDAS regulation.

The EU provide the list of all QTSPs in the form of a trusted list which includes the root certificates required for validation.

Before validation is carried out this trusted list needs to be downloaded into any validation module and updated on a regular basis. Please see 4.9 How frequently should a certificate be validated? on page 12 for a discussion on the frequency of checking.

More information on trusted lists is available at:

https://ec.europa.eu/cefdigital/DSS/webapp-demo/doc/dss-documentation.html#_eu_trusted_lists_of_certification_service_providers

Providers of System/Browser Root Certificate Stores (for example, Microsoft, Google, Apple, Mozilla) do not currently support trusted lists. For more information, please see Appendix B: QWACs & the CA/Browser Forum on page 21.

4.3 What is the EU Trusted List?

A list of Qualified Trust Service Providers (QTSPs) recognised by a supervisory body as meeting the requirements of Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) is issued by each country.

Each national trusted list is then referenced through a List of Trusted Lists issued by the European

Commission (EC). The combined national lists as referenced through the EC List of Trusted Lists is referred to as the EU Trusted List.

All the lists (both the EU Trusted List and the national trusted lists) are XML documents which can automatically processed

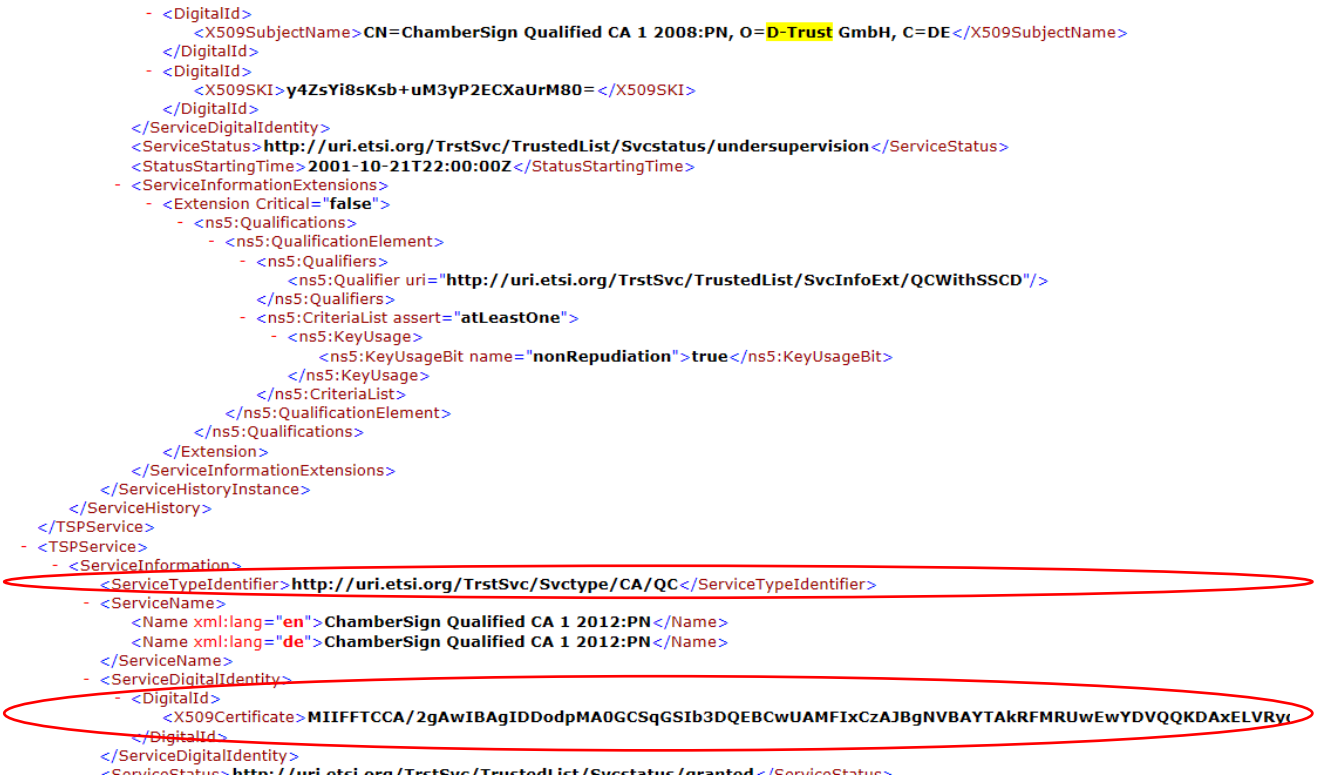
The EU Trusted List includes information for each trusted service a QTSP provides such as the service type (for example, issuing qualified certificates – Svctype/CA/QC[2]) and the QTSP's root certificate as used for verification (please see 4.2 Where do I get the QTSP root certificates for certificate validation? on page 9).

