ETSI TS 119 495 V0.0.0c (2017-10)

Electronic Signatures and Infrastructures (ESI);

Sector Specific Requirements;

Qualified Certificate Profiles and TSP Policy Requirements under the payment services Directive 2015/2366/EU;

The TS (ETSI Technical Specification) is the preferred deliverable when the document contains normative provisions and short time to "market", validation and maintenance are essential.

A TS may later be converted to an ES or an EN, or be used to publish the contents of a draft ES being sent for vote or a draft EN being sent for Public Enquiry or vote.

** The guidance text (green) shall be removed when no longer needed or   
the skeleton without guidance text also available via the editHelp! website should be used.**

**Additional Editor comments and guidance text (red) shall be removed when no longer needed.**

**All text highlighted needed to be reviewed, deleted or/and changed.**

<

**TECHNICAL SPECIFICATION**

Reference

DTS/ESI-0019495

Keywords

<keywords>

e-commerce, electronic signature, extended validation certificate, public key, security,

trust services, payments

***ETSI***

650 Route des Lucioles

F-06921 Sophia Antipolis Cedex - FRANCE

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

Siret N° 348 623 562 00017 - NAF 742 C

Association à but non lucratif enregistrée à la

Sous-préfecture de Grasse (06) N° 7803/88

***Important notice***

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

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

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

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

***Copyright Notification***

No part may be reproduced or utilized in any form or by any means, electronic or mechanical, including photocopying and microfilm except as authorized by written permission of ETSI.

The content of the PDF version shall not be modified without the written authorization of ETSI.

The copyright and the foregoing restriction extend to reproduction in all media.

© ETSI yyyy.

All rights reserved.

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

# Copyrights on page 2

This paragraph should be used for deliverables processed before WG/TB approval and used in meetings.

Reproduction is only permitted for the purpose of standardization work undertaken within ETSI.  
The copyright and the foregoing restriction extend to reproduction in all media.

Contents

*Copyrights on page 2* 4

Intellectual Property Rights 6

Foreword 6

Modal verbs terminology 6

Introduction 6

1 Scope 8

2 References 8

2.1 Normative references 8

2.2 Informative references 9

3 Definitions, symbols and abbreviations 9

3.1 Definitions 9

3.2 Abbreviations 9

4 Certificates supporting PSD2 10

4.1 General concept certificates supporting PSD2 10

5 General certificate profile requirements 12

5.1 PSD2 QCStatement 12

5.2 Encoding PSD2 specific attributes 13

5.2.1 Authorisation number 13

5.2.2 Role of payment service provider 13

5.2.3 Name of the competent authority 14

5.3 Requirements for QWACs Profile 14

5.4 Requirements for Electronic Seal Certificates Profile 14

6 Policy requirements 15

6.1 General policy requirements 15

6.2 Additional policy requirements 15

6.2.2 Initial identity validation 15

6.2.3 Identification and authentication for revocation requests 16

6.2.4 Certificate acceptance 16

6.2.5 Certificate renewal 17

6.2.6 Certificate revocation and suspension 17

Annex A (normative): ASN.1 Declaration 18

Annex B informative: Certificates supporting PSD2 – clarification of the context 20

History 22

# Intellectual Property Rights

Essential patents

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

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

Trademarks

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

# Foreword

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

# Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the [ETSI Drafting Rules](https://portal.etsi.org/Services/editHelp!/Howtostart/ETSIDraftingRules.aspx) (Verbal forms for the expression of provisions).

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

# Introduction

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

EBA RTS Regulatory Technical Standards [i.3] on strong customer authentication and secure communication are key to achieving the objective of the PSD2 of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union. EBA RTS defines requirements on qualified certificates for Web Site authentication and qualified certificates for electronic seal for communication among payment and bank account information institutions.

