ERPB/2018/006

ERPB PIS 007-18

Version 1.0

28 May 2018

Euro Retail Payments Board (ERPB)

Additional Report of the ERPB Working Group on Payment Initiation Services

ERPB Meeting 18 June 2018

Executive summary

At its November 2017 meeting the ERPB invited the Working Group on payment initiation services (PIS) (hereafter referred to as the "Working Group") to prepare an additional report to i) consider its November 2017 recommendations against the legal certainty of the final Regulatory Technical Standards[1] on strong customer authentication and common and secure communication (hereafter referred to as the "RTS") [and the impact] on the envisaged requirements, and ii) continue the work on those requirements that need a follow-up such as the standardisation of PSD2 certificates (in liaison with the European Telecommunications Standards Institute (ETSI)), the harmonisation of registers and the establishment of directory services, and the development of remaining business requirements. The Working Group was invited to provide its additional report to the June 2018 ERPB meeting.

At the same meeting, the ERPB welcomed the European Commission's (EC) willingness to support a joint effort by stakeholders to establish a group to assist the evaluation of standardised application programming interface (API) specifications. As a consequence of the creation of this API Evaluation Group, the Working Group did no longer focus on technical (interface) requirements.

The Working Group performed a gap analysis between the final RTS and the version of the RTS available at the time of finalising the November 2017 Working Group report. It concluded that the amendments in the final RTS did not impact the operational and business requirements that were included in the list of November 2017 recommendations (and covered by its new mandate).

The report provides progress updates and further clarification in relation to the identification of payment service providers (PSPs) relying on standardised certificates, containing PSD2 data elements provided by the national competent authorities (NCAs) and issued by Qualified Trust Service Providers (QTSPs), proposed enhancement of the national registers as well as in relation to operational pan-European directory services. In this context, the Working Group identified and recommends the following operational requirements:

- A complete official list of NCA names is to be kept updated in a public place so that QTSPs can find and enter the valid data into the eIDAS certificates
- A guidance document is to be provided, also in English (on top of the local language(s)), on how to read and understand the respective national registers for the purposes of PSD2.
- NCA registration update procedures should be sufficiently rapid, so as to reduce related risks to a reasonable level.

[1] https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32018R0389&from=EN

The report also provides further clarification of the requirements for an efficient and well-functioning communication and resolution process for event and dispute handling between account servicing payment service providers (ASPSPs) and third-party payment service providers (TPPs), i.e. mainly payment initiation service providers (PISPs) and account information service providers (AISPs).

The Working Group identified and recommends the following business requirements:

- A communication and resolution process for event and dispute handling within adequate timeframes is to be used; the report contains the use cases, high-level and detailed content requirements, with detailed data requirements.
- Production certificates should not be used for API testing with TPPs.

An overview of the recommended requirements can be found below:

Overview of the requirements recommended by the Working Group

Operational requirements

- A complete official list of NCA names is to be kept updated in a public place so that QTSPs can find and enter the valid data into the eIDAS certificates.
- A guidance document is to be provided, also in English (on top of the local language(s)), on how to read and understand the respective national registers for the purposes of PSD2.
- NCA registration update procedures should be sufficiently rapid, so as to reduce related risks to a reasonable level.

Business requirements

- A communication and resolution process for event and dispute handling within adequate timeframes is to be used; the report contains the use cases, high-level and detailed content requirements with detailed data requirements.
- A number of topics need to be revisited in 2019 including the need for i) continuity regarding the maintenance and evolution of the identified requirements on event and dispute handing between TPPs and ASPSPs, ii) harmonised communication solutions market-wide, iii) bilateral communication for fraud prevention and mitigation, iv) alignment with the latest relevant regulatory provisions and v) a governance approach based on a self-commitment process by TPPs and ASPSPs.
- Production certificates should not be used for API testing with TPPs.

0. Introduction

In its November 2016 meeting, the ERPB established the Working Group and adopted its mandate (see Annex 2). The task given was “to define a common set of technical, operational and business requirements for the development of an integrated market for PIS”.

At its June 2017 meeting, the ERPB considered the report from the Working Group, took note of the status of the work and invited the Working Group to present its final report, taking account of the final RTS and responding fully to the different dimensions of its mandate, for the November 2017 ERPB meeting.

The Working Group’s November 2017 report provided an overview of the EU legal and policy framework and acknowledged the expectation of stakeholders to have a well-functioning, pan-European market for PIS. The report also identified and listed relevant technical, operational and business–related issues, recommending requirements where the Working Group could find agreement or, where no consensus could be reached, reflecting the diverging positions. It also contained clarifications provided by the EC.

At its November 2017 meeting the ERPB took note of the Working Group’s report and the set of technical, operational and business requirements for pan-European PIS (see Annex 3), noting that these requirements might still evolve also on the basis of the final version of the RTS. Therefore, the Working Group was asked to:

- Consider its recommendations against legal certainty of the final RTS [and the impact] on the envisaged requirements.

- Continue the work on those requirements that need a follow-up such as the standardisation of PSD2 certificates (in liaison with ETSI), the harmonisation of registers, the establishment of directory services and the development of remaining business requirements.

The Working Group was requested to include the outcome of the above work in an additional report as input to the June 2018 ERPB meeting.

At the same meeting, the ERPB welcomed the EC’s willingness “to support a joint effort by ASPSPs, TPPs and payment service users (PSUs) to establish a European group (API Evaluation Group) to support the evaluation of standardised application programming interface (API) specifications, which would aim to ensure that APIs meet the needs of all market participants and comply with PSD2 and other relevant legislation, including on data protection” (see Annex 2). As a consequence of the creation of the API Evaluation Group, the Working Group did no longer focus on technical (interface) requirements.

It should also be mentioned that the EBA is expected to provide further clarification on the topics of authentication and communication following the entry into force of the RTS.

The present report is structured in line with the scope defined during the November 2017 ERPB meeting:

Section 1 assesses whether the recommendations included in the November 2017 report are still valid as per the final RTS. This in view of the fact that the November 2017 report was based on the (at the time) latest available version of the RTS from May 2017[2].

Section 2[3] provides a follow-up and/or further clarification on the operational and business requirements that were not yet finalised in the November 2017 report.

Section 3 presents the conclusions of the Working Group.

1. Assessment of the recommendations included in the November 2017 report of the Working Group

In its November 2017 report the Working Group had recommended a list of technical, operational and business requirements based on the draft RTS published by the EBA in May 2017. However, the Working Group had been kept informed by the EC about the changes it intended to make.

