ETSI TS 119 495 V1.1.2 (2018-07)

TECHNICAL SPECIFICATION

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

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

ETSI

Contents

Intellectual Property Rights

Essential patents

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

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

Trademarks

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

Foreword

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

Modal verbs terminology

In the present document "**shall**", "**shall not**", "**should**", "**should not**", "**may**", "**need not**", "**will**", "**will not**", "**can**" and "**cannot**" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

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

Introduction

Regulation (EU) No 910/2014 [i.1] of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (commonly called eIDAS) defines requirements on specific types of certificates named "qualified certificates".

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

The Commission Delegated Regulation with regard to Regulatory Technical Standards on strong customer authentication and secure communication (RTS henceforth) [i.3] is key to achieving the objective of the PSD2 (Directive (EU) 2015/2366 [i.2]) of enhancing consumer protection, promoting innovation and improving the security of payment services across the European Union. The RTS defines requirements on the use of qualified certificates (as defined in eIDAS) for website authentication and qualified certificates for electronic seal for communication among payment and bank account information institutions.

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

1 Scope

The present document:

1) Specifies profiles of qualified certificates for electronic seals and website authentication, to be used by payment service providers in order to meet the requirements of the PSD2 Regulatory Technical Standards (RTS) [i.3]. Certificates for electronic seals can be used for providing evidence with legal assumption of authenticity (including identification and authentication of the source) and integrity of a transaction. Certificates for website authentication can be used for identification and authentication of the communicating parties and securing communications. Communicating parties can be payment initiation service providers, account information service providers, payment service providers issuing card-based payment instruments or account servicing payment service providers. These profiles are based on ETSI EN 319 412-1 [1], ETSI EN 319 412-3 [2], ETSI EN 319 412-4 [3], IETF RFC 3739 [6] and ETSI EN 319 412-5 [i.6] (by indirect reference).

2) Specifies additional TSP policy requirements for the management (including verification and revocation) of additional certificate attributes as required by the above profiles. These policy requirements extend the requirements in ETSI EN 319 411-2 [4].

2 References

2.1 Normative references

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

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

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

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

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

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

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

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

[5] Recommendation ITU-T X.680-X.693 " Information Technology - Abstract Syntax Notation One (ASN.1) & ASN.1 encoding rules ".

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

[7] ISO 3166: "Codes for the representation of names of countries and their subdivisions".

2.2 Informative references

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

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

The following referenced documents are not necessary for the application of the present document but they assist the user with regard to a particular subject area.

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

[i.2] Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC.

[i.3] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (Text with EEA relevance).

[i.4] Directive 2013/36/EU of the European Parliament and of the Council of 26 June 2013 on access to the activity of credit institutions and the prudential supervision of credit institutions and investment firms, amending Directive 2002/87/EC and repealing Directives 2006/48/EC and 2006/49/EC.

[i.5] IETF RFC 5246: "The Transport Layer Security (TLS) Protocol Version 1.2".

[i.6] ETSI EN 319 412-5: "Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 5: QCStatements".

[i.7] IETF RFC 5280: "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

[i.8] CA/Browser Forum: "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates".

3 Definitions and abbreviations

3.1 Definitions

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

3.2 Abbreviations

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

CRL	Certificate Revocation List
NCA	National Competent Authority
OCSP	Online Certificate Status Protocol
PSD2	Payment Services Directive 2

NOTE: See Directive (EU) 2015/2366 [i.2].

PSP   Payment Service Provider
PSP_AI   Account Information Service Provider
PSP_AS   Account Servicing Payment Service Provider
PSP_IC   Payment Service Provider Issuing Card-based payment instruments
PSP_PI   Payment Initiation Service Provider
QSealC   Qualified electronic Seal Certificate
QWAC   Qualified Website Authentication Certificate
RTS   Regulatory Technical Standards

NOTE: See Regulation 2018/389 [i.3].

4   General concepts

4.1   Use of Qualified Certificates

RTS [i.3] Article 34.1 requires that, for the purpose of identification, payment service providers rely on qualified certificates for electronic seals or qualified certificates for website authentication.

A website authentication certificate makes it possible to establish a Transport Layer Security (TLS) channel with the subject of the certificate, which guarantees confidentiality, integrity and authenticity of all data transferred through the channel.

