PolishAPI

Specification of the Interface for the Needs of Services Provided by Third Parties on the Basis of Access to Payment Accounts

Public consultation 17.01.2018 – 31.01.2018

No.	Comment / Note	Suggested phrasing / Change justification	Taken into account in the specification?	Response / comment of the project team
1	As of 1 January 2017, a single transfer to ZUS was introduced which is based on a standard transfer order and the Elixir 11n message. Each ZUS contribution payer was assigned his/her own Contribution Account Number, in which - without limitation - his/her own NIP number and the ZUS settlement number are encoded. In the Polish API specification, the old transfer standard dedicated to ZUS payments which was effective until the end of December 2017 and was based on the Elixir 12n message was taken into consideration (the transfer contained, for example, fields related to the payer ID information, fund, type of payment, period etc.).	There is no need to take into account in the Polish API a transfer standard which ceased to exist as of the end of December 2017.	no	In the payment initiation service, the ZUS payment was not taken into account - due to the regulatory changes.
2	The Polish API standard takes into account an authentication mechanism based on the user redirection to the ASPSP's domain (the so-called 'redirection' mechanism). It is a secure authentication method successfully used in the Polish banking sector for years, e.g. in the pay-by-link service. However, the TRS on the SCA and CSC, in Article 32, it was clearly indicated that: Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing	It is worthwhile to allow in the Polish API standard other authentication methods that meet the legal requirements (RTS on SCA and CSC). In consequence, the Polish API will have a greater chance of becoming more popular.	yes	

	payment service provider's authentication or other functions, requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive (EU) 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services.			
3	The fields in the business specification should indicate example values, and specify whether they are optional or not, to make the format more readable	Add example values and optional indicator to the field list	no	The data range and the information if required may vary between different implementations. Fields become mandatory for ASPSPs in relation to the scope of information about payment accounts and transactions the given ASPSP makes available in its online interface, save exceptions stipulated in the law (e.g. with regard to particularly protected data concerning payments or personal data). Each ASPSP may add additional fields to the scope of data concerning the account and transactions made available.

4	The account identification field should have a corresponding field of „identification type”. The IBAN code as the default identifcation type adopted in the standard is not widely used in some countries, e.g. the UK. The IBAN code may also not be applicable to portfolios of some custodian banks that hold more diversified securities. As a result, it would not be easy to describe a transfer to a UK, a digital wallet, or a custodian bank account in Switzerland.	Add account identification type field with the default value of „IBAN code”	no	The problem will be addressed in the next version of the specification.
5	Every amount should have a corresponding field with the amount currency (e.g. in the getTransactionsDoneRequest request)	Add currency field to all relevant amount fields in the specification	yes	
6	The custom parameters of the API requests should be made optional (e.g. scope_details) and indicate the default values	Make the custom parameters optional in the specification	no	PolishAPI project group decision. The "scope_details" parameter contains crucial information.
7	The font chosen for the API specification should include Polish signs, it is visible that a substitute font is used for Polish characters (e.g. in word „Płatności”)		yes	
8	Regulatory Technical Standard (RTS) needs a better entry in the glossary		yes	
9	The PKI infrastructure should be described in the document or at least the model it is to operate in should be described.	The PKI model adopted may significantly impact the API implementation and, therefore, it should be imperative to decide what it look like and then to describe it in detail in the document.	yes	

10	While ASPSPs are free to accept the technical solutions (including the option not to use the Polish API), I suggest that the standard should be implemented in whole.	A partial implementation of the standard misses the point - creation of N implementations which would partially operate on an identical basis and partially - not identical at all. If the purpose of the development of a single solution is to reduce the costs of implementation on the consumers' side, this provision does not have a point. I propose to focus on the minimum subset which may be implemented in whole and then to develop the API based on a time frame which will allow a full implementation by a maximum number of entities.	yes	
11	General comment - the branch-specific nomenclature should be used all over the document, preferably in English.	The introduction (first part of the document) described relatively detailed elements using the term 'authorization codes' - it is not entirely clear which code is referred to. I propose a reference is made to a detailed document describing the given term, similarly as in the further part of the document.	yes	
12	It is unclear what is meant by 'a separate XS2A session'.	Is it a TLS session, i.e. each request-response cycle requires a separate connection cycle, or is it any other session type? It should be explained beyond any doubt.	yes	
13	There are financial products with an interest validity period shorter than 1 year (e.g. 2 months). How is the variable interest of such an account designated?		yes	
14	The payment card number hashed is a poor solution from the useability point of view.	Instead, I propose that the first four + last four digits of the card number or only last four digits of the card number be used.	yes	
15	What is the PSD2 HUB and what is its scope of responsibility?	I assume this issue will be explained in whole after the PKI model description has been added to the document.	yes	

16	The justification for item 2 is erroneous.	The use of mutual authentication by the TLS has absolutely nothing to do with the fact whether or not the client device (a non-defined term) may use the API.	yes	
17	A risk that the PolishAPI product may be difficult in the consumption by the TPP.	I propose to focus on the subset of functionalities with regard to which there is a certainty that it may be implemented by almost all participants.	no	PolishAPI project group decision. We are trying to go beyond the minimal, compliance scope, where it is possible.
18	Reasoning error.	There is no obstacle when it comes to ensuring the non-repudiation of individual messages via JWS (RFC7515), irrespective of the HTTP method used.	no	PolishAPI project group decision.
19	The requirement that each HTTP exchange was signed in order to ensure the non-repudiation only introduces an efficiency risk.	To generate JWS or any other digital signature, the entire text to be signed is necessary. This means that the entire message to be signed must be in the memory because the HTTP headers are send even before the text is sent. Resigning from this requirement, we obtain a possibility of an incremental dispatch of data to the client and the client may also process such data incrementally. This solution may be of significance in case of large volumes of data sent simultaneously.	no	PolishAPI project group decision. We recognise that security has priority in this case. Incremental data dispatch is planned by be resolved by paging.
20	Use of Accept-Language is doubtful.	It is difficult for me to find any scenario in which a return of data in various languages would have a point.	no	The transaction status decision requires a decision as to the language. The language is required in case of banks with multi-language systems.

21	Content-Type should be specific and not general, similarly as application/json.	Instead of a generic application/json, it would be proper to apply a specific type (http://www.iana.org/form/media-types), for example: application/polishapi.v1+json	no	We use application/json due to the fact that this standard is commonly used. Some tools may not support the approach proposed.
22	It is not clear why the authorization data may not be sent in the form of URI parameters.	Please explain the reason underlying this decision.	no	We assumed that the signature does not comprise URI, therefore we adopted the use of the POST method instead of GET. URI is a part of public communication and may be compromised.
23	Identity confirmations are confidential (...) - the term of identity confirmation is not defined anywhere, the public form is not defined.	Actually, it is not known what it means and in what context this decision is of significance - please explain.	yes	
24	This phrase seems to be taken out of context - is this maybe a remnant of some notes?	Please explain how the automation on the client's side would operate and why it is not allowed.	yes	
25	How do we manage the keys in the context of JWS signatures?	Please explain how the keys are allowed for use, how the rotation takes place and how it may be established that the key used for signature is still valid, etc.	yes	
26	I have an impression that any possible susceptibility to a CSRF attack may be only in case of the browser's interaction with ASPSPs.	Please explain the context to which this comment refers to, because it does not refer to the server-server type of interaction.	no	

27	If it is necessary to store the contents of HTTP requests and responses due to the non-repudiation, one should define the conditions in which the request will be accepted.	Depending on the implementation, the time from the request generation to request reception by the other party may be as long as one second even. The maximum clock difference between two participants should be determined.	yes	
28	It is difficult for me to see the validity of introducing callbacks to API in this form.	Beyond any doubt, the return of a list of accounts or a paged list of transactions should take less time than the readout timeout in HTTP (30 seconds), thus there is no reason that these endpoints in particular be supported by operations in an asynchronous mode. It would be reasonable, instead, if information about the changing payment status be provided but it is missing from API.	no	If the TPP's request for a history of transactions exceeds the size defined by the ASPSP in the implementation documentation, an error message is sent, advising about the necessity to use the asynchronous method.
29	The resources made available by API fit in perfectly with REST but for some reason the author chose something that reminds RPC. In my opinion, this is a decision the change of which will have the most positive impact on the extent to which API will be useful.	The remaining quantity of public APIs used in the web ecosystem uses REST as an architectural style and JSON as data representation. The conventions adopted by REST are commonly known in the developers' environment and I propose that they be applied here. The use of REST will radically simplify the construction of the whole API.	no	The project decisions were justified by the willingness to maintain the maximum security level
30	There is no information as to the way JWS should be constructed.	Please supplement the information. In case REST is used, JWS should be supplemented by data from the HTTP headers, which are necessary from the non-repudiation point of view.	no	PolishAPI project group decision. HTTP headers are used in limited way.

31	Instead of a few endpoints for retrieving transactions at different stages, a single endpoint with a filter is enough.		no	The data structure in the response is varied. The endpoint structure reflects the structure of business objects in the banking systems. In particular, some of these objects are not financial transactions.
32	How will the client using a TPP know what fees are applied to the given transfer? In Internet banking, there are fee alerts, e.g. from a savings account, when there usually is only one free-of-charge transfer per month and remaining transfers are at a fee. Fees or commissions usually appear in case of express and international transfers, etc. When reviewing the specification, I found no such mechanism. Do we assume that TPP is not obliged to inform the clients about the fees or the date then the transfer is effected (if, for example, it is ordered after the cut-off time), and the client agrees to ‘blind’ transfer ordering by the TPP?		no	The decision about making this information available remains at the discretion of the ASPSP.

33	The scheme described is unacceptable from the RTS point of view. In fact, there is a double consent - first on the TPP's side - and then on the ASPSP's side. The possibility to select accounts after logging in modifies the earlier consent for the retrieval of data from all accounts, which is not compliant with the RTS. For information: in practice, the AISPs such as Kontomatik will always need all accounts. This flow should be treated as common in the market practice.		yes	A new process was proposed.
34	The current Swagger leaves almost all technical fields as optional. I have in mind here the lines 'Required: ...'. For example, in case of an account, event the balance is not required, and in case of a transaction, neither the recipient nor the sender are required. As a developer and a CTO, I can guarantee that developers from external companies who will implement it at the ASPSPs' order, will not read the 'business' specification (where the situation is a little better), but will focus on the technical one (Swagger) and will squeeze the technical minimum from the systems. And then, as AISPs, we will have to 'beg' 26 banks for years to provide us the missing fields. And I am not speaking here about any 'bad will' of the ASPSPs, but about the most probable implementation scenario resulting from the Swagger and the realities of developers' work.		no	The data range and the information if required may vary between different implementations. Fields become mandatory for ASPSPs in relation to the scope of information about payment accounts and transactions the given ASPSP makes available in its online interface, save exceptions stipulated in the law (e.g. with regard to particularly protected data concerning payments or personal data). Each ASPSP may add additional fields to the scope of data concerning the account and transactions made available.
35	There is no, for example, account opening date, even as an optional field. This information is very often visible in Internet banking.		no	The standard comprises the field range on the basis of regulations (PSD2 and RTS).

36	In our opinion, the description of the process of granting consent for AIS is incorrect - especially as regards the redirection to the TPP's site; in our opinion it takes place after the PSU has selected the accounts. If it was the Bank to send all available accounts to the TPP, then there is a question whether or not it is authorised to do so. It is the TPPs approaching the Bank that should have the accounts already indicated. Provision by the Bank at this stage of account numbers, if the client has not indicated any specific ones, may be considered a breach of the banking confidentiality clause. On our part, we would appreciate if, when analysing this material, it was also verified whether or not the PSU may - as part of the process of granting consent to AIS - grant a consent to a few payment accounts indicated specifically. Clarifying, if the PSU has indicated, for example, two payment accounts, is it possible to confirm it by a single SCA (e.g by a text message)?		yes	A new process was proposed.
37	Why is 'the process of PSU's granting consent for the ASPSP to effect the COF service outside the scope of this document'?		yes	The process of the PSU's granting consent for the ASPSP to effect the COF service will be described in the subsequent versions of the specification.

