

Euro Retail Payments Board (ERP)

Report of the ERP Working Group on Payment Initiation Services

ERP Meeting 12 June 2017

1. Background

The Euro Retail Payments Board (ERP) decided at its November 2016 meeting to set up a working group with the participation of relevant other stakeholders (e.g. third-party providers as well as standardisation and market initiatives) to identify conditions for the development of an integrated, innovative and competitive market for payment initiation services (PIS) in the European Union (see participants list in Annex 1).

This report provides a summary of the main outcome of the work conducted by the ERP Working Group on PIS between January and May 2017, in line with its mandate as defined by the ERP (see Annex 2).

In order to progress quickly, given the limited time available, with the task of defining common technical, operational and business requirements, three dedicated expert subgroups were created which respectively focused on the topics of identification, interfaces and other operational and technical matters.

Due to time constraints the working group was unable to address:

- Potential technical requirements such as for the choice of the communication layer, message formats and for dealing with the complexity of co-signing in particular in the context of corporate payments.
- 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.

It should be noted that at the time of the working group's activities the process for adoption of the European Banking Authority (EBA) Regulatory Technical Standards (RTS) on strong customer authentication (SCA) and common and secure communication (CSC) had not yet been completed.

2. Key findings and recommendations

2.1. Key findings

The working group agrees on the following key objectives to help achieve the overall goal of an integrated, innovative and competitive market for PIS:

- Maintaining trust.
- Providing the information necessary for the effective operation of PIS.
- Avoiding fragmentation at European level.
- Ensuring clarity of the liability framework and regulatory requirements.

There however remain some diverging views within the working group on related topics which are highlighted in this report (and summarised in Annex 3).

Maintaining trust

In order to support the establishment of an integrated and secure PIS market it is necessary to create the conditions under which payment service providers (PSPs) can confidently interact with each other across the European Union. To ensure such trust between PSPs, account-servicing payment service providers (ASPSPs) need to reliably identify that an actor claiming to be a valid third party provider (TPP), is who it claims to be, and that it is duly authorised to provide the specific payment service that it wishes to provide. Key points in relation to the identification of PSPs include:

- The revised Payment Services Directive's (PSD2) requirement for the provision by the EBA of a central electronic register of payment institutions and,
- The requirement of the final draft EBA RTS on SCA and CSC to use certificates from qualified trust service providers (QTSPs) in accordance with the eIDAS¹ Regulation, in order to maximise efficiency and verifiability.

The EBA register may not contain sufficient information for the purposes of identification. In order to address this potential issue, the following two approaches were identified without any general consensus in the working group at this stage on the preferred direction:

- Include extra information in the certificate with the need for a process to handle certificate revocations and for the renewal of certificates to reflect changes in the status of the PSP.
- Use the certificate as a trusted key to a directory² which will contain additional and up-to-date information that the ASPSPs and TPPs may need to interact with each other securely and effectively. Ideally, this directory should be pan-European in scope, it should be machine-readable with proper service levels, and it should assume a sufficient level of liability to be trustworthy. The working group believes that there is a need for the directory to include information not only about TPPs but also about ASPSPs.

Moreover, it has to be assumed that fraudsters are continuously looking for ways to exploit vulnerabilities in payment systems, which would undermine trust in European electronic payments. Hence all processes related to PSP identification (i.e. directory and/or certificates) should be built with the understanding that they may be used as a vector for fraud. More generally speaking, effective fraud management is key and in all stakeholders' interest; hence a cooperative approach would be welcomed including through sharing information to help mitigate fraud, subject to legal requirements.

¹ The Regulation (EU) N°910/2014 on electronic identification and trust services for electronic transactions in the internal market.

² The term "directory" should not be understood as one monolithic central database but rather as a set of information resources (i.e. "directory services") that may be based on one or more published registers, but may also be other structured data and enablement services.

Providing the information necessary for the effective operation of PIS

Firstly, for PIS to function well and to ensure a positive end-user experience, it is necessary that the ASPSP readily provides or makes available to the payment initiation service provider (PISP) the information (i.e. the “what”) that allows the PISP to confirm to a merchant that it can rely on the fact that the payment has been initiated and should be executed. The actual content of the “what” will depend on the ASPSP’s infrastructure. The following three scenarios were identified:

- a. ASPSPs with real-time booking in their core banking applications: information that the payment order has been accepted and booked on the payer’s payment account.
- b. ASPSPs with batch-processing and delayed booking in their core banking applications (or during unavailability/maintenance of real-time booking): information that the payment order has been received, but the final availability of funds has not yet been checked, and the transaction has not yet been booked on the payer’s payment account. In this case the TPP performs an additional risk assessment based on a range of payment account related information to be provided or made available by the ASPSP, subject to legal requirements.
- c. ASPSPs offering instant payments (which are expected to be more widely available in the market by 2020).

Scenario a. and in particular scenario c. are considered to enable the provision of PIS in an efficient and effective manner. There is however disagreement within the working group, in particular in relation to scenario b., on the payment account related information that needs to be available. The working group discussed what type of information would have to be included, for example a list of available payment accounts, the last known account balance, any pending/scheduled transactions, and the overdraft limit (if any). There is also disagreement on the required regulatory status for requesting this additional information, i.e. does this fall within a PISP licence only, or would both a PISP and an account information service provider (AISP) licence be needed (see Annex 3). On the other hand, from a technical point of view, the working group agreed that AIS and PIS can be supported within the same inter-PSP communication session.

Secondly, the user experience is also influenced by the application of strong customer authentication (SCA) with dynamic linking as part of the payment initiation process. The following three approaches were discussed by the working group:

- Embedded: the personal security credentials of the payment service user (PSU) (e.g. user ID, One Time Password (OTP)) will be transmitted to the ASPSP by the TPP.
- Redirection: the PSU is redirected to the ASPSP’s website for the sole purpose of its authentication, and is then redirected back to the PISP’s website.
- Decoupled: SCA takes place via a dedicated device and/or app.

There however remain diverging views between the stakeholders in particular in relation to a situation whereby ASPSPs would not support the embedded approach (see Annex 3). The working group also recognises that the PSD2 itself - by requiring a dynamic factor - and technological evolutions (e.g. fingerprint scanning on the customer's device) will impact how SCA will be performed in the future.

Avoiding fragmentation at European level

There exists a risk of fragmentation in multiple areas which should be tackled in order to ensure an open, competitive and innovative pan-European market for PIS. A first layer of fragmentation could be introduced by diverging transpositions of the PSD2.

In general, the working group wishes to stress the need for harmonisation across all national competent authorities to avoid fragmentation for example in relation to the registration of TPPs and certificate handling. The working group sees an important role for the EBA to ensure consistent and efficient application of national processes related to the registration of TPP and in connection with certificate handling. Other areas for which harmonisation would be beneficial are the technical aspects related to certificates and the overall testing framework for interfaces.

The working group also took note of recent PSD2 related standardisation and market initiatives:

- Expected development of national application programming interfaces (APIs)³ to facilitate PSD2 implementation in France, Poland and the UK.
- Cross-border initiatives such as the Berlin Group⁴ and the Convenient Access to PSD2/Payment-related Services (CAPS)⁵.

In general, the working group welcomes these standardisation initiatives as they are expected to facilitate the practical implementation of PSD2. At the same time the working group identified a risk of fragmentation which would require for these standardisation initiatives (and any other that may appear) to

³ API (Application Programming Interface): set of clearly defined methods of communication between various software components.

⁴ The Berlin Group is a pan-European payments interoperability standards and harmonisation initiative with the primary objective of defining open and common scheme- and processor-independent standards in the interbank domain. It first met in 2004. The project comprises banking and payment associations, processors, as well as a few banks and card payment schemes.

⁵ The CAPS market initiative is a pan-European multi-stakeholder coalition-of-the-willing that aims to make PSD2 work safely, in practice and at scale for all. It is an open forum that proposes solutions to the technical, business and operational issues faced by potential PSD2 stakeholders across Europe. Banks/TPPs/Fintechs/service providers/corporates/mobile industry/etc. work together here to develop a framework that works for all – not just for one side of the industry or one geography. The CAPS community has developed a good deal of the framework, much of which it is contributing to ERPB especially in the areas of hubs, identification and directory services, and individual members are piloting CAPS concepts to harden the framework in 2017.

communicate with each other to come to a harmonised pan-European approach. However, some working group members pointed to existing or future global standards (e.g. ISO 20022⁶, HTTPS⁷).

Ensuring clarity of the liability framework and regulatory requirements

Although the working group refrained from interpreting the PSD2 or the final draft EBA RTS on SCA and CSC whilst carrying out its work, it produced a list of topics for which clarification would be welcome from the European Commission or the EBA (see Annexes 4 and 5).

The working group is of the view that the development of a competitive market for professional indemnity insurance, as well as the minimisation of inter-PSP disputes and their effective handling, require a clear liability framework. This will furthermore contribute to the achievement of the overall goal of an integrated, innovative and competitive market for PIS.

2.2. Recommendations

On the basis of the above, the working group suggests the following recommendations for consideration by the ERPB at its 12 June 2017 meeting:

#	Issue/rationale	Recommendation	Addressee
1.	Several legislative/regulatory topics (e.g. related to passporting, liability regime and insurance) are still unclear and create uncertainty within the market.	Provide further clarification in relation to the questions listed in Annexes 4 and 5.	European Commission / EBA
2.	The final draft EBA RTS on SCA and CSC stipulate - in order to maximise efficiency and verifiability - that identification would be based on certificates issued by QSTP under eIDAS. To date the working group is not aware of the availability of QSTPs in all countries of the European Union.	Promote timely establishment of QTSPs across the European Union.	Member State eIDAS competent authorities

⁶ ISO 20022: ISO standard that defines the platform for the development of financial message standards.

⁷ HTTPS (Hypertext Transfer Protocol Secure) is a communications protocol for secure communication over a computer network which is widely used on the Internet.

ERP WG on Payment Initiation Services

3.	Need for a common, secure, resilient, reliable, and up to date “directory service” on a pan-European level. Such directory could take the form of a central directory (based on the central EBA register) or of a ‘directory of directories’ (i.e. directories based on national registers).	Design a shared directory infrastructure for ASPSPs and TPPs and determine content and modus operandi.	ERP/ or market led initiative
4.	Harmonisation needed in relation to registration, certificate handling, notification and exiting processes across all national competent authorities.	Produce an operational guide describing how the registration, certificate handling, notification and exiting processes should work in a harmonised way across countries in the EU.	EBA
5.	There is a need for a multi-stakeholder initiative to standardise technical aspects related to certificates.	Establish a multi-stakeholder initiative to determine: <ul style="list-style-type: none"> - What data elements (and in which format) shall be stored in the certificate. - Where in the certificate these elements shall be carried. - Obligations on QTSPs relating to the above. 	European Telecommunication Standards Institute (ETSI) or other appropriate body
6.	There is a need for a standardised ASPSP-TPP transaction related dispute handling process on a pan-European level.	Develop the requirements for a standardised ASPSP-TPP dispute handling process to ensure a harmonised and efficient approach on a pan-European level.	ERP/ or stakeholder initiative

ERP WG on Payment Initiation Services

7.	Need for a harmonised framework for the testing of interfaces.	Define harmonised framework for the testing of interfaces.	ERP or stakeholder initiative
8.	In order to contain fraud, at a minimum ASPSPs should receive from TPPs the same level of behavioural and device related information as they would have received from their direct interaction with the PSU.	Define modus operandi for the provision of such information and investigate other fraud mitigation actions.	Standardisation initiatives
9.	To have an effective market for professional indemnity insurance for TPPs.	Clarify the liability framework.	EBA and national competent authorities

The ERP is invited to:

- Discuss the identified issues and recommendations outlined in the report.
- Agree on and endorse the recommendations and addressees summarised in the above table.
- Discuss whether further action will be necessary to address diverging views between stakeholders and the need for harmonisation between various market and stakeholder initiatives.

Annex 1: List of ERPB working group participants

Category	Name	Institution
Co-Chair	Alain Benedetti	EPC (BNP Paribas)
	Paul Alfing	Ecommerce Europe
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)
ECB	Pierre Petit	ECB
	Iddo de Jong	ECB
NCB	Dirk Schrade	Deutsche Bundesbank
	Gregorio Rubio	Banco d'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
Standardisation initiative	Ortwin Scheja	Berlin Group
	Michael Salmony	CAPS
	Thomas Egner	EBA
PISP	Chris Boogmans	Isabel Group
	Bartosz Berestecki	PayU
	Georg Schardt	Sofort GmbH (co-Chair 'Interfaces' subgroup)
	Oscar Berglund	Trustly Group AB
AISP	Kevin Voges	AFAS Personal
	Joan Burkovic	Bankin
Other PIS-stakeholder	Max Geerling	Dutch Payments Association / IDEAL
	James Whittle	Payments UK
	John Broxis	Preta / MyBank (co-chair 'Identification' subgroup)
Guest	Hans Georg Spliethoff	EMOTA (Otto)
	Christopher Kong	CAPS (Icon Solutions) (co-Chair 'Identification' subgroup)
	Mario Maawad	ESBG (CaixaBank) (co-Chair 'Other' subgroup)
	Oliver Bieser	EPC (Deutsche Bank) (co-Chair 'Interfaces' subgroup)
Secretariat	Etienne Goosse	EPC
	Christophe Godefroi	EPC

Annex 2: Mandate ERP WG on Payment Initiation Services



ERP Secretariat

ECB-UNRESTRICTED

28 November 2016

ERP/2016/012rev2

MANDATE OF THE WORKING GROUP ON PAYMENT INITIATION SERVICES

Based on Article 8 of the mandate of the Euro Retail Payments Board (ERP), 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 ERP 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: Diverging views between stakeholders

#	Topic
1.	<p>Objective criteria that ASPSPs can check (as part of the identification process)</p> <p>The ASPSPs argue that they have obligations to check the TPP's status including the TPP's role, in view of due diligence, operational risk management and liability vis-à-vis their customers.</p> <p>The TPPs argue that there is no obligation in either PSD2 or the draft final EBA RTS on SCA and CSC for the ASPSP to check regulated TPPs. It is the TPPs responsibility to comply with the law, otherwise they risk losing their licence.</p>
2.	<p>Payment account related information</p> <p>Can a TPP that only has a PIS licence, receive or obtain specific payment account-related information - directly related to a PIS transaction – in a single PIS request? This would relate to a list of payment accounts (and balances) if more than one payment account is managed within the same ASPSP/PSU relationship, as well as to the information needed for the cases in which the ASPSP cannot provide information that the amount has been booked.</p> <p>TPPs are of the view that the above is indeed the case based on PSD2 and the General Data Protection Regulation (GDPR). ASPSPs however contest this interpretation of the above mentioned legislation.</p>
3.	<p>Redirection and decoupled approaches for the purpose of SCA</p> <p>The ASPSPs are of the view that in order to be able to properly handle disputes, irrefutable proof of the PSU's authentication must be collected. Since there is no contractual relationship with the TPPs, and ASPSPs are liable (hence must refund the PSU upon a claim), ASPSPs are of the opinion that the PSU may be required to authenticate him/herself either directly in the ASPSP's systems or via a separate device/app provided or supported by the ASPSP. Furthermore, ASPSPs consider this to be more secure and it also ensures a consistent PSU experience. ASPSPs also believe that they must follow innovations and keep state of the art SCA methods and user experience. The same SCA methods and user experience are proposed on the website/app or through PIS (in compliance with the non-discrimination requirement).</p> <p>TPPs argue that redirection must not be imposed by the ASPSPs according to PSD2. Imposing redirection or requiring decoupled approaches would be in contradiction of PSD2. In case of non-compliant identification methods being offered by ASPSPs, PSD2 enables TPPs to seek alternatives.</p> <p>Furthermore, TPPs argue that a fundamental component of PIS is the control of the consumer</p>