A certificate for electronic seals allows the relying party to validate the identity of the subject of the certificate, as well as the authenticity and integrity of the sealed data, and also prove it to third parties. The electronic seal provides strong evidence, capable of having legal effect, that given data is originated by the legal entity identified in the certificate.

NOTE: Regulation (EU) No 910/2014 [i.1] requires that TSPs issuing qualified certificates demonstrate that they
         meet the requirements for qualified trust service providers as per the regulation. ETSI standards
         referenced in the present document include those aimed at meeting these requirements. Granting a
         "qualified" status to a TSP is the decision of the national supervisory body.

4.2   Roles

According to RTS [i.3] the role of the payment service provider can be one or more of the following:

   i)   account servicing (PSP_AS);

   ii)   payment initiation (PSP_PI);

   iii)   account information (PSP_AI);

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

A PSP can be authorized by their national competent authority (NCA) to act in one or more PSD2 roles.

4.3   Payment Service Provider Authorizations and Services Passporting

According to PSD2 [i.2] and Credit Institutions Directive [i.4], the competent authority (NCA) responsible for payment services approves or rejects authorization of PSPs in their own country. If authorization is granted, the NCA issues an authorization number and publishes that information in its public register(s). Subject to NCA approval PSPs can exercise the right of establishment and freedom to provide services in other member states. This is called passporting. Information about passporting is published in the public register in the home country of the PSP.

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

4.4 Authorization Number

For identification, the RTS [i.3] requires the registration number used in a qualified certificate, as stated in the official records in accordance with Annex III item I of Regulation (EU) No 910/2014 [i.1], to be the authorization number of the payment service provider. This authorization number is required to be available in the National Competent Authority public register pursuant to Article 14 of PSD2 [i.2] or resulting from the notifications of every authorization granted under Article 8 of Directive 2013/36/EU [i.4] in accordance with Article 20 of that Directive.

4.5 Registration and Certificate Issuance

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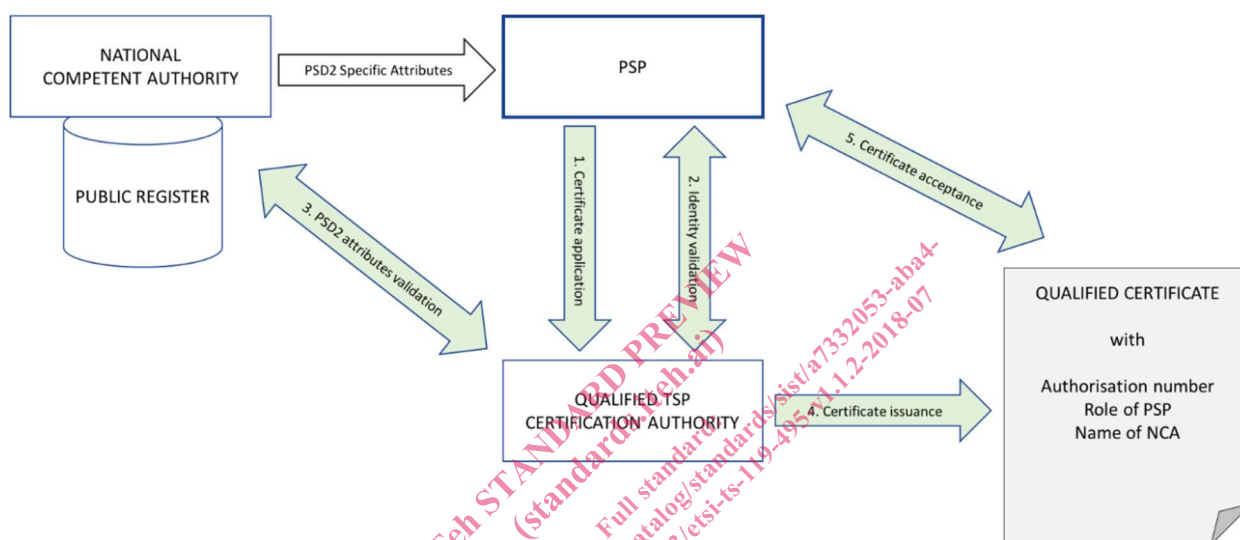

Figure 1: PSP Registration and certificate issuance

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

1) The PSP submits the certificate application and provides all necessary documentation containing PSD2 specific attributes to the Trust Service Provider (TSP) with granted qualified status according to eIDAS [i.1].

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

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

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

5) The PSP accepts the certificate.

