ETSI TS 119 495 V0.0.0e (2017-11)

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 General concepts 10

4.1 Use of Qualified Certificates 10

4.2 Roles 10

4.3 Payment Service Provider Authorisation and Passport 10

4.4 Authorisation Number 11

4.5 Registration and Certificate Issuance 11

4.6 Certificate Validation and Revocation 12

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 Roles of payment service provider 14

5.2.3 Name of the competent authority 14

5.3 Requirements for QWACs Profile 15

5.4 Requirements for Electronic Seal Certificates Profile 15

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 16

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 19

Annex C informative: Guidance for PSD2 Member States Competent Authorities 21

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%21/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 (commonly called eIDAS) defines requirements on specific types of certificates named "qualified certificates".

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

EBA RTS Regulatory Technical Standards [i.3] on strong customer authentication and secure communication are 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. EBA RTS defines requirements on qualified certificates (as defined in eIDAS ) for Web Site authentication and qualified certificates for electronic seal for communication among payment and bank account information institutions.

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

# 1 Scope

The present document:

1. 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].
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: EN 319 411-2 [4].

# 2 References

## 2.1 Normative references

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

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

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

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

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

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

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

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

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

## 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 [4] 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 [4] and the following apply.

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 Issuing Service Provider

AISP - Account Information Service Provider

TPP – third party provider

PSP – payment service provider

PSP\_IC – issuing card-based payment instruments

PSU – Payment Service User (e.g. a Bank Customer)  **[NOT USED IN STANDARD]**

SCA – Strong Customer Authentication **[NOT USED IN STANDARD]**

CSC – Common Secure Communications **[NOT USED IN STANDARD]**

XS2A - Access to Account (services for PISP & AISP) **[NOT USED IN STANDARD]**

CA/B – Certification Authorities / Browser Forum **[NOT USED IN STANDARD]**

ICANN – Internet Corporation for Assigned Names and Numbers **[NOT USED IN STANDARD]**

QTSP – Qualified Trust Service Provider

QSealC – Qualified Electronic Seal Certificate

QWAC – Qualified Website Authentication Certificate

OCSP - Online Certificate Status Protocol

CRL - Certificate Revocation List

# 4 General concepts

### 4.1 Use of Qualified Certificates

RTS [i.3] requires 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.

[NICK: Suggest place here some explanation of the different uses as in discussion document.]

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.

A certificate for electronic seals allows relaying party to validate authenticity and integrity of received data. The seal provides strong evidence that given data is originated by the legal entity identified in the certificate.

### 4.2 Roles

[NICK: Text required explaining different types of payment services, and payment service provider roles. Also, TPP and ASPS. Also, add that other roles can be used if recognised by a MSCA.]

There are four roles of payment service providers (PSP) specified in RTS [i.3]

* + 1. an account servicing payment service provider (ASPSP);
		2. a payment initiation service provider (PISP);
		3. an account information service provider (AISP);
		4. a payment service provider issuing card-based payment instruments (PSP\_IC).

Every payment service provider is authorised by MSCA to one or more roles.

PSPs which are authorised to at least one of PISP, AISP or PSP\_IC roles are recognised as third party providers (TPP).

### 4.3 Payment Service Provider Authorisation and Passport

According to PSD2 [i.2] the competent authority responsible for payment services in a member state (MSCA) approves or rejects authorisation of payment service providers, in particular TPPs and ASPSPs, in its own country. If authorisation is granted the MSCA issues an authorisation number and publishes that information in Member State public register. MSCA also approves or rejects operation of TPPs from other Members States in its own country,. The acceptance of a TPP in once Member State that is already registered in another Member State is called a passport. Information about passports is published in public registry in home country of TPP.

### 4.4 Authorisation Number

For identification, the RTS [i.3] requires the registration number used in a qualified certificate, as referred to in the official records in accordance Annex III (C) of Regulation (EU) No 910/2014 [i.1], to be the authorisation number of the payment service provider. This authorisation number is required to be 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.

### 4.5 Registration and Certificate Issuance

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

Before issuance process can start the ASPSP or TPP will need to be registered by MSCA and all relevant information available in public registry.

