Federal Office
for Information Security

Proposal for a Policy for the compliance of a qualified trust service provider with PSD2-specific requirements

PSD2-specific requirements defined by PSD2 and EBA RTS

Version 1.0, Draft 2, 05.05.2017

Document history

Version	Date	Editor	Description
0.1	12/12/16	SRC	First draft
0.2	8.03.2017	SRC	Document adopted due to remarks after BSI workshop (1.02.2017) and new version of the EBA RTS (final report)
1.0 Draft 1	10.04.2017	SRC	Document adopted due to remarks by BSI
1.0 Draft 2	05.05.2017	SRC	Document adopted due to remarks of Bundesbank

Federal Office for Information Security
Post Box 20 03 63
D-53133 Bonn
Phone: +49 22899 9582-0
E-Mail: payment@bsi.bund.de
Internet: https://www.bsi.bund.de
© Federal Office for Information Security 2018

Table of Contents

Figures

Tables

1 Management Summary

With [PSD2 2015] the European Union has published a new directive on payment services in the internal market. Among others [PSD2 2015] contains regulations of new services to be operated by so called third party payment service provider (TPP) on behalf of a payment service user (PSU). For operating the new services a TPP needs to access the account of the PSU which is usually managed by another PSP called the Account Servicing Payment Service Provider (ASPSP). An ASPSP has to provide an interface (called access to account (XS2A) interface) to its systems to be used by a TPP for necessary accesses regulated by [PSD2 2015]. Further requirements for the implementation and usage of this interface are defined by a Regulatory Technical Standard (RTS) to be published by the European Banking Authority (EBA).

Due to [PSD2 2015] a TPP shall identify itself every time it accesses an account using the interface provided by an ASPSP. Article 29 of [EBA RTS 2017] substantiates this by requiring that this identification shall rely on qualified certificates according to the regulation of the European Union on electronic identification and trust services for electronic transactions in the internal market ([eIDAS 2014]).

Qualified certificates are issued by a qualified Trust Service Provider (qualified TSP or QTSP). Supervision and qualification of a TSP as a QTSP are regulated by [eIDAS 2014]. In principal each QTSP may issue certificates needed by a PSP for its identification at the XS2A interface. But for issuing these certificates the TSP has to be compliant also with some additional requirements defined by [PSD2 2015] and [EBA RTS 2017]. On the one hand a certificate shall only be issued to a PSP if this PSP has got the necessary authorization to offer the new services as a TPP. On the other hand a certificate issued to a PSP shall be revoked as soon as the authorization of the PSP is withdrawn. For issuing and revoking certificates both the regulation of a TSP according to [eIDAS 2014] and the regulation of a PSP according to [PSD2 2015] have to be considered. Both spheres of regulation come together and have an influence on the question which TSP may issue certificates to which PSP.

Each QTSP has got its own certificate policy compliant with [eIDAS 2014]. This certificate policy has to be enhanced by some further requirements in order to be also compliant with [PSD2 2015] and [EBA RTS 2017]. The policy at hand defines these additional requirements.

The document at hand indicates that qualified Trust Service Provider according to [eIDAS 2014] provide a sound basis for the PKI needed for the identification of PSP at the XS2A interface. Only a few additional requirements have to be implemented by the TSP in order to achieve also the requirements of [PSD2 2015]. Essentially these additional requirements refer to the identification of the certificate owner, the revocation of certificates and the extension of the content of a certificate by some PSD2 specific attributes. However it has to be emphasized that a TSP needs some information from the national authorities according to [PSD2 2015] in order to be able to implement some of the additional requirements.

2 Introductions

With [PSD2 2015] the European Union has published a new directive on payment services in the internal market. Member States have to adopt this directive into their national law until 13th of January 2018.

Among others [PSD2 2015] contains regulations of new services to be operated by so called third party payment service provider (TPP) on behalf of a payment service user (PSU). These new services are

- payment initiation service (PIS) to be operated by a Payment Initiation Service Provider (PISP) as defined by article 66 of [PSD2 2015],
- account information service (AIS) to be operated by an Account Information Service Provider (AISP) as defined by article 67 of [PSD2 2015], and
- confirmation of the availability of funds service to be used by Payment Instrument Issuer Payment Service Provider (PIISP) as defined by article 65 of [PSD2 2015].