38	Why is 'the way in which such a functionality should be ensured beyond the scope of the Polish API Standard'?		no	It is beyond the scope of the document because we do not specify the interfaces on the TPP's side and on the ASPSP's side.
39	no definition of the components of the SCA (i.e. 'first' and 'second') – particularly significant in the context of the 'embedded' mechanism.		no	We do not see a necessity to make these provisions more detailed.
40	I do not understand the phrase '(…) within this range of dates'.		yes	
41	we think that the 'Account interest rate' should also be excluded from the scope of AIS data. Even though the interest rate of the given account is one of the pieces of information about account the AIS service concerns, it should be indicated that the interest rate, frequently agreed on an individual basis with the client, should be deemed a commercial secret and not provided to third parties.		yes	

42	there is an inconsistency between the business part and the technical part with regard to the fact which functionalities should be included in the Compliance section and which in the Premium section. In particular, the following functions are in mind: For AIS, the Compliance scope should be: 6.1. /accounts/{version}/getAccount - Gets a single payment account 6.2. /accounts/{version}/getTransactionsDone - Gets transactions done at the account 6.3. /accounts/{version}/getTransactionsRejected - Gets transactions rejected at the account 6.4. /accounts/{version}/getHolds - Gets holds at the account 6.5. /accounts/{version}/getTransationDetail - Gets details of a single transaction/hold For Premium AIS: 6.6. /accounts/{version}/getAccounts - Gets all accounts of the PSU 6.7. /accounts/{version}/getTransactionsPending - Gets the transactions pending at the account		no	A new process was proposed.
43	Has the question of banking secrecy been settled? In the amendment to the Payment Services Act, there is no information and there is no information about potential amendments to the Banking Law either.		no	In the draft Payment Services Act processed, some amendments to the Banking Law were allowed for, which release the bank from the banking secrecy in case of provision of the AIS and PIS services)

44	Depending on the decision concerning the definition of foreign EEA and nonEEA transfers, the ‘transfer type’ field should be changed. If a division into standard transfers (made on the D+1 basis) and express transfers (made on the D basis) is introduced, then the comment field must be updated. However, if only the standard mode remains, then ‘Constant value – SEPA” should be deleted from the comment field. By analogy, in case of foreign nonEEA transfers, the comment to the ‘Transfer type’ field should either be supplemented to include a standard mode (D+2), an express mode (D) and an urgent mode (D+1), or ‘-Constant value – nonEEA’ should be eliminated in whole.		yes	

45	There is an inconsistency between the business part and the technical part. Therefore, we propose that the provisions be changed from: Is: ‘Additionally, the ASPSP makes available its data filtering mechanisms in accordance with the criteria available on-line in the ASPSP system (i.e. via the electronic banking), e.g.: a) Transaction booking date, including a date range; b) Transaction amount; c) Data of the other transaction party; d) Description of transaction; e) Other features assigned to the transaction visible in the history of transactions of payment accounts. Should be: ‘ Additionally, the ASPSP makes available its data filtering mechanisms in accordance with the criteria available on-line in the ASPSP system (i.e. via the electronic banking), i.e.: a) Transaction booking date range; b) Transaction amount range; c) Payment account debits and credits.		yes	

46	a comment concerning /v1.0/payments/v1.0/standardDomestic- Request, /v1.0/payments/v1.0/expressDomestic- Request, /v1.0/payments/v1.0/standardNonEEA- Request: The filed indicated are redundant: "transferType": { "code": "string", "description": "string" }, We propose that for expressDomestic, there was another transferType field, which would be enumerative: ExpressElixir, BlueCash, Sorbnet, We also propose that for addTax pole transferType there would be an enumerative selection of Standard and ExpressElixir, if in terms of business a decision is taken to provide also tax transfers using ExpressElixir. If not, the transferType field is redundant.		yes	
47	With reference to the item concerning EEA and nonEEA transfers. We propose then to consider a change of endpoint names: payments/standardEEA into payments/EEA, payments/standardNonEEA into payments/nonEEA, then it would be possible to add a transferType field at the input with enumerators. For EEA: Standard, Express, For nonEEA: Standard, Urgent, Express.		yes	

48	We need to provide information about more than one rate in the transaction details. For example, when sending USD from an EUR account, there is first a conversion EUR->PLN (purchase of EUR), and then a conversion PLN->USD (sale of USD) and we display both exchange rates. A request, that in the TransactionDetailResponse class, the transactionRate field be replaced by a table: transactionRate: with the following fields (from 0 to 2 occurrences) rate: number($double) format 4,7 fromCurrency: string toCurrency: string Additionally, we need 7 decimal places in the field for the exchange rate. Currently: Transaction exchange rate, Format 4,6 / Currency exchange rate		yes	
49	The current proposal of asynchronous methods assumes a call-back with data. The data paging and the data delivery integrity are not supported and this, in case of considerable volumes of data, may bear problems. Maybe it would be better that the ASPSP signalled in the callback to the TPP that a downloadable file was generated (in a defined format) and then the TPP would download the file. Problem to be discussed		no	PolishAPI project group decision.
50	A request to add a rejectionDate field to getTransactionsRejected.		yes	
51	What is the use case of getMultiplePayments under the PIS service? What token would be validated here? I do not see an application of a one-time token in the context of the PIS as is in the Compliance scope - I propose that it be deleted from the swagger.		yes	

52	If the pending transactions are not to be covered by the Compliance scope, also getTransactionsPending and -Async should be eliminated from the swagger.		no	A definition of pending transactions was introduced to the specification.
53	If transactionSegment was eliminated from business requirements, it should be eliminated from the swagger of the TransactionDetailResponse class.		yes	
54	A lot of typos in the descriptions PSU Information Class Get list of user's hold operations Description of glossary items Single Account Information Request Class Status - Is the method made correctly / Status Class containing bank data used in AIS requests / AIS Bank Data Class Class containing name and address data in the form of four data lines / Simple name and Class containing sender/payee data used in AIS requests / AIS Sender Class containing data allowing the use of the paging mechanism / Paging Information Class Class representing information about the card as part of the transaction / Transaction Card Information		yes	

55	‘Performance of Compliance scope services Each ASPSP is obliged to make available the services from the Compliance Scope pursuant to PSD2 and the related acts of law. The ASPSP defines on its own which bank accounts are payment accounts and takes an independent decision as to the scope of payment account data available within the framework of the services. The performance of services within the Compliance Scope will not require a contractual relation between the ASPSP and the TPP.’ We refer to the fragment underlined. While the second part of the sentence can be deduced from the fact that the ASPSP actually decides what scope of data concerning the given payment account is made available online (and, consequently, it is obliged to make it available under AIS), the statement that the ASPSP defines on its own which bank accounts are payment accounts is in our opinion unacceptable. Firstly, not every ASPSP is a bank, therefore, the term ‘bank’ should be deleted. Most of all, it is our opinion that the ASPSP may not arbitrarily and freely decide which accounts they maintain are payment accounts and which are not. Thus concerns the heart of the discussion as to the definition of a payment account … If it were possible to decide on one’s own, it would be very easy for ASPSPs to circumvent the PSD2 provisions concerning the obligation to provide the payment account information under the AIS service and, consequently, also the obligation to build an interface, report etc. In conclusion: we are of the opinion that this provision may potentially stay in the form as below: ‘Each ASPSP is obliged to make available the services from the Compliance Scope pursuant to PSD2 and the		yes	

	related acts of law. The ASPSP takes independent decisions as to the scope of payment account data available online within the framework of this service. The performance of services within the Compliance Scope will not require a contractual relation between the ASPSP and the TPP.'			

56	I am concerned as to how standard this will be if adoption of this is not mandatory. Where can we see who has signed up to what elements of this? In other markets whilst the API is not mandatory banks have voluntarily committed to the API standards in that market in full	Published off banks that have voluntarily commited to the API in full. List of banks that have committed only to part (and to what part). Directory of banks that are providing an alternative with link to published documentation.	yes	
57	In the categories of service I believe this needs to cover more options. It is entirely possible (and likely) that TPPs will have dual AISP and PISP roles. Considering this will change the use case of how a TPP will interact with an ASPSP through a single call and get access to both data and payment initiaiton. Treating them as independent functions can lead to poor user experiences through bulding standalone APIs that only serve one role – see Open Banking in the UK	Recognise joint AISP & PISP role and document how a joint PISP and AISP may interact with and ASPSP through a single API call.	no	According to a legal interpretation, this service is outside the Compliance scope.
58	In discussing authentication methods it does not seem to allow for a TPP to perform the authentication directly with the customer. We believe the regulation (and statements by EU regulatory and industry bodies) encourages non-redirect to ASPSP with TPP taking responsibility for authentication	Remove statement that authentication method is at the discretion of the ASPSP. This should be at the discretion of the TPP. The ASPSP is required to provide a method by which a TPP can use it's own authentication. Worst case this is the customer sharing their credentials with the TPP to perform direct accesss (recognised as a valid route of access where APIs are not functional)	no	In our opinion, it is not acceptable from the regulatory point of view.
59	Definition of Authentication is a process by which ASPSP verifies the users identity. This is also possible by a TPP.	Change Authentication to „A proces in result of which the ASPSP or TPP verifies the PSU's identity"	no	In our opinion, it is not acceptable from the regulatory point of view.

60	1.4.5.2 4) details the ASPSP presenting the PSU a list of payment accounts to choose from. We believe that the TPP should be in control of this user experience. Once consent and authentication has been accepted the TPP should be in full control of the user experience they want to prsent to the customer.	Change to the „ASPSP or TPP present the PSU a list of payment account from which....”	no	Other processes will be added after the authentication methods have been determined.
61	1.4.5.2 Doesn’t reference that balance and transaction data (at a minimum) will also be shared under the PISP license	Include specific reference to the balance and transaction data being shared with the PISP so that they can decide if they wish to initate the transaction (Note a PISP should have access to this information without requiring access to an AISP license. This data is required in payment initiation as without it the PISP risks initiating payments which are unlikely to complete making this unusable)	no	As part of the PIS service, those data are made available which, pursuant to the regulation,s make the payment initiation possible.
62	Application of strong customer authentication. There are recognised exemptions as to when SCA can be applied e.g. low value payments, trusted benefciaries etc.	Change wording to „ASPSP’s or TPPs use any given strong authencation system (SCA) they selected and the Polish API standard does not define and does not recommend any way in which this procedure may be conducted. However transactions will be exempted (detailed below) in accordance with regulation. An ASPSP may only by exeption and with detailed reasons choose to apply SCA in these instances”	no	The regulations contain a description of exceptions, however it is the ASPSP to take a decision to apply an SCA procedure.

63	The scope of information in compliance should in principle be anything that the customer can view in their online bank account.	Include openting sentance that „Within the Compliance Scope is any data viewable by a customers within their online bank. At a minimum this will include data filtering mechanisms....”	no	The data range and the information if required may vary between different implementations. Fields become mandatory for ASPSPs in relation to the scope of information about payment accounts and transactions the given ASPSP makes available in its online interface, save exceptions stipulated in the law (e.g. with regard to particularly protected data concerning payments or personal data). Each ASPSP may add additional fields to the scope of data concerning the account and transactions made available.
64	Please ensure that balance and 3 months transaction data are included within the compliance scope of PIS service	As discussed above this data is required at a minimum in order for a PISP to be able to initiate a transaction	no	The comment concerns the AIS service.
65	There is a reference to a PSD2 hub	Please document what is meant by a PSD2 hub – who is this and what do they do?	yes	
66	It is not clear for me where item 2 is located in the diagram presenting the XS2A session initiation process (page10). Why is item 2 - initiation of communication between the TPP and the ASPSP located on the left and on the right side of the diagram and not at the bottom, between the TPP and the ASPSP? What does this communication comprise? If this is communication between the TPP and the ASPSP, then item 2 should be at the bottom of the diagram, after all the PSU’s activities are contained in item 3.		yes	

	If, however, item 2 comprises also the communication between the PSU and the ASPSP, then it should be described as appropriate and not as the TPP-ASPSP communication.			
67	Also the question of making the data filtering mechanisms under the AIS service made available by the ASPSP in accordance with items 3.1 and 3.1.3 is still not clear for me Who are these mechanisms made available to - the PSU or the TPP? If to the PSU, for what purpose? After all, in case of the AIS service, the PSU should only indicate the accounts the AIS service concerns. Is it that the PSU should indicate exactly, by filtering, the detailed scope of information the ASPSP is to make available to the TPP? If the TPP, then what is is all about - can the TPP not filter on its own a batch of data sent to it by the ASPSP?		yes	

68	The reading of this document would be facilitated if there were a reference to the terms used by the directive and the RTS	I propose that the terms occurring in the document be linked to the terms appearing in: PSD2: • Dynamic codes (motive 95) • Initiated payment (motive 29) • Evidence on transaction authentication (Article 72) • unique identifier (Article 4 (33)) RTS SCA: • Authentication code (Article 4) • Way of addressing the requirements of dynamic linking (Article 5) • Trusted beneficiaries •Session identifier (Article 29, (2)(a),	yes	
69	It should be clarified that the ASPSP is obliged to present to the PSU the information send in scope and in scope_details	Article 97 of PSD2, in particular: 'payment service providers apply strong customer authentication that includes elements which dynamically link the transaction to a specific amount and a specific payee.' And Article 64 (3) 'Consent to execute a payment transaction or a series of payment transactions shall be given in the form agreed between the payer and the payment service provider.	no	