# 1 Scope

The present document:

1. Profiles of qualified certificates for electronic seals and web sites for payment service providers meeting the requirements of the PSD2 Regulatory Technical Standards (RTS) [i.3] for providing evidence with legal assumption of a transaction, identification and authentication of the communicating parties and securing communications. Communicating parties may be Payment Initiation Service Provides, Account Information Service Providers, Payment Instrument Issuer Payment Service Provider and Account Servicing Payment Service Provider. These profiles will be based on: ETSI EN 319 412-1 [1], ETSI EN 319 412-3 [2], ETSI EN 319 412-4 [3], ETSI EN 319 412-5 [4]
2. Extends TSP policy requirements for management (including verification and revocation) of additional certificate attributes as required by above profiles. These policy requirements will extend the requirements in: ETSI EN 319 411-1 [5] and EN 319 411-2 [6].

# 2 References

## 2.1 Normative references

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

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

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

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

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

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

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

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

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

[6] 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

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

## 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] EBA RTS Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2)

[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

# 3 Definitions, symbols and abbreviations

## 3.1 Definitions

For the purposes of the present document, the terms and definitions given in PSD2 [i.2], in ETSI EN 319 412-1 [1], in ETSI EN 319 411-2 [6] and the following apply.

**third party provider:** Payment Initiation Service Provider or Account Information Service Provider according to PSD2 [i.2]

## 3.2 Abbreviations

For the purposes of the present document, the abbreviations given in ETSI EN 319 412-1 [1], in ETSI EN 319 411-2 [6] and the following apply.

<Check if necessary in standard, and delete if not or single usage long form proffered>

PSD2 – Payment Services Directive 2 – Directive (EU) 2015/2366 [i.2]

RTS – EBA Regulatory Technical Standards [i.3]

MSCA – Member State Competent Authority

ASPSP – Account Servicing Payment Service Provider (e.g. a Bank)

PISP - Payment Initiation Service Provider

PIISP - Payment Instrument Issuer Payment Service Provider

AISP - Account Information Service Provider

TPP – third party provider

PSU – Payment Service User (e.g. a Bank Customer)

SCA – Strong Customer Authentication

CSC – Common Secure Communications

XS2A - Access to Account (services for PISP & AISP)

CA/B – Certification Authorities / Browser Forum

ICANN – Internet Corporation for Assigned Names and Numbers

QTSP – Qualified Trust Service Provider

QSealC – Qualified Electronic Seal Certificate

QWAC – Qualified Website Authentication Certificate

OCSP - Online Certificate Status Protocol

CRL - Certificate Revocation List

TLS Transport Layer Security (replaces SSL – secure socket layer)

# 4 Certificates supporting PSD2

## 4.1 General concept certificates supporting PSD2

RTS [i.3] require that payment service providers ensure the confidentiality and the integrity of the personalised security credentials of the payment service user.

For this purpose, payment service providers are required to rely on qualified certificates for electronic seals or for website authentication.

For the purpose of this RTS [i.3], the registration number as referred to in the official records in accordance Annex III (C) of Regulation (EU) No 910/2014 [i.1] is the authorisation number of the payment service provider issuing card-based payment instruments the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of PSD2 [i.2] or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU [i.4] in accordance with Article 20 of that Directive.

According to PSD2 [i.2] MCSA approves or reject authorisation of TPPs and ASPSPs. If authorisation is granted MCSA issues authorisation number and publishes that information in Member State public register. MCSA also approves or rejects passport of TPPs from other Members States, already registered in their home country MSCA. Information about passport is published in public registry in home country of TPP.

Figure 1 presents general concept of registration and certificate issuance. Qualified certificate contains authorisation number of TPP or ASPSP available in public registry and issued by Member State Competent Authority (MSCA).