For operating the new services a TPP needs to access the account of the PSU which is usually managed by another PSP called the Account Servicing Payment Service Provider (ASPSP). An ASPSP has to provide an interface (called access to account (XS2A) interface) to its systems to be used by a TPP for necessary accesses regulated by [PSD2 2015]. Further requirements for the implementation and usage of this interface are defined by a Regulatory Technical Standard (RTS) to be published by the European Banking Authority (EBA). Due to article 98 of [PSD2 2015] EBA has got the task to prepare this RTS in close cooperation with the European Central Bank (ECB). Currently the final report on the draft of the RTS [EBA RTS 2017] has been published by EBA. After adoption of the RTS by the European Commission the RTS will be a binding part of [PSD2 2015].

Due to [PSD2 2015] a TPP shall identify itself every time it accesses an account using the XS2A interface provided by an ASPSP. Article 29 of [EBA RTS 2017] substantiates this by requiring that this identification shall rely on qualified certificates according to the regulation of the European Union on electronic identification and trust services for electronic transactions in the internal market ([eIDAS 2014]).

Qualified certificates are issued by a qualified Trust Service Provider (qualified TSP or QTSP). Supervision and qualification of a TSP as a QTSP are regulated by [eIDAS 2014]. In principal each QTSP may issue certificates needed by a PSP for its identification at the XS2A interface. But for the identification of the certificate owner and for the withdrawal of certificates further new requirements of [PSD2 2015] and [EBA RTS 2017] have to be considered by the QTSP. A certificate shall only be issued to a PSP if this PSP has got the necessary authorization to offer the new services as a TPP. On the other hand a certificate of a PSP shall be withdrawn if the authorization of the PSP has been withdrawn.

Notation: PSP authorized to work as an AISP, PISP and/or PIISP are called within this document authorized PSP for short. These are credit institutions (article 1 1.(a) of [PSD2 2015]), electronic money institutions (article 1 1.(b) of [PSD2 2015]) and payment institutions (authorized according to article 11 of [PSD2 2015]). For payment institutions the authorization and the withdrawal of the authorization are regulated in the articles of title II of [PSD2 2015].

In addition article 29 of [EBA RTS 2017] defines some special attributes to be included into the qualified certificate of the PSP. The values of these attributes are determined by the competent national authority as part of the authorization. The TSP issuing a qualified certificate to a PSP has to verify the correctness of these attributes as part of the identification of the PSP before issuing the certificate.

Each QTSP has got its own certificate policy compliant with the requirements of [eIDAS 2014]. The document at hand defines an enhancement to this certificate policy necessary to comply with the requirements defined by [PSD2 2015] and [EBA RTS 2017].

Some of the requirements defined by [EBA RTS 2017] are essential prerequisites for the policy defined by this document. For this reason this policy can only be finalized as soon as the adopted version of [EBA RTS 2017] will be available. It is expected that the RTS will not be adopted before October 2017. Requirements defined

by the RTS have to be implemented by all participating PSP 18 month after the adoption of the RTS by the European Commission, hence the requirements defined by the RTS have to be implemented approximately (not before) April 2019.

2.1 Overview

A third party PSP (i.e. PIISP, PISP or AISP) has to identify itself at the XS2A interface provided by an ASPSP. This identification has to be based on qualified certificates issued by a QTSP complying with the regulation [eIDAS 2014]. [PSD2 2015] and [EBA RTS 2017] define some further PSD2-specific requirements for the issuance, management and content of the certificates needed by a PSP. This policy defines these PSD2-specific requirements. A QTSP issuing certificates to PSP has to use this policy as an enhancement to its own certificate policy.

For an easy matching of this policy with existing certificate policies headings of sections to be enhanced are used according to [RFC 3647]. The keywords “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY” and “OPTIONAL” are to be interpreted as described in [RFC 2119] regardless if written in upper or lower case letters.