70	Besides scope, the TPP should also be provided the scope_details parameter, because it is in the scope_details parameter where the information about the account number the PSU agreed to debit can be given	Proposed phrasing: 'Together with the access token, also the scope parameter (the same as in the request or limited by the user during the authorisation) and the scope_details parameter supplemented by the information provided by the user are transferred to the TPP .	no	A new process was proposed.
71	How is the TPP supposed to send the form from item 2? As part of the request under OAuth or as part of the /payments/v1.0/* service calling?	The provision of the information should take place as part of the OAuth token request. it is the duty of the ASPSP to display the information as part of the PSU's consent granting.	yes	
72	The consent to effect the AIS service should be displayed by the APSPS and not by the TPP	See comment 69.	no	A new process was proposed.
73	If the consent revocation should be available via the TPP's interface, the PolishAPI should define a method for the consent revocation	Adding a token invalidating description – revoke – pursuant to the OAuth 2.0 standard.	no	A new process was proposed.
74	The 'consent granting' definition is not complaint with Article 64 of PSD2 and the technical assumptions of the Polish API (chapter 5.1, l.p. 3)	See comment 69. Proposal: 'Granting Consent – a process in result of which the PSU grants ASPSP consent to access his/her account held by the ASPSP in order to effect a service, including the AIS, PIS and COF services.'	no	A new process was proposed.
75	For payment services, there is no possibility to give a callback with a payment status update – a response under /payments/* may be submitted or pending, and, currently, the TPP mus make active requests for later statuses. Instead, we propose that the ASPSP, if	Proposed phrasing: 'The ASPSP will inform the TPP, if the latter requested so, immediately after the transaction status change by means of'	yes	

	so requested by the TPP, provided information about transaction status changes			
76	It is necessary to add a diagram of transactions statuses	Without information what statuses a transaction may have and which statuses are terminal, the TPP has no possibility to conclude when a given transaction can be assumed as accepted for effecting and when it can, for example, start performing a service or send goods.	yes	
77	'The ASPSP provides a possibility to authorise a transaction ordered by the PSU under a PIS service provided by the TPP' The PIS service is not provided by the TPP	Proposed phrasing: 'The ASPSP provides a possibility to authorise a transaction ordered by the PSU under a PIS service provided by the TPP'	yes	
78	Is the PIS service used to authorise the transaction or to effect it? The consent acquisition and the authentication token takes place via the flow Oauth	The ASPSP uses the OAuth 2.0 protocol in accordance with Chapter 7 to authorise the transaction ordered by the PSU via the TPP using the PIS service, irrespective of the authorization method and its complexity. The authorisation method is selected by the ASPSP.	no	The PIS service is used to initiate the payment.
79	A use of sequence diagrams and indication of specific API methods to be used would significantly facilitate the TPP to understand the standard, preferably with examples of messages to be exchanged between the TPP and the ASPSP		yes	
80	No chapter describing the authentication of the ASPSP		no	The mutual identification of the TPP and the ASPSP takes place on the basis of eIDAS certificates in accordance with the draft ETSI TS 119 495
81	The schema for scope_details should be documented, e.g. in the form of a json schema		yes	

82	Non-compliance of examples with the type descriptions in Chapter 5.13 - no type for duration - incoherent specification of duration (one time in minutes, one time in days) -e.g. maxAllowedHistoryLong vs scopeTimeDuration - the amount given is inconsistent with the type definition (PIS, amount.value) - some examples are not correct JSONs		yes	
83	The scope_details definition should be separated for requests from the TPP to ASPSP – where the fields are provided (e.g. information about amounts in case of PIS) and for what should be expected by the TPP in response (e.g. the selected account number etc.)		no	A new process was proposed. The scope_details definition has been added
84	No multiple PIS debiting supported	Add a subchapter in Chapter 1 where all the PolishAPI limitations with respect to PSD2 / RTS SCA would be listed. Chapter 1.3 suggests that the PolishAPI describes all the services required by PSD2. Article 64 (2) mentions multiple payments	no	In our opinion, this is not the Compliance area.
85	Getting an access token on the basis of the refresh token may take place in case of a multiple PIS	Such a situation will take place in case of a multiple AIS service, a multiple PIS service and a COF service.	no	Multiple PIS is beyond the scope of the Compliance services.

86	Because the communication is synchronous, then in this case one should probably speak of a TIMEOUT type situation. The ASPSP has no possibility to renew the message – no defined address to which such a message would be sent	Instead of 'Communication with the TPP impossible' – 'Request sent to the ASPSP and the ASPSP failed to respond' Instead of 'TPP renews its message x3' In 3.2.3.1, it is necessary to define a field identifying the transaction and to impose an obligation on the ASPSP that transactions ordered by the TPP on a multiple basis but with the same identifier should be effected only once	yes	
87	No defined message renewal and responsibility of the ASPSP and the TPP and no minimal TIMEOUT value the TPP should set The ASPSP should verify whether or not it receives a transaction with the same tppTransactionId for the given TPP. In case when tppTransactionId is repeated, a new response should be generated and information about the transaction that has already been registered should be returned – on condition that the OAuth token allows access to the given transaction. In this case, a dedicated http status should be set (e.g. 208 Already reported?). In case when tppTransactionId is repeated but the OAuth token does not allow access to the original transaction, a dedicated http status should be returned (maybe 409 Conflict?)		yes	
88	No defined interface for the provision of information about the order performance changes	See comment 74. – to be supplemented	yes	

89	The ‘Model dziedziny KMD – ModelKMD.xlsx’ Annex has not been made available for consultation		n/a	The content of the annex was included in the main document.
90	The consents granted by more than one user (e.g. business accounts) could be supported by the issue of an OAuth token, which does not authorise the transaction yet. The ASPSP or the PSU would be burdened with the provision of information to another user, who is authorised to confirm the transaction and would do so in the ASPSP’s system. Only after this operation would the token issued to the TPP authorise the performance of the operation proper (PIS, AIS, COF). It would be necessary to insert an additional endpoint, where the TPP would specify a callback address which would be called when the token status has changed (the second user confirms the access or rejects it)		no	To be allowed for in subsequent versions of the standard
91	There is no information about the way in which the TPP is authenticated in case of communication initiated by the ASPSP towards the TPP. Should there be a verification of the TPP’s certificate (e.g. whether or not it belongs to the TPP) and should the ASPSP present itself by the X.509 client certificate. And if so, (in case of AIS, the information thus provided is covered by the banking secrecy clause), which certificate/key should be used and how will the TPP obtain the information 6.1 TPP’s Authentication For services where the callback address is given, also the thumbnail of the certificate to be had by the address given when the ASPSP starts the connection is quoted besides the TPP’s address. In PolishAPI, it is necessary to add a service which confirms whether the certificate is the certificate used by the ASPSP when initiating the callbacks		yes	

92	The UserInfo class has not been defined in the yaml files	Does it concern the RequestHeader class?	yes	
93	Besides verifying the certificate, the ASPSP should verify that RequestHeader.tppID is complaint with what was determined on the basis of the certificate	If the fraud verifications are made on the basis of date in RequestHeader, and not data determined on the basis of a certificate – it should be ensured that there is a consistency between what was determined on the basis of the certificate and the tppID given	yes	
94	No description of the meaning for account/auxData		yes	
95	Writing addresses as a list of strings ensures a considerable flexibility for the TPP. There should be a description of the way this field should be completed, i.e. which information should be inserted in which line		no	The standard should not define the way of description of a transfer used by banks. ASPSPs are obliged to return data which they present in the WWW service.This is the Elixir system format. This field specifies what the client inserted when ordering the transfer. The ASPSP does not have any possibility of providing such data in any structure whatsoever.
96	requestHeader/tppID – how should the TPP determine the value of this field?	Field deletion, using only the information about the TPP resulting from the X.509 certificate. At the same time, determination of requirements concerning the certificate so that it contained information about the TPP's identifier (e.g. EUNIP)	yes	
97	Change of the status description 'Not found authorization header'	Proposed phrasing: 'Authorization header not found'	yes	
98	Clarification of the entry on what the method does	Proposed phrasing of the operation description: 'Get information about all user's payment accounts'	yes	

99	Change of the status description: 'Request limit for the requested service has exceeded'	Proposed phrasing: 'Request limit for the requested service exceeded'	yes	
100	The transactionIdFrom field assumes that the transaction identifiers are strictly increasingly monotone. The assumption that the ASPSP makes available an identifier meeting this condition is missing from the business part		no	The transactionIdFrom field does not assume that the identifiers are monotone - identifiers are not numbers and cannot be treated as such. The field allows the transaction scope to be narrowed down, indicating a point within the understanding of chronology as an alternative for timestamps.
101	The add prefix is not necessary in operation names	Should be: • expressDomestic • standardDomestic • standardEEA • standardNonEEA • Tax Pursuant to operation addresses	yes	
102	How should the TPP know the residence status? Whose residence status is it? Payee's? Sender's (it is probably known to the ASPSP)? What are the admissible values?		no	This is a scope of fields completed by the PSU.
103	PayerInfo instead of PayorInfo		yes	
104	No possibility to quote the debiting date	In Chapter 7.1.1, scope_details allow the specification of the transaction date, similarly as is mentioned in Article 80 (3) of PSD2. This information should also be added to the interface	no	The Compliance scope comprises transfers with the current date.

105	A possibility of a multiple PIS transaction ordering by the TPP despite a one-time consent for debiting. Currently, the ASPSP must implement a verification whether the transaction was effected on the basis of an AuthenticationToken issued (which, nevertheless, may be exchanged into another one – using the refreshToken).	We propose to ass a tppTransactionId field to scope_details. In consequence, the OAuth token will allow only such transactions that have a defined tppTransactionId. On the ASPSP's side, the verification whether the authorisations granted have already been exercised will be made on the basis of tppTransactionId. Such an approach will result in the fact that tppTransactionId will be used on a multiple basis in case of a multiple PIS. Depending on the approach to the timeout support (comments 19, 20) – there may be a necessity to define another field (e.g. accessGrantId), which should be sent by the TPP at each request)	no	In our opinion, this is not the Compliance area.
106	Our doubt concerns the payment performance, i.e. the PISP performance by the PTT. Will we receive, in response to PTT with regard to the performance of PISP, information about a correct transfer initiation or also about its actual performance, i.e. that the funds actually left the account and were received by the payee. It is not currently clearly defined in the API documentation. In 3.2.2, there is a statement that PIS will inform the PTT about the acceptance or rejection of the order - which may mean that it is a separate communication and not only a transfer order. In 3.2.4, there is information that the diagram in 4.2 presents a PIS message. Consequently, in 4.2 there is a description of communication (a diagram) which suggests that this is a request for an account history. Is it by any chance the AISP and not PISP? This entails that the PTT needs both the PISP and the AISP to fully support it.	Clear indication which methods in API are responsible for the provision of this information and to which actors they will be assigned to.	yes	

107	With regard to the Authentication mechanisms – as a process in result of which the ASPSP verifies the PSU's identity pursuant to 1.4.5.1. (p. 11).	Firstly, one should pay attention to the following provision of PSD2: • Article 1 (36) (a) ‘Consent to execute a payment transaction may also be given via the payee, payee’s provider or the payment initiation service provider.’ whereby pursuant to Article 40 (1) of the Payment Services Act ‘A payment transaction is deemed authorised if the payer has granted a consent for the execution of the payment transaction in the way as stipulated in the agreement between the payer and its provider. The consent may also concern subsequent payment transactions.’ - now, therefore, the Legislator equates the transaction authorisation term with the grant of consent for its execution and the grant of consent may take place via the TPP (PISP). • Article 1 (41) (b) (1a) ‘If the payment transaction is initiated through a payment initiation service provider, the burden shall be on the payment initiation service provider to prove that within its sphere of competence, the payment transaction was authenticated, accurately recorded in the system used to support the provider's payment transactions and not affected by a technical breakdown or other deficiency linked to the payment service of which it is in charge.” • Article 1 (42) (b) ‘1b. If the payment initiation service provider is responsible for the execution of an unauthorised payment transaction, at the request of the account servicing provider, immediately and not later than until the end of the next working day following the day when the given transaction was identified or a request was received, shall compensate to him/her the losses suffered or shall	no	Incomprehensible comment.

		reimburse the amounts paid in result of the return made on behalf of the payer, including the amount of the unauthorized payment transaction. The provision of Article 45 (1a) is applied. • Article 1 (47) (a) ‘2. Where the payment transaction is initiated by a payment initiation service provider or by or through the payee, the payer shall not revoke the payment order after giving consent to the payment initiation service provider to initiate the payment transaction or after giving consent to execute the payment transaction to the payee.’ - thus, the Legislator does not provide for a possibility that the transaction is not executed in terms the consent is granted (authorisation within the understanding of Article 40) to the TPP (PISP) • Article 1 (52) ‘3. The payment initiation service provider shall: 2) ensure that the personalised security credentials of the payment service user are not, with the exception of the user and the issuer of the personalised security credentials, accessible to other parties and that they are transmitted by the payment initiation service provider through safe and efficient channels;’ Article 1 (52) ‘4. The account servicing provider: 2) immediately after receipt of the payment order from the payment initiation service provider provides or makes available to that provider the information about the payment transaction initiation and the information about the payment transaction execution available to it; In relation with the foregoing, there are doubts whether the terms ‘authorisation’ ‘authentication’ and ‘consent granting’ are only three separate processes within the Polish API specification? Does		

		the authorization comprise both the consent grant6ing and authentication? How are these terms related to the statutory terms of authorisation (Article 40 of the Payment Services Act) and the liability principles? What is the moment the declaration of will within the understanding of Art. 60 of the Civil Code is made with regard to the granting of consent for the execution of a payment transaction in the light of provision 1.4.5.2. 1) i 5) and 3.2.5 of the Polish API specification. Pursuant to 1.4.5.2.5) of the specification, the PSU authorises the transaction in the ASPSP’s interface which, in the light of the regulations quoted, seems contrary to Article 40 of the Payment Services Act in its phrasing after amendment in accordance with the draft PSD2 ACT read in conjunction with Article 1 (47) (a) of the PSD2 ACT. Authorisation is a statutory term from Article 40 (this definition is, without limitation, of significance due to the fact that the liabilities of parties is made dependent on the transaction authorisation made – in particular, Article 46 in the context of the amendment to the PSD2 ACT and the liability of the PISP) and is to constitute a final confirmation of the obligation to effect the payment transaction initiated due to the fact that there is no possibility for the PSU to revoke it after the consent (authorisation) has been granted to the payment initiation service provider (PISP). Moreover, as part of its duties, the ASPSP is obliged, immediately after reception of the authorisation in the form of a payment order from the payment initiation service provider to transfer or to make available to the provider the information about the payment transaction initiation - and this		

		has not been made by the Legislator dependent on any further conditions. Consequently, the authentication process within the understanding of 1.4.5.1. of the Polish API specification should take place before the PSU is enabled to grant consent to the TPP (PISP) for the payment transaction initiation in the TPP's (PISP's) interface. This opinion is also confirmed by the scope of statutory liability of the TPP (PISP) in the form of the burden of proof of correct authorisation and the obligations to redress damage or reimburse funds in case of liability for an unauthorized transaction. The opposite way of reasoning expressed in the Polish API specification seems then a logical error (vicious circle), where first consent is granted to the TPP (PISP) within the understanding of Art. 40 of the Act and then there is authentication and further authorisation within the understanding of the Polish API specification but this time with respect to the ASPSP, whereby it is impossible for the PSU to revoke this order already at the first stage, irrespective of the efficiency of authorisation with regard to the ASPSP in accordance with 1.4.5.2.5). What is more, the process adopted in 1.4.5.2. of the Polish API specification seems to result in the fact that the provisions of Article 1 (42) (b) of the PSD2 ACT will be a dead letter because in item 1.4.5.2.5) the liability of the TPP (PISP) is excluded because the authorisation is to take place with regard to the ASPSP and in its interface. Consequently, the process in item 1.4.5.2.5) should be deleted in the light of the consent granted (authorisation) in item 1.4.5.2.1) and authentication in 1.4.5.2.3). Additionally, one should consider whether the		

		authentication process,, from the standpoint of usefulness of the PIS and AIS services, should be tantamount to the process of logging into the TPP’s (PISP’s, AISP’s), interface pursuant to the provisions of 1.4.4.2.1 b) of the Polish API specification and should not take place in the ASPSP’s interface, since the legally binding consent (authorisation within the understanding of Art. 40) will be granted in the TPP’s interface. After all, the Directive of the European Parliament and of the Council (EU) 2015/2366 of 25 November 2015 w on payment services in the internal market, amending Directives 2002/65/EC, 2009/110/EC and 2013/36/EU and Regulation (EU) No 1093/2010, and repealing Directive 2007/64/EC, in the preamble in item 32 stipulates that ‘Payment initiation services are based on direct or indirect access for the payment initiation service provider to the payer’s account. An account servicing payment service provider which provides a mechanism for indirect access should also allow direct access for the payment initiation service providers.’ It is proposed to eliminate the amendment 3.2.5 by changing the term authorisation into the term authentication. It is proposed to delete 1.4.4.1 and 1.4.4.2.1 a), leaving the authentication tool in the TPP's (PISP’s) interface, which seems to be consistent with the phrasing of the draft PSD2 ACT, provisions of the Civil Code (moment when the declaration of will is made) and intention of the Legislator to eliminate ‘unnecessary barriers to the development of the fintech market.’		

108	Re.: the list of payment accounts	The following phrasing is proposed: 1.4.5.2.4) In case there is no indication in the transfer initiation form of the transfer sender's bank account, the ASPSP presents to the PSU a list of payment accounts from which it is possible to initiate a payment transaction to select from. The PSU selects one account from the list. The above provision remains coherent with the assumptions of the Polish API specification 3.2.3. Comments to the Account Number fields	no	A new process was proposed.
109	Re.: Scope of information (Compliance)	Does the scope of history comprise holds/seizures at the payment accounts occurring in accordance with the law (blocks, seizures by ZUS, IRS, tax authorities, court bailiff etc.), and not with the payment instrument transactions? In case the above information is not covered by the scope indicated in item 3.1.3., it is proposed to add the said information to the scope in item 3.1.3 in accordance with the argumentation indicated in the item above, because it comprises the PSU’s financial situation in the wide sense and, as such, should, in the Legislator’s assessment, constitute an element of the account information service (AIS) and should be obtainable via the TPP (AISP).	yes	The specification will present all the holds and blocks, not only those resulting from payment instrument transactions

110	Re.: conditions of a payment that can be initiated only by the TPP – a single transfer	It is proposed that this condition be deleted in order to facilitate the introduction of a batch of transfers which will still be authorised by the PSU, or, alternatively, The following phrasing is proposed: 3.2.1.b) a single transfer, unless something else results from the framework agreement; or, alternatively, The following phrasing is proposed: 3.2.1.b) a single transfer in case of external transfers for payment accounts of a single PSU - lack of this requirement/limitation for the payment accounts of a single PSU, which would make it possible to introduce a batch of transfers within the framework of the payment accounts at the disposal of a single PSU. Pursuant to Art. 40 (1) of the Payment Services Act 'A payment transaction is deemed authorised if the payer has granted consent for the performance of the payment transaction in the manner as stipulated in the agreement between the payer and its provider. The consent may also concern subsequent payment transactions.' Making this provision more detailed pursuant to the PSD2 ACT allows the consent granting to the TPP (PISP) and should comprise subsequent payment transactions, which should be identified with payment orders as well as other long-term contractual relations in which a higher number of payment transactions is effected on the basis of a single consent from the payer. It should be recognised that the consent may concern both a defined number of transactions, their amount (also total amount), as well as a definite period of time	no	In our opinion, this is not the Compliance area.

		during which the given transactions may be executed from time to time in the future. In consequence, the consent revocation may concern single payment transactions from a series of payment transactions covered by the consent or all future payment transactions (cf. comment in item 6) covered by the previously granted consent. Such consent may also be modified with regard to certain elements, such as the time of the transaction execution or the maximum amount. Consent revocation concerns only transactions not done and does not result that the transactions already done become unauthorized. In the light of the foregoing, it should be remembered that the Legislator's intention is to eliminate 'unnecessary barriers to the development of the fintech market', and any limitation of payment initiation by the PSU via the TPP (PISP) to single and current payment, omitting subsequent payment transactions, does not seem valid. Elimination of this provision will also be consistent with the overall objective of the Legislator, i.e. the elimination of 'unnecessary barriers to the development of the fintech market'.		

111	Re.: conditions of a payment that can be initiated only by the TPP – a transfer with the current date	It is proposed that this condition be deleted or that provision be made 3.2.1.c) dated transfer, in order to facilitate the introduction of transfers with a future date, which will still be authorised by the PSU, or, alternatively, The following phrasing is proposed: 3.2.1.c) a transfer with the current date, unless something else results from the framework agreement; or, alternatively, The following phrasing is proposed: 3.2.1.c) a transfer with the current date in case of external transfers for payment accounts of a single PSU - Justification as in the item above.	no	In our opinion, this is not the Compliance area.
112	Re. the possibilities to flag a hold on funds at the account in case of a transaction with a future date	In case of a possibility to order transactions with a future date, one should consider the introduction of an optional field 'Funds hold flag'.	no	In our opinion, this is not the Compliance area.
113	Comment to the response_type parameter is incomprehensible: Wartone 'code'	In accordance with RFC 6749 4.1.1. Is: Wartone "code" Should be: 'Code' value	yes	
114	Typo in the phrase 'The scopes parameter defines …". There is no scopes parameter.	Is: scopes Should be: scope	yes	

115	Concerns the sample scope_details structure for multiple AIS services, which allows a 90 day access to the transaction history and details of transactions for the last 4 months (counted from the moment the client granted the consent) Questions: a) Do the 4 months counted from the moment the consent was given mean that on day 90 from consent granting the TPP will be able to retrieve the history of accounts indicated for the period of the last ~7 months? The values notBefore and notAfter added by the ASPSP, as is described on p. 40, indicate that the TPP will rather not have access to operations that appeared at the PSU's account history already after the consent to access the operation history was granted but please provide a confirmation that the period of 4 months of the account history scope apply throughout the consent duration and do not extend the TPP's access to the current history of the PSU's account. b) Is the empty creditCardAccount table of no significance here and the consent will concern only the payment account PL4536334634523423424332, or does it indicate a necessity to present, at the consent form in the ASPSP's system the possibility to select credit card accounts the consent will concern? The provision stating 'if the TPP does not know the account number, it may define the account type only' raises doubts.		no	The history will be made available for the period as defined in the consent.

116	At the list of access scopes on pages 36-37 there is no ais:transactionDoneDetails which is visible in the sample scopeDetails structure for a multiple AIS. Similarly, in the next example for a one-time AIS and in the example on page 40.	Is: ais:transactionDoneDetails Should be: ais:transationDetail	yes	
117	At the list of access scopes on pages 36-37 there is no ais:transactionDone which is visible in the sample scopeDetails structure for a multiple AIS. Similarly, in the next example for a one-time AIS and in the example on page 40.	Is ais:transactionDone Should be: ais:transactionsDone	no	scope_details was added again in a separate swagger file
118	Re.: sample scope_details structure for a single AIS. Question: Does the ais:accounts right concern the possibility for the TPP to retrieve a list of all accounts of the PSU, irrespective of the fact that the resource parameter in this request defines only one specific payment account PL4536334634523423424332?		no	scope_details was added again in a separate swagger file

119	Re.: sample structure of scope_details for a single PIS – consent for a domestic transfer/ Questions: a) Does sending by the TPP a request defining the PSU’s consent for a single performance of a transfer of PLN 454.34 to the payee’s account defined in the scopeGroup element without a simultaneous specification of an account or a list of accounts of the PSU from which such a transfer may be executed, mean that the PSU must openly indicate in the ASPSP’s system at least one account the consent will concern? The example on page 41 describes an account selected by the client (PSU), which would indicate the existence of such a requirement, but please confirm additionally. b) Does the token returned to the TPP by the ASPSP and generated on the basis of the PSU’s consent order always have to refer to a specific account/list of accounts? c) Is there any type of consent which would entitle the TPP to order a payment using a service, e.g. addStandardDomestic without a necessity for the PSU to authorise the payment? Does the authorization of consent for such a payment simultaneously authorise the same payment effected by the TPP without any interaction with the PSU after calling one of the PIS services?		no	scope_details was added again in a separate swagger file

120	In the sample scope_details structure for a single PIS – consent for a domestic transfer, the value of the scopeGroupType field is pisInformationService. If this should mean the PIS service, then the value should rather be paymentInitiationService. Similar error on page 41. In the same structure, no value of the paymentAccount field was given and the value of the privilegeList field was formatted incorrectly, therefore JSON is incorrect.	Is: pisInformationService Should be: paymentInitiationService	no	scope_details was added again in a separate swagger file
121	For consistency in the tables concerning request parameters, the names of the Code and Scope parameters should be all written in lowercase letters. Additionally, the information if the scope and scope_details parameters are required concerns item 8.1.1, and should concern 7.1.1.	Is: Code, Scope, 8.1.1 Should be: code, scope, 7.1.1	no	scope_details was added again in a separate swagger file
122	Why are the is_user_session, user_ip and user_agent parameters defined only for the access token validity refresh request? Should all requests executed by the TPP using the newly received token for which is_user_session = true has been specified be treated throughout the token validity as requests related to the interaction with the PSU (in order to ensure control over the API function availability limit)?		no	scope_details was added again in a separate swagger file
123	What is the relationship between the information included in this item and the procedure of new access token getting on the basis of a refresh token as described in item 7.1.5. Access token taking on the basis of the refresh token? In our opinion, in accordance with RFC 6749 (6. Refreshing an Access Token) the refresh token should be used by the TPP until the access token validity is refreshed after the expiry and not sent with each API function calling, a		no	scope_details was added again in a separate swagger file

	function using the access token allowing a multiple access action.			
124	Item 6 of the diagram of activities in the PIS service mentions a transfer of information to the TPP by the ASPSP about changes in the order execution status changes upon each instance. How is the ASPSP supposed to inform it about changes in statuses of the TPP's payment order, if no callback mechanisms are used in this process and no service on the TPP's side was described which would allow such a mutual interaction?		yes	A callback method for the provision of payment status information (PIS) was added.
125	Redundant word 'activities' in the first line.	Is: activities Should be: <<remove>>	yes	
126	On page https://polishapi.org, Annex No. 5 KMD Model (ModelKMD.xlsx) was not published		n/a	The content of the annex was included in the main document.
127	No complete specification of the scopeGroup type object (JSON Schema) was provided. Please advise if such a specification will be available after the termination of work on the basic PolishAPI standard version.		yes	scope_details was added again in a separate swagger file

128	The idea of paging mechanism using the pageId and perPage fields of the getAccountsRequest parameter is not entirely comprehensible. How is pageId described as ‘account number starting the page’ supposed to be used as an identifier of the next page with results? When retrieving the first page containing n accounts, we do not know what the account number starting page 2 is and, generally, how many pages of a defined size the list of client accounts not subject to any filtering comprises. such information is not returned by the response object defined for this method. For the AIS methods used to retrieve a list of blocks/holds or transactions, in the response object there is the pageInfo field which provides such information.		yes	
129	Transaction details are retrieved using, without limitation, the transactionID field. We assume that this is a unique transaction identifier in the ASPSP’s system. Questions: a) In the return object, we have a defined zusInfo field. In the light of changes that are effective from 01.01.2018 with regard to the liquidation of the ZUS transfer type, is this field still justified? b) In the return object, we have a defined tppTransactionIdID field and a defined tppName field. It is suggested that the name of the tppTransactionIdID field be changed to tppTransactionID. Should this field be completed for all transactions ordered via the TPP, where the TPP provides this value to the ASPSPS in PIS method calls. What about the tppName field in this case? What should the ASPSPS return in this field?		no	In the account history, there currently may be ZUS transfer transactions according to old principles. Fields related to the information about the TPP are to be returned for all transactions ordered via the TPP, provided the ASPSP has such data.

130	All PIS methods return the required detailedStatus field. What value should this field have? Is it simply a description of the meaning of the status provided in the generalStatus field from among the values in the dictionary?		no	Yes
131	Consent revocation by the PSU. In the document there is a statement that the way in which such a functionality should be ensured is beyond the scope of the Polish API Standard. Pursuant to the new scope, the TPP is responsible for the consent process - Does it mean that the TPP must agree/confirm with the ASPSP what such a process should look like? In our opinion, the process should be standardised.		no	The specification describes new processes related to AIS consent granting, edition and revocation.
132	Basic data formats: Amounts	Is: Saved as a number with 0 or 2 places after the decimal place (a dot) [...]. Should be: Written as digits with 0 or with a sign separating the integer part from the fractional part up to the second decimal place (the dot sign) [...].	yes	

133	In the above-mentioned item, there is a statement: As part of the PIS service within the Compliance Scope, the ASPSP will make available to the PSU, via the TPP (PISP), an initiation of payments that meet the following cumulative conditions: […] c) The payment is a transfer with the current date, […] If the transfer order made by the PSU is after the COT (Cut Off Time) for the given transfer type, then in the transactional system, that order will not be executed with the current date – the system should effect the transfer on the next working day. In the above-mentioned case, the order will await execution.		no	A field (optional) was added to allow the provision of information about an intention to hold the funds in relation with the payment initiation, e.g. on a day off-work.
134	It is necessary to publish a detailed process of PSU’s consent granting for the TPP to effect the COF service.		no	This process will be taken into consideration in the subsequent version of the standard.

135	in the data model, there is no information about the cost option concerning the foreign transfers (the addStandardNonEEA service, the transferCharges fee)	In the field concerning foreign transfer order fees (the addStandardNonEEA service, the transferCharges field), there should be one of the following values: • cost sharing, • charge beneficiary, • charge sender Justification: The Client should select this option when ordering a foreign transfer so that the bank knew what cost instruction to apply to execute the transfer. The cost option in case of foreign transfers has a considerable impact on total costs of the transfer and in case countries and currencies from outside of the EEA, this matter is not regulated.	yes	
136	Firstly, I have a purely technical comment and I would appreciate if a correction was made in the list of participants of the working group: the F. Stefczyk Cooperative Savings and Credit Union and the National Savings and Credit Union – we are two entirely separate legal and organisational entities and I would be grateful if this small change was introduced.		yes	
137	I would also like to draw attention to the fact that the specificity of all SKOKs (Cooperative Savings and Credit Unions) as regards the participation in the Elixir system is considerably different from the situation of banks because SKOKs are not direct participants of the Elixir settlement system - the settlement takes place via the National Savings and Credit Union, which has in this regard a direct agreement with KIR. Hence, I wonder if this completely different situation would		no	Does not concern the Polish API specification.

	have any consequences for the Polish API platform, especially in the context of the PIS service?			
138	please include in the specification a change to item 3.2.1. consisting in the clarification and direct formulation in the specification that within the framework of the PIS service, the ASPSP make available only such types of transfers, that are offered to the PSU, the same thing concerns the payment accounts made available by the ASPSP to the TPP under the AIS service.		yes	
139	Non-repudiation of query requests may introduce significant scalability issues. To ensure non-repudiation, it is not only necessary to record unforgable signature of the request, but also make the request uniquely identifiable. Uniquness of the identification of the requests must be enforced, and the only way to do that is to track used IDs at a barrier aware of all IDs used.	Consider if non-repudiation of query requests is really required (and if it can be replaced by audit logging, without a proof of issuing). If not, introduce a specification of generating unique IDs, that can be verified for uniqueness without a database lookup performed at high transaction isolation level (ISO SERIALIZED would be required). A potential solution may be based on monotonicity (ordering of IDs) and verifying IDs used are “greater than last seen”. Coodination of the uniqueness check across API instances and/or API gateway instances (potentially in hudreds ...) remains an issue, and can be a limitation to scalability.	no	Implementation issue, in our opinion, this may not be solved at the standard level.

140	Selected way of enforcing non-repudiation prevents RESTful Maturity Level 1 (or higher) API	Giving up adressability of resources, as well as semantic value of HTTP method may have negative impact on ability to generate standard clients of the API, scaffolding, testing, and thus adoption. De-facto standards, including HATEOAS based dicoverability nad self-descriptivity is difficult to implement (not in a standard way). PolishAPI is likely to be the only non-RESTful API (in the sense of Richardson maturity model) in EU, and this can negatively impact the adoption, and surely will not be regarded highly in developers community.	no	Implementation issue, in our opinion, this may not be solved at the standard level.
141	The standard, despite giving up on Maturity level 1+ RESTful API ideas does not capitalize on this as an opportunity to create a transport agnostic API.	Putting aside the decision to give up RESTfulness of the API, if the standard depends on the request body, and response body, there is no barrier to add ALL necessary elements to the message transported in the body, including the operation semantics, signatures and all kind of meta-information. The standard should allow to create self-contained messages. This will allow to abstract the transport mechanism, and transport agnostic API is a significant value. In particular adaptation of the API for example to the email based transport would be a relatively easy task. It makes it also significantly easier to manage protocol messages, for example within message brokers, as the full context is the message itself. IFX (ifxforum.org) can be referenced for an example of a standard similar in purpose, implementing the idea of a transport agnostic protocol.	no	PolishAPI project group decision. This decision (to use more data transfered in the body of the request) was taken due to the security reasons.

142	Unnecessary asymmetries in the operations are cluttering the interface (e.g. AccountsRequest vs AccountInfoRequest, getPayment vs getMultiplePayments)	Remove duplicate, redundant variants. Variability of information scope should be handled within a single schema, with optional information potentially omitted. Selection of the resources to be included in response should be based on query criteria, and not on spacial case schema for “single entity” query. E.g. criteria can include specific ID of resource, thus rendering a single entity in the response. There should be no difference between the response containing a single entity, because it was named by ID, or the response containing a single entity, cause only the entity matches given criteria - effectively the criteria being a composite ID. Also It allows common code for handling all case, reduces the number of variants, thus equivalence classes for testing etc.	no	PolishAPI project group decision.

143	Selective (and thus potentially misleading) description of account parameters	There is no justification is arbitrarily selecting some account / product parameters (such as InterestRate) as obligatory, while leaving out others. On the example of the interest rate, the information provided is not enough to describe given feature of an account. For example a tiered rate scheme cannot be described by a single value. Thus either introduce a more complete decription, or make the given element optional and introduce a method of indicating that the description is not complete (and potentially a free-form method of specifying the missing bits). Please refer to UK Open Data API spec for example of specifying similar account parameters in a way designed for automated comparision (while still incomplete it goes much further, and will cover vast majority of needs): https://www.openbanking.org.uk/open-data-apis/ https://openbanking.atlassian.net/wiki/spaces/DZ/pages/13369388/PCA+API+Specification+-+v2.1.1	no	The problem will be addressed in the next version of the specification.

144	Transfer types dictionary is limited, and not open to extension. Schema supporting transfers is different per transfer type, and non-generic.	The proposed API recognizes closed list of transfer types: domestic, SEPA, non-domestic, non-SEPA. It is impossible to use such an approach to model for example a domestic transfer of another country (e.g. UK BACS or Faster Payment transfer in UK adressed to / from sort code and account number). The transfer type should be a dictionary value determining interpretation of other fields (possibly auxiliairy or otherwise open for extension). If augmented by a mean of generic (open) specification of source / target accounts (a generic identification scheme able to encode arbitrary types of IDs), majority of cases can be unified under a single schema, with IDs abstracting the schema different (e.g. using BIC as an element of target account ID, using a country code as part IBAN, as opposed for BBAN, differientiating domestin / foreign transfers etc.)	no	PolishAPI project group decision. In current version, documentation describes functionalities provided by Polish banks or banks operating on the Polish market.

145	Identification of the accounts is only done using IBANs. IBAN numbers while popular in Poland, and standardized in SEPA, are not the only common ways. The assumption of using the IBAN to denote source accounts is particularly likely to be an issue for some banks, who tend to use internal identification for the accounts when returning them (while Polish API forces them to use IBANs). In many countries IBANs are virtually unheard of from end customer perspective (the PSU), and never used by end customers, which would result with the need of TPP using some form of (not standarized in the PolishAPI, thus not available from the bank itself!) way of converting the IBANs and the IDs known to the customer. Adressing from/to payment intruments' accounts (e.g. credit cards, identified by PANs or platic card numbers, e-wallets, with their own identification schems, or crypto wallets) is a logical future use case – and shoudl be supported. The designation of target account should be also allowed to be something that there exist a way of transalting to a real account identifier, e.g. the telephone number or e-mail of recipient, or a single BLIK cheque number – transalted at later moment. Future scenarios, such as transfers to socil media accounts, postal adresses, hotel rooms etc. Shoudl be supported in unified way	Identification of accounts should be abstract, and self-descriptive. Any identifiable entity, including accounts, but also transactions, holds etc. Should allow for multiple alternative ways of identification (for exampel: by the external party, by the bank, by the bank in different systems etc.). Those Ids can coexist . UK Read/Write APIs, and STET, more or less loosely based on ISO 20022, recognize the "other" type of account identification, with a meta field being the name / id of the identification scheme to interpret given identifier within). To simplify typical use cases, default values shoudl be defined for meta-fields, so that they can be omited (so using just a account id field value would be interpreted as the most typical king of identifier – possibly IBAN). Intive, designing for identification (of any identifiable entity) used a concept of recursive identification with 3 meta fields being themselves identifiers, and an implicit identified object type (pseudo code below): class Identifier { identificationAuthority : Identifier // who issues the identifiers identificationScheme : Identifier // what kind of of scheme it is – could possibly be flattened with identificationAuthority using separate scheme names for different authorities format : Identifier // option designator of the strcuture of encoding the identifier if there are multiple ways, e.g. sort code and accoutn number can be two separate subfields of id, or a single string separated by some characted, like dash or space, sort code can be written with dashes, or without them	no	PolishAPI project group decision. To be considered during work on subsequent versions.

		etc. id : string[1..N] } Feel free to borrow the idea.		

146	getAccount / getAccounts return accountNumber as an unspecified identifier, while other APIs require IBANs as identification of source accounts(see addStandardDomestic, addExpressDomestic, addStandardEEA, ...)	Describe the linkage between the identifiers return, and those used when initiating payments. Ideally introduce metadata mechanism to anonate the type of identifier returned, and allow to use arbitrary type as identification scheme to be used. Allow returning alternate identifications, in particulat: internal bank id of the account, IBAN, possibly a GUID, for the same accounts. Allow for defining new types (e.g. customer ID and account alias?). Add support for other, logically usable in the scenario identifiers such as PAN numbers – again, ideally by introducing a meta information encoding the identification scheme to interpret given identifier within.	yes	
147	Introducing corner cases (such as transfer to tax authorities), specific to a country (PL) and applying them to the main standard part	Corner cases should be handled by extension mechanism (such as the auxiliary field map). For those of special importance (such as tax transfers) a supplementing specification freezing the semantics and encoding of values of specific meaning - dictionaries (such as term lenghts etc.) should be issued outside of the main standard. e.g. in PL specific supplement. Breaking the symmetry of the way special, local cases, are handled is not desirable, and may prevent adoption outside of PL.	no	PolishAPI project group decision. In current version, documentation describes functionalities provided by Polish banks or banks operating on the Polish market.

148	Using of unstructured address as the only way of denoting customer address.	Adresses in the bank systems are very often semantically described by their individual components. It remains an issue to unify all possble fields combinations used across geographies, so an abstract way of describing an address as several free form lines remain important, however it would be also useful to maintain the ability to describe also the strcutured from, with city, post code, flat number etc. ss separate, semantically tagged fields.	no	PolishAPI project group decision.
149	Lenght of identifiers of transactions, especially the externally assigned ones, may be limiting.	TppTransactionId and similar identifiers are 32 characters long, which may be limiting. While there shoud be a limit (to prevent buffer overlows etc.), this should be really high, probably closer to 500 characters than 30. It is difficult to make assumptions about external identification schemes, but transaction ids tend to encode a lot of information, plus randomness of desired entropy – so can be really long. 32 charactecters seems a bit short.	yes	

150	Closed number of roles in transactions	The API describes the sender and recipient, in separate set of fields, strcitly related to the account. It would be desirable to be able any number of parties, and their role (by a role identifier, with some values predefined, like "sender" and "recipient"). For example a merchnat is a party related to the transaction (with a role of "merchant"), as well as the processor, acquirer, possible even the bank clerk who handled the money or cheque. The API shoudl allow, even if not standardize, for an open list of relationships. Standardize just some – by definign the role id nad its meaning in the standard.	no	PolishAPI project group decision.
151	Lack of information of relationship of parties to account	Being able to retrieve the list of owners, co-owners, trusties, beneficiaries / minors, attorneys ... as well as trusted beneficiaries, seems desirable in many scenarios.	no	PolishAPI project group decision.
152	Requirement of ability of deining trusted beneficiaries (as requested by PSD2 and the RTS) is not present in the API	Introduce APIs for manipulating, and retrieving the list of trusted beneficiaries. Can be unified with an API of retrieving the relationships between account and parties, with trusted beneficiary being a specific subtype of relationship type.	no	In our opinion, this is not the Compliance area.

153	Limited, and closed way of categorisation, for accounts, transactions and other entities	Allow for open number of categories, denoted by a category identifier, and the category value identifier, in an array. Unify concepts such as type of account – e.g. deposit account, credit card, etc. to be just one of the categoroes. Product type is also potentially to be modelled that way ("Super saver account" in "ProductType" category). Possibly allow customer defined categories to be passed back in that way – e.g. tags assigned by the customer to an account or transaction.	no	The problem will be addressed in the next version of the specification.
154	Adding a custom field to the Oauth2 spec as mandatory may impact some client libraries	Please make sure there exist a way of creating a valid, basic authorisation request by using just the basci fields described by the standard. Otherwise some of client libraries may be difficult to use Possibly defined the standard value of custom fields: e.g. scope_details shoudl have default value to denote no extra scope limitations.	no	PolishAPI project group decision.
155	Custom way of encoding additional scope narrowing (scope_details field), could be potentially replaced by a more standard mechanism	The scope parameter value can itself encode limitations	no	PolishAPI project group decision.
156	Consider using OpenID Connect to implement binding of access token as well as ensuring the tokens and codes are genuine, especially using at_hash and c_hash	Additional security measure	no	PolishAPI project group decision. To be considered during work on subsequent versions.
157	Consider using Proof Key of Token Exchange as part of the standard	Additional security measure	no	PolishAPI project group decision.
158	Consider usign OpenID Connect as standard way of returnign information about customer	Future implementation of mutual trust exchange, e.g. KYC, account opening etc.	no	PolishAPI project group decision. To be considered during work on subsequent versions.

159	Partial consent from the customer is not properly signalled	The standard, and nature of the open banking, imply the customer may be given more than just a binary decision ability, e.g. might select the accounts to give access to, while the request may only use generic terms such as "access to credit card accounts". For many scenarios, such as accoutn aggregation, the fact of partial consent is not important for the TPP, while for other – e.g. credit scoring, partial knowledge may be a problem. TPP shoudl get an indication their request has been only partialy consented to, so that they can act (e.g. inform the customer they can only proceed having full required ifnroamtion) Contact Intive to discuss options of returning feedback of the decision of the customer back to the requestor, within Oauth2 standard amd without releasign information the TPP is not entitled to (proprietary knowledge being part of IP of Intive).	no	PolishAPI project group decision. To be considered during work on subsequent versions.
160	general comment to the specification: please supplement the document providing detailed sequence diagrams and activity diagrams for particular processes	High level diagrams give only a general overview of the process but do not allow a deep analysis of the entire communication between the actors	yes	

161	please explain / clarify whether or not the scheme presented concerns the initiation of the first XS2A session or each separate session. In the legend to the scheme, in item 3, there is a description of an activity 'PSU's authentication in the mechanism indicated by the TPP from among the mechanisms made available by the ASPSP", which in the case of a multiple AIS will not be required on each instance.		yes	
162	The phrase: 'Each transaction within the framework of the AIS, PIS and COF services should take place during a separate and dedicated XS2A session.' is incomprehensible in the context of the AIS service Please explain / clarify.		yes	
163	please make the description for step 3) PSU's authentication more consistent with the provisions concerning the XS2A session initiation scheme, in accordance with the intention of the working group		no	The provisions of this chapter were changed in whole.
164	we propose a change for the re-direction method the Polish API refers to at the moment, consisting in the change of sequence of items 4) and 5), which will result in the selection of accounts on the side of the ASPSP and not on the side of the TPP. For other methods, it will be required to develop a new consent granting process.		no	The provisions of this chapter were changed in whole.
165	if the above-mentioned comment is not taken into consideration and the process indicated sequence of items 4) and 5) remains unchanged - please clarify what the minimum scope of information it will be possible / necessary to transfer as part of the 'list of accounts'? Will this be only account numbers or also information allowing the identification of the client, e.g. account name, type (credit card, current account, savings account) or a segment (consumer accounts,		no	The provisions of this chapter were changed in whole.

	SME accounts)? Should the list of accounts be sorted / grouped in any way?			
166	the process of the PSU's consent granting with regard to the AIS service ends on step 6) 'PSU indicates the accounts'. • Will the ASPSP receive a return information what accounts were selected by the Client under the consent? • When will the Access Token for the TPP be transferred in this process (optionally also the Refresh Token)? – after the PSU's re-authentication or after the selection of specific accounts? Please supplement the process, including these steps.		no	The provisions of this chapter were changed in whole.
167	please change the description of the payment account with regard to which the AIS service may be effected. Pursuant to the Directive and the RTS, there are two conditions: it must be a payment account (within the understanding of the Directive) and it must be available online for the PSU. The additional conditions indicated, i.e. the possibility for them to be both debited and credited, are incomprehensible.		yes	
168	please supplement the first sentence, including the phrase 'and information about the payment account'		yes	
169	please explain why the scope of information concerns only holds/blocks related to payment instruments?		yes	

	Will it be possible to present other holds/blocks visible in the history in the online channel?			
170	please rearrange the table with fields so that the fields were arranged by type, e.g. please add in table 3 the following sections: 1. information about the PSU 2. information about payment account 3. information about the transaction history and assign there particular fields; additionally, please include in the table additional fields auxData, as mentioned on page 19 • Also please insert standardised comments, best reflecting the general description of what the given field contains, who/ what order it concerns. Please note that not all fields concern ‘ each transaction in the account history’, e.g. the FX rate field. • Please supplement the field table, including all the fields that were added to the Swagger, e.g. Transaction date, currency, etc. – the specification should correspond to the annexes • Please merge in the table the fields Name and address of the payer / payee – Name and address will be provided in one field • The field Given names and surname / Name of PSU – to be verified, whether actually in case of a legal person the name will be given here. It seems that also in the case of business operators, a natural person will appear as the PSU (actual user). It seems that the business name in this case seems secondary. Of key importance is the PSU’s authorisation to the accounts of the business operator. • Payment instrument number – please clarify		yes	

	whether it concerns the masking out of the payment instrument number (e.g. by inserting 'x's)			
171	Request to add a new field in the category ;Information about the payment account' called: 'Payment account restrictions'.	There should be some information whether the given account has some restrictions, e.g. no possibility of crediting, not possibility of debiting, etc.	no	Each ASPSP may add additional fields to the scope of data concerning the account and transactions made available.
172	Please add the 'MCC' field for the 'card' transactions.	This field will allow the provision of this data to the ASPSPs which present it to the client online.	yes	
173	We propose that the 'client type' field be added with a dictionary, e.g.:	It is a field necessary to distinguish the account type for its correct presentation.	no	Each ASPSP may add additional fields to the scope of data

	• consumer • business operator (legal form)			concerning the account and transactions made available.
174	We propose to add new fields in the Information about the account category, i.e.: • card status (with a dictionary) • card account number • user information (name and surname) • main card number (n fields) • auxiliary card number (n fields) • card expiry date • current settlement cycle (date from-to) • total amount and repayment currency • minimum amount and repayment currency • interest rate • card repayment date (date) • limit used (amount and currency) • limit granted (amount and currency) • past due repayment amount from the previous settlement cycle (amount and currency)	These fields will allow us (as ASPSPs) to transfer the data about all payment accounts, in particular information about the credit card, pursuant to Art. 36 (1) (a) of RTS.	no	The data range and the information if required may vary between different implementations. Fields become mandatory for ASPSPs in relation to the scope of information about payment accounts and transactions the given ASPSP makes available in its online interface, save exceptions stipulated in the law (e.g. with regard to particularly protected data concerning payments or personal data). Each ASPSP may add additional fields to the scope of data concerning the account and transactions made available.
175	We propose to add new fields in the Information about the account category, i.e.: • balance of new funds • balance of your funds as at day DD-MM-RRRR/Initial balance;	These fields will allow us (as ASPSPs) to transfer data which seem of significance from the point of view of the client for products for new funds.	no	Each ASPSP may add additional fields to the scope of data of data concerning the account and transactions
176	The field, which is called '**name and type of account (defined by the Bank)**' is called in the Swagger '**name of the type of account (defined by the Bank)**'.		yes	
177	the field which in the specification is called '**available funds'** is called in the Swagger '**available funds - after the transaction'.**		yes	

178	the field which in the specification is called **'book balance of the account'** is called in the Swagger **'book balance of the account - after the transaction'.**		yes	
179	the field which in the specification is called '**value date**' is called in the Swagger '**currency exchange rate date'**		yes	
180	the field which in the specification is called **'transaction id',** is called in the Swagger **'transaction identifier'.**		yes	
181	the field which in the specification is called '**transfer type**' is called in the Swagger '**transfer type'**		yes	
182	request to explain / clarify the phrasing in line 3 in the context of the AIS. At this moment, we interpret it as follows: after a positive consent granting procedure and the provision by the ASPSP of the Access Token, the information about selected accounts and history may not be provided immediately. Was this the intention of this provision?		no	The provisions of this chapter were changed.
183	please clarify the meaning of a pending payment transaction? Do they mean transactions which were ordered (have a transaction date) and await booking? E - no information about such a transaction in Chapter 3.1.3. p. 17 – in our opinion, it should be supplemented)		yes	
184	please clarify according to what date the records returned will be sorted (transaction date of booking date)? and will there be any possibility to add this information under the Polish API?		yes	
185	Please insert in the first line of the table, in the line Date, the data format compliant with ISO, i.e.: YYYY-MM-DD changed to YYYY-MM-DDThh:mm:ss.ccczzzzzz This data format has been included in the swagger.	It is necessary to the presentation of the transaction in the history maintaining the time line (chronologically) in the order as presented to the client in his/her electronic banking.	yes	

186	We propose that under the PIS service, the SHA cost option be assumed by default for SEPA transfers and for transfers other than SEPA after IBAN from EEA countries is selected		yes	
187	Please include in the specification the principles of servicing payment accounts used to support the split payments both in the context of payment aggregation (AIS) and payment initiation (PIS)	No information about this matter in the specification.	no	The problem will be addressed in the next version of the specification.
188	Please include in the specification the principles of servicing the multi-person payment authorisation under the payment initiation service (PIS)	There is no information in the specification in this regard, while a multi-person payment authorisation concerns a large number of business payment accounts.	no	The problem will be addressed in the next version of the specification.
189	The provision is expanded: ‘The TPP has a valid certificate.’	‘The TPP has a valid certificate which identifies it before the ASPSP.’	yes	
190	Correction of the phrasing: ‘The required way of granting authorisation to access resources is the application by the server in response to the user's request of one-time authorisation codes OAuth 2.0 before the target access token is granted.’	‘The required method of authorisation of access to the resource is the return by the server in response to the user's request of a one-time authorisation code, which shall be changed at the next step into a proper access token in accordance with the OAuth 2.0 protocol.’	yes	
191	The phrasing ‘request state’ in the following sentence is unclear: ‘The access token is transferred to the TPP together with information on the request state.’ Authorization Response in the oAuth 2.0 protocol does not contain any information about the request state, unless the author has in mind the ‘state’ parameter.	Please clarify what the term ‘request state’ means or delete this fragment.	yes	

192	Correction of the suggested approach: ‘The authorisation code may be implemented at the server's side in the form of a reference to the database maintained by the server (i.e. an identifier of an object stored at the server) or may contain all the information in itself.’ We suggest a provision that the code/token should be the indication of the object in the database, where the data of the object indicated are used to identify the client for the benefit of whom the operations are effected. We recommend the use of the so-called stateless token (e.g. JWT Token - RFC 7519) only in case when the disclosure of the ASPSP’s customer data (including the identifier) is compliant with the security policy	‘It is suggested that the authorisation code on the ASPSP's server side and the access token were the object identifier in the database, where the indicated object data will be used to identify the customer for whom the access token is generated or the operation is effected. The use of the so-called stateless token (e.g. JWT Token - RFC 7519) should be resorted to only in case when the disclosure of the ASPSP’s customer data (including the ID) is compliant with the security policy.’	yes	
193	Implementation of a mandatory authentication mechanism 1.4.4.1 or a successor 1.4.4.2.1, subsequent - to be deemed additional.	The introduction of oAuth 2.0 as an authentication mechanism is a very good practice and, therefore, it is suggested that under the PolishAPI the obligation of implementation of the mechanism from item 1.4.4.1 or of redirection to a mechanism compliant with z 1.4.4.1 under 1.4.4.2.1 be introduced. Any liberty in this regard may result in the fact that each ASPSP will require a different mechanism, which will be an obstacle in the standard implementation.	no	The ASPSP side authentication method is not the only one method allowed by standard, which is in line with the regulations.
194	Correction of the phrasing ‘in the interface made available by the ASPSP’. It should be clearly stated that the authentication process must be effected in the interface that was made available.	‘ The PSU authentication is made in the interface made available by the ASPSP or indicated by the ASPSP. It is inadmissible to provide the client's authentication data in an interface not related to the ASPSP.’	no	PolishAPI project group decision.

195	Clarification whether the 24 hour counter of requests resets together with a request initiated by the PSU.	Under the current phrasing, it is not clear whether the counter of the number of requests admissible per 24 hours will be reset together with a new request initiated by the PSU.	no	No, the counter of requests initiated by the TPP during the period of 24 hours does not reset after a request initiated by the PSU.
196	The list of fields in the Compliance scope contains the name of the TPP and the transaction initiator. Is it certain that such data should be provided to other TPPs?	The purpose of making the TPP's and transaction initiator's data available is unclear and may result in the breach of the banking secrecy clause between the bank and the TPP.	no	Incomprehensible comment.
197	Suggested change to 'The PSU will complete all the data required to …' The TPP is responsible for the provision of data in order to make the transfer order. However, the TPP must take care to ensure that the data originate in part from its own knowledge and in part also from the PSU.	'The TPP in cooperation with the PSU will provide all the data required to …'	no	
198	it is suggested to expand the description of the transfer order by including the fact of immutability of data provided under the transfer order.	The data given by the TPP in the transfer order should not be modified by the PSU in the ASPSP's domain. The only modification possibility could concern the selection of the account from which the transfer should be made. We recommend that a provision as appropriate in this regard be added.	yes	
199	Introduction of a standardised definition of which fields are required. At this moment, the required fields are defined only for the List of fields required by the APSP in the Compliance scope (item 3.3.1), but this information is missing from the tables in 3.2.3.	At this moment, there is no clear information as to which fields are required and an introduction of such a column in one of the tables suggests that not all fields are required in previous tables	yes	
200	Correction to the description in Figure 7: 'The ASPSP may reject the transaction…'	'The ASPSP may reject the request…'	yes	
201	Correction to the description in Figure 8: 'The ASPSP may reject the transaction…'	'The ASPSP may reject the request…'	yes	

202	Correction to the description in Figure 9: 'user redirection into the ASPSP's domain.'	'user redirection to the ASPSP's domain.'	yes	
203	In the description, there is a term 'PSD2 Hub' which has not been introduced earlier.	The term PSD2 Hub should be explained due to the fact that it is a significant element of the PKI. Will there be - within the Polish Banking Association or the PolishAPI team - a Certificate Authority which will deal with the maintenance of the PKI?	yes	
204	In the description, there is a statement to the effect that the use of mutual authentication will protect the ASPSP against a situation when the client device would directly use the ASPSP's servers.	Mutual authentication will not protect the ASPSP against such a situation. There are no obstacles to the creation by the TPP of a mobile app (e.g. for the Android), in which it will configure the KeyStore in such a way so as to use the client certificate for communication with the server.	yes	
205	The existence of an institution to serve as an Identity Hub is unclear and the related costs of TPPs may be non-compliant with the PSD2 Directive.	In relation with the introduction of the mutual authentication and the need of PKI's existence, it is not clear whether or not the certificate obtaining should be related with any costs incurred? What is more, the related costs may be non-compliant with PSD2, due to the fact that the access to API should not entail any costs.	no	Provisions concerning the PSD2 Hub were limited, questions related to certificates and their obtaining are beyond the scope of this document.

206	We propose to resign from mutual authentication in favour of an API key.	The mutual authentication when compared to the solution with an API key introduces a requirement to maintain a safe public key infrastructure, which may be related to unnecessary costs and liability. We propose that the ASPSP made it possible for the TPP to generate an API access key with a limited validity. The application of PKI will not introduce in any way a higher level of security as regards the storage of access data by the TPP. A disclosure of a private key (even a secured one, since the password must be in the same place that the key) or the API key is equivalent.	no	PolishAPI project group decision.
207	Correction of ‘DNS domain/address – URL where the…’ The term ‘URL’ in this context is incorrect, because URL means a complete address of the resource.	“DNS domain – address where the…”	yes	

208	At this moment, among the statuses documented there is no differentiation between a request that is syntactically incorrect and a data validation error.	We propose that the server returned 400 Bad Request, if the request is syntactically incorrect - e.g. the data were provided in an incorrect JSON format. However, in case of a validation error concerning a syntactically correct request, the server should return status 422 Unprocessable Entity (https://httpstatuses.com/422). Such an approach will allow the ASPSP to implement the validation mechanism easier, because in most cases, the frameworks automatically return status 400 when the request was incorrect with a description in words. The introduction, in turn, of status 422 will allow one to always return the errors of validation in the JSON format. What is more, the TPP will be certain that status 422 may always be processed as JSON, while status 400 will contain a description in the form of a capture.	yes	
209	It is recommended to introduce the ‘Bearer’ prefix in the Authorization header.	The value of the Authorization header should comprise the ‘type’ + ‘credentials’, where, in case the ‘type’ token approach is applied, the ‘type’ should have the value of ‘Bearer’.	yes	
210	The transaction amount should be presented in Polish groszys in JSON.	We propose that the amount be represented as number type in JSON where the part with the first and second decimal place is eliminated by multiplication of the amount by x 100.	no	PolishAPI project group decision.
211	Representation of the actual amount in JSON should be the number type.	JSON allows the representation of actual numbers and number type.	no	PolishAPI project group decision.

212	The requirement that the API implementation must be secured against CSRF is incorrect.	We recommend to clarify the protection against CSRF. The ASPSP actually makes available 2 types: - API oAuth 2.0 (TPP - PSU - ASPSP) - API for communication TPP-ASPSP For API oAuth 2.0, the protection against CSRF should be made on the basis of the state parameter. The requirement to introduce protection against CSRF for API TPP-ASPSP should be eliminated because this type of communication I not susceptible to this type of attacks.	no	
213	The Authorization Request may not be in the form of a POST request but only a GET request	Pursuant to the requirements of RFC (4.1.1), for oAuth 2.0, the Authorization Request should be a GET type request and the query parameters should be encoded in accordance with the application/x-www-form-urlencoded.	yes	
214	What is client_id in Authorization Request.	In the oAuth 2.0 protocol, client_id is the client's identifier - is it assumed than, that in the PolishAPI, client_id is the TPP's identifier? How will, then, the ASPSP be able to connect the scope_details data (e.g. paymentAccount) with the ASPSP's client?	no	Incomprehensible comment.

215	Resignation from the introduction of the scope_details parameter due to the fact that it unnecessarily expands oAuth 2.0 and without encoding it will not operate correctly with the GET request.	We propose to resign from the introduction of scope_details in favour of making available the method in API for TPP - ASPSP, where the TPP will be able to register the definitions of the so-called scopeGroup in result of which it will obtain $ID. Obtaining $ID may be provided under the scope parameter, e.g. as 'pis:payment:$ID'. Resignation from scope_details will result in the fact that the PolishAPI will be fully compliant with oAuth 2.0 and all existing implementations of oAuth 2.0 will be available for use both on the side of the TPP and the ASPSP.	no	PolishAPI project group decision.
216	Elimination of the requirement to specify JWS for the oAuth 2.0 protocol	There is no need that the ASPSP required JSW at the oAuth level due to the existence of the client_id, state and redirect_uri parameters. Even in case of an attempted request forgery, the TPP implementation will deal with the incorrect redirect, using the state parameter.	no	PolishAPI project group decision.
217	Implementation of a requirement that the ASPSP verified redirect_uri.	It is recommended that in its configuration of the given client_id, the ASPSP should have a list of redirect_uri which may be used. Thus, the ASPSP will not redirect the client to a URL address which may be fraudulently submitted by an untrusted party.	no	PolishAPI project group decision.
218	Introduction of API to verify access_token and assigned scopeDetails.	We propose that a requirement to make available the API for the TPP be introduced in consequence of which the TPP, specifying access_token and client_id, will be able to obtain information about the token and the finally assigned scopeDetails.	no	PolishAPI project group decision.

219	No explanation why the requirement to provide is_user_session, user_ip, user_agent in the access_token generating procedure on the basis of refresh_token is introduced.	It is hard to find an application in which the TPP when generating access_token on the basis of refresh_token will do it within the framework of the PSU's session. We would appreciate if this requirement be explained.	yes	
220	Upon the redirection to the ASPSP's domain, error codes are returned which may be differently supported by browsers.	Returning error codes upon the PSU's redirection to the ASPSP from the 4XX scope is an incorrect approach because the browsers may support this type of situations in various ways and, what is more, the Location header, which could be used for redirection back to the TPP, will not be supported by the browser. We propose that all errors related to redirection to the ASPSP be supported by status 303 including the redirection to the TPP with a query parameter called 'error' with the request rejection reason stated.	yes	
221	Incorrect use of status 202 in the error code for no funds.	Status 202 means that the server accepted the request for asynchronous processing, without returning the operation result yet. We recommend that the no funds error be supported similarly as in comment 32.	yes	
222	In our view, this API is not in line with PSD2, i.e. it does not reflect ASPSP/banks' obligations under PSD2. As this proposal stands, TPPs would not and could not be obliged to rely on this interface. There are several deficiencies that need to be addressed if the API was to be offered in line with PSD2 and RTS obligations.		no	In our opinion, the standard meets the regulatory requirements.
223	First and most importantly, the standard has to ensure that PISPs receive all information on the initiation and the execution that they require to deliver their services and that are due under Art. 66 (4b) PSD2. This is currently not the case, as the PIS		yes	The PISP has a full possibility to obtain status information concerning the payment initiated; there are 3 ways of obtaining it: in response to a payment initiating

	use case does not include that information, and it cannot be a premium or extra service that is being offered for extra fees.			request and asynchronously in the way initiated by the PISP and asynchronously in the way initiated by the ASPSP.
224	Second, the redirection mechanism („ASPSP-side authentication”) can be offered as one option but must not be imposed. A mandatory redirect to the ASPSP website is not in line with PSD2/RTS (see e.g. Art. 32 (3) RTS). The same applies for Oauth, which needs to ensure that it can be used without redirection.		no	Version 1.0. allows for an additional method of authentication (decoupled).
225	Third, it needs to be ensured that the existing authentication procedures can be relied upon by PISP, AISP when using the API. There must not be an „extra set” of procedures for the API or for TPP, neither with regard to SCA nor regarding the exemptions from SCA. Equivalent treatment and non-discrimination requires that the authentication procedures are equivalent for direct access and indirect access via the API. The API should allow to rely on these existing procedures (without redirection mechanism, see above).		no	Version 1.0. allows for an additional method of authentication (decoupled). Work is under way on subsequent authentication methods. The redirection method is well adopted on the Polish market both by banks and third parties. Payment methods based on redirection constitute almost 50% of all e-commerce payments.
226	Fourth, the API should allow a combination of PIS and AIS, at least in one combined session. Based on PSD2, it has been consensus within the Euro Retail Payments Board (ERPB) Working Group on PIS that a dedicated API must support the provision of only PIS, only AIS, or both in one single combined communication session.		no	The problem will be addressed in the next version of the specification.

227	Furthermore, we would like to highlight that the below comments do not necessarily represent an exhaustive list of concerns. The consultation did not in the first step invite for a practical testing, but was conducted based on the papers only. In many instances, we cannot evaluate yet how the theory would be implemented in practice. Many terms such as „embedded" authentication mechanism are new creations, where the actual implementation in practice will be decisive. In a second step of this consultation, where the actual infrastructure is being presented for practical testing, we may very welll have more comments and questions.		no	Yes, we agree.
228	Providing necessary information for the role PISP The only use case assigned to the role of a PISP appears to be „Initiation of a Single Payment by the PISP". However, this use case is not sufficient to cover the full role of a payment initiation service. As discussed in depth within the ERPB Working Group on PIS, the PIS should not need a second license/registration as AIS for obtaining the data it needs to provide the PIS. The API should thus make available additional data to support risk-based evaluations on the likelihood of a non-execution of the transaction (in case there is no real-time execution in place).	The use cases that are currently only foreseen for the role of an AISP should also be available for TPP acting as pure PIS.	no	The PISP has a full possibility to obtain status information concerning the payment initiated; there are 3 ways of obtaining it: in response to a payment initiating request and asynchronously in the way initiated by the PISP and asynchronously in the way initiated by the ASPSP.

229	Providing information on the execution of the transaction PSD2 provides that the ASPSP "shall immediately after receipt of the payment order from a payment initiation service provider, provide or make available […] all information accessible to the account servicing payment service provider regarding the execution of the payment transaction to the payment initiation service provider" However, we could not find such a response on the execution of the payment transaction in the documentation. Within ERPB, parties discussed the information that has to be available to PISPs according to PSD2 ("the What"). It has been discussed within ERPB, corroborated by the European Central Bank and the European Commission, that this has to include, at least, either the confirmation of the payment in a real-time environment (immediate booking), or in a batch environment (i) the account balance, (ii) overdraft and (iii) pending/scheduled transactions.	For the role of PISP, add a response on the execution of the payment transaction (i.e. put forward the full information required by PSD2).	yes	
230	Session at the API It is crucial that the concept of a session is a mandatory part of the Polish API framework. If the customer decides to use a TPP for e.g. aggregating his account data and subsequently initiate a transaction, it must be possible to combine these use cases within a single session. Otherwise, the customer would have to log in for each use case, which would severely hamper the customer's user experience, thereby making it impossible for the PIS and AIS provider to provide a frictionless service.	The support of sessions at the API must be mandatory for an ASPSP. If the customer instructs the TPP to perform several use cases, it must be possible to execute these transactions/use cases without performing SCA for each single use case.	no	The problem will be addressed in the next version of the specification.

231	Consent It should be noted that consent for the initiation and execution of a payment transaction is always given via the PISP as far as he is involved. The PISP then passes on the information on the consent to initiate and execute the payment transaction to the ASPSP (see also draft final report of the ERPB WG on PIS). There is no extra consent or rather a separation needed between (a) expressing consent to use the PIS service and (b) authorizing the payment transaction. Please also see Art. 32 (3) RTS: "Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, (…) requiring additional authorisations and registrations in addition to those provided for in Articles 11, 14 and 15 of Directive 2015/2366, or requiring additional checks of the consent given by payment service users to providers of payment initiation and account information services."	Consent for the initiation and execution of a payment transaction is always given via the PISP as far as he is involved. A PSD2/RTS-compliant API must not require additional authorisations or checks of the consent given by PSU's to PISP and AISP.	yes	

232	Redirection / "ASPSP-side Authentication Mechanism" The "redirection approach" or "ASPSP-side Authentication Mechanism" is unacceptable for a TPP in many respects, i.a. as it is not compatible with the TPP's freedom to design the customer interface. All of these arguments have been discussed in detail within the ERPB Working Group on PIS. Please also refer to the (draft) final report of this group. Therefore, a forced redirection to the ASPSP website must not be imposed on the PIS and AIS providers. An API that relies on redirection violates PSD2 and the RTS, i.e. the ASPSP will breach its PSD2 obligations by offering it and TPPs will not be obliged to use this API. Please also see Art. 32 (3) RTS: "Account servicing payment service providers that have put in place a dedicated interface shall ensure that this interface does not create obstacles to the provision of payment initiation and account information services. Such obstacles, may include, among others, preventing the use by payment service providers referred to in Article 30(1) of the credentials issued by account servicing payment service providers to their customers, imposing redirection to the account servicing payment service provider's authentication or other functions (…)".	Delete the whole paragraph 1.4.4.1 ASPSP-side Authentication mechanisms	no	We do not agree with this opinion. The redirection methed itself is not forbidden by the regulator. It was stated several times by representatives of The European Commission, that redirection, if provided propoerly, without generating obstacles for the TPPs, is allowed. The redirection method is well adopted on the Polish market both by banks and third parties. Payment methods based on redirection constitute almost 50% of all e-commerce payments. This method is also supported by Polish Financial Supervision Authority

233	“Embedded authentication mechanism” PSD2 assumes the embedded approach as discussed in the ERPB WG on PIS, this is why i.a. Art. 66 (3b) states that it is the responsibility of the PISP to ensure that credentials are transmitted through safe and efficient channels. So whenever the ASPSP provides an authentication procedure based on transmittable/portable credentials, a PISP or AISP transmits the personalized security credentials to the ASPSP. However, the “embedded authentication mechanism” presented here is not acceptable from a TPP point of view, notably with regard to the requirement of a “prior agreement between the ASPSP and the TPP, based on implementation documentation, provided by ASPSP”. The PSU will give consent to and authenticate the payment transaction by means of SCA via the TPP. Art. 97 (5) PSD2 clarifies that TPPs shall be enabled to rely on all existing authentication procedures. Art. 66 (3b) PSD2 and Recital 30 show that this includes the ability to forward the credentials on behalf of the PSU.	While redirection has to be excluded, relying on the existing authentication procedures in an “embedded approach” as discussed in the ERPB WG on PIS has to be included in any API. However, the “embedded authentication mechanism” presented here, requiring a “prior agreement between the ASPSP and the TPP” is not acceptable.	no	The problem will be addressed in the next version of the specification.
234	Oauth2 protocol If the ASPSP decides to make use of the OAuth2 protocol, it must ensure that the returned token can be provided via the embedded approach discussed in the ERPB WG on PIS – and that redirection therefore is excluded, i.e. the API must not require leaving the website of the TPP at any point in the process.		no	PolishAPI project group decision.
235	We suggest to consider a change of the name of COF into CAF into the entire document	The change results from the guidelines and terminology used by the Polish Financial Supervision Authority	yes	
236	Should it not be clarified what certificate is meant?	Please clarify.	yes	

237	Is the access token also granted to the given TPP institution on a one-time basis?	Please clarify.	n/a	
238	It seems that it is not advisable to determine on a hard basis the number (‘three’) of mechanisms of authentication before the final determination of selected methods.	Editorial change	yes	
239	The phrasing ‘Pursuant to PSD2, the TPP… defines the framework of consent grant and revocation by PSUs.’ suggests that at the TPP level, the PSU should have a possibility to change the authorisations.	It may prove impossible to implement such a requirement because the final user may not have the rights to manage authorisations on the side of the company.	no	The problem will be addressed in the next version of the specification.
240	‘Granting Consent – a process in result of which the PSU grants ASPSP consent to access his/her account held by the ASPSP in order to effect a service, including the AIS, PIS and COF services.’ - for institutional Clients, the PSU (understood as the person representing the company) may not have the powers to grant such consent	Request to clarify the corporate/business area	no	The problem will be addressed in the next version of the specification.
241	What is understood by the term ‘express consent’?	Please clarify.	no	Provisions concerning the consents were amended and rendered more precise.
242	The phrasing may be understood so that the TPP submits the consent only and the ASPSP does nothing with it. Please clarify what is the ‘PSU’s consent’ in this context?	Please clarify.	no	The provisions of this chapter were changed in whole.
243	Will the standard foresee a possibility for a mutual repeated communication other than consent taking (or providing transaction status information)? e.g. when the Bank lacks some information	For example: if any data were missing from the ASPSP to execute the given service correctly (and this data is not covered by the Polish API specification), the ASPSP could ask TPP for this information	no	The problem will be addressed in the next version of the specification.
245	‘the PSU indicates the ASPSP” - Should it not be clarified what the process of the ASPSP indication by the PSU look like on the TPP’s side? (e.g. selection of the Bank from the list, and/or insertion of the name,	Please clarify.	no	

	and/or insertion of account number in a form or, alternatively, some other process)			
246	1. Should and, if so, how should the ASPSP verify these parameters? 2. Is the content of the consent submitted to the ASPSP? 3. With reference to the discussion at the latest legal&business meeting – should the PSU indicate at this stage the payment account from which the information is to be obtained or should this filter be at the ASPSP's level? 4. Isn't such a menu in the beginning for the PSU to indicate at the TPP's an 'obstacle' at some point?	Please analyse in legal terms and clarify	no	The provisions of this chapter were changed in whole.
247	'data range' – How will the range of such data defined?	Please clarify.	no	The provisions of this chapter were changed in whole.
248	'purpose and manner of utilisation of data' – Should the information provided in this regard be standardised – a closed list of purposes and ways of utilisation?	A defined list will facilitate the servicing and will standardise the approach on the market	no	The provisions of this chapter were changed in whole.
249	Isn't there, in this step sequence- a risk of double authorisation of the PSU in the ASPSP?	Please analyse in legal terms	no	The provisions of this chapter were changed in whole.
250	1. We assume that this fragment will be corrected in accordance with the discussion at the meeting of the PolishAPI working group on 30 January at the Polish Bank Association – consent taking for COF should take place on the ASPSP's side 2. Can SCA be used in every COF request?	Please analyse in legal terms and supplement	yes	
251	Is a revocation of consents granted to the TPP in the ASPSP's user interface foreseen?	Please clarify.	no	In our opinion, this is not admitted by the regulations.

252	Are the 4 times counted from the first request (and consequently for another first request?), or in the 0:00-24:00 cycles, everyday?	Please clarify.	no	From the first request.
253	How in this context should SCA operate for a simple functionality of displaying the account balance in Internet banking? Can it be so that it depends on the strategy of the given ASPSP and will vary on the market?	Please clarify.	no	In our opinion, this matter is beyond the scope of the standard specification document.
254	If the ASPSP’s interface shows holds/blocks and rejected transactions separately from the transaction history at the payment account, should such information (i.e. blocks and rejects) be sent to the TPP? In other words, does such information as blocks and rejected transactions definitively constitute information about the payment account and related transactions?	Please clarify.	no	The final decision about providing this information remains at the discretion of the ASPSP.
255	‘Account interest rate’ - 1. What happens in case the interest rate of a single payment account has three different values (e.g. funds up to 100 k, from 100 k to 1 m and from 1 m upwards)? 2. As regards the payment account, are we talking only about the interest rate applicable to the funds at the account or also about credited funds (in case of overdraft facilities or credit card accounts)?	Please clarify.	yes	
256	‘Given names and surname / Name of the PSU” - What should we disclose in case of co-owners? Do we show only the given name and surname of the person logged in?	Please clarify - a representative or a proxy of co-owners can see all owners with authorisation to the account.	no	The problem will be addressed in the next version of the specification.
257	‘Available funds’ – we understand that what is meant are funds expressed in the currency of the account?	Please clarify.	yes	

258	‘transaction ID ‘ - This field should be optional rather because it is not presented at each transaction. The ASPSP does not always provide this information in electronic banking (e.g. in card transactions it is, but it is not presented in case of a simple transfer).	Please clarify.	yes	
259	‘Number of sender’s account’ and ‘Number of payee's account’ – Shouldn’t it be ‘for each transfer transaction’?	Editorial change	yes	
260	‘Description/title” – We understand that in case of situations when there are transactions with both a description and a title, we return both values.	Please clarify or separate the field into two fields	yes	
261	‘Transfer type’ - Shouldn’t it be ‘Transaction type’?	In Swagger, there is ‘transactionType’	yes	
262	‘Transaction exchange rate – For each transaction at the account history’ - Shouldn’t it be ‘for transactions in a currency other than the account currency’?	Editorial change	yes	
263	‘Unique identifier of the payment instrument by which the transaction was effected - E.g. credit card number (hashed)’ - Shouldn’t it state ‘partially-hashed’?	If we were to hash the card number in whole, the client would not be able to tell which card was used to effect the payment (in case there are a few cards).	yes	
264	‘Operation type’ - We suggest to prepare a dictionary with definitions in order to standardise the field completion with specific data	Please supplement in order to standardise operation types	no	Each ASPSP may define the dictionary items on its own.
265	‘Name of the incoming transfer payee – For each account history transaction’ - Probably it should read ‘’for each incoming transfer’. General rule should be that the item data concern only transfers and not all transactions, e.g. ‘account maintenance fee’	Editorial change	yes	
266	‘Name of the incoming transfer payee – For each account history transaction. The field defines the card payment payee in a card transaction’ - Shouldn’t this field concern only the incoming transfer and not a card transaction too?	Editorial change	yes	

267	‘Name of the outgoing transfer payee – For each account history transaction’ - Probably it should read ‘’for each outgoing transfer’.	Editorial change	yes	
268	‘Code of the payee’s Bank’ and ‘BIC/SWIFT of the payee’s bank’ - What is the difference between the value of the field Payee’s bank code and BIC - how to interpret it? What code is it?	Please clarify.	yes	Changes were made with regard to foreign transfers
269	‘Name of the incoming transfer sender – For each account history transaction’ - It should read ‘only for incoming transfers’.	Editorial change	yes	
270	‘Name of the outgoing transfer sender – For each account history transaction’ - It should read ‘only for outgoing transfers’.	Editorial change	yes	
271	‘Transaction originator’ – is it the given name and surname of the originator?	Please clarify.	yes	
272	‘TPP’s name’ – please define the field length	It is important for domain systems	yes	
273	No tppID specified at the entry of the transfer order, and it should be returned later in operation details	Please supplement.	yes	
274	‘Name of the transfer sender’ - What if the sender is not the owner but only a representative? Do we give the representative's name?	Please clarify.	no	The sender is the account holder. Additional field has been added where information about the person ordering the given payment is provided
275	‘Currency - In case the field is empty, the ASPSP will make the transfer in the account currency.’ – in other words, de facto the indicated amount in the default account currency is converted into PLN and submitted to the settlement system? Maybe the actual activity of the ASPSP should be clarified.	Please clarify.	no	The ASPSP may decide that this field is required.
276	1. Why was the name changed to EEA? 2. What will be the determinant of qualification to this category – EUR and what else? 3. What is the reason there is no ‘cost clause’ field	Please clarify and, if necessary, return the name SEPA – from August of this year, all banks must use the term SEPA transfer order.	yes	Changes were made with regard to foreign transfers

277	'Name of the payee's bank' - What other payments should be under the new name? Will this field be also for payments other than SEPA?	Pursuant to Regulation 260/2012, the payee's bank must be identified by drawing conclusions from IBAN – this rule concerns SEPA.	yes	Changes were made with regard to foreign transfers
278	'Constant value - SEPA' - What is the relation of this field to the new transfer type name?	Please clarify.	yes	Changes were made with regard to foreign transfers
279	'Effective date of the transfer' - The comment should clarify what the effective transfer date is – is is the date the message is sent or the date the beneficiary's bank was credited or some other date(?)	Please clarify.	yes	Changes were made with regard to foreign transfers
280	'BIC/SWIFT of the payee's bank' – 1. If the common existence of the 4 fields concerning the payee's bank data should be maintained, the comments should provide information what it means for the client to fill each one of then, e.g. if the payee's bank data resulting from BIC are inconsistent with the data completed by the client in the remaining three fields, the payment will be rejected – is this the author's intention? 2. 'ABA number' should be added. This is the settlement number for the US instead of SWIFT	Please supplement.	yes	Changes were made with regard to foreign transfers
281	As regards the description in item 1 on the diagram, does the PSU actually 'initiate the payment transaction'?	Please clarify.	no	The diagrams and their descriptions were changed in the current version.
282	'Transaction exchange rate, Format 4,6 / Currency exchange rate' – incomprehensible numeric field format '4,6' (10 digits out which 6 in decimal places?)	Editorial change	yes	