The Working Group performed a gap analysis between the final RTS and the version of the RTS available at the time of submitting the November 2017 report. It concluded that the amendments in the final RTS did not impact the operational and business requirements that were included in the list of November 2017 recommendations (and covered by its new mandate). The Working Group did not assess the impact on the technical requirements as this was out of scope for this additional report and is currently being addressed by the API Evaluation Group.

2. Follow-up on operational and business requirements for an integrated market for PIS

This section covers the operational and business requirements for which further work or clarification was requested by the ERPB in November 2017.

[2] 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

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

Most of these topics are related to the identification of PSPs, including:

- Standardisation of PSD2 certificate requirements;
- QTSPs to be able to check PSD2 related information with NCAs;
- 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 a directory could take the form of a central directory or of a 'directory of directories' (i.e. directories based on national registers).

In addition, further clarification is provided on the topic of event and dispute handling between ASPSPs and TPPs (mainly PISPs and AISPs) as well as on usage of certificates for API testing with TPPs.

2.1. Standardisation of PSD2 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 that PSPs should rely upon, i.e. "Qualified Website Certificates" (QWACs) and "Qualified Certificates for Seals" (QSEALs), which are specified in Annex III and IV of the eIDAS regulation[4].

In its November 2017 report, the Working Group concurred that the issuers of certificates (QTSPs) will need to be able to check with NCAs using a documented mechanism and that, among other things, clarity should exist around which category of PSP is allowed to have which role(s) (in their certificates) and that certificates need to be standardised for the new PSD2 elements specified in the RTS.

In response to one of the recommendations listed in the June 2017 Working Group report, and in liaison with the Working Group, ETSI had started with the development of a standard for certificates to accommodate the aforementioned new PSD2 elements. The latest version[5] of the ETSI standard ETSI TS 119 495 was published on 15 May 2018 following a public consultation which ended in March 2018.

There is still a dialogue ongoing in relation to a topic which was initially included in an annex to the standard and which focuses on the relationship between the QTSPs and the NCAs. This will now be

[4] 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

[5] http://www.etsi.org/deliver/etsi_ts/119400_119499/119495/01.01.01_60/ts_119495v010101p.pdf

covered in a separate ETSI work item that is expected to be finished by the end of October 2018. It should be noted that this does not affect the standard itself.

The Working Group also noted that there is still some doubt in the market in relation to the availability (in certain countries)[6] and readiness of QTSPs. As of mid-April 2018, there were 29 QTSPs that can issue QWACs and 68 QTSPs that can issue QSEALs. The official list of QTSPs in the European Union can be found here on the EC's website.[7] Based on information gathered during the cooperation with ETSI it appears that QTSPs are ready to offer PSD2 certificate services, both domestically and cross border. The Working Group is of the view that there are and will be QTSPs offering services to the industry ready for PSD2 access to account, both domestically and cross-border.

Although good progress is made in this domain, the Working Group stresses the need for an up to date, complete official list of NCA names so that QTSPs can find and enter the valid data into the eIDAS certificates.

2.2. QTSPs to be able to check PSD2 related information with NCAs

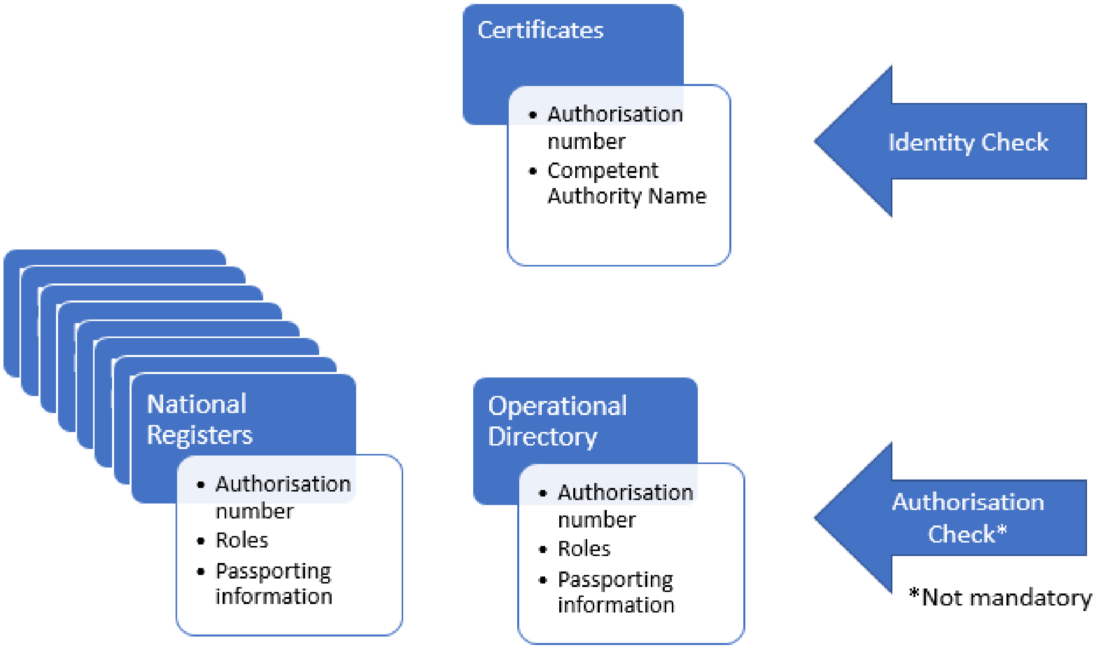
In order to issue certificates, QTSPs have a legal requirement to verify PSD2 related information. They will need to be able to check with NCAs using a documented mechanism.

To better comprehend the importance of communication between NCAs (registers) and QTSPs (certificates) it is critical to understand the purpose of the certificate which is to provide assurance about the identity of the entity, as has been common practice in internet communications. However, PSD2 certificates also contain information about the NCA, the registration number, and the role(s) of the entity, in order for PSPs to find and check the authorisation of PSPs in the NCA's registers. This distinction is visualised in the below diagram[8]:

[6] Article 5 of eIDAS makes it clear that a QTSP that is qualified in one country is permitted to offer and provide services in all other EU countries with equal legal certainty.

[7] https://webgate.ec.europa.eu/tl-browser/#/

[8] It is to be noted that as indicated above the role(s) at the time of issuance is (are) also included in the certificate.



In addition, the Working Group discussed the issue of revocations of certificates. In line with the eIDAS regulation, 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. NCAs). The QTSP, once informed, must check the information and is liable for revocation within 24 hours if applicable. Detailed information about the registration and certification processes can be found in Annex 4.