The EU Trusted List can be found at:

https://ec.europa.eu/information_society/policy/esignature/trusted-list/tl-mp.xml

Within the EU Trusted List, the **TSLLocation** tag contains the URL of each national trusted list. For example, here is the link to the German list:

The national list shows one or more records for each QTSP. In the example below (the German list which is found at https://www.nrca-ds.de/st/TSL-XML.xml) D-TRUST and one of their root certificates, which is found under the **x509Certificate** tag:



[2] Other "qualified" service types recognised under the eIDAS regulation include timestamping, signature/seal validation and signature/seal preservation. Further qualifiers to the service may indicate additional restrictions to the service (for example, only for QSealC or QWAC).

4.4 Can a certificate be accepted if the QTSP is no longer Qualified?

If a QTSP is no longer seen as meeting the requirements of the eIDAS regulation, then the QTSP will be removed from the national list of currently valid QTSPs and should only be used in validating historical information.

A QTSP is required (under the applicable ETSI Standards) to have a termination plan which, as far as possible, minimises the disruption resulting from termination of its service. This requirement includes the revocation handling for unexpired certificates and arrangements for the revocation status information to continue to be available following termination.

At the present time, there is commercial technology available to perform checks on whether a QTSP is still Qualified. However, this may not be readily integrated into the banks existing platforms, which may be problematic under circumstances where ASPSPs do not want to accept a certificate issued by a QTSP that is no longer operating.

4.5 How can a certificate's technical correctness be validated?

As with any certificate, the general validity of PSD2 Qualified Certificates can be checked using widely implemented standards for certificates, such as IETF RFC 5280. This includes checks on:

- The content of the certificate (e.g. certificate validity period),
- Whether the certificate can be validated against a known and trusted Certificate Issuer (a QTSP) (see 4.2 Where do I get the QTSP root certificates for certificate validation? on page 9), called certificate path validation, and
- That it has not been revoked.

As commercial technology is already available to perform these checks, there are no barriers to validating a PSD2 Qualified Certificate's technical correctness.

4.6 How can the Qualified status of a certificate be checked?

As well as checking that the certificate has really been issued by a QTSP, the certificate should declare itself as qualified in a QC statement.

Checking the QCStatement

The Annexes to the eIDAS regulation include specific requirements on Qualified Certificates. Most of these requirements are in line with general standards but includes the EU specific requirement for:

> *"(a) an indication, at least in a form suitable for automated processing, that the certificate has been issued as a qualified certificate for electronic signature;"*

This requirement is met by including a specific 'QCStatement' called **esi4-qcStatement-1** in the certificate which can be checked to ensure that the certificate is Qualified. **esi4-qcStatement-1** is defined in ETSI EN 319 412-5. Other specific requirements on the use of existing standard fields to meet the requirements of eIDAS are defined in:

- ETSI EN 319 412-4 for QWAC
- ETSI EN 319 412-3 for QSealC

Checking the presence of the **esi4-qcStatement-1** requires the use of certificate parsing tool to extract this information from a certificate. Such checking is a standardised procedure.