1. ASPSP or TPP starts with certificate application and provides all necessary documentation containing PSD2 specific attributes to Qualified Trust Service Provider (QTSP).
2. QTSP provides Identity Validation required by policy.
3. QTSP validates PSD2 specific attributes using information provided the MSCA (e.g. public registry, authenticated letter).
4. Issued certificate comprise profile requirements.
5. ASPSP or TPP accepts certificate.

### 4.6 Certificate Validation and Revocation

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 MSCA Name is included in the certificate QTSP revokes certificate when MSCA is identified in revocation request.



Figure 2 TPP/ASPSP Certificate validation and revocation

# 5 General certificate profile requirements

## 5.1 PSD2 QCStatement

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:

1. the role of the payment service provider, which maybe one or more of the following:
	* 1. an account servicing payment service provider (ASPSP);
		2. a payment initiation service provider (PISP);
		3. an account information service provider (AISP);
		4. a payment service provider issuing card-based payment instruments (PSP\_IC).
2. the name of the competent authorities where the payment service provider is registered.

The PSD2 QCStatement shall be a qcStatements extension as defined in IETF

RFC 3739 [2].

The syntax of the defined statement shall comply with ASN.1 [5]. The complete ASN.1 module for all defined statements shall be as provided in Annex A; it takes precedence over the ASN.1 definitions provided in the body of the present document, in case of discrepancy.

NOTE: This extension is not processed as part of IETF RFC 5280 [i.9] 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 ::=

{ 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,

 mSCAName MSCAName }

## 5.2 Encoding PSD2 specific attributes

### 5.2.1 Authorisation number

The authorisation number shall be placed in organizationIdentifier:

1. for QWACs: as defined in clause 5.3;
2. for QSealCs as defined in clause 5.4.

The authorisation number shall be encoded using the syntax identified by the legal person semantics identifier as defined in EN 319 412-1 [1] clause 5.1.4 extended for PSD2 authorisation identifier as follows:

Editor’s note: Change request required for EN 319 412-1 to include “PSD” as allowed identifier.

To decide how we can do it basing on national schemas – interoperability issues.

TALK to Sonia if we need change to standard.

Authorisation number shall contain information using the following structure in the presented order:

* “PSD” as 3 character legal person identity type reference;
* 2 character ISO 3166 country code representing the MSCA country;
* hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
* 2-8 character MSCA identifier (A-Z uppercase only, no separator)
* hyphen-minus "-" (0x2D (ASCII), U+002D (UTF-8)); and
* identifier (according to country and identity type reference).

EXAMPLE1: PSDES-BDE-3DFD21 – means certificate issued for TPP or ASPSP where authorisation number is 41513244A, authorisation was granted by Spanish MSCA Banco de España (identifier after first hyphen-minus is decided by Spanish numbering system)

NOTE: Any separator in MSCA identifier will be removed.

### 5.2.2 Roles of payment service provider

RolesOfPSP shall be one or more roles. A role shall be either as required by the RTS – (see clause 5.1) represented by the following object identifiers or a role object identifier registered by an organisation recognised by a MSCA.

Syntax:

RolesOfPSP ::= SEQUENCE OF RoleOfPSP

RoleOfPSP ::= OBJECT IDENTIFER

-- Object Identifier arc for roles of payment service providers

-- defined in the present document

etsi-psd2-roles OBJECT IDENTIFIER ::=

{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) }

-- Account Servicing Payment Service Provider (ASPSP) role

id-psd2-role-asps OBJECT IDENTIFIER ::=

{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 1 }

-- Payment Initiation Service Provider (PISP) role

id-psd2-role-pisp OBJECT IDENTIFIER ::=

{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 2 }

-- Account Information Service Provider (AISP) role

id-psd2-role-aisp OBJECT IDENTIFIER ::=

{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 3 }

**Editors note: [To decided beelow if we use PSP\_IC role – like in RTS or**

**PIISP - Payment Instrument Issuing Service Provider]**

-- Payment Service Provider issuing card-based payment instruments (PSP\_IC) role

id-psd2-role-pspic OBJECT IDENTIFIER ::=

{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) id-roles(1) 4 }

Editors note: There is no official naming reference for roles of PSP.

### 5.2.3 Name of the competent authority

The MSCAName shall be plane text name provided by MCSA itself for purpose of identification in certificates.