There is currently a 'liability gap' between the eIDAS regulation and PSD2, considering that the NCA is not obliged to inform the QTSP and the QTSP is not obliged to check the NCA register after issuance. It is clear that although PSPs can trust the certificates for identification purposes, in cases that an NCA has withdrawn a license and the certificate has not yet been revoked, there is a period when the role(s) included in the certificate will no longer be accurate. In order to check the actual role(s) of a PSP, one must look at the register of the home NCA of that entity.

The Working Group is however of the view that this topic should not cause disruption, if the national registers would contain adequate and accurate information (see next section).

2.3. Enhancement of NCA registers

In the November 2017 report it was reported that there is a need for clarity on i) which type of entity in principle can perform which type of service and ii) how to recognise each type of entity as labelled in the national register. A good register would allow an easy mapping from category to role, from role to category and the correct data to be identified.

The Working Group noted that since the PSD2 transposition date, some registers have been improved and now provide sufficient information to understand exactly what an entity can do from a regulatory perspective[9]. However, at the time of writing, fewer than ten registers contain sufficient PSD2 related information, mainly due to the fact that PSD2 has not yet been transposed in all Member States. Even where there are “good” registers, there are still implicit rules (e.g. for credit institutions – see Annex 5) that have to be understood and interpreted. The Working Group concurs that the following attributes should be unambiguously retrievable in the registers: the relevant authorisation number as used in the certificate and the role(s) of the PSP.

The Working Group stresses the need to ensure clarity and to facilitate cross-border use and hence proposes the NCAs to be invited to offer a guidance document on how to read and understand their respective national register(s) for the purposes of PSD2 (i.e. the authorisation number and role(s) of PSPs) and to provide an English version of this guidance documentation (on top of the local language version(s)).

Indeed, the Working Group concurs that this topic still presents significant risks. In particular, in the case that a PISP, AISP or a card-based payment instrument issuer service provider (PIISP) roles are not clear, there is the risk that they are wrongly blocked or are wrongly allowed access.

Indeed, the registers will be used by ASPSPs in particular as a source of information (e.g. on the role(s) of the TPPs) and for taking operational decisions. The decisions will include whether the ASPSP can allow or should deny access to entities wishing to provide PIS or AIS. This would plead for an operational approach to such registers, i.e. 24/7 availability, machine-readability, real-time updating.

There are various instances in which the information needed by an ASPSP may have changed. These include the (first) registration of the newly regulated entity, upon which the ASPSP should allow access, the addition of new roles (allowance to provide additional services), the addition of passporting rights (i.e. rights to provide services in other countries), as well as the removal of such roles and rights, and finally the revocation of the authorisation itself and the cancellation of registration.

There is a concern there may be a lag between the administration of an NCA making a decision, e.g. to authorise an entity, change its licence (roles) or passporting rights, or to deauthorise the entity, and the subsequent update of the public national register. The lag between such a decision and the subsequent publication may create risks, either leading to unintentionally refusing access or to unauthorised payments or unauthorised data sharing, with subsequent liability issues.

[9] Examples: French register www.regafi.fr; UK register https://register.fca.org.uk/

The Working Group hence proposes the NCAs to be invited to ensure that their registration update procedures are sufficiently rapid so as to reduce related risks to a reasonable level.

2.4. Establishment of directory services

In the November 2017 report, the Working Group indicated the need 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).

There are currently a number of initiatives in the market, driven by national organisations, or, in one case, a pan-European initiative from a consortium of banks.

A further description of the operational directory service’s features is found in Annex 6.

The Working Group is of the view that this topic is progressing well, and it appears that there will be operational directories in the market in time for access to account.

2.5. Event and dispute handling processes

In the November 2017 report, 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 event 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.

Whilst the rights and obligations in the relationship between the ASPSP/TPP and the PSU are defined in detail in PSD2, communication and process standards for the interaction and the resolution of events and/or dispute handling between ASPSPs and TPPs are defined neither in Level 1 legislation nor in the Level 2 regulations. Likewise, it should be noted that both commercial disputes between the payer and payee and the way to resolve this such as a refund service are out of scope of this report.

The aim, thus, should be to establish efficient and well-functioning communication and process standards for event and dispute handling within adequate timeframes. Once the definitions of these standards are finalised they should be reviewed from a legal perspective to ensure that these are not in breach of any relevant local or EU law.

It is agreed that not all events which trigger a communication between ASPSP and TPP will result in a dispute situation. The main objective of these standards is to base the communication on a pre-defined minimum procedure to ensure effective and efficient response and/or resolution of the matters within an adequate timeframe, in the ultimate interest of the PSU.

Below is an overview of possible events/disputes initiated by either a TPP or ASPSP for different use case categories:

Use case categories	Events/disputes initiated by TPP	Events/disputes initiated by ASPSP
Access	(1) TPP access refused/not available (2) (N) Too many requests (Denial of Service (DoS) protection) (3) Strong customer authentication (SCA)	(1) Unauthorised/wrong data sharing (2) Unauthorised access notification (3) (N) Too many requests (DoS protection)
Performance	(4) Performance issues (customer interface/dedicated interface)	
Processing	(5) Payment not initiated/accepted (6) Failed payment (7) Inconsistent account history	(4) Unauthorised payment (5) Inaccurate/late payment
Escalation	(8) Notification to competent authority	(6) Notification to competent authority

If required, the market participants need to be able to contact the right institution and explain the request/issue in a comprehensive manner. The Working Group hence proposes minimum requirements for a communication and resolution process for event and dispute handling within adequate timeframes.

The objectives of these minimum requirements include:

- Serve intention of the regulations and protect PSUs;
- Ensure compliance with applicable rules and regulations, specifically the General Data Protection Regulation (GDPR);
- Be applicable to both the ASPSPs and TPPs;
- Solve events in an adequate timeframe and in the interest of PSU protection;
- Preserve ongoing relationship and prevent repetitive events/dispute cases;
- Commit to use common processes, communication and behavioural standards (reference to existing applicable standards (e.g. ISO20022) has to be considered where relevant);
- Apply proportionate or automated methods to solve standard disputes (over time the market will be able to identify standard disputes).

High-level content requirements including for example the definition of central contact points and maximum reaction times, as well as detailed content requirements for PIS versus AIS related messages, and detailed data requirements can be found in Annex 7.

Moreover, the Working Group considered further detailed requirements related to the process. First, if the exchange of sensitive payment data would be required in a specific case, a secure communication method should be agreed upon by email/ telephone, prior to sharing such data in a mutually supported secure manner. Widely used standard technical solutions were considered such as email, API, Web interface/electronic form and file transfer solution. To ensure efficiency and security, it is however recommended to adopt harmonised solutions market-wide.

