# Report 11th ETSI PSD2 Workshop Wednesday 29 May 2018

# Attendees

ERPB / OBE Experts

|  |  |
| --- | --- |
| Chris Boogmans (Absent apologies received) | Co-Chair of the ERPB PIS WG - Identity sub-groupIsabel |
| John [Broxis](https://portal.etsi.org/webapp/TelDir/ListAnonDetails.asp?PersId=119033&m_id=33007)  | Co-Chair of the ERPB PIS WG - Identity sub-group,OBE |
| Chris [Kong](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

|  |  |
| --- | --- |
| Nick [Pope](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) |
| Arno [Fiedler](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) |
| Kornél [Réti](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) |
| Luigi Rizzo | InfoCert S.p.A. |
| Michal [Tabor](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 |
| Sonia Compans  | ETSI |
| Metin Simsek  | Tubitak Uekae (Turkey) |

# Confirm Agenda

Agreed

# Report from Previous Meeting

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

Done: See email from Arno sent Fri 11/05/2018 12:50 (UK Summer time). Discussed below

**Action 9.2** : Michal to prepare some slides to clarify points for EBA discussion.

* + Clarify roles and how to add. What additional roles needed?
	+ Authorisation number: How to handle this in cases where there is no unique authorization number.
	+ Re-iterate main points in life cycle

Done: See [ESI(18)000088](https://docbox.etsi.org/ESI/ESI/05-CONTRIBUTIONS/2018/ESI%2818%29000088_Annex_C_presentation_for_discussion.pptx), discussed below

No further comments on report of previous meeting.

# Status of current activities

## Liaison to CA/Browser Forum

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

It is proposed that the CA/B Forum EV guidelines are updated to specifically allow this. Proposed change being considered by CA/B Forum:

**Certificate field**: organizationIdentifier (OID 2.5.4.97)

**Required/Optional**: Optional

**Contents**: This contains subject additional registration information as required for specific regulatory purposes other than the registration as described in 9.2.6.  This field shall be encoded as specified in ETSI TS 119 412-1 v1.2.1 clause 5.1.4.  This shall not contain registration number from a national trade register as identified by “NTR” in ETSI TS 119 412-1 v1.2.1 clause 5.1.4.

## Other OBE / ERPB Updates

ERPB: Finished report to be submitted on Friday to ERPB. To be discussed on 18th June. This report notes success of ETSI standard. The problem of consistency across national registers was also noted in the report. No further action expected from ERPB.

OBE: signed agreement. OBE plan to send out a press release shortly. This is to be coordinated with ETSI.

A new group is being formed - API evaluation group. The aim of this group is to define define common requirements on API interface. The group is supported by EU commission and includes representative from: 3 banking associations, 3 TPPs, 3 e-commerce association. The group is also in contact with 5 API initiatives.

A question arising is how to attach X.509 certificate in JSON. JSON Web Signature (JWS) RFC7515 exists but a profile needs to be defined. XML is being considered as an alternative. There is a potential problem with not having state information as each signature needs to be verified at each time. Extra network traffic is caused by re-doing full check each time. This may be improved by caching information. Key management overhead can also be a problem. Suggest always use TLS to secure communication. May use seal for specific sensitive operation.

Main concern is to provide clear guidance for API implementations on how to efficiently implement signature verification. Rather than ETSI produce guidance document it is suggested that a joint working group meeting is held with the “API Evaluation Group”. Chris Kong offered to help move this forward, and will report back after their next meeting on 7/8 June.

**Action 11.1**: Chris Kong to report back on progress with working with API Evaluation Group to assist with guidance of use of PSD2 qualified certificates and distribute any summary document that is produced this issue

Nick Mentioned that ETSI ESI have started discussion on profiling JSON Web Signatures for eIDAS. This is very early stage with the scope of a potential new work item still under discussion. Chris K emphasised the importance of quick resolution of use of JSON Web Signature.

**Action 11.2**: Nick to raise the need for PSD2 a JSON Web Signature Profile at the ESI #63 meeting.

# EBA Collaboration on TSP / NCA Interfaces

Joint workshop proposed for 4th and 5th July – ETSI Sophia Antipolis. It was proposed to start this at 11:00am 1st day and finish 13:00 2nd day. It was requested that the meeting start earlier. Nick has proposed to EBA to change start at 9:30 – awaiting feedback.

Inputs to EBA workshop

1. Annex C text
[ESI(18)000090](https://docbox.etsi.org/ESI/ESI/05-CONTRIBUTIONS/2018/ESI%2818%29000090_Draft_Annex_C_-_TS_119_495.docx)
2. Presentation
[ESI(18)000088](https://docbox.etsi.org/ESI/ESI/05-CONTRIBUTIONS/2018/ESI%2818%29000088_Annex_C_presentation_for_discussion.pptx)

It was agreed to submit the draft Annex C to EBA as is with reference to the published TS 119 495 document.

Comments were made on the presentation and initial changes made to the document. Michal undertook to complete the update to the presentation by beginning of next week (4 June), for review by PSD2 workshop members by end of next Thursday, and completion by Michal by 9th June.

**Action 11.3**: Michal to produce updated draft EBA slides by start 4th June, all comment by end Thursday 7th. For completion by Michal by 9th June.

# Clarification on PSD2 Certificate Usage: Public facing

See email from Arno sent Fri 11/05/2018 12:50 (UK Summer time)

Key points:

* If certificate is without “certificate transparency” Google gives negative indicator.
* Not every QWAC is recognised by Browsers as EV. Each browser has its own policy for acceptance of certificates.

Arno will update document to take account of comments.

**Action 11.4**: Arno update document on recognition of PSD2 certificates by web browsers. This includes addition of statement from Google regarding green bar and support of SCT, addition of column on indicator of QWAC status and indication of how OrganisationIdentifier is handled by browsers.

# Future Areas of Work

See report of last meeting.

No further comments.

# Future Plans

The next meeting will be have day sometime 26-28 June just before EBA workshop. Please complete doodle to indicate availability: https://doodle.com/poll/wztz8rrw4dmr2kpm.

**Action 11.5:** Nick prepare 1 page PPT briefing for ESI #63 on work of the PSD2 workshops.