4.6 Certificate Validation and Revocation

Figure 2 presents the general concept for certificate validation and revocation. Validation process is based on certificate status services provided by the TSP. A revocation request can originate from the certificate subject (PSP) or from the NCA which has issued the PSP authorization number contained in the certificate. TSP revokes the certificate based on a verifiably authentic revocation request.
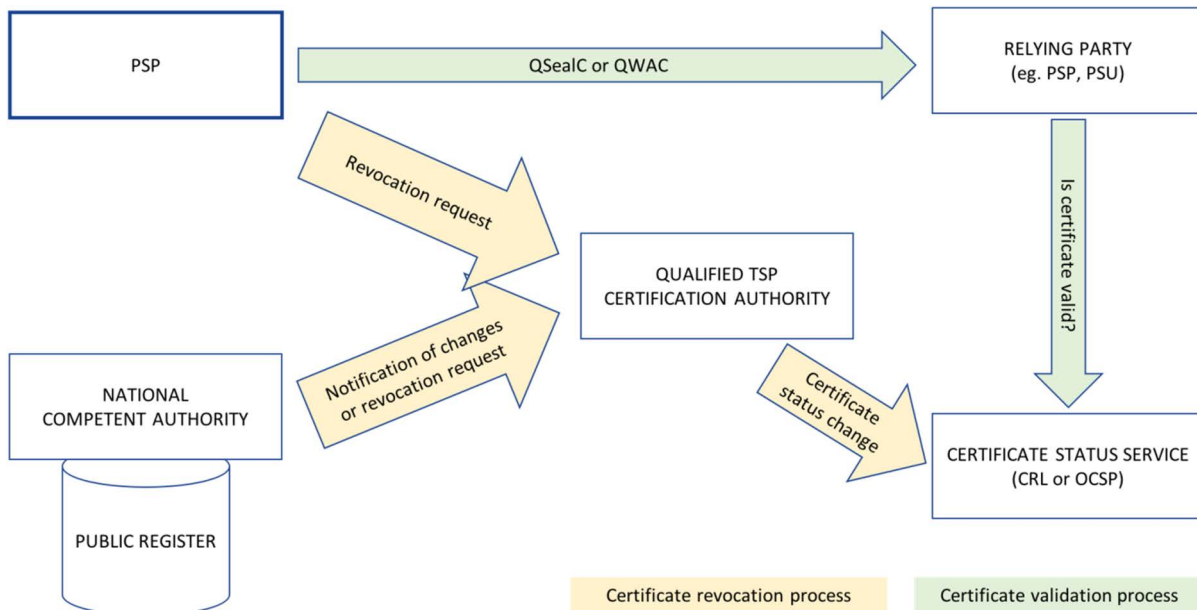
Figure 2: PSP Certificate validation and revocation

5 Certificate profile requirements

5.1 PSD2 QCStatement

GEN-5.1-1: The PSD2 specific attributes shall be included in a QCStatement within the qcStatements extension as specified in clause 3.2.6 of IETF RFC 3739 [6].

GEN-5.1-2: This Qcstatement shall contain the following PSD2 specific certificate attributes as required by RTS [i.3] article 34:

a) the role of the payment service provider, which maybe one or more of the following:

   i) account servicing (PSP_AS);

   ii) payment initiation (PSP_PI);

   iii) account information (PSP_AI);

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

b) the name of the competent authority where the payment service provider is registered. This is provided in two forms: the full name string (NCAName) in English and an abbreviated unique identifier (NCAId). See clause 5.2.3 for further details.

GEN-5.1-3: The syntax of the defined statement shall comply with ASN.1 [5]. The complete ASN.1 module for all defined statements shall be as provided in Annex A; it takes precedence over the ASN.1 definitions provided in the body of the present document, in case of discrepancy.

NOTE: This extension is not processed as part of IETF RFC 5280 [i.7] path validation and there are no security implications with accepting a certificate in a system that cannot parse this extension.

Syntax:

```
etsi-psd2-qcStatement QC-STATEMENT ::= {SYNTAX PSD2QcType IDENTIFIED BY id-etsi-psd2-qcStatement }

id-etsi-psd2-qcStatement OBJECT IDENTIFIER ::=
{ itu-t(0) identified-organization(4) etsi(0) psd2(19495) qcstatement(2) }


PSD2QcType ::= SEQUENCE{
```