MSCAName ::= utf8String (SIZE (256))

Editors note: The name shall be as defined in a European register of MSCAs established under PSD2.

## 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:

1. The PSD2 QC Statement as identified in clause 5.1 shall be included in the certificate.
2. The organisationalIdentifier shall be present in the Subject’s Distinguished Name and encoded with legal person syntax as specified in clause 5.2.1.

## 5.4 Requirements for Electronic Seal Certificates Profile

If certificate issued is for QSealCs than the requirements EN 319 412-3 [2] shall apply.

In addition:

1. The PSD2 QC Statement as identified in clause 5.1 shall be included in the certificate.
2. The organisationalIdentifier shall be present in the Subject’s Distinguished Name and encoded with legal person syntax as specified in clause 5.2.1.

# 6 Policy requirements

## 6.1 General policy requirements

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

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

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

6.2.1 Certificate profile

In addition to requirements specified in ETSI EN 319 411-2 [4] 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 [4] clause 6.2.2 the following requirements apply:

 In addition:

1. The PSD2 QC Statement as identified in clause 5.1 shall be included in the certificate.
2. The organisationalIdentifier shall be present in the Subject’s Distinguished Name and encoded with legal person syntax as specified in clause 5.2.1.

QTSP shall apply rules for validation of authorisation number and roles against the official registry as specified by the MSCA.

NOTE: Validation based on MSCA registry rules is based on principles:

* TPP provides in certificate application information about claimed roles and other PSD2 attributes to be included in certificate.
* MSCA provides rules on how to validate TPP roles and other PSD2 specific attributes as defined in 5.1
* QTSP validates information provided by TPP against information in the official registry basing on rules provided by MSCA.

Note: Guidance for MSCAs to support QTSP validation of PSD2 specific attributes is given in Annex C.

### 6.2.3 Identification and authentication for revocation requests

In addition to requirements specified in ETSI EN 319 411-2 [4] clause 6.2.4 the following requirements apply:

The QTSP shall provide email address for notifications from MSCA about changes which can relevant information changes which affect validity of the certificate.

The QTSP shall document procedure for submission request for certificate revocation from MSCAs.

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

### 6.2.4 Certificate acceptance

In addition to requirements to requirements specified in ETSI EN 319 411-2 [4] clause 6.3.4 the following requirements apply:

If MSCA requires information about issued certificate after certificate acceptance MSCA shall be informed about issued certificate according to obligations stated in the QTSP policy.

Note: Guidance for MSCAs for maintaining PSD2 certificate information so that QTSPs can be made aware of to changes in PSD2 specific attributes is given in Annex C.

### 6.2.5 Certificate renewal

In addition to requirements to requirements specified in ETSI EN 319 411-2 [4], clause 6.3.6 apply:

QTSP shall apply rules for validation of authorisation number and roles against the official registry as specified by the MSCA before certificate renewal.

### 6.2.6 Certificate revocation and suspension

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

If MSCA as the owner of the information notifies the QTSP, that relevant information has changed which affects validity of the certificate, QTSP shall investigate and revoke if necessary.

If MSCA as the owner of the information requires certificate revocation, QTSP shall revoke certificate after MSCA identity validation.

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.

Annex C informative:
Guidance for PSD2 Member States Competent Authorities

[TO BE DONE]

Introduction

Describe some information what is this standard

Some information about QTSP obligations (context)

What information is in a certificate

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
* qualified certificates for website authentication.

Certificates are issued by Qualified Trust Service Providers (QTSPs) on request from payment service provider PSP. Any QTSP issuing certificates is allowed to issue certificates for PSPs if complies with this document.

PSD2 specific attributes in certificates

Certificates contain PSD2 Specific Attributes which are:

* authorisation number
* roles of PSP
* MSCA name

Validation of information about granted PSP authorisation number

QTSP before issuance of certificate validates PSD2 specific attributes in public registry.

Rules of validation may be provided by MSCA. If are provided information about these rules shall be available to QTSPs.

How MSCA can get information about issued certificate for PSP

MSCA can decide to request information about every issued certificate to PSP which has granted authorisation as PSP be this MSCA.

How MSCA can request to revoke issued certificate

MSCA may request revocation of certificate or certificates issued to PSP if information in registry is changed (e.g. status of PSP is withdrawn)

.

# History

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