Remark:

According to article 29 of [EBA RTS 2017] the identification of PSP shall rely on qualified certificates for electronic seals or for website authentication as defined by (30) respectively (39) of article 3 of [eIDAS 2014]. Nothing is said by whom or by which circumstances it has to be decided whether qualified certificates for electronic seals or for website authentication have to be used. The PSD2 specific requirements of this enhancement for the certificate policy are valid regardless whether certificates for electronic seals or for website authentication are used. Nevertheless certificates should always only be used for a purpose intended by [eIDAS 2014]. Qualified certificates for electronic seals shall be used if the integrity and origin of data shall be proved (article 35 2. of [eIDAS 2014]) while qualified certificates for website authentication shall be used to authenticate a domain which domain name has to be part of the certificate (article 45 and annex IV (e) of [eIDAS 2014]). In addition due to section 9.6.3 of [CAP-BR] the owner (subscriber) of a certificate for website authentication has the obligation to install the certificate only on a server that is accessible by the subjectAltName listed in the certificate.

2.2 Document Name and Identification

This document contains the PSD2 specific enhancement for a Certificate Policy for the PKI for identification at the XS2A interface. It is identified by the following information:

	Value
Title	Certificate Policy for the PKI for identification of PSP at the XS2A interface
Version	Version 1.0, Draft 2, 05.05.2017

Table 1: Identification of this document

This document is available under the URL www.bsi.bund.de/payment

2.3 PKI Participants

At the usage level of the certificates considered in this document a certificate issuing TSP, a certificate using PSP and an ASPSP as relying party are participants of the PKI defined by this document.

A TSP issues end user certificates according to its certificate policy and this enhancement. These end user certificates are issued to TPP (AISP, PISP and PIISP). In addition the TSP provides a service for withdrawal of certificates. It manages and provides corresponding certificate revocation lists (CRL) and an Online Certificate Status Protocol (OCSP) responder.

A TPP uses his certificate to identify itself at the XS2A interface as required by [PSD2 2015] (articles 65, 66 and 67) and [EBA RTS 2017] (article 27 and 29). The TPP signs its requests using the corresponding private key and includes its certificate into the request message.

An ASPSP is participating as relying party. The ASPSP is verifiying the electronic signature and the certificate which are part of an incoming request message at the XS2A interface provided by the ASPSP according to article 27 of [EBA RTS 2017]. The ASPSP has to decide based on its own risk analysis and management about the detailed steps to be performed for the verification of a certificate (check against a white list of certificates managed by the ASPSP, check against a CRL managed by the TSP or online requests at an OCSP responder provided by the TSP, check of the trusted list containing QTSP certificates as trust anchor).

The following figure shows the relationship between the participants of the PKI at the usage level:

