ERPB/2017/012
ERPB PIS 034-17
Version 1.0
15 November 2017

Euro Retail Payments Board (ERPB)

Final Report of the ERPB Working Group on Payment Initiation Services

ERPB Meeting 29 November 2017

Executive summary

In its 28 November 2016 meeting, the Euro Retail Payments Board (ERPB) established the Working Group on payment initiation services (PIS) (hereafter referred to as the "Working Group") and adopted its mandate. The task given was "to define a common set of technical, operational and business requirements for the development of an integrated market for PIS" in view of the concern that PIS might develop in a way that would require merchants to use many different providers in order to reach all potential customers and their respective account-servicing payment service providers (ASPSPs). A market-led standardisation effort would be needed to avoid fragmentation.

In June 2017, the ERPB took note of a report prepared by the Working Group, which contained a number of key objectives to help achieve the overall goal of an integrated, innovative and competitive market for PIS. The ERPB invited the Working Group to present its final report in November 2017 - taking account of the finalisation of the European Banking Authority (EBA) Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication (hereafter referred to as the "RTS"). After the June 2017 ERPB meeting, important progress has been achieved within and outside of the Working Group, including notably ensuring the commitment of the European Telecommunications Standards Institute (ETSI) to develop a standard for certificates compliant with the revised Payment Services Directive (EU) 2015/2366 (PSD2).

The report provides an overview of the European Union (EU) legal and policy framework as defined by the EU legislator and acknowledges the expectation of stakeholders to have a well-functioning, pan-European market for PIS.

The report identifies and lists all issues - technical, operational and business related - the Working Group considered as relevant, recommending requirements where the Working Group could find agreement or reflecting diverging positions in case no agreement could be reached, as well as clarifications provided by the European Commission (EC). For several complex matters such as the provision of consent by the payment service user (PSU), further work will be needed. As a consequence, the requirements provided in the report should be considered as recommendations.

Possible implications or synergies that its work may have for the provision of account information services (AIS) (and for the confirmation on the availability of funds) have been considered by the Working Group and covered in the report as appropriate. It was agreed that more work would be needed in this area.

At the time of the Working Group's activities the process for adoption and publication of the final RTS had not yet been completed, but the Working Group was kept informed by the EC about the changes it

intended to make. Notably, the Working Group was informed about the introduction of an exemption, under certain conditions, from the obligation to provide a fall-back for a dedicated interface.

The EC stressed that the goal is to standardise the dedicated interfaces. The EC invited market players to establish a European group that could organise the evaluation of standardised application programming interfaces (API) specifications with the aim of identifying the features and functionalities an API has to provide to satisfy the needs of market players. The Working Group made a first step towards the establishment of such an evaluation process by establishing an API Expert Subgroup. This work should continue, albeit no longer under a mandate of the ERPB.

A possible way forward - which was not yet discussed in detail with the Working Group - could be for ASPSPs, third-party service providers (TPPs) and PSUs at European level to appoint members to a small steering group that would i) plan and oversee the evaluation of standardised API specifications, ii) establish criteria to enable the objective evaluation of standardised API specifications (in line with the requirements of ASPSPs, TPPs and PSUs), iii) appoint technical experts to carry out this evaluation and iv) monitor the implementation of API standards. This group of technical experts would report to the steering group and identify in particular any issues that are problematic with a particular standardised API specification, and best practices that could be recommended for wider use in other API specifications or APIs. The EC, EBA and European Central Bank (ECB) should support this evaluation process as active observers, providing guidance to market players whenever required. A highly desirable outcome of this work could be a checklist with criteria for APIs which could then be used by national competent authorities (NCAs) as a basis for deciding whether an API meets the requirements for an exemption from the obligation to provide a fall-back mechanism. This work could also lead to the development of a European standard for PSD2 APIs, which could be submitted to a European Standardisation Organisation (ESO) for a formal endorsement. The steering group should report regularly to the ERPB.

Overview of the requirements recommended by the Working Group

Technical requirements

- PSU consent for the execution of the payment may be given via the payment initiation service provider (PISP), and the PISP passes on the information on the consent to the ASPSP.
- The interface should be future proofed, open to innovation and should support all authentication procedures provided by the ASPSP to the PSU. The PSU should not be required to access an ASPSP webpage as a part of the authentication process or any other relevant function as this would limit the PISP in the innovative design of its customer interfaces,
- The necessary information (i.e. the "What") the ASPSP should provide to the PISP will depend on whether the ASPSP supports immediate booking ('real-time') versus delayed booking.
- APIs must support the provision of only PIS, only AIS, or both AIS and PIS (in case of a payment) in one single combined communication session, subject to the appropriate consent given by the PSU.
- To ensure pan-European harmonisation the access to payment account (i.e. the "How") should be accommodated via common dedicated interfaces, taking the form of an API due to its combination of outward stability and inward flexibility.
- Metrics of performance should be defined in a uniform way to ensure a common well-defined and measurable basic level of API performance, and consistent with the RTS.
- APIs should work in a secure manner that will support the needs of both the ASPSP and TPP to mitigate the risk for fraud and have reliable and auditable API exchanges.
- Establish a common testing framework for a dedicated interface on a pan-European level.

Operational requirements

- Standardisation of certificate requirements. In response to one of the recommendations listed in the June 2017 Working Group's report, the ETSI started with the development of standardised certificates to accommodate new PSD2 elements. This work should be followed up by the industry.
- Qualified trust service providers (QTSPs) to be able to check PSD2 related information with NCAs, using a documented mechanism.
- Harmonisation in relation to registration, notification and exiting processes across all NCAs.
- A common, secure, resilient, reliable, and up to date operational directory service on a pan-European level. Such directory could take the form of a central directory or of a 'directory of directories' (i.e. directories based on national registers).

Business requirements

- Standardised ASPSP-PISP transaction related dispute handling process on a pan-European level.

0. Introduction

In its 28 November 2016 meeting, the ERPB established the Working Group and adopted its mandate. The task given was "to define a common set of technical, operational and business requirements for the development of an integrated market for PIS".

In June 2017, the ERPB discussed a report prepared by the Working Group. It took note of that report, which contained a number of key objectives to help achieve the overall goal of an integrated, innovative and competitive market for PIS. The ERPB invited the Working Group to present its final report - taking account of the finalisation of the RTS - at the November 2017 ERPB meeting.

The present report is the final report of the Working Group. It is organised as follows.

Section 1[1] sets the scene, i.e. the EU legal and policy framework as defined by the EU legislator and the expectation of stakeholders, notably e-commerce merchants, of a well-functioning, pan-European market for PIS. This provides the framework within which the common set of technical, operational and business requirements should be defined.

Section 2[2] identifies and lists all issues the Working Group considered as relevant, recommending common requirements where the Working Group could find agreement. For the issues where the Working Group could not find agreement, the report reflects the positions taken by the stakeholders, as well as the clarifications provided by the EC.

Section 3[3] presents a possible way forward.

It should be noted that at the time of the Working Group's activities the process for final adoption and publication of the RTS had not yet been completed. The Working Group based its conclusions on the latest published version of the RTS[4]. However, the Working Group was kept informed by the EC about the changes it intended to make to these RTS (hereafter referred as the "final RTS").

[1] This section was jointly provided by the EC and ECB.

[2] This section was based on input provided by the 'API', 'Identification' and 'Other operational and technical matters' expert subgroups, which were established by the Working Group.

[3] This section was jointly provided by the EC and ECB.

[4] http://www.eba.europa.eu/documents/10180/1806975/%28EBA-2017-E-1315%29%20Letter+from+O+Guersent%2C%20FISMA+re+Commission+intention+to+amend+the+draft+RTS+on+SCA+and+CSC+-Ares%282017%292639906.pdf/efbf06e1-b0e9-4481-88e5-b70daa663cb9

Furthermore, it should be noted that for several complex matters such as consent more work will be needed. As a consequence, the requirements provided in the report should be interpreted as recommendations.

1. Setting the scene

PSD2 includes in its scope two new main types of payment services, the PIS and the AIS. These new services provide ASPSP PSUs with another way to access online their payment account to make online payments without the need to use a credit or debit card or an e-money wallet, and to manage their personal finances in more convenient ways.

The aim is to offer PSUs a wider choice of payment services and lower costs thanks to enhanced competition. This aim is most likely to be achieved if ASPSPs offer common dedicated interfaces through which TPPs can obtain the information they need and can initiate payments. Without such common dedicated interfaces, TPPs would continue to have to rely on their own software that collects information from the online banking interfaces through a process known as 'screen scraping'. This process was regarded by many as unsafe. Moreover, this process is not as efficient, due to the investments required on the TTP side to adapt the software to a large number of different online banking interfaces which tend to evolve constantly. Therefore, for the RTS, the EBA and EC sought to create a strong incentive for ASPSPs to develop common dedicated interfaces. The incentive stems from the obligation on TPPs to use a dedicated interface when it is offered, and the prohibition to use the online banking interface in such a case. The goal is to standardise the dedicated interfaces in order to avoid fragmentation.

TPPs expressed fears that their activity might be severely disrupted if they are forced to use dedicated interfaces that may not function properly or that may prevent them from offering the same quality of service that they could achieve by going through the online banking interface. The RTS respond to these concerns by requiring ASPSPs to define transparent key performance indicators (KPIs) and service level targets for the dedicated interfaces at least as stringent as those set for online banking interfaces. The EC introduced some further safeguards for TPPs, notably in the form of a fall-back mechanism, which is basically the use of the online banking interface with a PSD2-compliant identification by TPPs. The use of the fall-back mechanism has to be duly justified by the TPP and must be strictly monitored by the NCAs which are responsible for monitoring that the dedicated interfaces work properly.

ASPSPs are keen to avoid having to offer a fall-back mechanism alongside the dedicated interface and want to avert the additional costs this represents. The final RTS therefore foresee that NCAs may exempt ASPSPs from having to provide also a fall-back mechanism, and spell out the conditions for such an exemption, which can only be granted by the NCA after having consulted the EBA:

- The dedicated interface must offer the same level of availability and performance, including support, as the online banking interface, and this must be measured through transparent KPIs and service level targets which are at least as stringent as those set for the online banking interface;
- The dedicated interface must not create obstacles to the provision of PIS and AIS;
- The dedicated interface must have been tested for at least three months, and widely used by the market players for another three months, and it must have satisfied market players;
- All problems related to a dedicated interface must have been resolved without undue delay.