The representatives of TPPs expressed their preference for a high-level solution (e.g. making available email and telephone contact details as described in the high-level content requirements in Annex 7). Plain text emails should not be refused solely for not being encrypted/signed or for allegedly being in an ‘unsupported’ format, provided these do not contain sensitive information.

Diverging views exist within the Working Group in relation to the required governance approach. For consistency purposes in the European payments environment some participants recommended to apply a similar governance approach as for the SEPA payment schemes in terms of ownership, change management and adherence, however without applying the same level of detail and complexity to the present communication, event and dispute handling standards. Other participants favoured a more flexible, use case-centric solution for TPP-ASPSP communications, based on high-level principles. A process based on a self-commitment by TPPs and ASPSPs according to the above principles is recommended.

The Working Group also agreed that continuity should be ensured regarding the maintenance and evolution of the event and dispute handling process between TPPs and ASPSPs. For example, the SEPA payment schemes are updated every two years to reflect market needs and evolutions in the relevant technical standards. This evolution should be guided through a transparent change-management process, open to all stakeholders.

Moreover, the Working Group expressed the need for bilateral communication in case of a fraud scenario allowing to stop and mitigate any type of fraud-related risk. If an ASPSP prior to execution blocks a specific payment transaction initiated through a PISP due to an identified fraud scenario, the ASPSP should inform the Payer and the PISP, as far as allowed pursuant relevant rules and regulations.

The Working Group recommends updating the work done in relation to event and dispute handling processes once the forthcoming EBA Guidelines on fraud reporting are made public.

2.6. Certificate usage for API testing with TPPs

The Working Group also discussed the topic of testing, specifically the use of certificates during testing[10]. In the test phase, the TPP will have to access the API in compliance with the ASPSP requirements. It is up to the ASPSP to decide which certificate is to be used for testing, if any. The ASPSP should decide based on the trade-off between promoting broad testing of its API without usage of any certificate, and the usage of a certificate for testing similar to the live environment. When the ASPSP requires a certificate for API testing with TPPs, it was agreed and recommended that it should not be the production certificate of the live environment.

3. Conclusions

The ERPB is invited at its June 2018 meeting to:

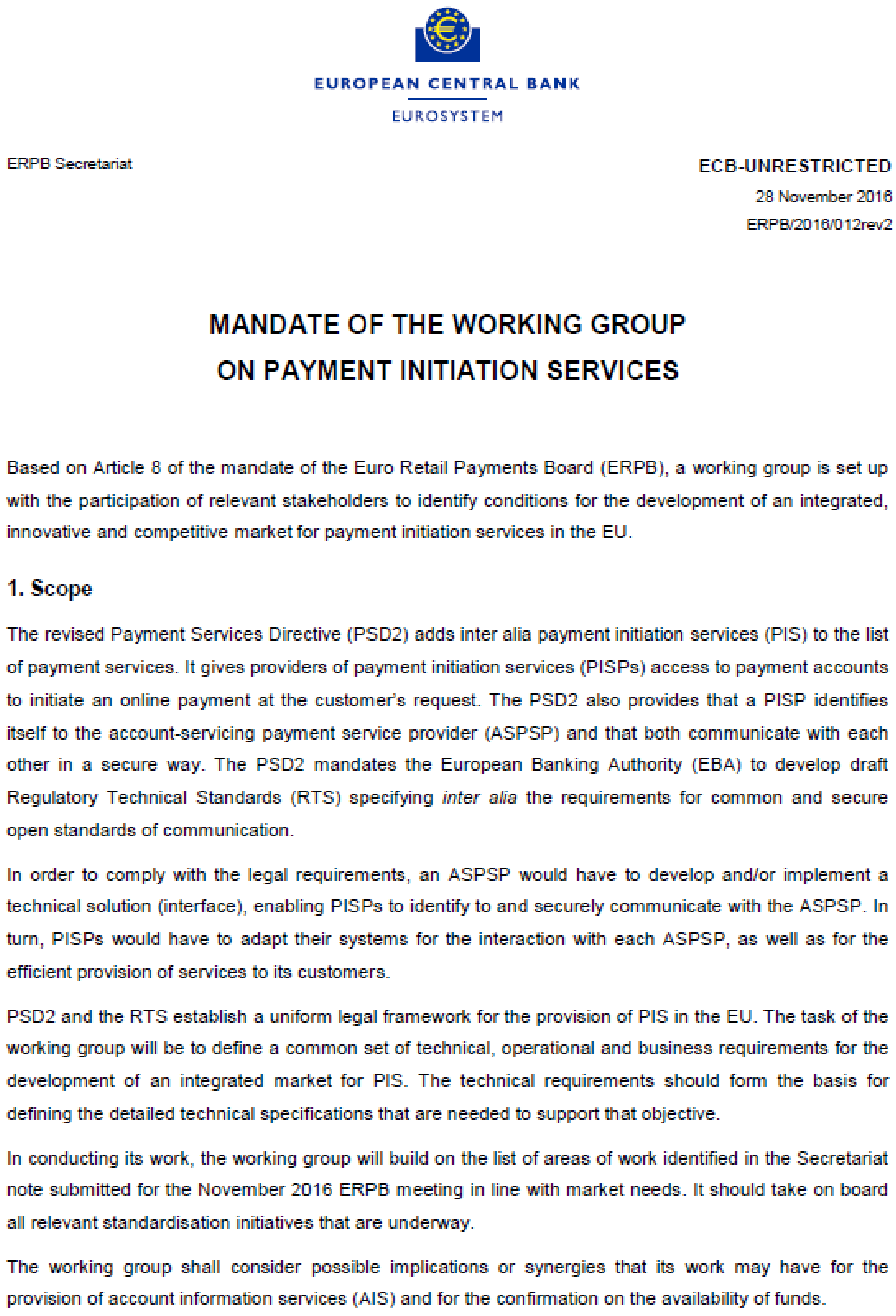
- Take note of this additional report of the Working Group;
- Endorse the recommended requirements at the end of the executive summary.

[10] At its November 2017 meeting the ERPB noted that the definition of high-level principles for a common testing framework was part of the work of the API Evaluation Group.

