# Report 9th ETSI PSD2 Workshop Wednesday 2 May 2018

Starting 10:30 CEST

Goto meeting: https://global.gotomeeting.com/join/710242613

# Attendees

ERPB / OBE Experts

|  |  |
| --- | --- |
| Boogmans, Chris | Co-Chair of the ERPB PIS WG - Identity sub-group  Isabel |
| [Broxis, John](https://portal.etsi.org/webapp/TelDir/ListAnonDetails.asp?PersId=119033&m_id=33007) | Co-Chair of the ERPB PIS WG - Identity sub-group,  OBE |
| [Kong, Chris](https://portal.etsi.org/webapp/TelDir/ListAnonDetails.asp?PersId=119026&m_id=33007) | Delegated SME for ERPB PIS - Identity Subgroup to ETSI/ESI WG,  Azadian |

ETSI Experts

|  |  |
| --- | --- |
| [Pope, Nick](https://portal.etsi.org/webapp/TelDir/ListPersDetails.asp?PersId=10483&m_id=33007) | [Vice](https://portal.etsi.org/webapp/TelDir/QueryOrgaInfo.asp?OrgaId=70) chair ETSI ESI |
| Thomas Kopp | [Luxtrust SA](https://portal.etsi.org/webapp/TelDir/QueryOrgaInfo.asp?OrgaId=15188) |
| [Fiedler, Arno](https://portal.etsi.org/webapp/TelDir/ListPersDetails.asp?PersId=30361&m_id=33007) | [Nimbus Technologieberatung GmbH](https://portal.etsi.org/webapp/TelDir/QueryOrgaInfo.asp?OrgaId=14058) |
| [Réti, Kornél](https://portal.etsi.org/webapp/TelDir/ListPersDetails.asp?PersId=48470&m_id=33007) | [Microsec Ltd](https://portal.etsi.org/webapp/TelDir/QueryOrgaInfo.asp?OrgaId=13237) |
| Rizzo, Luigi | InfoCert S.p.A. |
| [Tabor, Michal](https://portal.etsi.org/webapp/TelDir/ListPersDetails.asp?PersId=66477&m_id=33007) | [TIMT](https://portal.etsi.org/webapp/TelDir/QueryOrgaInfo.asp?OrgaId=15460) |
| Christian Seegbarth | Bunderdruckerei |

# Confirm Agenda

The meeting is to plan future ETSI activities on PSD2.

# Status of current activities

## **TS 119 495 publication status:**

Final draft available at:  
<https://docbox.etsi.org/ESI/Open/Latest_Drafts/TS_119495v007-public.pdf>

ETSI Edit Help has started work on the document.

## Liaison to CA Browser

See ESI(18)62\_059r1 :“Request for Clarification on Use of organizationIdentifier in subjectDN of EV Certificates”

## OBE :Liaison agreement

Agreement signed. ETSI and OBE will do a joint press release.

## Other OBE / ERPB Updates

Final report is being prepared including reference ETSI PSD2 Cert profile. ERPB would like to have more consistency on information from national registers which hopefully should be addressed by ETSI EBA discussions with NCAs.

14 countries have transposed to national legislation. Still to be adopted by many countries.

# EBA Collaboration on TSP / NCA Interfaces

1. Agreed to collaborate on old Annex C replacement

<https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=54717>

1. EBA concern regarding conflict of interest:

“EBA and is members cannot participate in an ETSI working group/forum that includes firms that are directly regulated by national competent authorities or other firms/participants that could directly or indirectly gain a commercial advantage linked to PSD2 from this work and its output, compared to firms that are not participating.”

“We believe there is a distinction that we can make when working with ETSI and ETSI members, who will have a commercial interest in the final output, because of the role of ETSI (as a standard setting body) and the role of QTSPs under the eIDAS regulation and the related legal requirements under the RTS. We assume that ETSI will have considered any conflict of interest or commercial advantage pertaining to ETSI members participating in this work.”

It was agreed to accept this situation. Nick reported that it was his aim that any revisions the ETSI TS 119 495 would be available for public review before ratification.

1. Joint workshop proposed for 4th and 5th July – ETSI Sophia Antipolis

It is proposed to start this at 11:00am 1st day and finish 13:00 2nd day.

# Future Areas of Work

Points carried forward from earlier meeting:

1. 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 319 412-1 clause 5.1.4.

For publicly facing certificates. See CAB Forum liaison.

Action: Nick to check with Sonia regarding need to issue TS 119 412-1 as EN

1. The need for extension to current EN 319 411-2 policy requirements to cover PSD2 qualified certificates.

Aim to define policy requirements as additions to EN 319 411-2 which should not conflict with the base standard.

1. Possible need for types of certificates not supported by eIDAS (e.g. SSL/TSL client certificates).

Two aspects of this were identified aspects:

* + 1. PSP public facing certificate
    2. Client authentication certificate

Question PSP public facing certificate whether it is legally required under RTS. Whether need PSD2 specific attributes. Need to consider whether get CAB F recognition and eIDAS QWAC recognition. May be greater interest is CADF OV rather than EV.