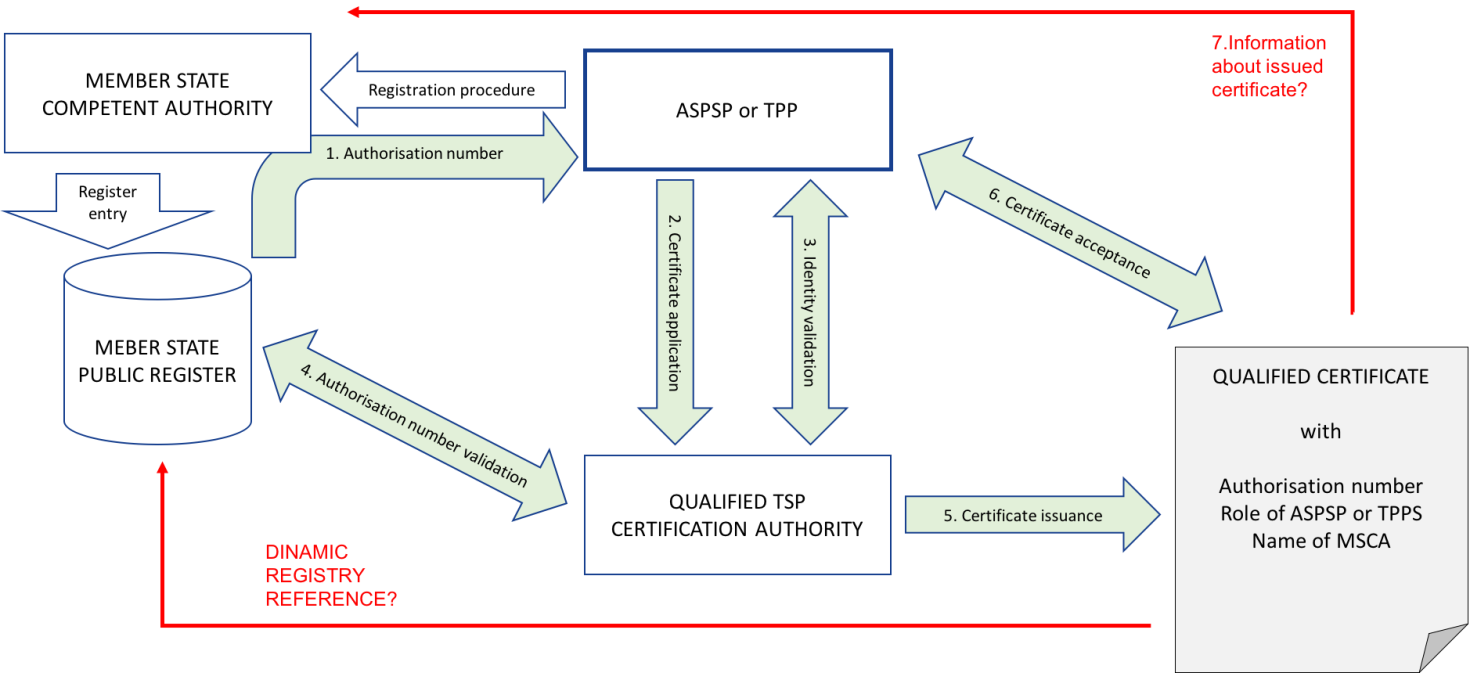


Figure 1 TPP/ASPSP Registration and certificate issuance

1. Certificate issuance process starts when authorisation number is available in public registry to ASPSP or TPP.
2. ASPSP or TPP starts with certificate application and provides all necessary documentation to Qualified Trust Service Provider (QTSP).
3. QTSP provides Identity Validation required by policy.
4. QTSP provides authorisation number validation required by policy.
5. Issued certificate comprise profile requirements.
6. ASPSP or TPP accepts certificate.
7. MSCA is informed by QTSP? ASPSP/TPP about issued certificate (issuer, number, profile)

Red arrows in Figure 1- to be changed or deleted and for decision if dynamic link as URI can be present in certificate. And to be decided point 7 – how to inform MCSA about certificate acceptance.

Figure 2 presents general concept for certificate validation and revocation. Validation process is based on certificate status service. Revocation request can origin form the certificate subject or from MSCA. If MCSA Name is included in the certificate QTSP revokes certificate when MCSA is identified in revocation request.