Annex 1: List of ERPB Working Group participants (as from December 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)
	Diederik Bruggink	ESBG
	Pascal Spittler	EuroCommerce (IKEA) (co-Chair 'Other' subgroup)
	Jean Allix	BEUC
ECB	Iddo de Jong	ECB
	Ann Börestam	ECB
NCB	Dirk Schrade	Deutsche Bundesbank
	Gregorio Rubio	Banco de España
	Olivier Catau	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 and Industry initiatives	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
AISP	Kevin Voges	AFAS Personal
	Joan Burkovic	Bankin'
Other PIS-stakeholder	Max Geerling	iDEAL
	James Whittle	NPSO
	John Broxis	Preta / MyBank (co-chair 'Identification' subgroup)
Secretariat	Etienne Goosse	EPC
	Christophe Godefroi	EPC

Annex 2: Mandate ERPB Working Group on Payment Initiation Services



EUROPEAN CENTRAL BANK

EUROSYSTEM

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.

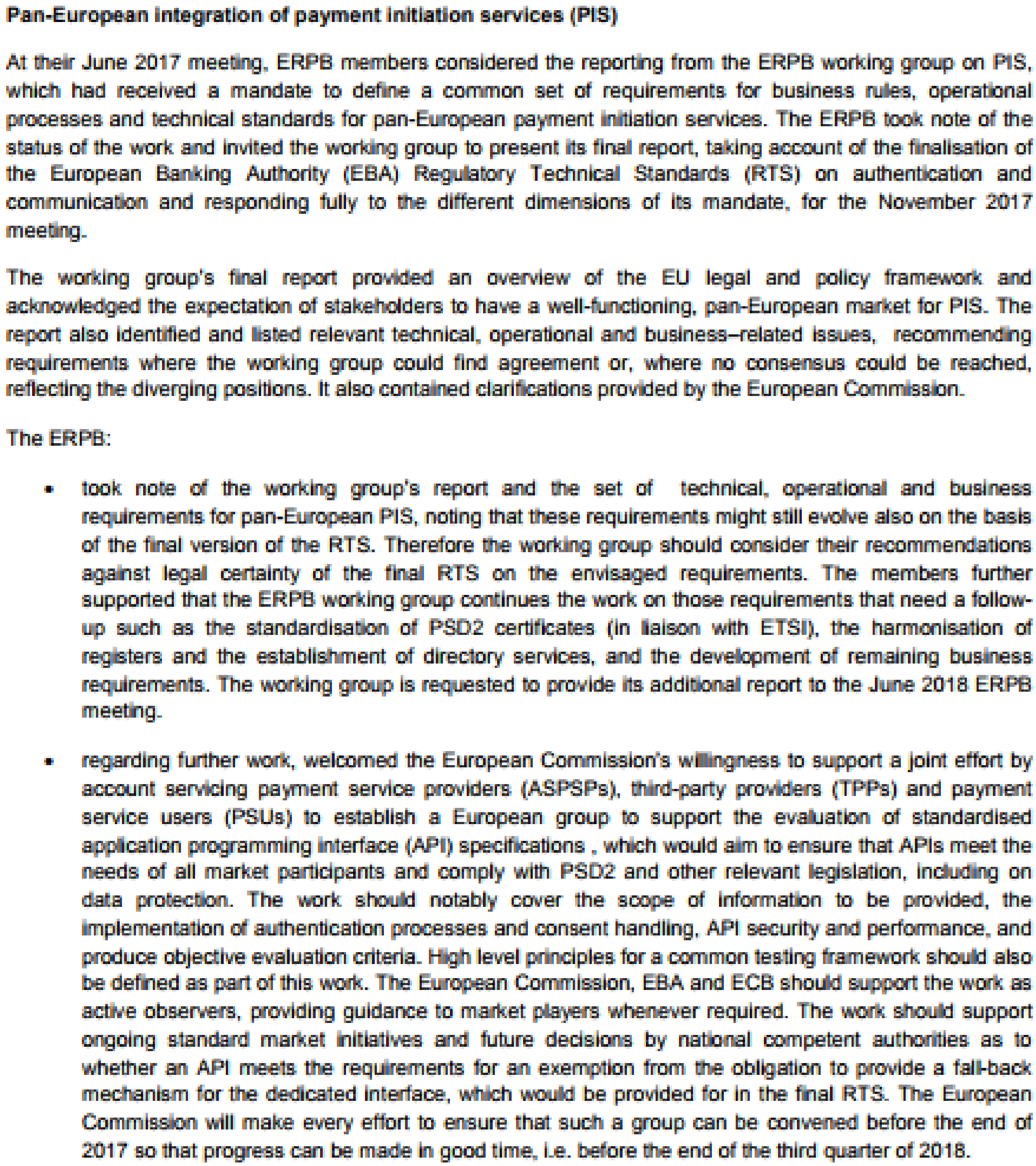
In order to comply with the legal requirements, an ASPSP would have to develop and/or implement a technical solution (interface), enabling PISPs to identify to and securely communicate with the ASPSP. In turn, PISPs would have to adapt their systems for the interaction with each ASPSP, as well as for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

Updated scope as per the November 2017 ERPB statement:



Pan-European integration of payment initiation services (PIS)

At their June 2017 meeting, ERPB members considered the reporting from the ERPB working group on PIS, which had received a mandate to define a common set of requirements for business rules, operational processes and technical standards for pan-European payment initiation services. The ERPB took note of the status of the work and invited the working group to present its final report, taking account of the finalisation of the European Banking Authority (EBA) Regulatory Technical Standards (RTS) on authentication and communication and responding fully to the different dimensions of its mandate, for the November 2017 meeting.

The working group's final report provided an overview of the EU legal and policy framework and acknowledged the expectation of stakeholders to have a well-functioning, pan-European market for PIS. The report also identified and listed relevant technical, operational and business–related issues, recommending requirements where the working group could find agreement or, where no consensus could be reached, reflecting the diverging positions. It also contained clarifications provided by the European Commission.

The ERPB:

- took note of the working group's report and the set of technical, operational and business requirements for pan-European PIS, noting that these requirements might still evolve also on the basis of the final version of the RTS. Therefore the working group should consider their recommendations against legal certainty of the final RTS on the envisaged requirements. The members further supported that the ERPB working group continues the work on those requirements that need a follow-up such as the standardisation of PSD2 certificates (in liaison with ETSI), the harmonisation of registers and the establishment of directory services, and the development of remaining business requirements. The working group is requested to provide its additional report to the June 2018 ERPB meeting.