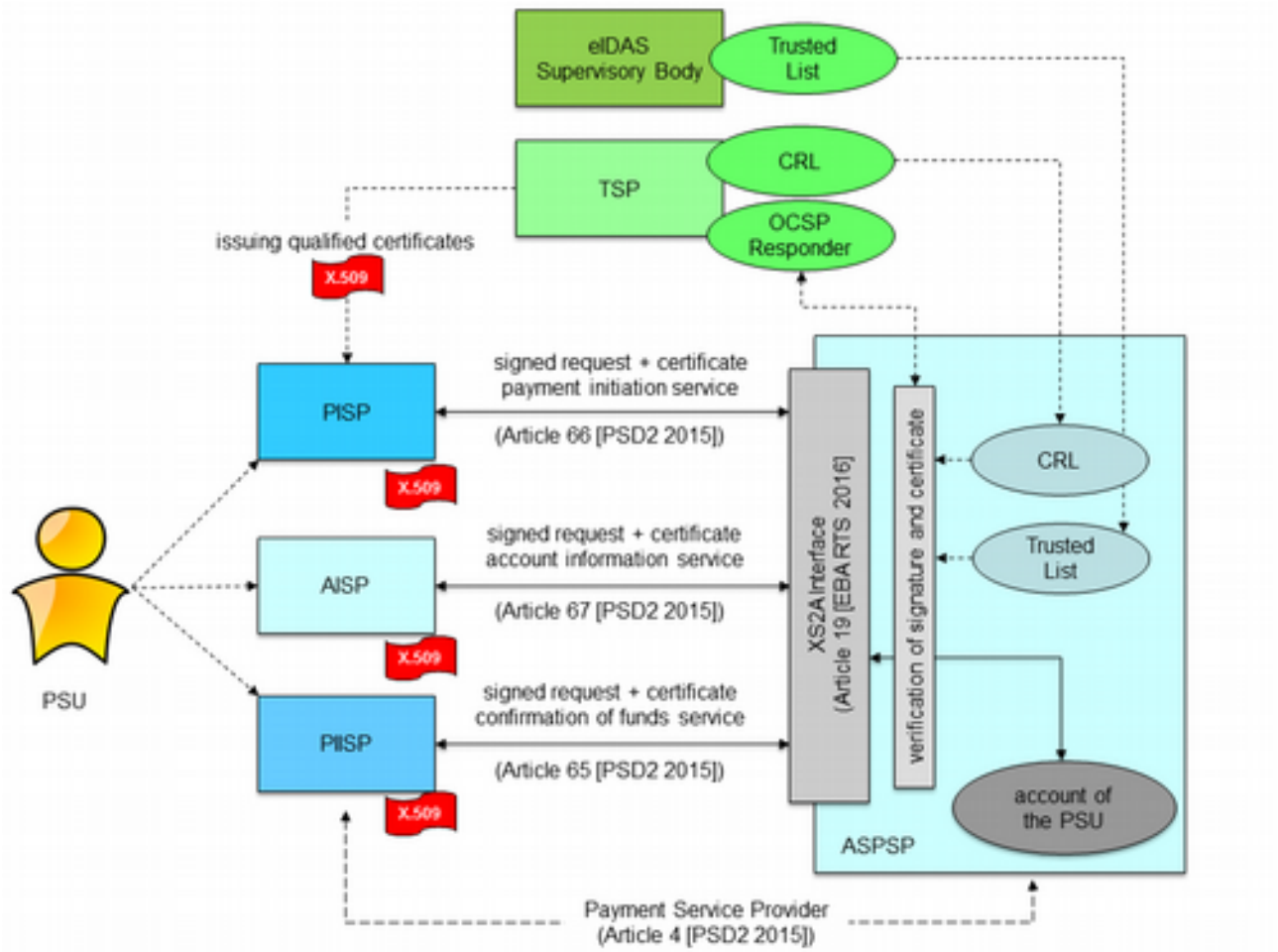

Figure 1: Participants of the PKI at the usage level

For future enhancements of the XS2A interface it might be necessary that also an ASPSP identifies itself at the XS2A interface. In this case end user certificates will also be issued to ASPSP. An ASPSP will sign its messages to a TPP using the corresponding private key and will include its certificate into the messages sent to the TPP and the TPP will be the relying party.

In order to issue certificates according to this policy the TSP shall be authorized as a qualified trust service provider. Supervision and qualification of a TSP as a qualified trust service provider are regulated by [eIDAS 2014]. On the other hand certificates according to this policy shall only be issued to a PSP if it is an authorized PSP, i. e. has been authorized to offer the new services as TPP. By these requirements also the supervision bodies of the [PSD2 2015] regulation and other regulations of the finance sector and of the [eIDAS 2014] regulation are participating in the PKI defined by this certificate policy. Both spheres of regulation come together and have an influence on the question which TSP may issue certificates to which PSP.

The following figure shows the relationship between participants of the PKI from the point of view of the supervision for the example of the PSP being a payment institution:

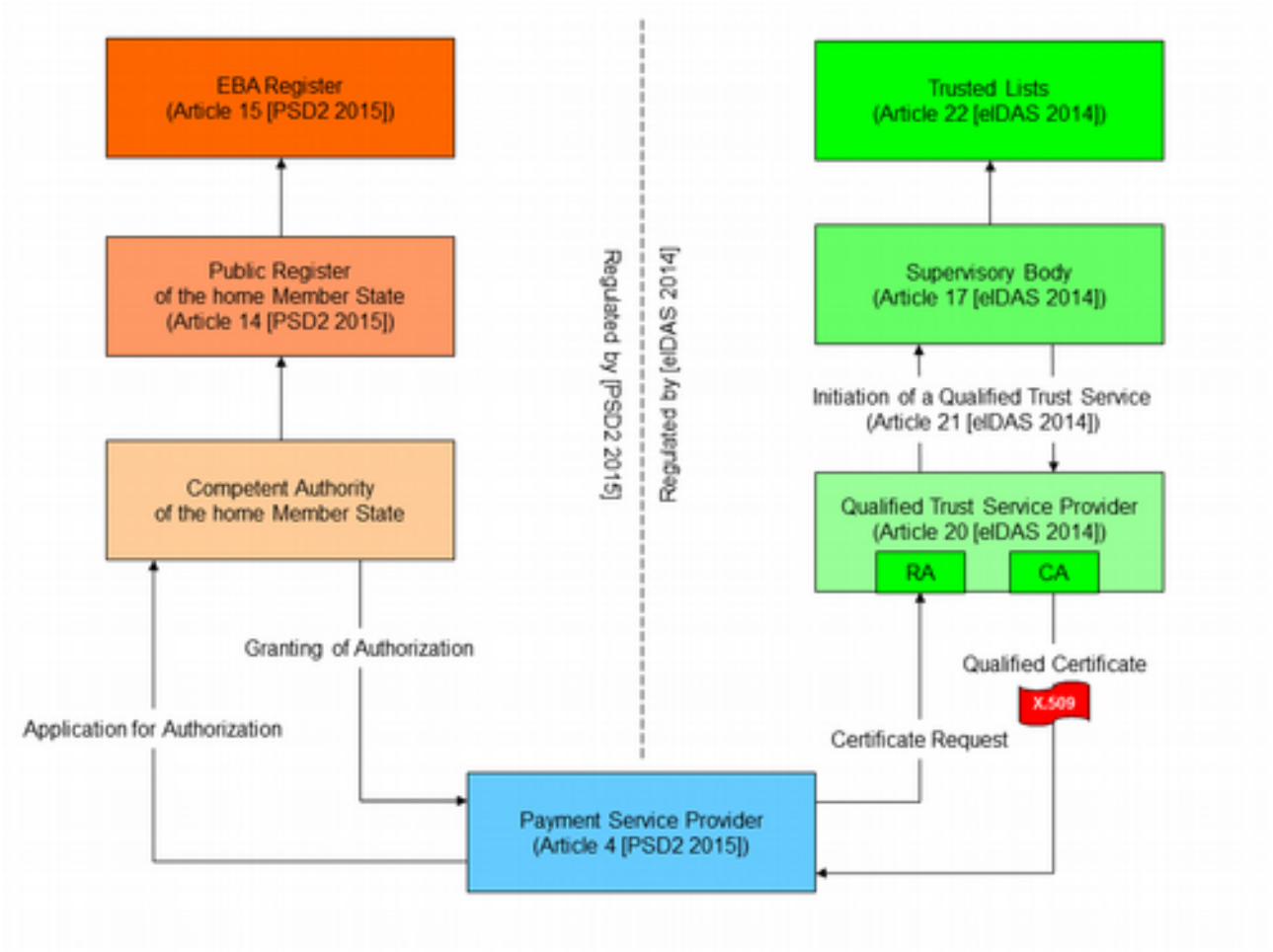

Figure 2: Spheres of regulations relevant for the PKI

Please notice: Figure 2 contains only an overview of the organizations participating as part of the PKI. Communication flow between the participants is not shown. If the PSP is not a payment institution but belongs to another category of authorized PSP other organizations and registers have to be considered on the side of the regulation of the finance sector.

A TSP may only issue qualified certificates if it has initiated a qualified trust service. For this it has to submit a notification to a supervisory body. The supervisory body verifies that the TSP complies with the requirements of the regulation [eIDAS 2014]. This verification is done based on a conformity assessment report issued by a conformity assessment body.

If a TSP complies with the requirements for a qualified TSP the supervisory body includes the certificate of the TSP in its trusted list. Relying parties can use the content of the trusted list as trust anchor for verifying certificates issued by a qualified TSP.

A PSP has to be authorized by the competent authority of its home Member State. For example for payment institutions this authorization is regulated by [PSD2 2015]. The competent authority of a Member State manages and publishes one or more public registers containing all PSP authorized by this authority. In addition these public register will also contain information of any withdrawal of an authorization of a PSP. Coverage and accessibility of these registers are different depending on the actual Member State.

For authorized payment institutions EBA will publish in future an EBA register containing the aggregation of the content of all national public registers of the Member States. Development, operation and maintenance of this EBA register will be regulated by a further RTS to be published by EBA.

The Certification Authority (CA) of a TSP shall issue a certificate to a PSP only if this PSP is contained in a public register of one of the Member States and only if no information about a withdrawal of its authorization is contained in this register. Since the national competent authorities are responsible for the accuracy of the information contained in their national public register these national public registers have to be taken into account by the Registration Authority (RA) of the TSP deciding if a certificate may be issued to a PSP or not.

2.4 Certificate Usage

Certificates according to this policy are only issued to ASPSP, PIISP, PISP or AISP authorized by competent authorities of the home Member state.

A PIISP, PISP or AISP has to use these certificates according to article 65 2.(c) (for a PIISP), article 66 3.(d) (for a PISP) and article 67 2.(c) (for an AISP) to identify itself at the XS2A interface offered by an ASPSP.

This policy places no further constraints on the usage of the certificates issued according to this policy.

2.5 Policy Administration

###OP: Responsibilities and processes to be defined. ###

3 Identification and Authentication

3.1 Initial identity validation

The initial identity validation by the RA of the TSP has to be compliant with the following additional requirements:

- The subject of a certificate is a PSP. Hence, only the case of a legal person as subject has to be considered.
- The TSP SHALL verify that the authorization of the PSP has been entered in a public register and that no withdrawal of that authorization has been entered in this public register. For this verification the public registers of the home Member state of the PSP are the relevant register.
- For the specific attributes defined by article 29 of [EBA RTS 2017] the TSP SHALL verify the correctness according to the public registers of the home Member state of the PSP.
- The specific attributes defined by article 29 of [EBA RTS 2017] are
    - the authorization number of the PSP (Article 29 2. of [EBA RTS 2017]),
    - role of the PSP which can be one or more of ASPSP, AISP, PIISP or PISP (Article 29 3.(a) of [EBA RTS 2017], and
    - the name of the competent authority where the PSP is registered (Article 29 3.(b) of [EBA RTS 2017]).

The RA of the TSP has to verify the correct authorization of the PSP by the competent authority of the home Member state of the PSP and the correctness of the specific attributes. The procedure to be used for this verification has to be defined by the TSP depending on the circumstances determined by the competent authority of the Home Member which has registered the PSP.

3.2 Identification and authentication for revocation request

The identification and authentication for revocation requests by the CA of the TSP has to be compliant with the following additional requirements:

- A certificate SHALL be revoked without any undue delay if the authorization of the PSP has been withdrawn by the competent authority of the home Member state of the PSP.
- It is within the responsibility of the TSP to inform itself about possible withdrawals of authorization by inspecting information available by the competent authorities of the home Member states of PSP to which it has issued certificates.

Remark:

It is recommended that processes are set up by competent authorities in order to inform TSP actively about the withdrawal of an authorization of a PSP. Since it is expected that the withdrawal of an authorization will occur only very infrequently these may be a manual processes.

4 Certificate Life Cycle Operational requirements

4.1 Certificate Issuance

The certificate issuance by the CA of the TSP has to be compliant with the following additional requirements:

- The identifier given in section 2.2 of this document SHALL be used as identifier of the certification policy.

4.2 Key Pair and Certificate Usage

The subscribers obligations shall include the following items:

- The use of the subjects private key is immediately and permanently discontinued, if
  - the authorization of the PSP has been withdrawn by the competent authority of its home Member state,
  - the PSP discontinues its services and/or business,
  - any attributes contained in its certificate have changed, or
  - the private key of the PSP is suspected to be compromised.
- The TSP has to be notified by the subscriber (PSP) without any undue delay , if
  - the authorization of the PSP has been withdrawn by the competent authority of its home Member state,
  - the PSP discontinues its services and/or business,
  - any attributes contained in its certificate have changed, or
  - the private key of the PSP is suspected to be compromised.