4.7 How can the fact that it is a PSD2 compliant certificate be validated?

The RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2) requires the Qualified Certificate to include the Authorisation Number or equivalent, and as well as the name of the National Competent Authority (NCA) and the role(s) granted to the Payment Service Provider (PSP).

These are carried in further *QCStatement* extensions to the certificate, as defined in ETSI TS 119 495. If this information is not present, then the certificate is not compliant with TS 119 495.

A certificate parsing tool is required to extract the PSD2 information from a certificate.

4.8 How can certificate revocation information be obtained?

Information on whether a certificate is no longer valid because it has been revoked following issuance is published either in a Certificate Revocation List (CRL) listing all the certificates that have been revoked, or on a per certificate basis using an Online Certificate Status Protocol (OCSP). The standards require that this revocation information is updated within 24 hours of a confirmed notification.

The revocation information for a specific certificate is readily accessible from the QTSP, given the information carried within a Qualified Certificate. In particular:

1. For QSealCs from QTSPs using CRLs, it is required that the certificate includes the CRL distribution point extension which points to a publicly available download for the CRL.
2. For QSealCs from QTSPs using OCSPs, it is required that the Certificate includes Authority Information Access extension with *accessLocation* pointing to the OCSP service.
3. For QWACs, which follow the rules of the Certification Authority & Browser Forum Extended Validation (for more information, please see Appendix B: QWACs & the CA/Browser Forum on page 21), it is required that the certificate includes either the CRL distribution point extension pointing to a publicly available download for the CRL, or Authority Information Access with *accessLocation* pointing to the OCSP service.

The use of OCSPs or CRLs for revocation status checking is commonly handled by commercial certificate validation software. Commercial technology is already in place to perform these checks, so this information can be easily obtained.

4.9 How frequently should a certificate be validated?

There is a significant overhead validating Qualified Certificates, particularly with regards checking external information on the revocation (see 4.8 How can certificate revocation information be obtained? above) and the EU Trusted List (see 4.6 How can the Qualified status of a certificate be checked? on page 11).

This overhead can be reduced by caching this information, but the use of cached information needs to be balanced against the risks. The following should be taken into account in considering any caching policy:

- Technical Correctness & PSD2 Formatting: this is unlikely to change during the life of a certificate.
- Certificate Expiry: A certificate includes an expiry date after which it is no longer valid.
- Trusted List: A certificate that is issued as Qualified will remain as Qualified for its lifetime, unless the QTSP loses its Qualified status, or a new QTSP may be added to the trusted list, in either case the EU Trusted Lists are updated (see 4.4 Can a certificate be accepted if the QTSP is no longer Qualified? on page 11).
- Revocation: the revocation information is regularly updated at least every 24 hours but can be quicker depending on the QTSPs practices, and as indicated by the ‘next update’ in the CRL or OCSP revocation information. Also, in some cases, a QTSP may make changes to revocation status immediately available without waiting for the next update.

In conclusion, an ASPSP will (probably) not download all the information needed to check a certificate validity for every transaction but must make a risk/cost based decision on how frequently or when to check against the latest download.

5. Qualified Certificates & National Competent Authority Registers

5.1 What is the NCA Registration Number?

All systems use identifiers to uniquely identify who is who in a system. In the consumer space, these can be email addresses, identity card numbers, or specially issued numbers or codes (such as your insurance policy number). In payments, these can be BICs, sort codes, or national clearing codes.

Within PSD2, Article 34 of the RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2) makes it clear that the number issued by the National Competent Authorities (NCAs) will be the identifier used.

Within Open Banking Europe (OBE), we call this the Unique Reference Number or URN.