- regarding further work, welcomed the European Commission's willingness to support a joint effort by account servicing payment service providers (ASPSPs), third-party providers (TPPs) and payment service users (PSUs) to establish a European group to support the evaluation of standardised application programming interface (API) specifications , which would aim to ensure that APIs meet the needs of all market participants and comply with PSD2 and other relevant legislation, including on data protection. The work should notably cover the scope of information to be provided, the implementation of authentication processes and consent handling, API security and performance, and produce objective evaluation criteria. High level principles for a common testing framework should also be defined as part of this work. The European Commission, EBA and ECB should support the work as active observers, providing guidance to market players whenever required. The work should support ongoing standard market initiatives and future decisions by national competent authorities as to whether an API meets the requirements for an exemption from the obligation to provide a fall-back mechanism for the dedicated interface, which would be provided for in the final RTS. The European Commission will make every effort to ensure that such a group can be convened before the end of 2017 so that progress can be made in good time, i.e. before the end of the third quarter of 2018.

Annex 3: Overview of recommended requirements in the November 2017 report of the ERPB WG

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).

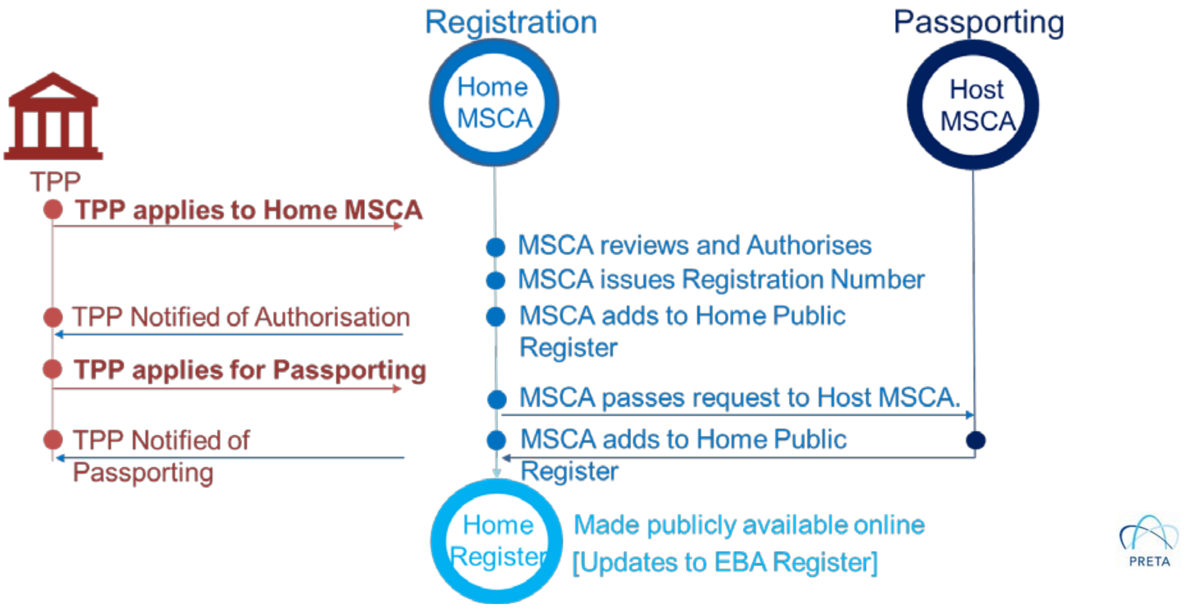
Business requirements

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

Annex 4: The Registration and Certificate Lifecycle (prepared by the ‘Identification’ Expert Subgroup as included in the November 2017 report of the ERPB WG on PIS)

The Registration Process

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


Registration
Passporting
Home MSCA
Host MSCA
TPP
TPP applies to Home MSCA
MSCA reviews and Authorises
MSCA issues Registration Number
TPP Notified of Authorisation
MSCA adds to Home Public Register
TPP applies for Passporting
MSCA passes request to Host MSCA.
TPP Notified of Passporting
MSCA adds to Home Public Register
Home Register
Made publicly available online
[Updates to EBA Register]
PRETA

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.

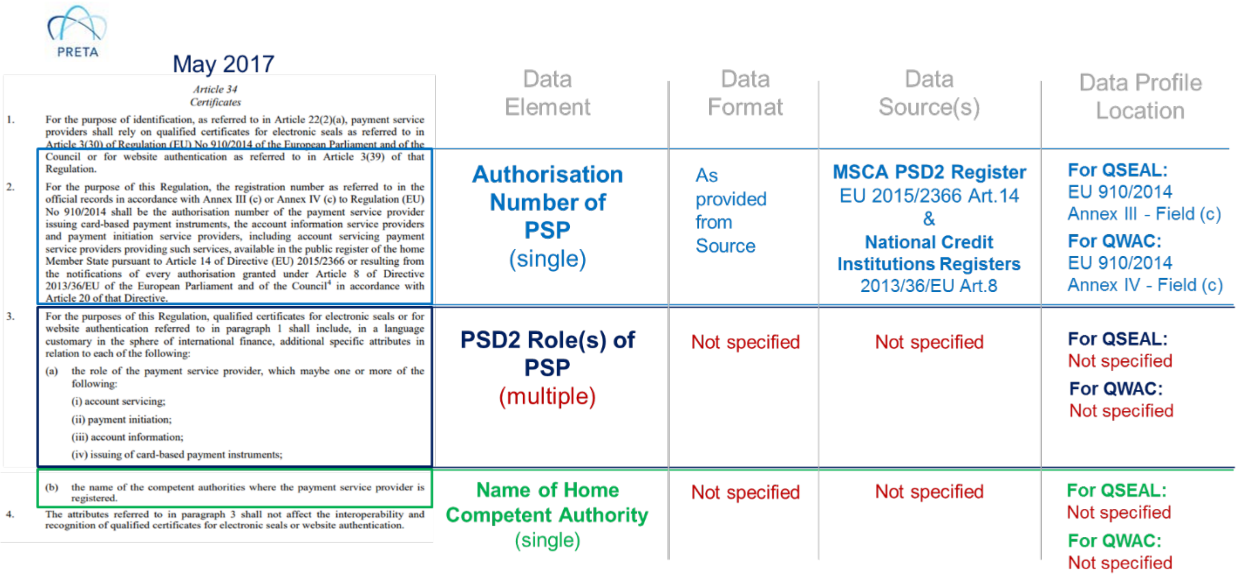
1. A Registration Number
2. A Competent Authority Name
3. The Roles of the PSP

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.



May 2017

Article 34
Certificates

1. For the purpose of identification, as referred to in Article 22(2)(a), payment service providers shall rely on qualified certificates for electronic seals as referred to in Article 3(30) of Regulation (EU) No 910/2014 of the European Parliament and of the Council or for website authentication as referred to in Article 3(39) of that Regulation.

