POSitivity magazine

THE OFFICIAL MAGAZINE OF MERCHANT PAYMENTS ECOSYSTEM • ISSUE 79 / MARCH 2019

mpe Merchant Payments Ecosystem

MPE 2019, Feb 19-21, Berlin

Key moments from conference chairs, speakers and press

MPE 2019 chair summaries *on page 6*

MPE Awards 2019 *on page 25*

Articles by MPE 2019 Speakers *on page 40*

MPE 2019 speakers turned their presentations into articles.
What they were speaking about? …

Brendan Jones
Chief Commercial Officer
Konsentus

The Challenge of TPP Identity & **Regulatory Checking for FIs** delivering PSD2 open banking

In January 2018 the European Union Payment Services Directive 2 (PSD2) came into force across Europe, delivering a consistent vision for open banking across all member states. Payment Service Users (PSUs), e.g. consumers and SMEs, will have a legal right to share their personal transactional account data from their Financial Institutions (FIs) with regulated third parties to enable better financial outcomes.

FIs must provide regulated third parties access to end user transactional account data. Key critical dates that FIs must work to, as directed by the European Banking Authority (EBA) and local National Competent Authorities are:

- March 2019 - FI's must have platforms available for external market testing
- Sept. 2019 - FIs must go live or face the risk of fines from regulators

FIs must comply with this regulation and can only provide data to regulated/authorised Third Party Providers (TPPs).

Who is Covered by PSD2 open banking

PSD2 uses the term 'Transactional Account'. The UK FCA defines a transactional account in the FCA handbook as a 'Payment Account' and a "Payment account" is defined in the FCA regulation 2 as:

"an account held in the name of one or more payment service users which is used for the execution of payment transactions"

So who is covered, almost every account that is accessible vis an online interface (i.e. mobile / internet banking etc.):

- E-wallet Wallet
- Reloadable Prepaid Card
- Bank Current and Payments Accounts

In total there are some 9,000 plus FIs in Europe that need to be ready for open market testing under mandatory PSD2 timescales.

The EBA recently stated: "Ignorance of them can of course not be used to justify non-compliance. And added, non-compliance amounts to a breach of law, with the resultant consequences for the legal entity."

The Challenge on Checking Who You Provide Data To

The regulations are clear that it is the job of the FI to validate the identity of the TPP and check their regulatory status, this is crucial to establishing the trust factor as part of the PSD2 open banking. This means that all FIs need to ensure that they only ever supply PSU data to approved/regulated TPPs. If they supply data to a TPP who is not, then they are in breach of PSD2 and GDPR.

When an FI is approached to provide data for the first time by a TPP they need to:

1. Validated the TPP eIDAS Certificate via the Qualified Trust Service Provider (QTSP) to confirm identity of TPP and associated National Competent Authority (NCA)
2. Check with the correct NCA that the TPP is regulated/approved
3. Issue the Access Token to the TPP as appropriate (PSD2 schema)

Then each time the TPP accesses the FIs API the FI needs to:

1. Validated the TPP eIDAS Certificate via the correct QTSP to confirm identity of TPP and associated NCA
2. Check with the correct NCA that the TPP is regulated/approved
3. Validate the Access Token checking that end user has not revoked Consent

Can FIs rely on eIDAS certificates?

Although Qualified Certificates and Seals provide some of the security mechanisms required by the PSD2 they do not provide all. The security and assurance that ASPSPs need to authorise a PSD2 transaction with a TPP across its dedicated interface, they need to know, in real-time, that:

- A TPP is still regulated by its National Competent Authority
- It is still approved to perform the role which is consistent with its API request
- The consents it received from the PSU are still valid, and have not been revoked by the PSU

However, verification of the TPP eIDAS certificate is not sufficient in itself. Qualified Trust Service Providers (QTSPs) have a legal obligation to validate the regulated status of a TPP, with the host NCA, at time of issuance of the eIDAS certificate(s). However, there is no requirement for them to subsequently check the status of TPP. The NCA also has no legal duty or obligation to inform a QTSP if TPP revocation has taken place and a NCA will probably not know who the QSTP is. The TPP eIDAS certificate thus states what regulated status a TPP held at time of issue, but not in the intervening period.

Is the EBA Register the solution?

Final Report on Draft RTS setting technical requirements on development, operation and maintenance of the electronic central register and on access to the information contained therein, under Article 15(4) of Directive (EU) 2015/2366 (PSD2), and Draft Implementing Technical Standards on the details and structure of the information entered by competent authorities in their public registers and notified to the EBA under Article 15(5) of Directive (EU) 2015/2366 (PSD2).

During the development of the CP, the EBA considered but disregarded the possibility of introducing a functionality in the EBA Register which would allow external applications to communicate automatically with the EBA Register. The EBA considered this 'machine-readable' functionality to be too costly for the EBA to develop and implement.

The EBA re-assessed the case for and against the development of an API and decided it would result in a significant increase in the implementation and operational costs for the EBA and could also delay the development of the EBA Register. The requested functionality was thus found to not be directly linked to the objectives of PSD2 related to the EBA Register in accordance with recital 42 of PSD2: increasing transparency, ensuring a high level of consumer protection and facilitating cooperation between the home and host competent authorities.

The result is the EBA database is not an online real time machine readable database. It is only updated twice daily with NCAs updating it once daily.

Are NCA Registers the solution?

There are 31 National Competent Authorities in the EEA and each NCA publishes data in a different structure, with different fields, many in different languages. Further each NCA publishes updates at different times, many in different ways. NCA Databases are also not generally machine readable, real-time. Some National Competent Authorities do not publish/state where TPPs have passported to and National Competent Authorities that publish "Inward Passporting EEA Authorised Firms" do not indicate which Home Member Sate passported from.
In Summary the Challenges of TPP Identity and Regulatory Checking

- The EBA Register is not an onlilne machine readable database

- National Competent Authority Databases are generally not Machine Readable
- National Competent Authorities have no legal obligation to notify Scheme Regulatory Databases other than a general published bulletin when they revoke a TPP
- National Competent Authorities have a 20 day SLA in place to notify passported NCAs when a TPP is revoked
- - There are 70+ Qualified Trust Service Providers who issue eIDAS seal Certificates that need to be integrated to check on eIDAS certificates