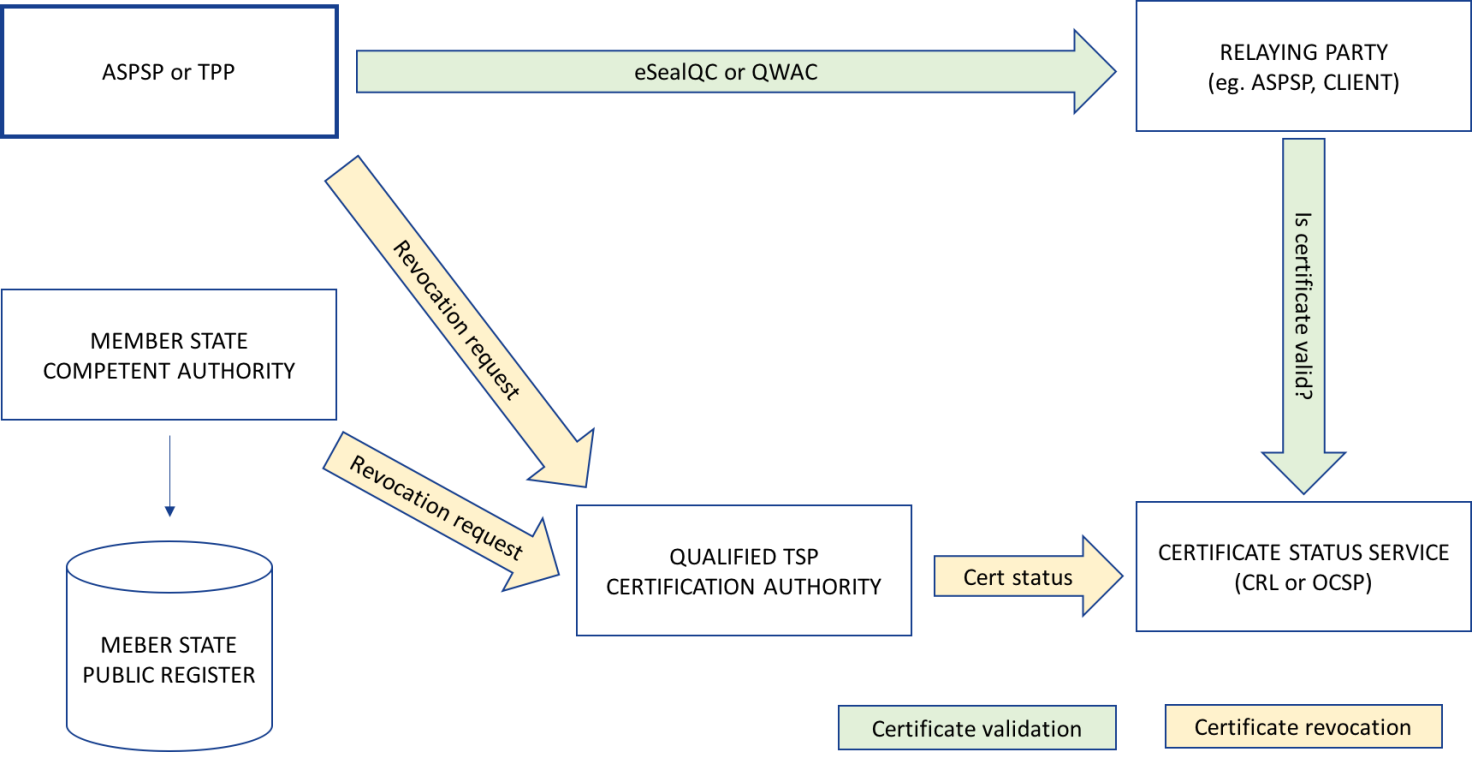


Figure 2 TPP/ASPSP Certificate validation and revocation

# 5 General certificate profile requirements

## 5.1 PSD2 QCStatement

BASING ON RTS European Commission Draft version: 24 May 2017

The PSD2 QC statement shall be a qcStatement extension as specified in clause 3.2.6 of IETF RFC 3739 [2].