These numbers are not standardised or checked for duplicates across countries. So, to be made unique, the country code and the code of the NCA are added together to create a Global Unique Reference Number (G-URN), formatted as follows:

- 2 character country code representing the NCA country
- Hyphen-minus
- 2-8 character NCA identifier
- Hyphen-minus
- Authorisation Number as specified by the NCA

For example:

PL-PFSA-1234567890

The above is the G-URN for a Polish Regulated Entity that is created by the Polish Financial Standard Authority with number '1234567890'.

As the Authorisation Number may contain non-Latin characters, for example, ' ' (space) or '-' (hyphen-minus), this will also be included in to the Global URN. For example:

MT-MFSA-A 12345 (note the space after the 'A')

19

5.2 What is the link between the NCA Register & the Registration Number in the certificate?

The Registration Number of a Payment Service Provider (PSP) is placed in the *organizationIdentifier* attribute of the **Subject Distinguished Name** field of its Qualified Certificate, as specified in Clause 5.2.1 of ETSI TS 119 495. This can be encoded in the certificate as a PSD2 Authorisation Number, using the encoding as specified.

This encoding of a PSD2 Authorisation Number includes the country code and identifier of the National Competent Authority (NCA). This information can be used to identify the relevant Register as listed in Appendix A: National Competent Authority (NCA) Registers

on page 19.

5.3 What are the PSP's Roles?

According to the RTS on CSC and SCA**,** there are four PSP Roles:

- Account Servicing
- Payment Initiation
- Account Information
- Issuing of Card-Based Payment Instruments

The Roles are derived from the NCA Registers which publish 'Services' or 'Authorisations', in line with the Services found in Annex 1 of PSD2.

The mapping from Services to Roles is as follows (as set out in the Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC):

a) *Account servicing – in accordance with Article 4(17) of PSD2, an 'ASPSP' means a payment service provider providing and maintaining a payment account for a payer. However, there is not a specific payment service corresponding to that role, but in almost all cases PSPs that should be able to provide and maintain payment accounts for PSUs are those that provide the payment services as referred to in points (1), (2) and/or (3) of Annex I to PSD2.*

b) *Payment initiation – this corresponds to payment initiation service as referred to in point (7) of Annex I to PSD2.*

c) *Account information – this corresponds to account information service as referred to in point (8) of Annex I to PSD2.*

d) *Issuing of card-based payment instruments – this corresponds to the issuing of payment instruments and/or acquiring of payment transactions as referred to in point (5) of Annex I to PSD2.*

ETSI TS 119 495 describes how these Roles are encoded into the certificates.

5.4 Are PSP Authorisation & Roles updates synchronised with certificates?

A Qualified Certificate contains information on a PSP which is checked by the Qualified Trust Service Provider (QTSP) when the certificate is first issued. If the status of the PSP changes such that any authorisations are revoked, the QTSP will not revoke the certificate unless informed of the change by the NCA responsible for PSD2 or the PSP itself. Thus, it is possible for certificates to remain valid, even if the authorisations implied by the certificate are no longer valid, although the identity authenticated through the certificate is still correct.

Thus, considering that the NCA is not obliged to inform the QTSP and the QTSP is not obliged to check the NCA register, it is clear that although we can trust the certificates for identification, in the case that an NCA has withdrawn a license and the certificate has not yet been revoked, there is a period when the roles in the certificate will not be accurate. In the case that any party wishes to check the up to date role of a PSP, then they must look at the Home NCA of that entity.

5.5 Is NCA revocation notification harmonised between the NCAs & QTSPs?

There is no obligation on NCAs to revoke certificates if the role assigned to a PSP is revoked.

ETSI TS 119 495 obliges the QTSP to provide an interface to enable the NCA to revoke certificates issued based on its Register but there are no assurances that this will be done.

Considering the above and despite the aspirations of the Regulators, it is not guaranteed that the possession of a Qualified eIDAS Certificate means that the entity holding that certificate is still regulated. This issue is best documented in The Euro Retail Payments Board (ERPB): Final Report of the ERPB Working Group on Payment Initiation Services published in November 2017.