Already at the ERPB meeting in November 2015, when the PSD2 was just being adopted, one member raised the concern that PIS might develop in a way that would require merchants to use many different providers of such services in order to reach all potential customers and their respective ASPSPs, especially regarding cross-border e-commerce payments, thus leading to fragmentation. In practice, PSD2 and the RTS will not cover all aspects that are relevant for the development of an integrated market of PIS in the EU. And in fact, not all of these aspects should indeed be regulated, e.g. in order to leave room for innovation. Market players need to agree on common rules, practices, and standards in line with the requirements set by EU legislation, specifically PSD2, the RTS, and competition law. For example, some kind of "rulebook" covering business practices, data elements, and processing formats may be considered at some stage. It might also be helpful to harmonise the technical communication between the PISP and the ASPSP by the adoption of common technical solutions based, for example, on APIs developed by the industry.

This led the ERPB to consider in its June 2016 meeting the possible role it could play with regard to defining the concrete deliverables needed for achieving a pan-European approach as regards the provision of PIS. At a stakeholder meeting on 6 October 2016 with the participation of standardisation initiatives, providers, as well as ERPB member organisations, there was consensus on the objective of the provision of PIS at pan-European level and that a market-led standardisation effort would be needed to supplement the legal framework provided by the PSD2 and the RTS. In its 28 November 2016 meeting, the ERPB established the Working Group and adopted its mandate. The task given was "to define a common set of technical, operational and business requirements for the development of an integrated market for PIS".

The Working Group presented a report to the June 2017 meeting of the ERPB. Since then, the work progressed also thanks to clarifications provided by the EC at the subsequent Working Group meetings.

2. Requirements for the development of an integrated market for PIS

The Working Group has discussed all relevant issues, whether these are related to technical, operational or business requirements. Some issues were of a legal nature, but needed to be tackled as they had a

strong relevance for the specifications for APIs. This section will start with the technical requirements, i.e. those that relate to the interface between the ASPSP and PISP. For each issue common requirements are recommended where the Working Group could find agreement. For the issues where the Working Group could not find agreement, the report only reflects the positions taken by the stakeholders, as well as the clarifications provided by the EC.

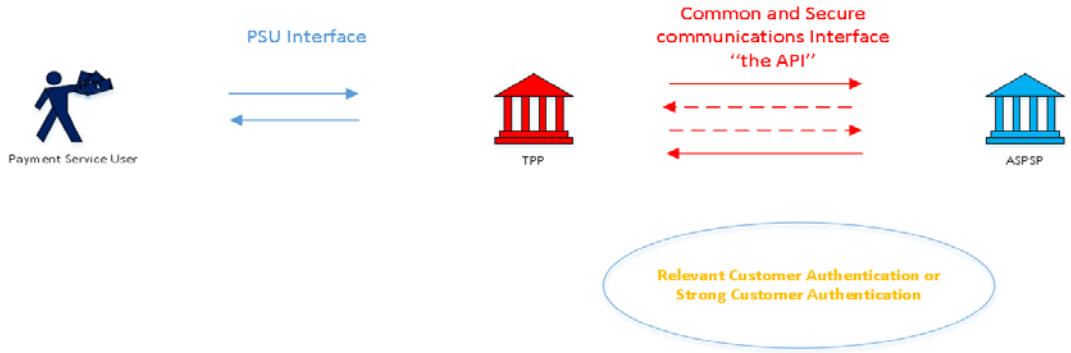
2.1. Technical requirements

2.1.1. Giving user consent

The understanding is that the 'user consent' process can refer to different stages of the payment service flow, i.e.:

- Consent to initiate a payment (to the TPP);
- Consent to execute the payment (through a TPP or not) (authorisation);
- Consent to access, process and retain (store) data;
- Consent to share data with TPP (authorisation).

The Working Group focused on the interaction between the TPP and ASPSP (see red arrows in below diagram):



Several PISPs argue that the PSU does not need to give consent to the ASPSP, but can do so to the PISP. Specifically, PISPs want to avoid that consent needs to be given in a separate process and/or twice, as this could block or disturb the PIS transaction.

Several ASPSPs argue that the consent data should be passed on from the PISP to the ASPSP, in order to be verified by the ASPSP for traceability and proof management purposes. Information on the scope of

the user consent given is especially important, in view of the General Data Protection Regulation (GDPR), in case the ASPSP needs to provide account-related information to the PISP concerning a PIS transaction (see requirements on the "What").

The provision of consent is a complex matter and further work will be needed. Moreover, the approaches for PIS and AIS differ.

The EC clarified that consent for the execution of a payment may be given via the PISP, i.e. not directly to the ASPSP, as foreseen in Article 64(2) PSD2. ASPSPs are required (see Art. 66(4) PSD2) to provide or make available to the PISPs all information on the initiation of the payment transaction and all information accessible to the ASPSP regarding the execution of the payment transaction. The EC's current view is that the processing of personal data by the ASPSP for PIS is to be considered as necessary for compliance with a legal obligation to which the controller is subject (see Art. 6(3) GDPR). On the PISP or AISP side, the information provided to the PSU before entering into the contract would need to clearly state which personal data will be accessed to provide the requested services and for what purpose. PISPs and AISPs will be liable for the content of this information and for complying with the GDPR requirements, while ASPSPs can rely on the clear identification of TPPs and on customer authentication as foreseen under PSD2 to ascertain that they have the right to pass on personal data to a third party.

The Working Group agrees on the following requirements for giving user consent:

Consent for the execution of the payment may be given via the PISP, and the PISP passes on the information on the consent to the ASPSP. Moreover, the PSU needs to have a clear view of the consent to be given including its scope and purpose.

2.1.2. Relying on the authentication procedures provided by the ASPSP

If APIs are to accommodate PIS/AIS services delivered on any device or channel, then the API must allow for the exchange of all necessary data elements (only) between the TPP and APSP throughout the PIS/AIS session, without requiring the PSU to perform its SCA on a webpage provided by the ASPSP.

However, some ASPSPs argue that they can require such authentication procedure, which would imply that the PSU needs to use a browser-based interface.

PISPs argue that such authentication procedure is not compatible with their freedom to design the customer interface as it would limit the PISP when providing PIS including at the Point of Sale and/or via voice-based technology. In the view of the TPPs, whenever the ASPSP provides an authentication

procedure based on transmittable/portable credentials, a PISP[5] or AISP[6] transmits the personalised security credentials to the ASPSP.

The EC clarified that requiring the PSU to perform its SCA on the webpage provided by the ASPSP cannot be imposed on the PIS and AIS providers.

The Working Group agrees on the following requirements for relying on the authentication procedures provided by the ASPSP:

The interface should be future proofed, open to innovation and should support all authentication procedures provided by the ASPSP to the PSU.

The ASPSP may require the use of the authentication devices and/or authentication applications normally used for customer authentication (e.g. the PSU's mobile telephone for sending an SMS, mobile banking app, mobile ID app, fingerprint reader, TAN-code generator) but should not require that the PSU has to access an ASPSP webpage as a part of the authentication process or any other relevant function as this would limit the PISP in the innovative design of its customer interfaces.

TPPs should pass on as much security relevant information as possible to ASPSPs for fraud and sanctions / financial crime / AML detection purposes.

2.1.3. Providing the necessary information (the "What")

All customers whose payment account is accessible online should be able to use PIS. All ASPSPs should provide information enabling the PISP to confirm to a payee/merchant that the payment has been initiated and that it will - in all likelihood - be executed. If SEPA Instant Credit Transfer (SCT Inst) is used, certainty that the payment has been executed is provided in a matter of seconds to the PISP (barring regulatory exceptions).

[5] Article 66 3. (b): The PISP shall "ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels"

[6] Article 67 2. (b): The AISP shall "ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that when they are transmitted by the account information service provider, this is done through safe and efficient channels"

However, for payments to be initiated from accounts at ASPSPs which are not immediately processing the transactions, a risk of non-execution exists. PISPs believe that the following data should as a result be in scope for TPPs holding a PIS license only:

- Pre-payment initiation "available balance", corresponding to the last known account balance, any pending/scheduled transactions, and the overdraft limit (if any);
- Account statement history for the same period as available for the PSU directly;
- Post payment initiation "available balance" (for the cases when a batch is processed in between initial log-in and the initiation of the payment).

ASPSPs argued that the PISP should also have an AIS licence if it wants to obtain information needed to assess whether a payment can be initiated. PISPs disagreed, even though it might not be a major obstacle for some PISPs (but it could be an obstacle for new, smaller PISPs). One member warned that all licensing does cost money, time and effort, and requires professional indemnity insurance; a clear description of activities would be needed. One AISP argued the services should not be presented as necessarily combined, as there should also be "pure" AIS (which could have lower insurance premiums).

The EC indicated that the RTS oblige ASPSPs to provide PISPs with the same information that is available to a PSU when directly initiating the payment through the online banking interface. This information can be used to assess whether a payment can be initiated without running the risk of an unauthorised overdraft or a rejection of the payment order. The PISP should be able to make such an assessment prior to confirming to the merchant that the payment will, in all likelihood, be executed.

The EC further clarified that a PISP does not need a second license for receiving the data it needs for the provision of PIS (as long as it is not storing or using that information for other purposes).

The Working Group agrees on the following requirements for providing the necessary information (the "What"):

An ASPSP processing in real-time with immediate booking on the payer's payment account informs the PISP that the initiated transaction has been booked, with funds reserved; the PISP may be assured that it will - in all likelihood - be executed. If SCT Inst is used, certainty that the payment has been executed is provided in a matter of seconds to the PISP (barring regulatory exceptions).

An ASPSP working with delayed booking informs the PISP on the "available balance" (= account balance, plus any overdraft limit, minus pending/scheduled transactions) and ex-post available balance (post payment initiation) - if such information is accessible to the PSU when initiating an online payment and with the PSU's consent on the type of data accessed and the purpose of the processing (and as long as

the PISP is not storing or using that information for other purposes) - and acknowledges that the payment order is placed; on that basis the PISP is able to assess the risk of non-execution.