This QCstatement contains the following PSD2 specific certificate attributes as required by RTS [i.3] article 34:

Editor comment: To be decided if authorisation number is part of QCstatement or Domain Name

1. authorisation number granted by MCSA and published in the public registry
2. the role of the payment service provider, which maybe one or more of the following:
   1. an account servicing payment service provider;
   2. a payment initiation service provider;
   3. an account information service provider;
   4. a payment service provider issuing card-based payment instruments.
3. the name of the competent authorities where the payment service provider is registered.

The syntax of the defined statements shall comply with ASN.1 [7]. The complete ASN.1 module for all defined statements shall be as provided in Annex A; it takes precedence over the ASN.1 definitions provided in the body of the present document, in case of discrepancy.

Syntax:

[TO BE DEFINED]

## 5.2 Encoding PSD2 specific attributes

### 5.2.1 Authorisation number

The encoding of authorisation number is defined in following clauses:

authorisation number for QWACs serialNumber (see clause 5.3)

for QSealCs organizationIdentifier (see clause 5.3)

[TO BE DONE]

* EDITOR PROPOSAL “PSD" as 3-character legal person identity type reference
* EXAMPLE1: PSDFR-41513244A – means certificate issued for PSP where authorisation number 41513244A was issued by French MCSA
* EXAMPLE2: PSDES-BDE-3DFD21 – means certificate issued for PSP where authorisation number 41513244A was issued by Spanish MCSA Banco de España (but identifier after first hyphen-minus is decided by Spanish numbering system)

*For information from: ETSI EN 319 412-1 V1.1.1 (2016-02)*

*When the legal person semantics identifier is included, any present organizationIdentifier attribute in the subject field shall contain information using the following structure in the presented order:*

* ***3 character legal person identity type reference;***
* *2 character ISO 3166 country code;*
* *hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and*
* *identifier (according to country and identity type reference).*

*The three initial characters shall have one of the following defined values:*

1. *"VAT" for identification based on a national value added tax identification number.*
2. *"NTR" for identification based on an identifier from a national trade register. Or*
3. ***Two characters according to local definition within the specified country and name registration authority, identifying a national scheme that is considered appropriate for national and European level, followed by the character ":" (colon).***

### 5.2.2 Role of payment service provider

The role of PSP shall be as follows:

[TO BE DONE]

??? roles naming required/ to be constructed

### 5.2.3 Name of the competent authority

The MCSA name shall be as follows:

[TO BE DONE]

??? MCSA naming/dictionary/registry required

<http://ec.europa.eu/internal_market/payments/docs/framework/transposition/authorisation_supervision_en.pdf>

## 5.3 Requirements for QWACs Profile

If certificate issued is for Website Authentication (QWAC) than the requirements EN 319 412-4 [3] shall apply.

In addition, the PSD2 [i.2] specific attributes shall be included as specified in 5.1

The serialNumber within Subject’s Distinguished Name shall be authorisation number as defined in RTS [i.3] article 34. Article number may be changed in final RTS version. If authorisation number is part of QCStatement whole paragraph to be deleted.

*To be deleted:*

*The requirements for the certificate contents for QWACs are as specified in [CA/B EV] clause 9.2 (as referenced from EN 319 412-4), with additional attributes relating to the qualified status. This includes:*

*i. Subject Organization Name Field: the legal person identity*

*ii. Subject Alternative Name Extension: the (DNS) domain name (or set of domain names) of the web site.*

*The domain name may also be held in the Common Name field although this is “deprecated”. Only a single domain name can be held in the Common Name.*

*iii. Subject Business Category: This shall be one of "Private Organization", "Government Entity", "Business Entity", or "Non-Commercial Entity". (see [CA/B EV] 9.2.4).*

*iv. Subject Jurisdiction: country, state or other locality information.*

*v. Subject Registration Number: Registration (or similar) Number assigned to the Subject by the Incorporating or Registration Agency in its Jurisdiction of Incorporation or Registration, as appropriate.. This is held in the serialNumber field (note this is different from requirement for QSealC).*

*vi. Optional Subject Physical Address of Place of Business.*

*vii. Other attributes are allowed but shall be checked by the CA. See CA/B EV clause 9.2.8.*

*Specific requirements for PSD2 attributes are to be addressed separately based on input from PSD2 experts.*

## 5.4 Requirements for Electronic Seal Certificates Profile

If certificate issued is for QSealCs than the requirements EN 319 412-3 [?] shall apply.