It is for this reason, that most ASPSPs are choosing to separately check that the entity identified in the certificate is (still) authorised for the role that they are trying to perform, by checking in the NCA Register, or in a consolidated operational directory.

6. Commercial Relations with QTSPs & Procuring Certificates

6.1 Who issues PSD2 Qualified Certificates?

While there are many Qualified Trust Service Providers (QTSPs) that can issue the right kind of certificates, not all of them will want to do so. It is a commercial choice of the QTSP.

Open Banking Europe (OBE) has issued a list of QTSPs which declare themselves ready and willing to meet the requirements of PSD2 Qualified Certificates for financial institutions.

https://www.openbankingeurope.eu/qtsps-and-eidas/

6.2 What are the liability models of QTSPs?

Article 13.2 of Regulation No 910/2014 on electronic identification and trust services (eIDAS) states:

> *"…trust service providers [including QTSPs] shall be liable for damage caused intentionally or negligently to any natural or legal person due to a failure to comply with the obligations under this Regulation"*

However, in Article 13.2 this can be overridden by limitations stated by the QTSP in the Certificate Policy. A QTSP will make generally available any limitations of liability which should be checked by any party relying on the certificate in its terms and conditions. This is generally defined within the context of national legislation and specified in the Certificate Policy.

6.3 Where can Test PSD2 Certificates be obtained?

The RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2) makes it a requirement that Account Servicing Payment Service Providers (ASPSPs) must provide a Test Facility. There is an expectation that this Test Facility will include demonstrations of the security mechanisms that will be used in the live environment, and that parties will want to become familiar with the type of certificates that will be used in production. This generates a demand for test certificates.

Some QTSPs are already offering test certificates. Contact the QTSPs (see ????) for further information.

7. Other

7.1 Are there any character restrictions on PSD2 Authorisation Numbers?

The encoding used for the PSD2 Authorisation Number as held in a Qualified Certificate (see clause 5.2.1 of ETSI TS 119 495) does not place any restrictions on the characters that may be used in a PSD2 Authorisation Number.

7.2 Are there any PSP requirements on Private Key management?

There are no specific hardware requirements for the management of Private Keys related to Qualified Certificates for Website Authentication (QWACs) used for Transport Layer Security (TSL) nor when using Qualified Certificates for Electronic Seals (QSealCs).

However, Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) defines two levels of Electronic Seal, either of which may be used with a QSealC, but one places further requirements on the management of the private key:

- Advanced Electronic Seals, which can be met using a QSealC without any requirements on the use of a specialised device to hold the private key.
- Qualified Electronic Seals which requires the private key to be held within a device certified as meeting requirements as specified in the eIDAS regulation, referred to a Qualified Signature/Seal Creation Device (QSCD). Qualified Electronic Seals are given specific legal presumption under the eIDAS Regulation.

Some countries may expect Payment Service Providers (PSPs) to use Qualified Electronic Seals with a certified Qualified Signature/Seal Creation Device. A list of notified QSCDs is available at:

https://ec.europa.eu/futurium/en/content/compilation-member-states-notification-sscds-and-qscds

Advice on the most relevant device should be obtained from the eIDAS National Supervisory Body or QTSP.

7.3 Will a Web Browser accept a PSD2 QWAC?

Certificates issued for PSD2 are aimed primarily at security of communications between PSPs. However, the PSPs may want to use the same certificate to secure access to customers which are likely to be using a Web Browser.

Currently, there is some uncertainty whether the rules applied by Web Browsers will allow this. For more information, please see Appendix B: QWACs & the CA/Browser Forum

on page 21.

7.4 Does an ASPSP need to use a qualified certificate?

The best practice is to always use a Qualified Certificate.

Credit Institutions or other PSPs must use a Qualified Certificate when they are playing the role of an Account Information Service Provider (AISP), Payment Initiation Service Provider (PISP) or Payment Instrument Issuer Service Provider (PIISP).