Need for greater clarity:

* Must QWAC be EV, can it OV or even DV?
* Must a PSD2 QWAC be EV, can it OV or even DV?
* What is the intent of putting PSD2 information in Certificates to be used for secure communications? We have 2 scenarios PSP to PSP, PSP to PSU on a web browser
* Need to clarify for market of different types of certificates and what is of concern to EBA?

Agreed to draft out different types of certificates for later feeding into EBA especially PSP public facing certificate. Separate out discussion on client certificates, outside scope of eIDAS but could be of interest.

RTS may cover where public facing web site is used for PSP to PSP communications.

Action 9.1: Arno to produce table covering: usage scenario, eIDAS QWAC vs Public facing (e.g. EV or OV).

1. Other uses of eIDAS standards in context of PSD2  
   Not of specific interest
2. How can PSD2 certificate information provided by QTSPs be manually read   
   Not of specific interest
3. All the use cases in [ESI(17)000125r1](https://docbox.etsi.org/ESI/ESI/05-CONTRIBUTIONS/2017/ESI(17)000125r1_PSD2_Workshop_Discussion_Document_on_Issues_and_use_cases.docx) need to be considered (see extract at the end of this document).

Not discussed

1. Preparation for discussion for EBA discussion.
   * Clarify roles and how to add. What additional roles needed?
   * Authorisation number: how handle this in countries don’t currently have this. How this might be handled.
   * Re-iterate main points in life cycle

Action 9.2 : Michal to prepare some slide to clarify above points for EBA discussion.

# Conclusions and Next Steps

Two work areas:

1. Clarification of certificate usage including public facing certificates
2. Preparation for EBA workshop

Meet again last week in May.

Please complete Doodle: https://doodle.com/poll/xf9m87uzbxxuuwmq

# Extract from [ESI(17)000125r1](https://docbox.etsi.org/ESI/ESI/05-CONTRIBUTIONS/2017/ESI(17)000125r1_PSD2_Workshop_Discussion_Document_on_Issues_and_use_cases.docx" \t "_blank)

**Use Cases for Common Secure Communications & Identity, under PSD2**



Note: Web browser user interface does not support indication that a certificate QWAC.

Technically are then any new risks with having separate certificates?

As same application would be using the certificate there are not any obvious additional risks from having the two roles (client and server) in the same certificate.

Next meetings to consider mainly at C & D.

1. **PSU establishes secure communications with TPP:**
   * 1. Secure Communications via Internet Browser
        1. Certificate Used?
        2. Protocols Used?
        3. Certificate Data Used?
2. **PSU establishes secure communications with ASPSP:**
   * 1. Secure Communications for Internet Browser
        1. Certificate Used?
        2. Protocols Used?
        3. Certificate Data Used?
3. **TPP establishes secure communications with ASPSP:**
   * 1. Secure Communication via APIs
        1. Certificate Used?
        2. Protocols Used?
        3. Data Used?
        4. Use of PKI or other Security?
4. **ASPSP establishes secure communications with TPP:**
   * 1. Secure Communication via APIs
        1. Certificate Used?
        2. Protocols Used?
        3. Data Used?
        4. Use of PKI or other Security?

Can the same QWAC be used as the certificate for calling and called party at transport level? Under CA/B same certificate is a TLS client and server authentication certificate.

On legal side discuss between Lionel / Riccardo / Nick in a separate call.



**[E] TPP provides PSD2 Identity to ASPSP:** Proof of Regulatory Identity under PSD2

- Certificate Used?

- Protocols Used?

- How to Proof Ownership/identity?

- Data Elements & Locations?

- Certificate Status Checking and Policies?

- Assurance and Liability?



**[F] ASPSP provides PSD2 Identity to TPP:** Proof of Regulatory Identity under PSD2

- Certificate Used?

- Protocols Used?

- How to Proof Ownership/identity?

- Data Elements & Locations?

- Certificate Status Checking and Policies?

- Assurance and Liability?

**Other Considerations:**

1. **CA/B Forum & QWACs**
   1. Differences between BV, OV and EV?
   2. Alignment to eIDAS Definition?
   3. Use of existing non-Qualified Website Certificates?
   4. Requirements for PSD2 QWACs for BV, OV and EV?
   5. Data Elements of PSD2 – differences with BV, OV and EV for Certificates profiles?
2. **ASPSP and TPP – SSL/TSL**
   1. Mutual Authentication Benefits/Downsides?
   2. Unidirectional Authentication Benefits/Downsides?
   3. Checking Storage of SSL/TLS Certificates?
3. **ASPSP and TPP – OAUTH2.0 & Certificates?**
   1. Certificates Required?
   2. Protocols Required?
4. **ASPSP and TPP – PKI**
   1. Methods of checking Signatures per Certificate?
   2. Further Security/Cryptography after PKI, per Protocols?