2. For the purpose of this Regulation, the registration number as referred to in the official records in accordance with Annex III (c) or Annex IV (c) to Regulation (EU) No 910/2014 shall be the authorisation number of the payment service provider issuing card-based payment instruments, the account information service providers and payment initiation service providers, including account servicing payment service providers providing such services, available in the public register of the home Member State pursuant to Article 14 of Directive (EU) 2015/2366 or resulting from the notifications of every authorisation granted under Article 8 of Directive 2013/36/EU of the European Parliament and of the Council[4] in accordance with Article 20 of that Directive.

3. For the purposes of this Regulation, qualified certificates for electronic seals or for website authentication referred to in paragraph 1 shall include, in a language customary in the sphere of international finance, additional specific attributes in relation to each of the following:

(a) the role of the payment service provider, which maybe one or more of the following:

(i) account servicing;

(ii) payment initiation;

(iii) account information;

(iv) issuing of card-based payment instruments;

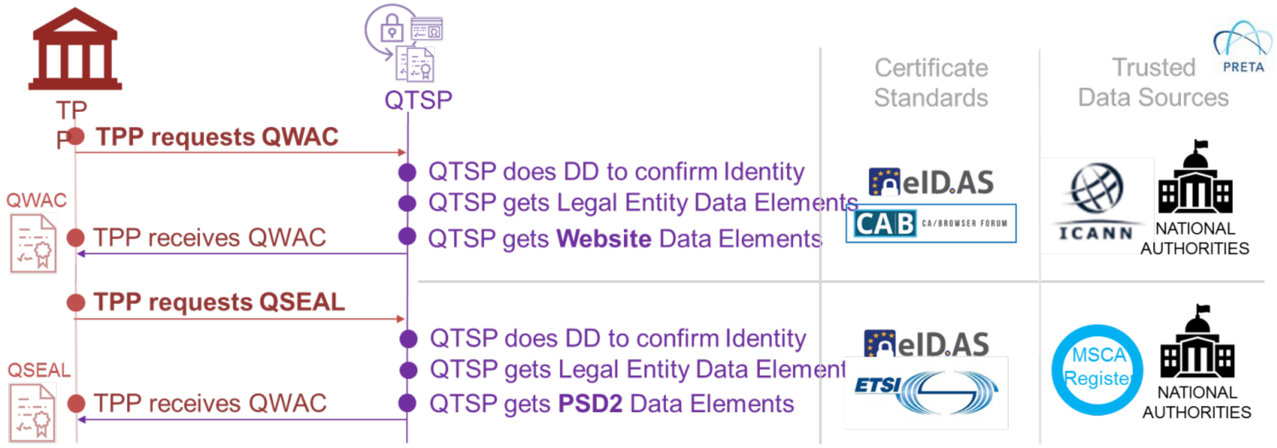
(b) the name of the competent authorities where the payment service provider is registered.

4. The attributes referred to in paragraph 3 shall not affect the interoperability and recognition of qualified certificates for electronic seals or website authentication.

Data Element	Data Format	Data Source(s)	Data Profile Location
Authorisation Number of PSP (single)	As provided from Source	**MSCA PSD2 Register** EU 2015/2366 Art.14 & **National Credit Institutions Registers** 2013/36/EU Art.8	**For QSEAL:** EU 910/2014 Annex III - Field (c) **For QWAC:** EU 910/2014 Annex IV - Field (c)
PSD2 Role(s) of PSP (multiple)	Not specified	Not specified	**For QSEAL:** Not specified **For QWAC:** Not specified
Name of Home Competent Authority (single)	Not specified	Not specified	**For QSEAL:** Not specified **For QWAC:** Not specified

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 5: Focus on Credit Institutions as ASPSPs and TPPs (prepared by the 'Identification' Expert Subgroup)

For Credit Institutions there is less PSD2-relevant information available in the national registers, and implicit rules must be used to know that Credit Institutions are allowed to provide all services. As an example, in the UK register is it is not so obvious which organisations are actually Credit Institutions.

Topic	Detail
Identifying who are credit institutions[11]	It is implicit that Credit Institution automatically have all the rights granted in PSD2 Annex 1, and automatically have the rights to perform PIS, AIS and PIISP services. It is not always possible to tell if an organisation is a credit institution or not • UK based Santander Insurance Services UK Ltd. Are they a credit institution? • UK based Barclays Bank. I guess yes – how can I be sure? • Here is Spanish example, ABANCA SERVICIOS FINANCIEROS E.F.C., S.A. Credit Institution or not? • Here is a French example, BPCE. This is clearly a credit institution.
Credit institution passporting	It is commonly, but not universally assumed that the Credit Institutions can automatically passport into all countries. This should be clarified at a European level, and if required the passporting information that the NCA's hold needs to be put into the register.
Credit institution numbers	There are indications that at least one NCA that while the Credit institutions have numbers allocated, these numbers are not planned to be in the public register.
Credit institution, commercial names	The French register shows commercial names for Payment Intuitions, but not for Credit Institutions. We presume this might happen in other cases. Consumers will know the commercial name, but the legal name will be passed onto the account statement. Unless the bank can link the two, consumers will be confused.

[11] At the moment it is unclear whether credit institutions, in their role as ASPSPs are legally obliged to use eIDAS certificates for authentication and security or whether they are free to use non-eIDAS certificates.

Annex 6: Operational Directory functionality (prepared by the 'Identification' expert subgroup)

The following was published in the November ERPB PIS report:

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).

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.

Annex 7: High-level content requirements and detailed content requirements (prepared by the ‘Other operational and technical matters’ Expert Subgroup)

High level content requirements

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, phone and fax number) will be published on the PSPs’ 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)
- Event and dispute use cases
    - Ensure consistency in terminology and definitions for the various use cases identified (as used in different environments such as for example SWIFT specifiers)
    - Define common minimum information to be exchanged (per use case)
    - Categorisation of events/dispute cases
    - Documentation of events/dispute cases
        - General
        - Specific use cases (see table below)
- Define event/dispute resolution mechanisms in case parties are not 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).[12]
        - 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.

Technical issues

- Both parties keep PSU informed

[12] This option is not supported by all members of the sub-group.

Detailed content requirements

It is recommended that the types of messages used for communication between ASPSPs and AISPs/PISPs, as well as for escalations with the Competent Authorities (CAs), include at least the following common minimum information (the below information could be shared both in the context of dedicated and non-dedicated interfaces). Specifications of further content for individual use cases are defined in the Annex.