When playing the role of an ASPSP they must use certificates for mutual authentication, and it is **recommended** that this certificate is qualified, but it is not a regulatory requirement. This question is handled specifically in Article 20 of the Opinion of the European Banking Authority on the use of eIDAS certificates under the RTS on SCA and CSC.

Bibliography

More information about can be found at the following sources:

- Certification Authority & Browser Forum (CA/Browser Forum)
  https://cabforum.org/
- ETSI EN 319 122: CAdES digital signatures
  https://www.etsi.org/standards-search#page=1&search=EN319122
- ETSI EN 319 132: XAdES digital signatures
  https://www.etsi.org/standards-search#page=1&search=EN319132
- ETSI EN 319 142: PAdES digital signatures
  https://www.etsi.org/standards-search#page=1&search=EN319142
- ETSI TS 119 412-1: Certificate Profiles; Part 1: Overview and common data structures
  https://www.etsi.org/standards-search#page=1&search=TS119412-1
- ETSI EN 319 412-3: Certificate Profiles; Part 3: Certificate profile for certificates issued to legal persons
  https://www.etsi.org/standards-search#page=1&search=EN319412-3
- ETSI EN 319 412-4: Certificate Profiles; Part 4: Certificate profile for web site certificates
  https://www.etsi.org/standards-search#page=1&search=EN319412-4
- ETSI EN 319 412-5: Certificate Profiles; Part 5: QCStatements
  https://www.etsi.org/standards-search#page=1&search=EN319412-5
- ETSI TS 119 495: Qualified Certificate Profiles and TSP Policy
  Requirements under the payment services Directive (EU) 2015/2366
  https://www.etsi.org/standards-search#page=1&search=TS119495
- The Euro Retail Payments Board (ERPB): Final Report
  of the ERPB Working Group on Payment Initiation Services
  https://www.ecb.europa.eu/paym/retpaym/shared/pdf/8th-ERPB-meeting/PIS_working_group_report.pdf
- The European Technology Standards Institute (ETSI)
  http://www.etsi.org/
- IETF RFC 5246: The Transport Layer Security (TSL) Protocol Version 1.2
  https://tools.ietf.org/html/rfc5246
- IETF RFC 5280: Internet X.509 Public Key Infrastructure
  Certificate and Certificate Revocation List (CRL) Profile
  https://www.ietf.org/rfc/rfc5280.txt
- IETF RFC 8446: The Transport Layer Security (TSL) Protocol Version 1.3
  https://tools.ietf.org/html/rfc8446
- ITU-T X.509: Information technology - Open Systems Interconnection -
  The Directory: Public-key and attribute certificate frameworks
  https://www.itu.int/rec/T-REC-X.509
- Opinion of the European Banking Authority on the use
  of eIDAS certificates under the RTS on SCA and CSC
  https://eba.europa.eu/documents/10180/2137845/EBA+Opinion+on
  +the+use+of+eIDAS+certificates+under+the+RTS+on+SCACSC.pdf
- PRETA Open Banking Europe: Understanding Internet Security & eIDAS Certificates
  https://www.openbankingeurope.eu/wp-content/uploads/2018/09/PRETA-OBE-MG-
  001-003-PSD2-XS2A-Understanding-Internet-Security-eIDAS-Certificates-Guide.pdf

- Regulation (EU) No 910/2014 of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) http://data.europa.eu/eli/reg/2014/910/oj
- The Revised Payment Services Directive (PSD2 - Directive (EU) 2015/2366) http://eur-lex.europa.eu/eli/dir/2015/2366/oj
- The RTS for Strong Customer Authentication & Common Secure Communications Under PSD2 https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32018R0389