In addition, the PSD2 specific attributes shall be included as specified in 5.1

The organizationIdentifier within Subject’s Distinguished Name shall be authorisation number as defined in RTS [i.3] article 34 Article number may be changed in final RTS version. If authorisation number is part of QCStatement whole paragraph to be deleted.

*To be deleted:*

*The requirements for the certificate contents for QSealCs are as specified in EN 319 412-3. The following attributes are required as part of the subject name. Additional attributes are required relating to the qualified status.*

*i. countryName: the country in which the subject (legal person) is established.*

*ii. organizationName: the full registered name of the subject (legal person)*

*iii. organizationIdentifier: an identification of the subject organization different from the organization name. Certificates may include one or more semantics identifiers as specified in clause 5 of ETSI EN 319 412-1.*

*iv. commonName: a name commonly used by the subject to represent itself. This name need not be an exact match of the fully registered organization name.*

*The DNS name could optionally be carried in the Subject Alternative Name Extension as for QWACs but generally this is not included.*

*Specific requirements for PSD2 attributes are to be addressed separately based on input from PSD2 experts.*

.

# 6 Policy requirements

## 6.1 General policy requirements

The requirements for verification of attributes in QWACs are mostly covered by CA/B EV section 11. EN 319 411 parts 1 and 2 clause 6.2.2 includes a few additional requirements.

The requirements for verification of attributes in QSealCs are covered by EN 319 411 parts 1 [5] and 2 [6] clause 6.2.2.

For TSPs issuing QSealCs (QCP-l) policy requirements shall be applied as specified in EN 319 411-2 [6]

For TSPs issuing QWACs (QCP-w) policy requirements shall be applied as specified in EN 319 411-2 [6]

Other PSD2 attributes are also required to be verified but there are currently no specific procedures for how this is done. The TSP shall to check claimed PSD2 attributes with the PSD2 member state competent authority. It is planned to include requirements on the TSP to carry out checks in the work item referred to in the introduction.

## 6.2 Additional policy requirements

General policy requirements but not to build whole new policy requirements.

Conditional policy requirements depending if PSD2 attributes are present.

6.2.1 Certificate profile

In addition to requirements specified in ETSI EN 319 411-2 [6] clause 6.6.1 the profile requirements specified in 5.1 of this document shall apply.

### 6.2.2 Initial identity validation

In addition to requirements specified in ETSI EN 319 411-2 [6] clause 6.2.2 the following requirements apply:

Describe procedure for validation

ASPSP, PISP, PIISP, AISP Registration by TSP in MSCA – Member State Competent Authority

* Documents provided in certificate application
* MCSA identification
* Authentication number form public registry validation

### 6.2.3 Identification and authentication for revocation requests

In addition to requirements specified in ETSI EN 319 411-2 [6] clause 6.2.4 the following requirements apply:

The TSP shall document procedure for submission request for revocation from MSCAs.

**For discussion from 319411-1:**

**REV-6.2.4-01:** The TSP shall document as part of its CPS (see clause 5.2) the procedures for revocation of end user and CA certificates including:

1. **a)  Who can submit requests for revocation or reports of events which may indicate the need to revoke a certificate.**
2. b)  How they can be submitted.
3. c)  Any requirements for subsequent confirmation of requests for revocation or reports of events which may indicate the need to revoke a certificate.

EXAMPLE 1: Confirmation can be required from the subscriber if a compromise is reported by a third party.