Within the context of the event and dispute handling framework it is not intended to duplicate messages/information exchanged between the ASPSP and the AISP/PISP via the API and/or interface.

PIS-related messages

- PISP name/ identifier in accordance with EBA Registry definitions
- ID user
- ID transaction
- Timestamp
- Error type (as per direct interface/API specification)
- Information of the transaction sent to the API
  - Amount
  - Label
  - Balance (if accessible)
  - Beneficiary
  - 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
  - Level
  - Who performs the authentication?
  - Technical means of authentication
- Time of response of the API
- Complementary information

AIS-related messages

- AISP name/ identifier in accordance with EBA Registry definitions
- ID user
- Timestamp
- Error type (as per direct interface/API specification)
- 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

Use cases with detailed data requirements[13]

The definition of data requirements in this table is in addition to the content requirements set out above.

USE CASE/ SCENARIO	DESCRIPTION	DATA REQUIREMENTS AIS	DATA REQUIREMENTS PIS	Response Timeline
Communication initiated by TPP				
1. Access				
1.1 TPP access	Precondition: the TPP has a valid certificate and license	Date and time of the access attempt(s)	Date and time of the access attempt(s)	
1.1.1 Access refused	TPP receives notice from ASPSP that access is refused. ASPSP to notify NCA of refusal and explain. TPP contacts the ASPSP to ask for reason.	In case the problem affects one or a small number of PSUs, the identifier of the said PSUs Log proving the access refusal		2 business days
1.1.2 Interface not available	TPP identifies that interface to PSU account is not available. TPP contacts ASPSP to ask for reason.			1 business day

[13] Note: this list is not exhaustive. Other use cases might be identified at a later stage.

USE CASE/ SCENARIO	DESCRIPTION	DATA REQUIREMENTS AIS	DATA REQUIREMENTS PIS	Response Timeline
2. Performance	*Note: this section is to be aligned with the forthcoming business continuity plans of ASPSPs and TPPs (Art. 33 RTS)*			
2.1 Customer-facing interface performance issues 2.2 Dedicated interface performance issues	Data format & connectivity issues (e.g. slow response times, occasional down time) Contact ASPSP directly, asking for immediate feedback/problem solving Dedicated interface does not operate at the same level of availability/ performance as customer-facing interface Contact ASPSP directly, asking for explanation and problem-solving timeframe	Date and time of the access attempt(s) In case the problem affects one or a small number of PSUs, the identifier of the said PSUs Log proving the connectivity issues	Date and time of the access attempt(s) Response times for a specific transaction	2 business days 2 business days
3. Processing				
3.1 Payment not-initiated / accepted	Contact ASPSP directly, asking for explanation and problem solving. A failed payment would be reported by the PSU	Not applicable to AIS	In case the problem affects one or a small number of PSUs, the identifier of the said PSUs	2 business days

USE CASE/ SCENARIO	DESCRIPTION	DATA REQUIREMENTS AIS	DATA REQUIREMENTS PIS	Response Timeline
3.2 Failed Payment	(beneficiary) to the TPP in case the payment is not processed correctly and/or no information about its state is reported.		Real-time payments: 3 possible responses: 1- payment order is correctly completed, 2- beneficiary PSP has rejected the payment 3- No response available yet The status of the payment is always available through a GetStatus functionality providing one of these responses. (note: in principle there is no foreseen case where this could end up with a dispute)	
3.3 Inconsistent Account history	a. PSU complains to TPP about inconsistency of account history. b. TPP detects inconsistency in balance received from ASPSP There are two scenarios for this case.	Description of the inconsistencies detected	Not applicable to PIS	Upon identify-cation of root cause immediately.

USE CASE/ SCENARIO	DESCRIPTION	DATA REQUIREMENTS AIS	DATA REQUIREMENTS PIS	Response Timeline
	1. Account history is inconsistent in the dedicated interface, but consistent in the customer-facing interface. 2. Account history is inconsistent in both interfaces (dedicated and customer-facing interface) In both cases the TPP notifies the ASPSP that transaction history is inconsistent and requests investigation.	Log proving the inconsistencies detected		
4. Escalation				
4.1 Notification to ASPSP of escalation to national competent authority (NCA)	In accordance with the provisions of PSD2 the TPP may notify an NCA in case of certain circumstances. This use case represents the ultimate escalation of any issues that were not solved in preceding correspondence in the area of access, performance and processing.	Reason for notification Proof that ASPSP was notified and there was no timely solution Information as per use case that generated the escalation	Reason for notification Proof that ASPSP was notified and there was no timely solution Information as per use case that generated the escalation	Simultaneously with the notification to the NCA, copy to the ASPSP.

Communication initiated by ASPSP				

1. Access				
1.1 Un-authorised/ wrong data sharing (upon client notification)		Date and time of the access attempt(s) Identifier of the PSU Log proving the data provided to client		
1.2 Un-authorised access notification	2 situations which can result in the ASPSP to contact a TPP to ask for investigation/ clarification: 1) PSU reports to ASPSP an un-authorized log on to the account according to account access log 2) ASPSP identifies unsuccessful access attempts.	▪ Date and time of the access attempt(s) ▪ Identifier of the PSU ▪ Log proving the access by TPP		
2. Performance	*Not relevant for ASPSP*			
3. Processing				
3.1 Un-authorised Payment (upon client notification)	Legal basis: PSD2 Art. 73(2) "Payment service provider's liability for unauthorised payment transactions" The process would be as follows: 1. PSU notification to ASPSP 2. ASPSP refunds immediately 3. ASPSP notifies TPP	Not applicable to AIS	▪ Name of the account holder ▪ IBAN/BIC ▪ Date and time of the payment ▪ Payment reference	2 business days

	4. TPP to prove not responsible a. if successfully done = nothing further happens if not able to prove = TPP compensates the ASPSP			
3.2 Inaccurate / late payment	PSU notifies the ASPSP that a payment has been executed inaccurately or too late. According to art. 90 of PSD2, ASPSP is initially responsible to restore /compensate the damage towards the PSU. In the subsequent investigation of root cause the ASPSP will contact the involved TPP to investigate/clarify responsibilities		- Name of the account holder - IBAN/BIC - Date and time of the payment - Payment reference	2 business days
4. Escalation				
4.1 Information request by competent authority	In case a competent authority such as law enforcement agencies, NCA, National AML Authority requests information, the ASPSP will gather all relevant and available information and if necessary will ask the TPP for complementary information.	Dependent on the NCA	Dependent on the NCA	1 business day