Appendices

Appendix A: National Competent Authority (NCA) Registers

Country	National Competent Authority	Link
AT	Financial Market Authority (FMA)	https://www.fma.gv.at/en/search-company-database/
BE	National Bank of Belgium (NBB)	https://www.nbb.be/fr/supervision-financiere/controle-prudentiel/domaines-de-controle/etablissements-de-paiement-et-5?l=fr
BG	Financial Supervision Commission (FSC)	http://www.fsc.bg/en/supervised-entities/lists/
HR	Hrvatska Narodna Banka (HNB)	https://www.hnb.hr/en/core-functions/supervision/list-of-credit-institutions
CY	Central Bank of Cyprus (CBC)	https://www.centralbank.cy/en/licensing-supervision
CZ	Czech National Bank (CNB)	https://apl.cnb.cz/apljerrsdad/JERRS.WEB09.DIRECT_FIND?p_lang=en
DE	Bundesanstalt für Finanzdienstleistungsaufsicht (BaFin)	https://portal.mvp.bafin.de/database/ZahlInstInfo/
DK	Finanstilsynet (FSA)	https://vut.finanstilsynet.dk/en/Tal-og-fakta/Virksomheder-under-tilsyn/VUT-database.aspx
EE	Finantsinspektsioon (FSA)	https://www.fi.ee/index.php?id=593
ES	Banco de Espana (BDE)	http://app.bde.es/ren/app/GetData?CFG=ConsultaTipos.xml&TipoFormato=XSL&Paginate=OPEN&HIST=N
FI	Finanssivalvonta (FIN-FSA)	http://www.fin-fsa.fi/en/About_us/Supervised/Pages/supervisedentities.aspx
FR	Autorité de Contrôle Prudentiel (ACPR) "Regafi"	https://www.regafi.fr/spip.php?page=results&type=advanced&id_secteur=1&lang=fr&denomination=&siren=&cib=&bic=&nom=&siren_agent=&num=&cat=21-TBR07&retrait=0
GB	Financial Conduct Authority (FCA)	https://register.fca.org.uk/
GR	Bank Of Greece	https://www.bankofgreece.gr/Pages/en/Supervision/SupervisedInstitutions/default.aspx
HU	Magyar Nemzeti Bank (MNB)	https://www.mnb.hu/en/supervision/licensing-and-institution-oversight/market-participants/search-of-market-participants
IE	Central Bank of Ireland (CBI)	http://registers.centralbank.ie/DownloadsPage.aspx
IS	Fjármálaeftirlitið (FME)	https://en.fme.is/supervision/supervised-entities/
IT	Banca d'Italia	https://infostat.bancaditalia.it/giava-inquiry-public/flex/Giava/GIAVAFEInquiry.html#
LI	Finanzmarktaufsicht Liechtenstein (FMA)	http://register.fma-li.li/
LT	Bank of Lithuania (LB)	https://www.lb.lt/en/sfi-financial-market-participants?market=1
LU	Commission de Surveillance du SecteurFinancier (CSSF)	https://www.cssf.lu/entites-surveillees

Country	National Competent Authority	Link
LV	Finansu un Kapital Tirgus Komisija (FKTK)	http://www.fktk.lv/en/market/payment-institutions/authorized-payment-institution.html
MT	Malta Financial Services Authority (MFSA)	https://www.mfsa.com.mt/pages/licenceholders.aspx
NL	De Nederlandsche Bank (DNB)	https://www.dnb.nl/en/supervision/public-register/index.jsp
NO	Finanstilsynet (FSA)	https://www.finanstilsynet.no/en/finanstilsynets-registry/
PL	Komisja Nadzoru Finansowego (KNF)	https://www.knf.gov.pl/en/ENTITIES/entities_search
PT	Banco De Portugal	https://www.bportugal.pt/en/entidades-autorizadas
RO	Banca Nationala a Romaniei (BNR)	http://www.bnro.ro/NBR-Public-Registers-1701.aspx
SE	Finansinspektionen (FI)	https://www.fi.se/sv/vara-register/foretagsregistret/
SK	Narodna Banka Slovenska (NBS)	https://subjekty.nbs.sk/?ll=en
SI	Banka Slovenije (BSI)	https://www.bsi.si/en/financial-stability/banking-system-supervision/supervisory-disclosure