2.1.4. Combining AIS with PIS in one communication session

TPPs are of the view that in order to provide a good PIS product, it is not unusual to require AIS elements, and vice versa. From a technical point of view, the Working Group agreed that AIS and PIS can be supported within the same inter-PSP communication session. However, there is some disagreement on whether the ASPSP is obliged to offer such combined session per se, partly based on different views on what a "session" constitutes. More work is hence needed to clarify this.

If a TPP combines the role of AISP with the role of PISP, access should be provided in one single communication session to ensure a seamless PSU payment experience and/or avoid double customer authentication. A typical example is the AISP presenting an overview of all the PSU's payment accounts.

The EC clarified that it agrees with such understanding.

The Working Group agrees on the following requirements for combining AIS with PIS in one communication session:

APIs must support the provision of only PIS, only AIS, or both AIS and PIS (in case of a payment) in one single combined communication session, subject to the appropriate consent given by the PSU. This can be achieved technically via different calls to the ASPSP.

2.1.5. Offering an interface (the "How")

Without further work by the market, each of the more than 4,000 ASPSPs will have to develop the specifications for its own interface, which takes time and money, and will lead to a lot of diversity in the technical way of connecting with each ASPSP. As a principle, there should be one or a few common interfaces, as this would increase the efficiency of PIS, its usability throughout Europe, as well as facilitate market entry by new PISPs. Only dedicated interfaces can be standardised, as one cannot (realistically) expect 4,000+ ASPSPs to standardise their online banking interfaces, which are their primary communication and commercial channel with their customers. APIs are seen as the state-of-the-art method for building such interfaces, as these combine inward flexibility and outward stability.

Currently, five standardisation initiatives providing API specifications are known, namely the Berlin Group, Open Banking UK, STET, Polish Bank Association and Slovakian Banking Association. The Working Group organised a survey in order to be able to analyse similarities and differences between the work of these initiatives. The survey outcome (see Annex 3) clearly shows high-level alignment. It is noted that

harmonisation efforts are being undertaken, including in the context of the International Standardization Organisation (ISO).

The providers of API specifications should make efforts to limit their specification to the ASPSP - PISP domain, without affecting the PISP - merchant domain. However, these providers should ensure that their specification cater for interoperability at the level of the merchant.

The EC confirmed that it supports the use of common APIs, provided that these fully comply with the provisions of PSD2 and RTS and open the market for the provision of PIS and AIS services.

The Working Group agrees on the following requirements for offering an interface (the "How"):

ASPSPs should opt for a dedicated interface, taking the form of an API due to its combination of outward stability and inward flexibility. The interface should cover at least all new PSD2 services. ASPSPs should make use of common implementation specifications (if and once available).

Providers of API specifications should take on board all ERPB recommendations, specifically on the "What" in as far as agreement was reached. They should allow various options, if this is market practice, and should not technically leave out or force an option. "European approaches" are to be preferred over "national" initiatives, to facilitate cross border e-commerce and the respective payments.

2.1.6. Delivering performance and metrics

APIs must perform at least as well as the PSU's online banking interface, i.e. API performance requirements should at least be as stringent as those set for online banking interfaces. Metrics of performance should be defined in a uniform way to ensure a common well-defined and measurable basic level of performance, and consistent with the RTS.

The Working Group discussed that possible metrics could include availability (uptime for the API), API response time, peak API load, data quality, error rate, authentication failures and equal performance vis-à-vis online banking.

The EC clarified that it agrees with such understanding.

The Working Group agrees on the following requirements for delivering performance and metrics:

Metrics of performance should be defined in a uniform way to ensure a common well-defined and measurable basic level of performance.

Possible metrics could include availability (uptime for the API), API response time, peak API load, data quality, error rate, authentication failures and equal performance vis-à-vis online banking.

2.1.7. Ensuring security of the interface

The Working Group concurs that the API should work in a secure manner that will support the needs of both the ASPSP and TPP to mitigate the risk for fraud and have reliable and auditable API exchanges.

The Working Group agrees on the following requirements for ensuring security of the interface:

APIs should work in a secure manner that will support the needs of both the ASPSP and TPP to mitigate the risk for fraud and have reliable and auditable API exchanges.

2.1.8. Common testing framework of a dedicated interface

The RTS stipulate that ASPSPs shall make available a testing facility to allow TPPs to test their software and applications used for offering a payment service to users.

The Working Group sees benefit in harmonising the testing framework on a pan-European level. Therefore, the Working Group agreed on a detailed list of key common requirements which would help to ensure reaching a minimum level of harmonisation (see Annex 4).

In relation to the possible exemption from the fall-back option, the EC clarified that the final RTS will require that the dedicated interface must have been tested for at least three months, and widely used by the market players for another three months, and it must have satisfied market players.

More objective criteria are needed at European level based on which the NCAs will certify APIs.

The Working Group agrees on the following requirements for testing of TPP services in a dedicated interface:

Publication of API related changes should include common basic functional, security and service requirements, a maintenance plan and supported versions of the dedicated interface.

Issuance of a testing check list, KPIs and statistics demonstrating the well-functioning dedicated interface version in the test environment.

The test environment should support full end-to-end testing.

Access to test environment and quality of service during business hours should be ensured.

Documentation for dedicated interface testing shall at least be available in English.

2.2. Operational requirements

2.2.1. Certificates

The RTS require that a registration number, the NCA name and the role(s) of the PSP are included in the two types of certificate i.e. “Qualified Website Certificates” and “Qualified Certificates for Seals”, which are specified in Annex III and IV of the eIDAS regulation[7].

In response to one of the recommendations listed in the June 2017 Working Group report, and in liaison with the Working Group, ETSI has already started with the development of standardised certificates to accommodate new PSD2 elements.

The Working Group agrees on the following main requirements for certificates:

In order to issue certificates QTSPs have a legal requirement to verify PSD2 related information. They will need to be able to check with NCAs using a documented mechanism.

It is important that QTSPs are able to check with NCAs whether PSD2 specific data in the certificates continues to be valid.

Clarity should exist around which category of PSP is allowed to have which role(s) (in their certificates), in each country (see Annexes 5 and 6).

In line with eIDAS, the subject (i.e. the PSP who holds the certificate) is obliged to inform the QTSP of any changes. However, other parties may also inform the QTSP of changes (e.g. NCA). The QTSP once informed, must check the information and is liable for revocation within 24 hours if applicable.

Certificates need to be standardised for new PSD2 elements. ETSI has started this work via the creation of a dedicated work group. In order to complete this work, ETSI requires the existence of a consolidated and uniform list of NCA names to be inserted into the certificate and respecting certain rules (see Annexes 5,6 and 7).

2.2.2. Operational directories

There is a need for harmonisation in relation to registration, notification and exiting processes across all NCAs and for a common, secure, resilient, reliable, and up to date operational directory service on a pan-European level. Such directory could take the form of a central directory or of a ‘directory of directories’ (i.e. directories based on national registers).

[7] Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC

Discussions within the Working Group fell under the following three headings:

- For ASPSPs: use a directory as a single source of truth about the regulatory status of a TPP, using the certificates to authenticate them.
- For ASPSPs: use a directory to obtain operational data (e.g. contact numbers) that are stored in the directory.
- For TPPs: provide a single view of where the documentation of each ASPSP is stored, as well as the support telephone number or other operational information.

Many ASPSPs will base their trust on the public register of PSPs that will be published on the website of the NCA of their member state (or if needed other member states). However, from a more operational point of view, ASPSPs would prefer having one consolidated directory of all data (i.e. contained in the public registers but also including certificates) that would be machine readable, online and up-to-date. And it should contain data from all PSPs of the EU (so that there are no boundaries to business activities). At this stage, it is not yet clear whether this would be feasible (and by when).

Diverging views exist concerning the scope of the information to be included in the directory:

- Some ASPSPs communicated a requirement for operational data, such as contact information for each PSP (i.e. role; name; telephone number with country code; email address).
- Some TPPs would like to see a single repository of operational data for ASPSPs. For each ASPSP this could include the list of supported APIs and for each API, the Uniform Resource Locator (URL) of the developer website (i.e. documentation), the URL of the testing system / sandbox and the URL of the live site, support hours and contact details.
- Some Working Group members do not see the need for the directory to list information that in any case is to be found on the ASPSP website. In their view, it only extends the workload for the directory providers and risks having them put less focus/effort on more important tasks.

The Working Group agrees on the following main requirements for operational directories:

The directory should provide a real-time accessible, machine readable and standardised repository of the details of all authorised and revoked TPPs as published by NCAs. These details should include regulatory information such as passporting information, and could also include operational information such as contact details.

The directory should not be a single point of failure, but could be shared and distributed via different types of technical architectures, and provided by multiple legal entities in order to prevent internal problems from having an effect on all European PIS and AIS transactions.

The directory should not permit any user or entity (participant) registered in the directory to change the regulatory data, whose only source should be the NCAs. The directory should allow participants to update their own operational data. No participants should be allowed to change another participant's data, unless permissions have been explicitly assigned (e.g. in the context of groups, with many separate legal entities).

NCAs to provide clear instructions as to where to find each category of PSP in their register, considering local language. The NCA could for example provide a mapping from local language to English.

For providing proof in case of disputes on past transactions it must be possible to access historical data over a period of at least 13 months.

(see Annexes 5 and 6)

2.3. Business requirements

2.3.1. Incident handling and dispute resolution

The Working Group identified the need for a standardised ASPSP-PISP transaction related dispute handling process on a pan-European level.

The aim is to maintain trust among relevant parties and improve the efficiency of incident and dispute handling. This to ensure that any issue is solved in a timely and effective manner, with good cooperation and in good faith, and in the ultimate interest of the PSU.

The standardisation of dispute handling processes - and especially the need to automate some of these processes - has been discussed by the Working Group but without reaching a consensus due to diverging views on the expected volumes, ranging from zero to several thousand per year. Should the number be significant, further work will be needed; no process is however foreseen to initiate and manage such work at this stage. A high-level proposal for dispute handling has been included in Annex 8.

The Working Group has diverging views on whether the mediation process, in case parties cannot reach an agreement, should be harmonised at a pan-European level.

The EC clarified that dispute handling between PSU and PSPs is already covered by PSD2.

The Working Group agrees on the following main requirements for incident handling and dispute resolution:

Each party should have a central point of contact for incidents and disputes. Procedures to be adapted to the relevant use case/scenario (see Annex 9 for dispute use cases).

English should be supported (in addition to any local language).

Implementation of a manual process as a minimum service. An (optional) automated communication mechanism for dispute/incident reporting through a specific dedicated interface (API) could be considered to generate further efficiencies.

Contact details to be provided on the PSPs websites and in the dedicated interface documentation and/or NCA register, as relevant.

Disputes to be handled bilaterally. If the parties cannot reach an agreement, mediation could be considered before going to court.

2.4. Possible implications or synergies for AIS

Possible implications or synergies that its work may have for the provision of AIS (and for the confirmation on the availability of funds) have been considered by the Working Group. This has been covered in the various sections above as appropriate. More work is however needed in this area.

3. A possible way forward

The task of the Working Group was "to define a common set of technical, operational and business requirements for the development of an integrated market for PIS". These were seen as needed for the deployment of PIS as a safe and efficient payment service also working at pan-European level.

As listed in Section 2, several common requirements have been recommended, whereas on other issues diverging positions remain, including as regards their importance and the need for further work. For example, the standardisation of dispute handling processes has been discussed but without reaching a consensus due to diverging views on the expected volumes.

It is clear that a PISP will be dependent on other actors for the day-to-day quality of the payment service it provides. In case of problems with a specific actor, it would need to engage in bilateral communications which might end up in legal proceedings which can take many years. Unlike most other payment services, an organisation with the responsibility to ensure swiftly that the basic elements for the provision of the payment service are put in place, maintained and complied with at all times, is absent.

The Working Group considers that it has made significant progress in identifying issues that may arise in relation to dedicated interfaces between ASPSPs and TPPs, and in working out solutions. However, the Working Group is of the opinion that a lot of work is still to be done e.g. on API performance and features

that fully satisfy the needs of market players. Moreover, it is likely that during the development and implementation of dedicated interfaces further issues will emerge.

The transition to common dedicated interfaces, which is desired by regulators and all market players alike, will only happen if all these issues can be resolved. While the Working Group was examining requirements for interfaces for PIS, the EC considered the EBA proposal for RTS that spell out the requirements for communication interfaces between ASPSPs and TPPs. The final RTS will be adopted shortly after the finalisation of this report, but the EC signalled that the final RTS will create strong incentives for ASPSPs to offer dedicated interfaces for TPPs; if these meet the requirements of market players, then ASPSPs should be exempted from having to offer TPPs an access to account also through the online banking interfaces as a fall-back mechanism.

If ASPSPs want to avoid having to invest in both a dedicated interface (API) and in the adaptation of their online banking interfaces to make them compliant with PSD2 for TPP access, then they have to move fast: their APIs would have to be made available for testing six months before the end of the 18-month implementation period foreseen in the final RTS. The period of 18 months starts counting from the publication of the final RTS in the Official Journal. It is to be expected that the final RTS would become applicable in September 2019. Market players will thus have to develop and implement dedicated interfaces, offer them for testing for three months, and afterwards offer them to the market for another three months at least. By early 2019, the interfaces will therefore have to be ready; standardisation efforts will for many ASPSPs be crucial in order to meet this tight deadline.

With the adoption of the final RTS by the EC, market players will have received as much guidance as they can expect from the EC on how to deploy PSD2-compliant communication interfaces, and this guidance also reflects the discussions held in the Working Group. The adoption of the final RTS and the publication of the first API standards open a new phase during which market players should jointly review the different standards for dedicated interfaces, clarify the liability rules, and ensure that all their needs are met: TPPs' needs in terms of reliability and functionality, and ASPSPs' needs for legal certainty, notably in relation to the protection of funds and data.

While the final RTS will leave it to NCAs to decide whether an API is good enough to justify an exemption from having to provide a fall-back mechanism, it also requires NCAs to consult EBA before granting an exemption, and subject to market players having confirmed that the API is working for them. The final RTS thus makes it crucial that ASPSPs and TPPs cooperate on dedicated interfaces at the European level, to promote standardisation and to ensure that PIS and AIS can be smoothly provided across borders. Such cooperation at the European level will also reveal any divergences in national practices and will help the EBA in its task of overseeing exemption practices of NCAs and, thus, ensuring supervisory convergence. This is essential to avoid any disputes over whether TPPs should be allowed to

access account information and initiate payments via online banking interfaces, as they would be should the dedicated interfaces fail to deliver.

The EC therefore invited market players to establish a European group that could organise the evaluation of standardised API specifications with the aim of identifying the features and functionalities an API has to provide to satisfy the needs of market players. This work could not have been carried out by the Working Group, as API standards were being developed during its mandate and the regulatory context (notably the final RTS) was not yet fully clear. However, the Working Group made a first step towards the establishment of such an evaluation process by establishing an API Expert Subgroup. This work should continue, albeit no longer under a mandate of the ERPB. It must be added that ASPSPs have stressed the need for a clear governance framework for such a new group.

A possible way forward - which was not yet discussed in detail with the Working Group - could be for ASPSPs, TPPs and PSUs at European level to appoint members to a small steering group that would i) plan and oversee the evaluation of standardised API specifications, ii) establish criteria to enable the objective evaluation of standardised API specifications (in line with the requirements of ASPSPs, TPPs and PSUs), iii) appoint technical experts to carry out this evaluation and iv) monitor the implementation of API standards. This group of technical experts would report to the steering group and identify in particular any issues that are problematic with a particular standardised API specification, and best practices that could be recommended for wider use in other API specifications or APIs. A highly desirable outcome of this work could be a checklist with criteria for APIs which could then be used by NCAs as a basis for deciding whether an API meets the requirements for an exemption from the obligation to provide a fall-back mechanism. This work could also lead to the development of a European standard for PSD2 APIs, which could be submitted to a ESO for a formal endorsement.

The steering group should report regularly to the ERPB.

The EC, EBA and ECB should support this evaluation process as active observers, providing guidance to market players whenever required.

It will be for individual ASPSPs to decide whether they want to offer a dedicated interface and how this would be specified. However, it should also be clear that if other market players are not satisfied with this interface (based on objective criteria which will emerge from the evaluation process described above), and if guidance from the EC, EBA and ECB has been ignored to a significant extent in the design of this interface, then the NCA would not be able to exempt this ASPSP from having to provide a fall-back mechanism, and the TPPs could not be prevented from using this fall-back mechanism.

The above-mentioned evaluation process should push ASPSPs towards the implementation of well-functioning interfaces from both a technical and a functional perspective. ASPSPs also have a strong

incentive to make use of the standardised API specifications that are being developed, as this would simplify their work on an API and give them assurance that they comply fully with legislative requirements.

For the further work on some other ('non-API') issues seen as relevant for the efficient and pan-European provision of PIS the way forward is that for example work on the standardisation of PSD2-certificates has started at ETSI and that at least one provider has announced its intention to offer directory services. The standardisation of dispute-handling might also need to be looked into by the steering group, ideally based on early experiences with the new payment services.

Furthermore, the Working Group was of the view that more work was needed for AIS including with regard to the process of evaluating APIs.

The ERPB is invited to:

- Take note of the report.
- Endorse the recommended requirements as provided in section 2.
- Support the way forward as summarised in section 3.

Annex 1: List of ERPB Working Group participants (as from June 2017)

Category	Name	Institution
Co-Chair	Alain Benedetti	EPC (BNP Paribas)
	Michel Van Mello	EuroCommerce (Colruyt)
Member	Marieke van Berkel	EACB
	Massimo Battistella	EACT (Telecom Italia)
	Bettina Schönfeld	EBF (BdB)
	Just Hasselaar	Ecommerce Europe
	Thaer Sabri	EMA
	Hervé Robache	EPC (French Banking Federation)
	Derrick Brown	EPIF (Worldpay)
	Beatriz Kissler	ESBG (Caixa Bank)
	Pascal Spittler	EuroCommerce (IKEA) (co-Chair 'Other' subgroup)
	Jean Allix	BEUC
ECB	Pierre Petit	ECB
	Iddo de Jong	ECB
NCB	Dirk Schrade	Deutsche Bundesbank
	Gregorio Rubio	Banco de España
	Antoine Lhuissier	Banque de France
	Ravenio Parrini	Banca d'Italia
	Jakob Rotte	De Nederlandsche Bank
	Anna Sedliaková	Národná banka Slovenska
Observer	Krzysztof Zurek	European Commission
	Mario Maawad	ESBG (CaixaBank) (co-Chair 'Other' subgroup)
Standardisation initiative	Ortwin Scheja	Berlin Group (SRC Consulting)
	Michael Salmony	CAPS (EquensWorldline)
	Thomas Egner	EBA Association
PISP	Chris Boogmans	Isabel Group (co-Chair 'Identification' subgroup)
	Bartosz Berestecki	PayU
	Aoife Houlihan	Sofort GmbH
	Oscar Berglund	Trustly Group AB (co-Chair 'API' subgroup)
AISP	Kevin Voges	AFAS Personal
	Joan Burkovic	Bankin
Other PIS-stakeholder	Max Geerling	Dutch Payments Association / iDEAL
	James Whittle	Payments UK (co-Chair 'API' subgroup)
	John Broxis	Preta / MyBank (co-chair 'Identification' subgroup)
Guest	Hans Georg Spliethoff	EMOTA (Otto)
Secretariat	Etienne Goosse	EPC
	Christophe Godefroi	EPC

Annex 2: Mandate ERPB Working Group on Payment Initiation Services

ERPB Secretariat

ECB-UNRESTRICTED
28 November 2016
ERPB/2016/012rev2

MANDATE OF THE WORKING GROUP ON PAYMENT INITIATION SERVICES

Based on Article 8 of the mandate of the Euro Retail Payments Board (ERPB), a working group is set up with the participation of relevant stakeholders to identify conditions for the development of an integrated, innovative and competitive market for payment initiation services in the EU.

1. Scope

The revised Payment Services Directive (PSD2) adds inter alia payment initiation services (PIS) to the list of payment services. It gives providers of payment initiation services (PISPs) access to payment accounts to initiate an online payment at the customer's request. The PSD2 also provides that a PISP identifies itself to the account-servicing payment service provider (ASPSP) and that both communicate with each other in a secure way. The PSD2 mandates the European Banking Authority (EBA) to develop draft Regulatory Technical Standards (RTS) specifying *inter alia* the requirements for common and secure open standards of communication.

In order to comply with the legal requirements, an ASPSP would have to develop and/or implement a technical solution (interface), enabling PISPs to identify to and securely communicate with the ASPSP. In turn, PISPs would have to adapt their systems for the interaction with each ASPSP, as well as for the efficient provision of services to its customers.

PSD2 and the RTS establish a uniform legal framework for the provision of PIS in the EU. The task of the working group will be to define a common set of technical, operational and business requirements for the development of an integrated market for PIS. The technical requirements should form the basis for defining the detailed technical specifications that are needed to support that objective.

In conducting its work, the working group will build on the list of areas of work identified in the Secretariat note submitted for the November 2016 ERPB meeting in line with market needs. It should take on board all relevant standardisation initiatives that are underway.

The working group shall consider possible implications or synergies that its work may have for the provision of account information services (AIS) and for the confirmation on the availability of funds.

2. Deliverables and time horizon

The working group is expected to start working shortly after the November 2016 ERPB meeting. The group will prepare a report for the June 2017 meeting covering the technical, operational and business requirements needed for the provision of efficient and integrated PIS services. The working group shall particularly focus on technical requirements and those operational elements (in particular the PISP directory service) which may be more time critical. This timeline should leave sufficient time for relevant players to implement all conditions identified by the ERPB as critical for development of an EU wide integrated market for PIS by the time the EBA RTS start to apply, i.e. towards the end of 2018. In view of the wide market interest in this matter, the working group shall aim for full transparency, e.g. by sharing their work on the ERPB website.

3. Participants and chairmanship

The working group shall include relevant stakeholders, including representatives of i) ERPB member associations, ii) European standardisation initiatives, and iii) PISPs and, for aspects of the work that would be relevant to AIS, providers of AIS (AISPs). One representative of the ECB and a limited number of representatives of euro area NCBs are invited to join the working group as active participants. A representative of the EU Commission will be invited as observer. The working group will be co-chaired by E-Commerce Europe (demand side) and the European Payments Council (supply side).

Members representing their associations and the co-chairs will be appointed by the ERPB Chair based on suggestions from their respective associations. Other participants – after expressing interest to the ERPB secretariat – may be invited by the ERPB Chair to join the group based on consultation with the members of the ERPB.

5. Rules of procedure

The mandate of the ERPB defines a broad set of rules for the procedures of its working groups: the working group takes positions on a ¾ majority basis; dissenting opinions are mentioned in any relevant documents prepared by the working group. The members of the group decide on how to organise secretarial support, timing and rules of meetings and communication via written procedure, as well as on the need and format of any interim working documentation produced. Costs related to the operation, meetings, chairmanship and secretariat are carried by the members of the group themselves.

Annex 3: Overview survey API standardisation initiatives

Background					
Name initiative	**Berlin Group**	**Open Banking UK**	**PSD2 Polish API**	**Slovak Banking API Standard**	**STET PSD2 API**
URL (documentation)	Drafts published for consultation under https://www.berlin-group.org/market-consultations	https://www.openbanking.org.uk/read-write-apis/		http://docs.sbaonline.apiary.io (draft version)	https://www.stet.eu/#article247
Licensing conditions	Exact licensing model not agreed but will not have a cost to use.	MIT Open Licence			Creative Commons – Attribution 3.0 France (CC BY 3.0 FR).
Contact	Ortwin Scheja (SRC)	Chris Michael	Maciej Kostro (The Polish Bank Association)	Marcel Laznia	Hervé Robache (STET)
Email	Ortwin.scheja@src-gmbh.de	Chris.Michael@openbanking.org.uk	maciej.kostro@zbp.pl	Marcel.laznia@sbaonline.sk	psd2@stet.eu
Technical Characteristics					
Transport protocol 1	TLS	MA TLS v1.2 for communication between TPP & ASPSP.	TLS	TLS	TLS v1.2 minimum
Transport protocol 2		HTTPS 1.1		HTTP	HTTP v1.1 minimum
Applicative protocol	REST	REST	REST	REST	REST (Maturity model level 3 using HAL (Hypertext Application Language).
Authorization protocol 1	OAUTH2 (as an optional pre-step, depending on the ASPSP infrastructure).	OIDC (can optionally regress to OAUTH2).	OAUTH2	OAUTH2	OAUTH 2 (Authorization code token + client credential token).

Authorization protocol 2		OIDC with FAPI profile & OB profile			
Character set 1	UTF-8	UTF-8	UTF-8	UTF-8	UTF-8
Character set 2					
Data structure 1	JSON	JSON	JSON	JSON	JSON
Data structure 2	XML (XML only used as an additional option where pain.001 messages or camt.5x messages need to be transported)			XML	
Data model origin	ISO20022	ISO20022		ISO20022 (ISO 20022 is preferable used for attributes name)	ISO20022
Identifier naming convention 1	ISO20022 extended names	ISO20022 extended names		ISO20022 extended names (JSON)	ISO20022 short names
Identifier naming convention 2				ISO20022 short names (XML)	
Character case convention 1	snake_case	UpperCamelCase	LowerCamelCase	LowerCamelCase	UpperCamelCase (UpperCamelCase is used respectful of ISO20022 XML identifiers)
Character case convention 2					LowerCamelCase
Security features					
TPP authentication by ASPSP 1	Based on TLS	Transport layer - MA TLS 1.2 Application layer - Oauth2 / OIDC	Based on TLS	Based on TLS	Based on TLS

TPP authentication by ASPSP 2	As an option, ASPSP might mandate TPPs to use an electronic signature on application level in addition.			OAUTH2	
ASPSP authentication by TPP 1	Based on TLS	Transport layer - MA TLS 1.2	Based on TLS	Based on TLS	Based on TLS
ASPSP authentication by TPP 2				OAUTH2	
PSU authentication 1: Processed independently by the TPP and the ASPSP	Yes (For clarity, we support 3 SCA Models – Embedded, Re-direct and De-coupled.)				Yes
PSU authentication 2: Delegated by the TPP to the ASPSP	Yes (For clarity, we support 3 SCA Models – Embedded, Re-direct and De-coupled.)	Yes	Yes	Yes	
PSU authentication 3: Processed by the TPP and forwarded to the ASPSP					
PSU authentication: other					
Data encryption	Based on TLS	TLS 1.2	Based on TLS	Based on TLS	Based on TLS
Proof management	Optional (signing the body based on IETF Draft Http-Signature).	OIDC Signed Request Parameter (Section 6.1).			Non-repudiation mechanism based on IETF Draft Http-Signature.
Fraud detection support	TPPs are asked to forward PSU related technical data to support fraud mechanisms within	Header fields defined by FAPI. Additional fields in body.	TPPs are asked to forward PSU related technical data to support fraud mechanisms within	Fraud Prevention Solution based on Gratner L1-L5.	requested additional http-headers providing information on PSU/TPP connection

	the ASPSP.		the ASPSP.		
How can the TPP trigger the PSU authentication through the API? Please provide details of all available flows and methods?	Embedded, Decoupled, Redirect supported in the BG API Standard. Implementation decision by ASPSP.	Based on Oauth2 flows where TPP redirects PSU to ASPSP interface to authenticate and authorise, then PSU redirected back to TPP. OBIE believe other methods could be adopted over time, but ONLY if they follow an appropriate and secure standard which is supported and maintained by a credible global body.	Polish API standard, at this point, assumes implementing the model which requires PSU to confirm its identity by entering credentials on ASPSP's website. In Poland, majority of TPPs are using this method at the moment (e.g. pay-by-link solution which is dominant e-commerce payment method in Poland). In the next phase of standard development we will consider to add alternative methods as a part of the standard in line with regulatory and business requirements.	Slovak Banking API Standard at the first phase will describe redirect method of PSU authentication. But ASPSP will be able choose also another method.	STET PSD2 API v1.2.3, to be published in November 2017, is supporting redirect and decoupled authentication methods. The choice of the authentication method is based on the agreement between the PSU and the PSP, as specified by PSD2 (Art 64-2). The usage of an embedded method should be studied with a next version.
PSD2 services					
AISP: Retrieval of accessible payment accounts	Yes	Yes	Yes	Yes	Yes (The retrieval of accounts embeds some balance information).
AISP: Retrieval of one given account balances	Yes	Yes	Yes	Yes	Yes
AISP: Retrieval of one given account transaction history	Yes	Yes	Yes	Yes	Yes
AISP: Other 1		Multiple balance types can be retrieved. Support for retrieving SO, DD and beneficiaries.			

PIISP: Fund coverage check of one given amount	Yes	Yes - via balance endpoint.	Yes	Yes	Yes
PIISP: Other 1		Not via API but through ASPSP interface.			
PISP: Submission of a payment initiation request	Yes	Yes	Yes	Yes	Yes
PISP: Distinct Execution request				Yes	Yes (The distinct execution request is more likely a confirmation of the payment request by the TPP).
PISP: Retrieval of the payment initiation report		Yes (Optional for ASPSP to implement).	Yes	Yes	Yes
PISP: Other 1	Questions of the form unclear. The Payment Initiation will lead normally to an execution. The TPP will receive a payment status at the end of the payment initiation process.	We provide status query – but not all ASPSPs will provide this functionality for first release.			
Does the API allow for a combination of AIS and PIS within the same inter-PSP communication session?	Yes, but is an implementation option e.g. for batch booking banks. This is then independent of the communication session, but is a functional feature.	Not specifically disallowed. Up to ASPSP to implement.	At the moment, there is no such functionality in the draft of Polish API standard.	Yes, it is possible.	The STET PSD API is a RESTFUL stateless API. Being stateless means there is no notion of session. the functional context being exchanged at each request/response sequence. Thus, the only way we can imagine a "session"

					within a RESTFUL API is to combine this functional context with the security context which is handled as follows. The TPP has to provide within each request : - its TLS qualified certificate in order to perform its own authentication (for AISP, PISP and PIISP use cases) - the OAUTH2 token being either an "authorization code" token materializing the authorization given by the PSU to access the API (for AISP and PIISP use cases), or a "Client Credential" token provided by the ASPSP (PISP use cases) Those two elements represent the security context. Consequently, at each request the full context can be retrieved by both parties (TPP/ASPSP) allowing the TPP, in a transparent way, to alternate AISP, PISP and PIISP requests.

What specific data elements that are available for the user (directly) are not available for a TPP holding an AIS license?	This question cannot be answered because every bank supports different data elements in online banking.	Depends on the ASPSP, but OBIE standards have been designed to be extensible and already include many optional fields (e.g. location of a transaction) which do not currently exist in many ASPSP online platforms.	We are currently working on the list of fields to be available as a compliance service for TPPs under AIS and PIS license. The complete list will be discussed in the Polish API working group with a participation of representatives of ASPSPs and TPPs in order to reach common approach. We have to remember that every individual ASPSP provides different scope of data elements to its users and standard should take it into account. However, all information according the PSD2 requirements which are available for PSU will be available also for a TPP.	All information according the PSD2 requirements which are available for PSU will be available also for a TPP.	Every piece of data that is under the scope of PSD2 for AIS use cases (i.e. payments accounts and related balances and transactions), and is available to the PSU through the ASPSP web-banking interface, is also available to the AISP, provided the PSU has explicitly given his consent for the AISP to access this piece of data, in respect of GDPR. So, if the PSU prefers to mask some information, they will not be available to the AISP.
Payment API details					
What are the possible return codes/statuses for a payment initiation – also please provide a detailed description of these codes/statuses:	The ISO20022 offers a transaction status field which is in use today by banks towards corporate customers when using pain.002 as an initiation report message. This field is filled with CODE elements, which are defined within ISO20022. This transaction status field with its corresponding	ISO20022 Payment Status Code AcceptedCustomerProfile AcceptedSettlementCompleted AcceptedSettlementInProcess AcceptedTechnicalValidation Pending Rejected	Under development.	Payment status returns subset of ISO 20022 - Payment Status Codes: ACTC – AcceptedTechnicalValidation; PDNG – Pending; ACSP – AcceptedSettlementInProcess; ACSC – AcceptedSettlementCompleted; ACWC – AcceptedWithChange; RJCT – Rejected.	The return status values are based on ISO20022 pain.014 status code. In case of rejection, the ISO20022 reason value is also provided

	code values are used by the Berlin Group Standard.				
What additional data, apart from the payment initiation status, is returned by the Payment Initiation API, and under which conditions and at which stage is this data provided?	The question is unclear to the Berlin Group initiative. Please make an example.	PaymentId CreationDateTime		Payment initiation returns: “paymentID”; paymentStatus; reasonCode; paymentStatusDateTime	None
Documentation					
Technical Specification	This is to be defined yet. For time being, Implementation Guidelines are written as text.	Swagger	Part of Polish API Specification (Swagger)	OpenAPI (Swagger)	OpenAPI (Swagger) version 2.0
Other Documentation	Explanatory “Operational Rules” Document, which is abstractly defining the API, data models and processes.	Detailed specs available on OB Website. OBIE also putting together a Developer Zone website with more technical documentation and support, including a service desk.	Specification of Polish API standard being developed by The Polish Bank Association (in development).	PSD2 Security documentation.	Detailed specifications including use case and activity log examples.
Incident reporting and dispute resolution					
How is incident reporting and dispute resolution handled?	Not defined (yet).	This is very much on the radar of OBIE, and now a separate work stream within OBIE. More info will be available soon.	At the moment, the standard doesn’t address this area but we are analysing this aspect.	Not yet discussed.	This topic is not related to an API specification as such. Each actor who implements this API will need to define its own reporting and dispute resolution procedures
Testing					

How is testing handled? Has a testing framework been put in place?	Up to now only API standard defined. Testing is up to implementation projects.	Enrolled participants will have access to a test instance of the OB Directory, which will include test ASPSP implementations/end points. OBIE is also providing a suite of TPP reference apps and a number of testing tools, including the FAPI Conformance Suite (which will allow ASPSPs to do their own self assertion that their end points meet the OB FAPI spec).	Based on Article 27 (6) of the Regulatory Technical Standards it is ASPSP which is responsible for providing testing environment.	Not yet discussed.	This topic is not related to an API specification as such. Each actor who implements this API will have to provide a testing environment (sandbox).
Comments					
Comment 1	The Berlin Group specification work is not yet finished. All comments have to be seen as preliminary.	Please note that the functional scope of Open Banking concerning access to account for the purposes of AIS and PIS is closely aligned to that required for access under PSD2.	Polish API specification is under development and it is not finished yet, we will review the specification once final version of RTS will be published.		This version might be updated upon adoption of the final version of RTS.
Comment 2		OB Directory is a key enabler for Open Banking, which allows all accredited/authorised ASPSPs and TPPs to self-manage their own credential and certificates so that they can talk securely. It also supports auto discovery and a concept called dynamic client registration, which			

		allows TPPs to automatically on-board with any ASPSPs who support this (without the TPPs needing to manually onboard with each ASPSP's API portal).			

Annex 4: Testing facility in case of a dedicated interface (prepared by the 'Other operational and technical matters' Expert Subgroup)

	Topic	Proposed requirements
1	Identification TPP vis-à-vis ASPSP	Ensuring mechanism of TPP identification and ASPSP acknowledgement of such identification works. This test should also be compatible for any non-dedicated interface, as applicable.
2	Format of API responses	The format of the API responses provided by the ASPSP through the testing facility should not differ from those provided in the live environment, and from those that will be provided in the future environment as the next release goes live.
3	Testing of different features	It should be possible to test within the testing facility all dedicated interface features provided in the future (next release live, within the next – at least – 3 months as per the RTS) and in the live environment. – All the routes/resources must be listed, documented and testable with necessary parameters. – All the different fields and their descriptions must be listed and documented. – The calls and the parameters to send in order to test the API must be the same as it is in production for the live environment, as they will be in the future live environment after the next release goes live – The responses of the test must be structured in the same way (have the same fields, same types). – Being able to test all the different authentication methods and the associated errors. – All the errors during a transfer phase must be testable: o An example of transfer with a threshold overcome error o An example of transfer with an unknown beneficiary error o An example of transfer with a double check error because of exact same transfer asked o Etc… TPPs have identified the following features for inclusion with the dedicated interface: i. All TAN (Transaction Authentication Number) systems provided by the respective ASPSP (mTAN, pushTAN, photoTAN etc.) and how

		it is displayed in case a consumer can choose between different TAN systems ii. All login methods provided by the respective ASPSP iii. Display of all different payment accounts accessible on-line (e.g. Giro, Saving, Credit card etc.)[8] iv. The transaction history should contain at least one transaction for each available type (credit transfer, direct debit, standing order, pre-booked transaction, cancelled transaction, etc.)[9] v. Support for different currencies vi. At least one account with an overdraft limit configured and the "available" should differ from the "balance" vii. If the ASPSP charges transfer fees per transaction then these should be recognisable in the transaction history Common test data should be provided by the ASPSP ("12345" as TAN code to check the functioning of e.g. the mTAN system)
4	Testing of special cases	Any conceivable cases that can occur in the live environment should also be available for testing in the test environment since TPPs should be able to process even special cases properly This, in particular, refers to different error cases (account is locked, TAN system is not activated, not sufficient funds available etc.) If the ASPSP supports localised messages (e.g. error messages), the test environment should display them in all languages supported by the ASPSP.
5	SLA on testing services	Access to test services shall be ensured during working times 8-18h00 CET.
6	Functional, operational & security descriptions and changes documentations	Access to documented functional and security and business requirements, maintenance work plan and versioning support.
7	Support several testing environments	TPP shall have access in the testing environment to at least two versioning of APIs.
8	Language support	The testing facility and related documentation should in all instances be available in English and in any local language.

[8] This is necessary in order for certain TPP software to know how the information in the account is structured. Such TPP software does not use or store any information on non-selected accounts, in particular, the account number and the respective balance of such accounts

[9] As per certain TPPs, this, again, is for the software to be able to handle the different formats correctly.

9	Industry governance on Change management rules and releases	Change management and release date shall be published 3 months in advance and enforcement implementation shall follow international standards rules (EMV, PCI, ECSG, EPC). ASPSP may mandate sunset of supported API versions ensuring standardisation and convergence of APIs version deployed.
10	Stakeholders group to be consulted	Consultation period on functional and operative changes. Security issues shall be addressed in shorter time lapse.
11	Statistics	Statistics on the global access of the dedicated interface could help managing the synchronisations. – Average response times – Statistics on error handling

Annex 5: Summary of Key Functional/Directory and Certificate issues (prepared by the 'Identification' Expert Subgroup)

#(priority) Recommendation	Topic	Requirement	Recommendation	Who
1 (Medium)	Certificate	In order to issue Qualified certificates, QTSPs have a legal requirement to verify information. They will need to be able to check with NCAs.	Provide a documented mechanism for QTSPs to verify data. Recommended that this is the national public register. The national public register must contain relevant data.	NCAs
2 (Medium)	Certificate	There is uncertainty about which category of PSP are allowed to have which role in their certificates, with possible national differences. (The regulatory perimeter).	Define for each country, which category of PSP of party can perform which PSD2 Role.	NCAs
3 (Medium)	Directory	Once it is clear which category of PSP, there is uncertainty how to recognise these actors when checking specific national registers.	Provide clear instructions as to where to find each category of PSP in the national directory, considering local language.	NCAs
4 (Medium)	Certificate	In order to verify that the PSD2 specific data in the certificates continues to be valid, the QTSPs must be	Verify that critical data elements are present in public registers.	NCAs

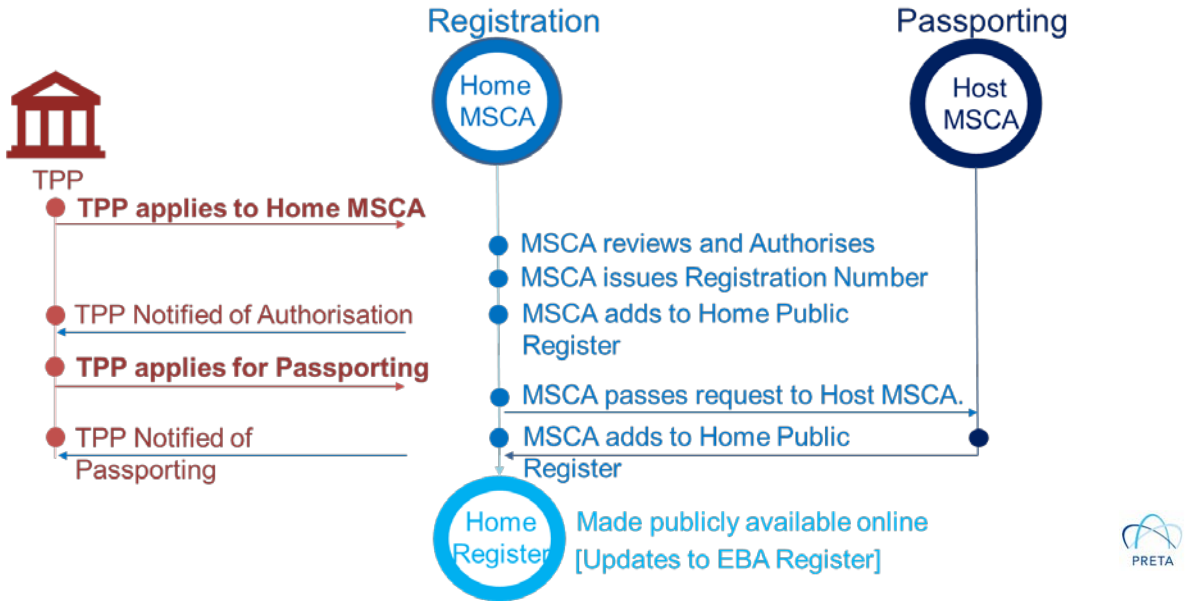
		able to check with NCAs.		
5 (Low)	Certificate	Certificates need to be standardised for new PSD2 elements.	ETSI / ESI[10] have started the standardisation process.	ETSI
6 (Medium)	Certificate	A complete list of NCA names is needed so that QTSPs can enter the valid data into the eIDAS certificates.	Provide a list of names, and keep it updated in a public place.	EBA / ECA / ERPB
7 (Highest)	Directory	In order to verify that the PSD2 specific data continues to be valid, ASPSPs need to verify the regulatory status of a TPP, and require this in a machine readable, single source, that takes a level of liability.	A directory or other solution is provided that meets this requirement.	The Market
8 (Medium)	Directory	ASPSPs need to know TPP names and contact details in order to follow up issues after a transaction has occurred, and to provide information before the transaction has occurred.	A directory or other solution is provided that meets this requirement.	The Market
9 (Medium)	Directory	Some TPPs require a standardised list of URLs where relevant documentation can be found.	A directory or other solution is provided that meets this requirement.	The Market

[10] e-Signatures and Infrastructure Working Group, set up by ETSI.

Annex 6: The Registration and Certificate Lifecycle (prepared by the 'Identification' Expert Subgroup)

The Registration Process

The following Image describes the Registration Process (note: MSCA stands for Member State Competent Authority and is the equivalent of NCA)



The Registration Process

The key requirements from an NCA Register are:

1. That it should be publicly available to those that need to verify information. (#Recommendation 1).
2. The ability to identify relevant actors
    1. In terms of which category of PSP (under article 1.1) is allowed to play which role (articles 65, 66 and 67). (#Recommendation 2).
    2. How local language and practice describes these actors. (#Recommendation 3).
3. The ability for each relevant actor to retrieve the following data:
    1. A Registration Number
    2. A Competent Authority Name
    3. Roles per country

    (#Recommendation 4).

It is noted that today, national registers do not (all) meet these requirements. Further detail is given below.

Problems with identifying the relevant actors

The group recognised that there is real concern around the "regulatory perimeter" of PSD2 access to account and the interpretation of who can be a TPP or an ASPSP, which may be subject to national variances. This interpretation has two elements:

1. **There is a need for clarity on which type of entity in principle can perform which type of service.**
2. **There is a need for clarity on how to recognise each type of entity as labelled in the national register.**

Which type of entity in principle can perform which type of service

The following table needs to be completed and validated for each type of institution in each country.

Role **RTS SCA CSC Article 24 v17/05**	**PSD2 Annex I**	**Entity Category from PSD2 Article 1.1**
Account Servicing (AS)	1. Services enabling cash to be placed on a payment account as well as all the operations required for operating a payment account. 2. Services enabling cash withdrawals from a payment account as well as all the operations required for operating a payment account.	Credit Institutions E-money institutions with article 1 or 2 Payment institutions with article 1 or 2 Does this definition miss out other national actors that may perform account servicing functions, e.g. (post offices)
Payment Initiation (PIS)	7. Payment initiation services.	Credit Institutions E-money Institutions with Article 7 Payment Institutions with Article 7

		Do all member states make the same assumptions about the role of Credit Institutions?
Account Information (AIS)	8. Account information services.	Credit Institutions E-money Institutions with Article 8 Payment Institutions with Article 8 Account Information SPs (NEW)*
Issuing of card based instruments (PIIS / FCS)	5. Issuing of payment instruments and/or acquiring of payment transactions.	Credit Institutions E-money Institutions with Article 5 Payment Institutions with Article 5

At least one NCA considers that AISPs are not a new category of Entity, but are considered to be simply Payment Institutions who are granted the right to perform article 8 of Annex 1 of PSD2, nevertheless PSD2 article 32 seems to give a special status to AISPs that ONLY perform AIS servicing, and the RTS on the EBA Directory also consider them as a separate category type.

How to recognise each type of entity as labelled in the national register

It is not enough to agree that Credit Institutions can perform PIS functions, we must understand which entities are Credit institutions in the National register.

Example 1. In the Spanish Register today, there are three entities that are considered "Credit Institutions"

Banco,

Cajas de Ahorros,

Cooperativas de Credito,

Example 2. In the Portuguese national register today, Banco de Portugal has a category called Credit Financial Institutions (Sociedades Financeiras de Crédito), however these companies are not considered Credit Institutions as per the definition on the Capital Requirements Regulation defined as an undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account, instead there are four categories of entity that do seem to be relevant.

Warning!

Many registers also have information that is not relevant and possibly misleading. For example, the Portuguese register has PayPal as an entity that is a credit institution, that has been passported in (from Luxembourg). In the Portuguese register, this PayPal record has been issued a number. that is not the number which is found in the Luxembourg register.

Finding the correct data for each entity

A registration number	Some registers have a clear registration number but other registers have: • No registration number (Finland, Lithuania, Netherlands) • Multiple registration numbers (France, Sweden, UK) • One registration number, but not the correct one. (Netherlands - publishes the local companies house legal identifier, not the registration number)
A competent authority name	We will need a clear list of permitted names, ideally one per country, with no confusion over acronyms. In Belgium, the Belgian Central Bank can be officially known by its name in each of the three official languages (to know Dutch, French, and German
Roles per country	Some NCA registers publish roles and to which countries those roles have been passported. Some NCA registers publish roles, but not to which countries those roles have been passported. Some NCA registers publish neither roles nor countries.

Understanding the ccertificate process

The RTS require that three data elements are in two separate types of certificate.

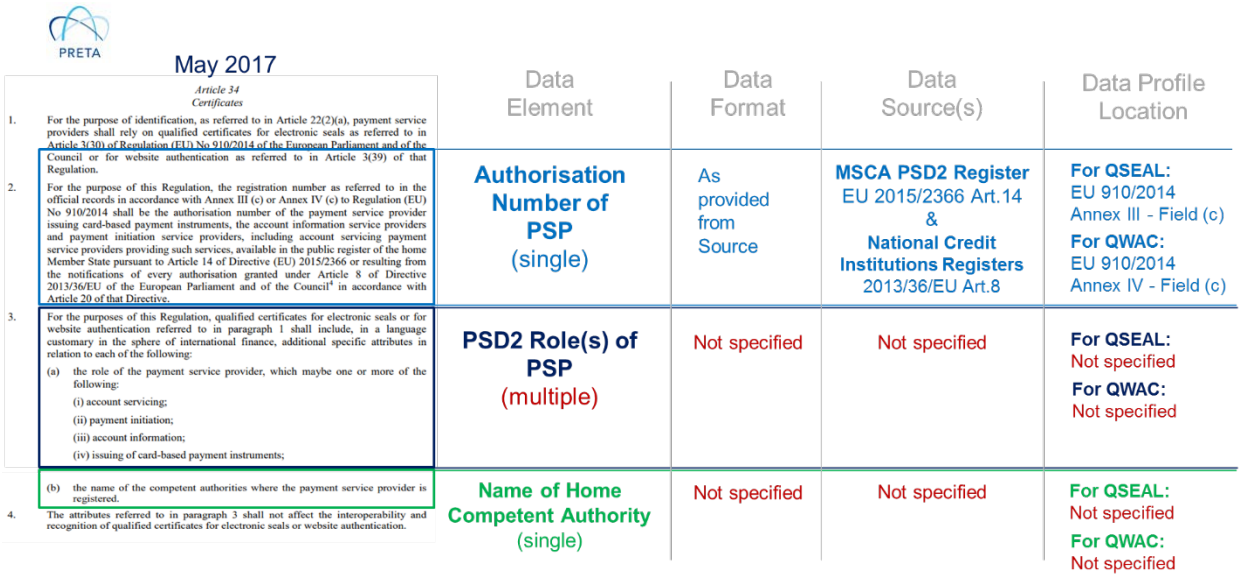
1. A Registration Number
2. A Competent Authority Name
3. The Roles of the PSP

The two types of certificate are Qualified Website Certificates and Qualified Certificates for Seals. These two types of certificate are specified in Annex III and IV of the eIDAS regulation.

In order that the industry can use certificates in an interoperable way, they need to be standardised. This work is being undertaken by ETSI, and needs to be completed. (Recommendation #5).

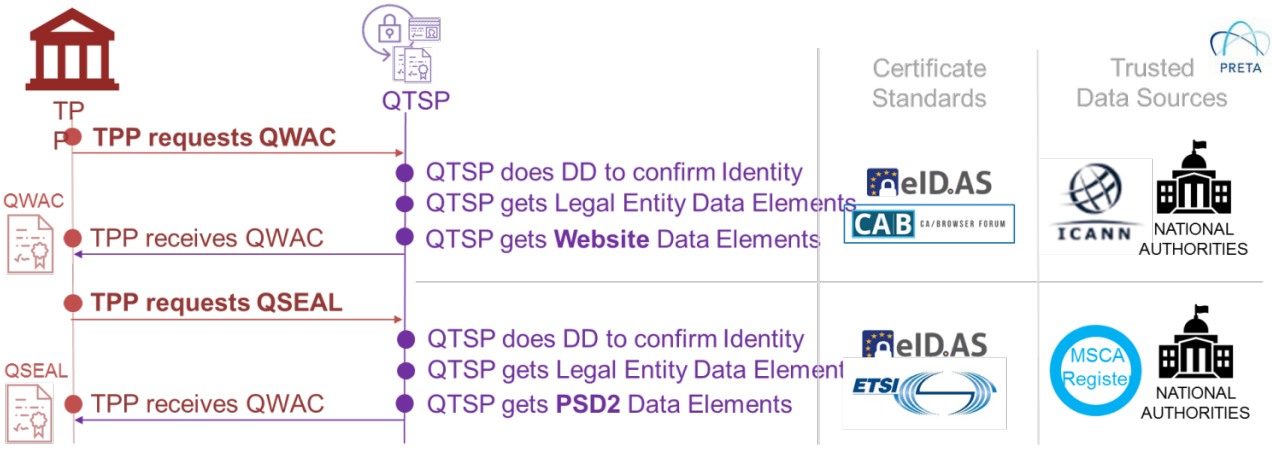
In order to complete this work, ETSI requires the location of the list of competent authority names that will be inserted into the certificate. (Recommendation #6).

- Which competent authorities are and are not in scope?
- Each competent authority has one name (and one name only) in whichever language is chosen.
- From a certificate standardisation point of view, any character set can work. From a market point of view, it may be preferable to limit this to Latin characters.



Required PSD2 Data (EBA/EC)

The certificate is issued following the process below:



Certificate Issuing Process

It is noted that the QTSPs have requirements for understandable accurate data from NCA's. Requirement #1

Process for when issuing a certificate

The QTSP is required (under eIDAS Article 24 & article 13 on liabilities) to verify the content of the certificate on issuance and renewal.

The subject (the TPP or ASPSP) must request the certificate, handing over documents that support their claim that they are allowed this certificate.

The QTSP must verify that the information is correct by checking with the relevant bodies (including the NCA).

Process when revoking a certificate (general)

If any part of the information changes, a certificate revocation can / should be requested to the QTSP. The certificate is recorded in a Certificate Revocation List (CRL) which can be checked by any party.

The PSP may request a new certificate but this will need to go through registration checks.

Process when PSD2 status changes

If a regulator removes the role of a PSP, they have an obligation to

i) Inform the PSP

ii) Update the public register.

The NCA has no obligation to inform the QTSP and indeed will not know who is the QTSP of that PSP.

Under current practice QTSP is not responsible for collecting information on changes to the certificate content.

The subject (i.e. the PSP who holds the certificate) is obliged to inform QTSP of any changes. Other parties may inform QTSP of changes (e.g. regulatory authority).

The QTSP once informed, must check the information and is liable for revocation within 24 hours if appropriate. The QTSP practices defines what revocation requests are handled.

Considering that the NCA is not obliged to inform the QTSP, and the QTSP is not obliged to check the NCA register, it is clear that although we can trust the certificates for Identification, in the case that an NCA has withdrawn a license and the certificate has not yet been revoked, there is a period when the roles in the certificate will not be accurate.

In the case that anybody wishes to check the up to date role of an ASPSP, then they must look at the Home NCA of that entity.

As there will be 31 NCA's, this raises the need for a machine readable, standardised repository of TPP details, as published by NCAs (Recommendation #7).

Only TPPs who have had their licence revoked / reduced need to be in the market provided directory (since the rest have valid certificates) and it could be that the owner of the directory takes an action to inform QTSPs when licenses are revoked. After the QTSP has revoked a certificate the market provided directory could remove its entry since it'll be in the CRL.

Annex 7: Questions that have been passed to the ESI PSD2 WG (prepared by the 'Identification' Expert Subgroup)

CERTIFICATE USAGE FOR PSD2

1. Qualified Electronic Seals "or" Qualified Website Authentication Certificates?
    a. When should they be used and for what purpose?
    b. Can either be used interchangeably/in place of each other?
    c. Is only one needed, or are both needed?
    d. What Certificates Standards are to be followed and who manages these?
    e. Recommend Uses & Non-Uses for eIDAS Certificates under PSD2

SOURCES OF DATA

2. Where must the mandatory information SOURCED for a QWAC (and for which type of QWAC)? (Standardisation)
3. Where must the mandatory information SOURCED for a QSEAL (and for which type of QSEAL)? (Standardisation)

DATA ELEMENTS AND CERTIFICATE PROFILE

4. What is the mandatory information and where must it GO in a QWAC (and for which type of QWAC)? (Standardisation)
5. What is the mandatory information and where must it GO in a QSEAL (and for which type of QSEAL)? (Standardisation)

DUE DILLIGENCE BY QTSP BEFORE CERTIFICATE ISSUING

6. What is the KYC and Due Diligence procedure for the QTSP with the TPP/ASPSP, to check they are who they claim to be, related to the Sourced Data BEFORE a cert has been issued:
    a. For QWAC & for QSEAL

CERTIFICATE MANAGEMENT AND LIABLITY

7. Accuracy of information (and whose Liability) AFTER the cert has been issued:
    a. For QWAC & for QSEAL
8. How to manage revocation of Certificate AFTER cert has been Issued:
    a. For QWAC & for QSEAL
9. Responsibility for status/revocation (and whose liability) AFTER the cert has been issued:
    a. For QWAC & for QSEAL

RECEIVING PARTIES USING CERTIFICATES

10. How does an ASPSP/TPP check the validity/status of a Certificate AFTER cert has been Issued:
    a. For QWAC & for QSEAL
11. How does an ASPSP/TPP check the signature of a Certificate AFTER cert has been Issued:
    a. For QWAC & for QSEAL

Responses to these questions:

https://docbox.etsi.org/ESI/Open/ESI(17)60_035r1_Discussion_Document_on_PSD2_Requirements_for_Qualified_Cert.pdf

Further, the work item that was agreed by the ETSI plenary meeting (in order to do the standardisation work on request of the Working Group) can be found here:

https://portal.etsi.org/webapp/WorkProgram/Report_WorkItem.asp?WKI_ID=53961

Annex 8: High-level proposal for dispute handling (prepared by the 'Other operational and technical matters' Expert Subgroup)

General	▪ Define Central contact point for initial request ▪ PSU to PSP (i.e. ASPSP and/or PISP/AISP) ▪ Between ASPSP and PISP/AISP • It is recommended to use secure communication channels. • Both ASPSPs and TPPs appoint a central contact point for dispute handling within their organisation • Contact details (name, e-mail address such as complaints@company.com and fax number) will be published on the PSP's website and possibly also in the official registers of the competent authorities (this could (also) feature in the directory(ies) that the market might develop) • Some members suggest using a dedicated communication channel (e.g. API) ▪ Agree maximum reaction times. including for acknowledgement (e.g. as per SEPA rulebook 4.3.2. Recall Processing Flow a max of 10 days upon receipt of request from originator) ▪ Ensure consistency in terminology and definitions ▪ Define common minimum information to be exchanged (per use case) ▪ Categorisation of dispute cases ▪ Documentation of dispute cases ▪ General ▪ Specific use cases (see table below) ▪ Ensure compliance with applicable rules and regulations, specifically GDPR ▪ Define dispute resolution mechanisms (after parties not being able to solve the issue together): ▪ Escalation process: ▪ Escalation procedure (e.g.: via National Central Banks) ▪ Third party arbitration (voluntary, fast, technical). ▪ A standing arbitration panel could also be established (e.g.: as part of a "scheme" - details would need to be defined and "recognition" organised).[11] ▪ Complaint with competent authority (to be clarified in the context of cross-border transactions). ▪ Redress in court A detailed cost-benefit analysis on the different mechanisms could be considered.

[11] This option is not supported by all members of the subgroup.

Payment Recovery	• Extend application of existing SEPA credit transfer model on payment recovery (based on camt.056 based-message) including defined standards to be processed between ASPSP and TPP (e.g.: Recovery reason codes).
Technical issues	• Both parties keep customer informed

It is recommended that the types of reports used for disputes between ASPSP and AIS/PIS, as well as escalation with the NCAs, include at least following common minimum information:

PIS issues	• ID user
	• ID transaction
	• Timestamp
	• Error type (see below for details)
	• Information of the transaction sent to the API
	  o Amount
	  o Label
	  o Balance (if accessible)
	  o Beneficiary
	  o Date
	• Phase of connection: authentication passed OK/NOK
	• Phase of connection: Information of the transaction sent OK/NOK
	• Phase of connection: Transaction validated OK/NOK
	• Information received from the API
	• Authentication mode
	• Time of response of the API
	• Complementary information

AIS issues	• ID user • Timestamp • Error type (see below for details) • Phase of connection: Authentication passed OK/NOK • Phase of connection: balance received OK/NOK • Phase of connection: transaction list received OK/NOK • Time of response of the API • Complementary information

Error types	The error type is one of the key data allowing the ASPSP, TPP and NCA to understand what went wrong during the communication between the TPP and the ASPSP. Therefore, we suggest that a list of error types would be a good way to define a simple standard.
	• Technical error
	  o API down
	  o Timeout
	  o Identification failed
	  o …
	• API error

	o Empty field o Unauthorized access o Access denied (may be categorized as functional) o … • Functional error o Missing transaction o False transaction o False balance

The aforementioned information could be shared both in the context of dedicated and non-dedicated interfaces.

Annex 9: Dispute cases (ASPSP-TPP relationship) (prepared by the 'Other operational and technical matters' Expert Subgroup)

	Dispute initiated by TPP	Dispute initiated by ASPSP
Single case	(1) TPP access refused /not available (2) Missing payment (3) Wrong payment (4) Inconsistent account history (5) Notification to competent authority (6) Data format & connectivity issues (e.g. slow response times, occasional down time) (7) Payment recall (8) Interface does not offer same level availability/performance as customer-facing interface	(9) Un-authorised payment (upon client notification) (10) Un-authorised/ wrong data sharing (upon client notification) (11) Suspicious / fraudulent payments[12] (12) Duplicate payments (13) Un-authorised access notification by PSU (14) Failed payment (15) Returned payment (16) Data-format & connectivity issues (17) Notification to competent authority
Multiple cases	(1) Same as above but multiple (2) Duplicate file (3) Inconsistent batch notification (4) Payment recall	(5) Same as above (6) Re-current failed access

[12] Fraudulent payments to be defined as per PSD2 Guidelines on Fraud Reporting