	<p>experience through the possibility for the TPP to design and provide a graphical user interface to the PSU that is convenient and adapted to the specific situation/device of the PSU (“look and feel”). A redirection implies a very poor user experience (the payer is moved from one interface to another web page and then back again in a confusing and time-consuming process) which is further exacerbated when the ASPSPs have not adapted their redirection domains for different mobile devices (small screen of e.g. a mobile phone).</p> <p>A redirect does not only as mentioned above eliminate the prerequisites for an adequate user experience but also violates the principle of technology neutrality as it only works in a web-browser setting. Regarding security and disputes, TPPs note that PSD2 has already established that TPPs may transmit the credentials of the PSU to the ASPSP. It should furthermore be clear that it is still the ASPSP that owns the authentication procedure and the PSU authenticates itself vis-a-vis the ASPSP, even if it is the TPP that transmits the credentials, as much as the PSU authenticates itself vis-a-vis the ASPSP when the PSU enters the credentials into a web browser that transmits the credentials to the ASPSP. If the TPP would not transmit the credentials, the whole idea of bringing TPPs into the scope of regulation in the first place would be moot, as would e.g. the requirement on the TPP to hold insurance coverage in order to provide activities. If TPPs would have to redirect the PSU to a domain hosted by the ASPSP for authentication, the TPP would no longer have a product of its own, but be reduced to merely a “redirection plug-in” at the merchant’s website.</p>
--	--

Annex 4: List of clarification requests for the European Commission

#	Clarification requests
1.	Can a TPP who only has a PIS licence, receive or obtain payment account-related information - in relation to a specific PIS transaction – in a single PIS request?
2.	What are the implications of the General Data Protection Regulation (GDPR) on the international bank account number (IBAN) versus PSD2?
3.	Is mutual authentication a legal requirement (e.g. must TPP also check the ASPSPs authentication)?
4.	Would an ASPSP be either allowed, required or prevented from checking the authorised country (i.e. passporting) during a payment initiation or payment account information request? If this check should or may be done and the ASPSP fails to do it, what is the liability regime and refund mechanism in case of dispute? Is there any other factor regarding the TPP that the ASPSP should be allowed, required or prevented from checking?

Annex 5: List of clarification requests for the EBA

#	Clarification requests
1.	<p>Article 10 (2) in the final draft EBA RTS on SCA and CSC stipulates that PSPs are not exempted from applying SCA exemptions if PSU is accessing online information specified in Article 10 (1) for the first time or SCA was applied more than 90 days ago. Is this 90 days per channel (i.e. online banking, mobile, AIS) or per user for all channels used?</p>
2.	<p>It is not clear what Member States will do as far as credit institutions that also want to be TPPs are concerned, e.g.:</p> <ul style="list-style-type: none"> • In which register is their information stored? • Do they need to be passported? • Are their certificates the same as TPP certificates? <p>Clarity is needed as to which information registers hold which information - either for the QTSP to check before issuing a certificate, or for a PSP to check if qualified certificates are not enough.</p> <p>The same question applies to e-money institutions.</p>
3.	<p>Should there be a choice between certificates for websites and certificates for electronic seals or should only one of these options be retained for the sake of harmonisation?</p> <p>It is currently not clear who can choose which option is used. Must the ASPSP support both? Does the ASPSP by defining an interface decide on which one the TPP will need to use? Also, it is not clear whether these two types of certificates (i.e. for electronic seals and for website authentication) are equivalent from an identification point of view.</p>
4.	<p>ASPSPs require further guidance in order to harmonise the fulfilment of the reporting obligations to national authorities for dedicated interfaces. Can EBA provide this guidance?</p>
5.	<p>The liability regime for TPPs, insurance companies, MSCA registers and QTSPs is currently unclear. Can EBA provide further clarity?</p>