1. **d)  Whether and for what reasons certificates can be suspended or revoked.**
2. e)  The mechanism used for distributing revocation status information.
3. f)  The maximum delay between receipt of a revocation or suspension request and the decision to change its status information being available to all relying parties.
4. g)  The maximum delay between the confirmation of the revocation of a certificate, or its suspension, to become effective and the actual change of the status information of this certificate being made available to relying parties.

### 6.2.4 Certificate acceptance

In addition to requirements to requirements specified in ETSI EN 319 411-2 [6] clause 6.3.4 the following requirements apply:

Procedure of dissemination information to MSCA (Registration body) with information about revocation procedure.

Alternatively, MSCA is informed by TPP or ASPSP after issuance but it needs to be included in certification policy subscriber obligations or in RTS.

After certificate acceptance MCSA shall be informed about issued certificate according to obligations stated in policy.

### 6.2.5 Certificate renewal

Note: The requirements identified in ETSI EN 319 411-2 [6], clause 6.3.6 apply.

The QTSP is required under eIDAS Article 24 & article 13 on liabilities to verify the content of the certificate on issuance and renewal. Under current practice QTSP is not responsible for collecting information on changes to the certificate content (except on registration). The subject is obliged to inform TSP of any changes. Other parties may inform QTSP of changes (e.g.PSD2 member state competent authority).

Additional requirements and checks in renewal process if needed. Information or validation from/to MCSA?

### 6.2.6 Certificate revocation and suspension

Note: The requirements identified in ETSI EN 319 411-2 [6], clause 6.3.9 apply.

Certificate revocation and suspension shall be in line with the documented procedure for submission request for revocation from MSCAs (see clause 6.2.3 of this document).

Revocation can be requested by MSCA. Additional requirements to QTSP.

QTSP once informed has to check the information is liable for revocation within 24 hours if appropriate. The QTSP practices defines what revocation requests are handled.

If any part of the information changes the certificate is revoked by the QTSP. The PSP may request a new certificate but this will need to go through registration checks.

Some non-critical changes (e.g. email address) do not force a revocation.

Additional requirements may needed to be added to EN 319 411-1 / 2 to handle revocation requests for PSD2.

Annex A (normative):  
ASN.1 Declaration

To be here…

Annex B informative:  
Certificates supporting PSD2 – clarification of the context

The main purpose of a digital certificate is to identify the owner of a public key (and the corresponding private key). Using the certificate it is possible to communicate securely with its owner. What "securely" means exactly depends on the type of certificate.

A website authentication certificate makes it possible to establish a Transport Layer Security (TLS) channel with the owner 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 communications channel ( which is 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.

An electronic seal is a digital signature of a legal person. A certificate for electronic seals makes it possible for the owner of the certificate to create electronic seals on any data. The digital signature technology guarantees the integrity, and authenticity of the signed/sealed data. This means that the person 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 seal provides strong evidence that given data is originated by the legal entity identified in the certificate.

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

Both QWACs and QSealCs are based on widely implemented technology. QWACs are derived from web sites 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 such as widely employed for document security, business to business and in modern banking networks.

In consequence:

• A qualified website authentication certificate (QWAC) should be used to establish a secure TLS channel to protect the communication (in the transport layer) from potential attackers on the network. The person or system connecting to the website can be sure who they are communicating with, but cannot prove this to third parties. Using QWAC does not give legally assumed evidence of a transaction.

• A qualified certificate for electronic seals (QSealC) should be used to protect the data or messages (in the application layer) from potential attackers during or after the communication. The electronic seal does not provide confidentiality (i.e. there is no encryption of application data). The person receiving the sealed data can be sure who sealed the data, and can also prove this to third parties even after the communication has ended. QSealC provides evidence of a transaction with legal assumption.

• A certificate can be either for website authentication or electronic seals, but not both. Therefore, these two types of certificates are not interchangeable.

.

# History

|  |  |  |
| --- | --- | --- |
| **Document history** | | |
| V0.0.0 | October 2017 | Early draft for PSD2 Workshop |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |