ETSI PSD2 Workshop – Online meeting
21 July 2017 10:00 to 13:00 CEST

Draft Meeting Report

Attendees

ERPB Experts

Boogmans, Chris	Member of ERPB PIS WG
Broxis, John	Co-Chair of the ERPB PIS WG - Identity sub-group
Kong, Chris	Co-Chair of the ERPB PIS WG - Identity sub-group

ETSI Experts

Pope, Nick	Vice chair ETSI ESI
Antunes, Lionel	Luxtrust SA
Thomas Kopp	Luxtrust SA
Caccia, Andrea	Uninfo
Compans, Sonia	European Telecommunications Standards Institute
Fiedler, Arno	Nimbus Technologieberatung GmbH
Huehnlein, Detlef	TeleTrusT Bundesverband IT-Sicherheit e. V.
Kjærsgaard, Jan Ulrik *	Dansk Standard
Réti, Kornél *	Microsec Ltd
Tabor, Michal *	TIMT

1 Introductions

Attendees will give a brief introduction of themselves and their interests regarding eIDAS and PSD2.

2 Workshop Terms of Reference

The aim of the workshop is to support the ECB ERPB (European Central Bank - European Retail Payments Board) in providing guidance / standards for the use of eIDAS in the context of PSD2. Initially, this is aimed at guidance / standards for the use of qualified certificates as required by the PSD2 Regulatory Standards. ERPB will identify the requirements, ETSI will establish the technical standards / guidance to meet the requirements. ERPB is to be represented by the chairs of the co-chairs of the ERPB sub-group on Identification, part of the Working Group on Payment Initiation Services, along with other ERPB members as deemed appropriate by the Identification sub-group co-chairs. The workshop should complete its activities by mid-2018.

This was agreed.

3 PSD2, RTS and ERPB

Document ETSI ESI(17)59_016r1 provides background information on 3 PSD2, RTS and ERPB

It was reported that the next ERPB meeting will be on 7th September. At the meeting Chris Kong and John Broxis will give a general report that an initial meeting had taken place between ETSI experts and ERPB experts. It is planned to await the October ERPB meeting, before reporting any details to ERPB, in order to give sufficient time for this ETSI ESI WG to review and align on the issues raised.

The following requirements and issues were identified by the ERPB experts that need to be address by the workshop. Those highlighted in yellow, were identified as the priority issues as previously discussed and reviewed within the ERPB PIS WG.

- Can same certificate be used for seals & web site certificate ?
- First objective is to establish identity of the payment service provider and the financial authority with which it is registered.
- Including regulatory role of PSP as attribute in certificate for given countries
    - Changes to status – whether this should be reflected in the certificate
        - Delay in updating certificate (may take 1 day)
        - Decision made by financial regulatory authority
    - Can be read automatically and also manually ?
    - Alternative to use separate attribute certificates / separate database or directory ?
    - Need special process for revoking certificate
    - How to represent these attributes in a certificate ?
    - What importance should be placed on these attributes ?
        - It is suggested that the PSD2 specific attributes well need to be defined. Any views from the meeting regarding the additional PSD2 specific attributes may not be accepted
        - Do we need put effort into
    - How to Synchronisation of national register with TSP certificate ?
- Relationships
    - Member state competent authority for payment service provider (MSCA) to QTSP
    - Bank to QTSP
    - Supervisory to QTSP
- Consider TSP policy/practice implications
    - How much liability does the TSP take on these
      Under eIDAS TSP is liable at time of issuance for the contents for the certificate

It may be that the TSP is not responsible for tracking changes in certificates

- Member state register are in different forms (PDF, Directory …)
- There is no required process for MSCA (member state competent authority) to provide information to QTSP
    - May have a central directory
    - May have to review each MSCA Financial Register manually

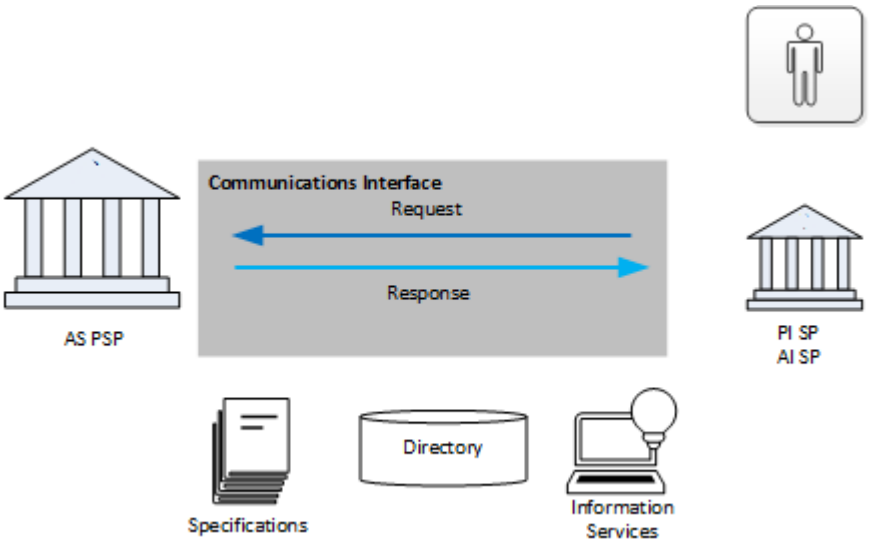
4 PSD2 RTS Requirement for use of Qualified Certificates

On the first point: can same certificate be used for seals & web site certificate ?

- Answer: A clear response was given by ETSI experts: No, each certificate should only one purpose. However, a QTSP may issue both certificate types based on the based on same registration information.

The meeting considered the use cases relating to Bank (ASPSP) and TPP (Third party payment provider PISP / AISP) interactions. Interactions with the customer were not of direct concern to ERPB use of qualified certificates.

Use scenarios:

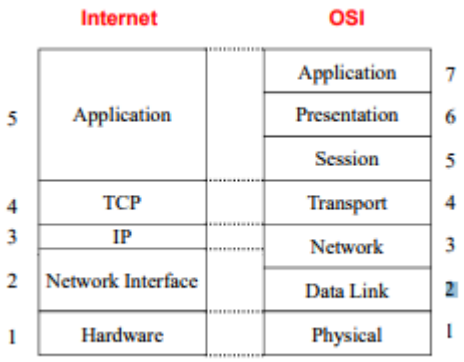


(See use cases appended to minutes.)

Main points made during discussions:

- As well as TPP to Bank (ASPSP) can also have transport connections from ASPSP to TPP
- **Electronic Seal** = authenticity of origin and integrity information at application level. This provides independently verifiable evidence that can subsequently be used as proof that a transaction took place.
- **Website Certificate** = used to protect channel, secure communication at transport level. It cannot be directly used to prove that a given traction took place.

Transport and application levels are used in line with the OSI reference model as shown below.



(It was suggested, for clarity, that OSI structure be used in conversations on this ETSI ESI as the reference for specific layers.)

The follow questions were raised and clarification (underlined and in italics) provided by ETSI experts as follows:

- **Can you use a Seal for SSL?** *No, SSL (and recent equivalent TLS) is at Transport Layer, therefore a Website Certificate should be used.*

- **Can you use Website Certificate for seals?** *No. Web site and seal certificates should not be used other than for the specific purpose for which they are issued*

- **Does everyone need a new PSD2 Certificate, or can a TPP/ASPSP use an existing SSL certificate they already have?** *Existing (non-qualified) certificates cannot be used as qualified certificates.*
  Note: per EBA RTS SCA, there is a requirement for Qualified Certificates to be used, therefore new Certificates should be required to comply.

- For PSD2 specific attributes, as defined in RTS 34.3, a new certificate will need to be issued including the new certificate attribute to a new syntax which will need to be defined.

Requirements of the ASPSP / TPP:

- **Which Certificate to Secure the Channel?**
  ASPSP will require a web site certificate to secure the channel from TPP connecting to the ASPSP
  A TPP may require web site certificate if the ASPSP requires to call the TPP back on a separate channel

- **Does the TPP needs to mutually authenticate on SSL/TLS channel?**
  Web (SSL/TLS) client certificates may be required by the TPP to mutually authenticate the client TPP to the ASPSP.
  If mutual authentication of the ASPSP required on the call back from the ASPSP to the TPP is required the client certificates of the ASPSP may be required. Such client certificates will be non-qualified as eIDAS does not support such certificates.

- **Which Certificate is required to Verify the "PSD2 Identity" of the ASPSP/TPP (WC or ES?) for a specific transaction**
  ASPSP and TPP Electronic Seal certificates will be required to protect the authenticity of sensitive application data exchanges (e.g. payment requests).

- **How might the ASPSP verify the PSD2 Access Rights (Role/Attributes) - PISP, AISP,ASPSP, jurisdiction- of the TPP?**:

  Points regarding PSD2 specific certificate attribute (as in 34.3):

  - Information on registered PSPs will be held on a register operated by the Member State Competent (financial) Authority : For example of see: https://register.fca.org.uk/ShPo_FirmDetailsPage?id=001b000000m4IWpAAM

  - There is currently no obligation on the MSCA to provide this information in any specific format, nor inform QTSPs of any changes in state.
  -
  - ETSI require further information on the lifecycle of these attributes to determine how this is done. Whether using Certificate or directory or attribute certificates (new standards required to support attribute certificates)

Cost of issuing web site and seal certificate might not be significantly more than just providing one of these certificates. ETSI experts would suggest use both to protect channel (using web site certificate) and also secure the data (using seal certificate).

Further advice was given on procedures for handling of OCSP and CRL revocation, which is generally the same as for other types of certificate.

Other points to be discussed in future meeting:

a) The inclusion of PSD2 registration identifiers, including competent authority, in the distinguished name of the Payment Service Provider (PSP) e.g. using OrganisationIdentifier with legal person semantics identifier as defined in EN 319 412-5 clause 5.1.4.
b) The need for extension to current EN 319 411-2 policy requirements to cover PSD2 qualified certificates.
c) Need for mutual authentication on the TLS / SSL channel
d) Possible need for types of certificates not supported by eIDAS (e.g. SSL/TSL client certificates).
e) Other uses of eIDAS standards in context of PSD2
f) How can PSD2 certificate information provided by QTSPs be manually read
g) Liability and responsibilities of parties – SLAs of info maintenance and updates.

5 Initial conclusions regarding RTS Article 34 requirements

Both qualified web site certificates and qualified seal certificates have an important role in securing TPP / ASPSP interactions. Web site certificates are important for securing transport connections, seal certificates are important for protecting the authenticity of sensitive application level transactions.

A clarification to the RTS SCA wording “or” (both certificates potentially required) may be recommended at ERPB to avoid ambiguity/disparities in the market and the operations implemented by the ASPSPs and TPPs.

Regarding the need for additional qualified certificate attributes as currently specified in the RTS Article 34.3 and the possible role of PSD2 directories outside the scope of eIDAS.

a) ETSI experts were not able to give advice at this meeting on the appropriateness of the inclusion of the attributes as defined in RTS article 34.3 in qualified certificates for seals / web sites. This will depend on the lifecycle of this information, how the QTSP is to be informed of this information, how often the information might be changed, and if there is a change of status how quickly will this need to be reflected in certificate revocation information (note: under current practices revocation can take up to 1 day to be reflected in status information).

b) Initial suggestions are that it may be more appropriate to use a directory (or other technology – attribute certificates, SAML) to publish this information.

c) ETSI can specify how these attributes will be reflected electronically in a web site or seal certificate for use as required.

6 Next Steps

Actions:

1) ERPB experts to send role life-cycle example.
2) ERPB experts to send attributes and identification data format examples.
3) ETSI secretariat to investigate requirements for formalising relationship between ERPB and ETSI.

Currently, it is not possible to identify specific requirements for new work items covering new standards (e.g. new part for certificate profiles) or changes to existing standards.

Plans for future ETSI workshops on PSD2.

Next meetings 8th September and 22nd Sept 10am CEST to 13:00 CEST.

Appendix to minutes – Suggested Use Cases

USE-CASE #1: a TPP server application connects to the dedicated interface of an AS-PSP

This is the main use-case. The connection is setup between two infrastructures. A TPP application connects to the dedicated XS2A interface of an AS-PSP. The Regulatory Technical Standards require that "eIDAS compliant certificates" are used for the authentication. We refer to the RTS (Article xx) for somewhat more details. It is very likely that TLS will mostly be used for (a) mutual authentication between the communicating parties and (b) session confidentiality. However, the goal is to be as much as possible technology agnostic. Therefor, the certificates should not be bound to a given protocol or algorithm.

USE-CASE #2: an AS-PSP server application calls back to a TPP application

From a technical point of view, this use-case is almost the same as the previous one. The difference is that this communication session is initiated by the AS-PSP, and the target URL of this connection was given to the AS-PSP application during a previous communication session (one that was initiated by the TPP).

USE-CASE #3: an end-user connects to a TPP server application

As an initial remark, I have to say that I am not 100% sure whether or not the European Banking Authority intended this use-case to be in scope. Taking the RTS literally, it is in scope though.

An end-user connects, for example using a standard browser, to a TPP application. In this connection, the TPP (application) must authenticate itself to the end-user. The RTS do not impose that the end-user uses an eIDAS compliant certificate to authenticate to the TPP.

USE-CASE #4: a TPP application running on an end-user device connects to the dedicated interface of an AS-PSP

For the time being I suggest to place this use-case out of scope, since it may require the private key of the TPP to be "usable" by the end-user device. Moreover, this use-case would not lead to additional requirements on the certificate, would it?