4.3 Certificate Revocation and Suspension

The CA of the TSP has to be compliant with the following additional requirements:

- The TSP SHALL generate and distribute Certificate Revocation Lists (CRL). This CRL shall be published at least every 24 hours and shall be signed by the CA or an entity designated by the TSP.

4.4 Certificate Status Services

The CA of the TSP has to be compliant with the following additional requirements:

- OCSP SHALL be supportd by the CA.
- CRL SHALL be supported by the CA.

5 Certificate and CRL Profile

5.1 Certificate Profile

The profile of the certificates issued by the CA of the TSP has to be compliant with the following additional requirements:

- The certificate SHALL include the policy identifier as defined in section 2.2.
- The certificate SHALL include the CRL distribution point extension.
- The Authority Information Access extension SHALL include accessMethod OID (id-at-ocsp) with an accessLocation value specifying at least one access location of an OCSP responder of the TSP.
- The certificate SHALL include the following extensions containing the additional specific attributes required by article 29 of [EBA RTS 2017]. All of these extensions SHALL NOT be marked as critical.
  - pspAuthorzationNumber
  - pspRole
  - pspRoleOID
  - pspAuthoririty Name
  - pspAuthorityCountry

The following table specifies these extensions:

Extension	OID	Value
`pspAuthorzation Number`	###OP: tbd ###	Authorization number of the PSP (certificate owner) available in the public register according to article 14 of [PSD2 2015].
`pspRole`	###OP: tbd ###	One or more of the fixed values AISP, ASPSP, PIISP or PISP.
pspRoleOID	###OP: tbd ###	One or more OID identifying the role of the PSP.
`pspAuthority Name`	###OP: tbd ###	Name of the competent national authority where the PSP (certificate owner) is registered.
`pspAuthority Country`	###OP: tbd ###	Country of the competent national authority.

Table 2: Extensions for the attributes according to article 29 of [EBA RTS 2017]

The country of the national authority SHALL be coded as 2 character ISO 3166 country code.

According to article 29 3. of [EBA RTS 2017] the role has to be included in English. For this the abbreviations AISP, ASPSP, PIISP and PISP shall be used within the attribute pspRole. If the PSP may work using different roles the abbreviations for the roles SHALL be separated by a "+", i.e. for a PSP working as AISP and as PISP the attribute pspRole shall contain the value AISP+PISP.

The attribute pspRoleOID SHALL contain one or more OID representing the roles contained in the attribute pspRole.

The content of the attribute pspRoleOID shall be used for automatic examination of the certificate while the attribute pspRole will be used for visual inspection if necessary. In the case of a divergence between the

content of both attributes the content of the attribute pspRoleOID shall be used for further processing of the certificate.

###OP: It has to be defined who will be in charge to define the OIDs (for example ETSI?) ###

Appendix

Reference Documentation

PSD2 2015	EU: Directive (EU) 2015/2366 of the European Parliament and the Council on payment services in the internal market, 25.11.2015
EBA RTS 2017	EBA: Final Report on Draft Regulatory Technical Standards on Strong Customer Authentication and common and secure communication under Article 98 of Directive 2015/2366 (PSD2), EBA/RTS/2017/02, 23.02.2017
eIDAS 2014	EU: Regulation (EU) No 910/2014 of the European Parliament and the Council on electronic identification and trust services for electronic transactions in the internal market, 23.07.2014
RFC 3647	Network Working Group: RFC 3647 - Internet X.509 Public Key Infrastructure, Certificate Policy and Certification Practices Framework, 11.2003
RFC 2119	Network Working Group: RFC 2119 - Key words for use in RFCs to Indicate Requirement Levels, 03.1997
CAP-BR	CA/Browser Forum: Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates, Version 1.4.1, 7.09.2016

Keywords and Abbreviations