Appendix B: QWACs & the CA/Browser Forum

A group of Web Browsers and Certificate Issuers, called the Certification Authority & Browser Forum (CA/Browser Forum or CABF), formed a community to develop guidelines for the issuance and management of publicly trusted certificates. This group is international and includes some European Qualified Trust Service Providers (QTSPs) who also issue PSD2 Qualified Certificates for Website Authentication (QWACs). The main aim of these guidelines is for suppliers of Web Browser software (Google, Microsoft, Apple, and Mozilla) to establish criteria for acceptance of Website Authentication Certificates by Web Browsers.

Before use of QWACs for securing PSD2 communications was envisaged, it was expected that the use of QWACs overlapped with that of the CA/Browser Forum guidelines with security of Web-browser to Website communications being the primary use case. Thus, the general standard for QWACs issued by the European Telecommunications Standards Institute (ETSI), as referenced in the ETSI PSD2 Standard TS 119 495, included requirements from the CA/Browser Forum guidelines.

The ETSI requirements for QSealCs do not include any requirements which are impacted by the CA/Browser Forum guidelines.

The CA/Browser Forum issued two guidelines: 'Baseline' which establishes a baseline for any certificate to be used by Web Browsers, and 'Extended Validation' (EV) which add additional requirements to ensure the validity of the identity held in Website certificates. The CA/Browser Forum EV Guideline requirements were included in ETSI standards for QWACs.

With the extension of the ETSI requirements for QWACs in TS 119 495 to include the PSD2 Authorisation Number as required by the RTS for Strong Customer Authentication and Common and Secure Communications Under PSD2 (RTS SCA/CSC for PSD2), ETSI added a requirement for an additional field (referred to as *organizationIdentifier*) to carry the PSD2 Authorisation Number or equivalent as required for Credit Institutions. This was in line with the approach already taken to carry the Registration Number in a QSealC and believed to be in line with the requirements stated in the CA/Browser Forum EV Guidelines.

Following further discussions with the CA/Browser Forum about the ETSI use of *organizationIdentifier*, it became clear that some CA/Browser Forum members considered the relevant text to be ambiguous and further clarification of the current text in the CA/Browser Forum EV Guidelines was considered necessary to address the ETSI approach. Thus, ETSI and CA/Browser Forum members are in discussion how to update the CA/Browser Forum EV Guidelines to encompass the use of *organizationIdentifier* in TS 119 495.

In considering future alignment of the ETSI PSD2 QWAC Standard and the CA/Browser Forum EV Guidelines, the following is noted:

1. PSD2 QWACs and EV certificates (i.e. certificates issued according to the CA/Browser Forum EV Guidelines) are for different purposes:
   - PSD2 QWACs are aimed at securing PSP to PSP communications.
   - EV certificates are aimed at securing communications between Web Browsers and Websites.
2. The acceptance of PSD2 QWACs and EV Certificates is governed by different bodies:
   - The acceptability of PSD2 QWAC is decided by eIDAS national supervisory bodies.
   - The acceptance of EV certificates is decided by the suppliers of Web Browser software.

Alignment between ETSI TS 119 495 and the CA/Browser Forum EV Guidelines has benefits to both Payment Service Providers (PSPs) and QTSPs in widening the applicability of such certificates. It allows the same certificate to be used both for securing Web Browser access to the public-facing Website of PSPs (as standardised by the CA/Browser Forum) and to secure PSP to PSP communications. However, if this is not possible, then the ETSI Standard can be updated to make it clear that the existing ETSI requirements for carrying PSD2 related information has precedence over any requirements stated in the EV Guidelines. Such a change would not impact the ability of QWACs to be applied to PSD2.