PolishAPI

Specification of an interface for the needs of services provided by third parties on the basis of access to payment accounts

Document developed by the PolishAPI Project Group

17 April 2018
Version 1.0.0

Licence

PolishAPI specification

Table of Contents

Table of Figures

1 Introduction

1.1 Context

The implementation by the European Union of the new directive on payment services in the internal market (PSD2) introduces a possibility to offer new products and services related not only to the payment service market but also the financial service market in the wider sense. Both the entities present on the market, such as banks, cooperative savings and credit unions (SKOK) or branches of foreign credit institutions, as well as new types of entities (third party providers - TPP) will be able to take advantage of the possibility to offer new services built on the basis of the PSD2 Directive, the implementing acts (including the regulatory technical standards - RTS) and national acts of law. The new categories of services are:

a) **Account Information Service (AIS)** – as defined in Art. 67 of PSD2
b) **Payment Initiation Service (PIS)** – as defined in Art. 66 of PSD2
c) **Confirmation of the Availability of Funds (CAF)** – a service defined in Art. 65 of PSD2

Allowing the performance of the above-mentioned services by entities authorised to do so required the preparation by account servicing payment service providers (ASPSP) of dedicated interfaces allowing access to payment accounts (the XS2A interface) by authorised third party providers (TPP), based on an open API.

Banks and other entities cooperating with the Polish Bank Association took a decision on the creation of a common and universal API standard drawing on the existing achievements of the Polish banking and payment sectors, the best practices and experiences, including those resulting from foreign API standards, as well as the existing interfaces of the interbanking infrastructure. Banks and other ASPSP will be able to implement the standard, depending on the business decisions they take independently. During the work of the business, IT, security and legal task forces, assumptions were formulated and then the standard description was created as presented herein below.

The basis assumed for this standard version was the Delegated Regulation with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication (RTS), as published in the Official Journal of the European Union on 13 March 2018 (https://eur-lex.europa.eu/legal-content/PL/TXT/?uri=uriserv:OJ.L_.2018.069.01.0023.01.POL&toc=OJ:L:2018:069:TOC).

The following entities took part in the preparation of this standard (in an alphabetical order):

1) Allegro Group
2) Biuro Informacji Kredytowej S.A.
3) Billbird S.A.
4) Blue Media S.A.
5) Diners Club Polska
6) Krajowa Izba Rozliczeniowa S.A.
7) Kontomierz.pl Sp. z o.o.
8) National Savings and Credit Union
9) Polish Association of Cooperative Banks
10) PayU S.A.
11) Polish Chamber of Information Technology and Telecommunications (PIIT)
12) Polish Insurance Association (PIU)
13) Polski Standard Płatności Sp. z o.o.
14) Polish Organisation of Non-banking Payment Institutions (PONIP)
15) Skycash Poland S.A.
16) F. Stefczyk Cooperative Savings and Credit Union

17) Polish Bank Association together with its associated bank members[1]

PolishAPI drafted specification was consulted during the public consultation, which took place between 17th and 31st of January 2018. 21 Polish and foreign entities submitted almost 300 comments and remarks, partially included to the specification.

1.2 Document Structure

The document consists of two fundamental parts and of annexes:

a) Part concerning the business characteristics of the PolishAPI Standard (Chapters 1 – 4)
b) Part concerning the technological solutions adopted in the PolishAPI Standard (Chapters 5 – 13)
c) Annexes, the list of which is given in Chapter 14

1.3 Mission of the PolishAPI Standard

The main objective of this document is to define interfaces for services described in PSD2 and related acts of law as regards the interactions between ASPSPs and TPPs during the performance of the AIS, PIS and CAF services. The requirement of open APIs also provides a chance that ASPSPs and TPPs will obtain an opportunity under a single standard to offer not only law-required services but also additional services the scope of which exceeds the framework defined by the legislator. Therefore, the following scopes of services can be identified within the PolishAPI standard:

a) **Compliance Scope** of the AIS, PIS and CAF services - services required by PSD2
b) **Premium Scope** of the AIS, PIS and CAF services - services exceeding the requirements laid down in PSD2, outside the scope of this document

Each ASPSP and TPP may use the PolishAPI standard as an open standard. The application of the standard is not mandatory. Each of the entities operating on the market on the basis of the PSD2 Directive may use any solution compliant with PSD2 and the related acts of law.

The interactions between the TPPs and PSUs and between ASPSPs and PSUs, as well as the matters related to the processes of making an entry in the national register of TPPs, and of granting of authorisations for the operation of TPPs in the scope related to PSD2-related services by public administration authorities are outside the scope of this document.

A part of the problems remaining within the standard specification scope will be systematically added over time as the project and agreement work (including public consultation) will advance. The above reservation concerns, without limitation, the problems related to specific functionalities of corporate accounts and technical details concerning the methods of authentication as described in Chapter 1.4.3.

[1] Alior Bank S.A., Bank BGŻ BNP Paribas S.A., Bank Handlowy w Warszawie S.A., Bank Millennium S.A., Bank Pekao S.A., Bank Pocztowy S.A., Bank Polskiej Spółdzielczości S.A., Bank Zachodni WBK S.A., Credit Agricole Bank Polska S.A., Deutsche Bank Polska S.A., DNB Bank Polska S.A., Eurobank S.A., Getin Noble Bank S.A., Idea Bank S.A., ING Bank Śląski S.A., mBank S.A., Nest Bank S.A., PKO Bank Polski S.A., Raiffeisen Bank Polska S.A., SGB-Bank S.A.

1.4 Main Assumptions

1.4.1 Actors in the PolishAPI Standard-defined Processes

The standard defined only three categories of actors that can take part in processes defined by the PolishAPI standard:

a) **Payment Service User (PSU)** – User of the payment account the given payment transaction refers to
b) **Account Servicing Payment Service Provider (ASPSP)** – Provides maintaining the payment account and making the XS2A interface available for TPPs
c) **Third Party Provider (TPP)** – Entity using the XS2A interface on the basis of and in accordance with the consents granted by the PSUs. The ASPSP may also act as a TPP and use the interfaces made available by other ASPSPs

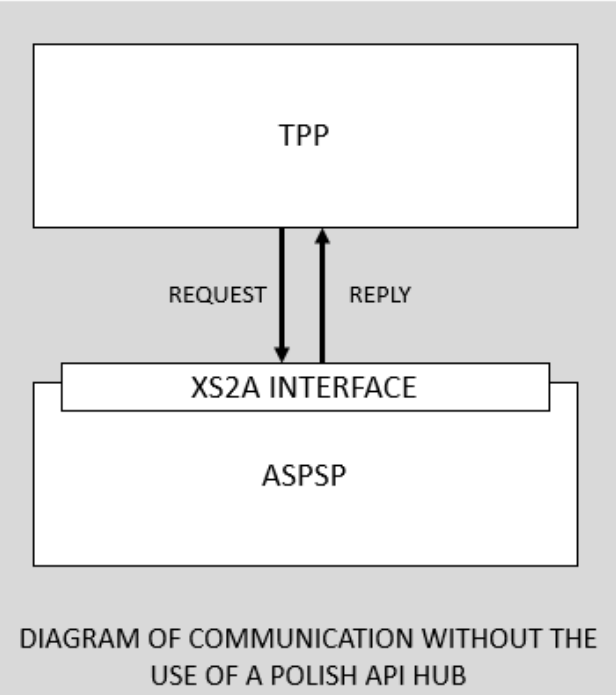


Figure 1: General diagram of PolishAPI Standard communication

The standard defined three roles which the actors taking part in the PolishAPI standard-defined processes can play. The categorisation below does not restrict the entities acting as TPPs to apply for an entry in the national register in more than a single role but aims at defining the roles of particular actors in the description of communication under the PolishAPI standard.

a) **Account Information Service Provider (AISP)** – TPPs using the XS2A interface to access information about the PSU's payment account
b) **Payment Initiation Service Provider (PISP)** – TPPs using the XS2A interface to initiate the a payment transaction debited to the PSU's account
c) **Payment Instrument Issuer Service Provider (PIISP**) – TPPs using the XS2A interface to confirm the availability at the PSU's payment account of an amount necessary to effect the payment transaction performed on the basis of an instrument issued by the PIISP

The actors may play the following roles:

Role \ Actor	PSU	ASPSP	TPP
AISP	NO	YES	YES
PISP	NO	YES	YES
PIISP	NO	YES	YES

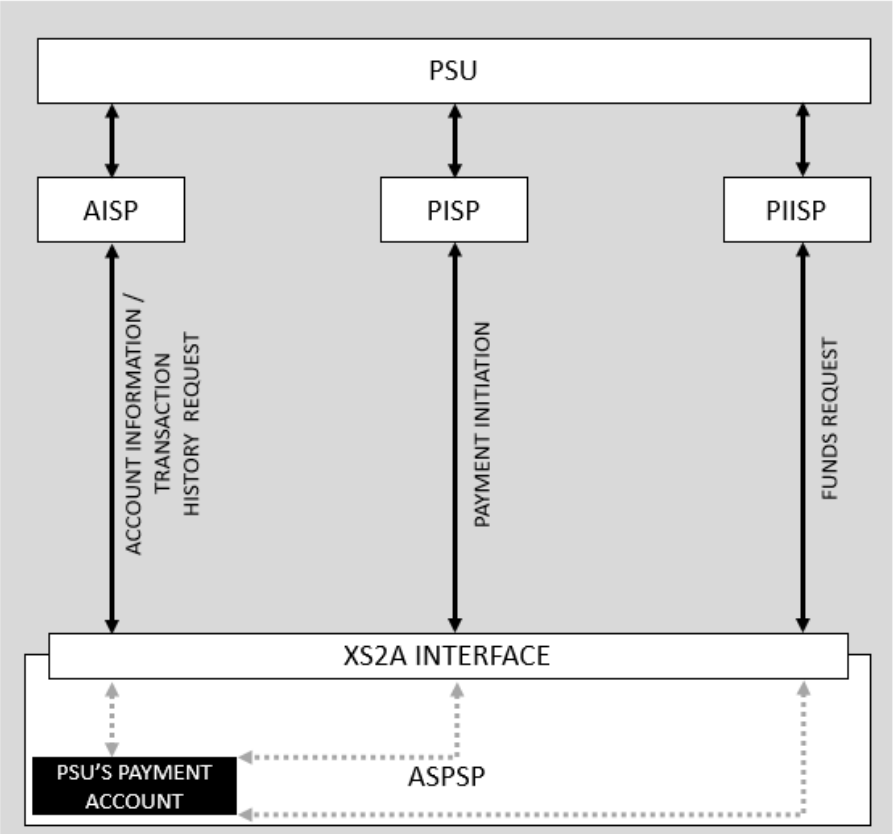


Figure 2: General diagram of dependencies between actors in the PolishAPI Standard

1.4.2 Requirements concerning Actors in the PolishAPI Standard-defined Processes

a) The ASPSP must implement an XS2A interface compliant with the PolishAPI standard. The ASPSP may also implement other XS2A interface standards, which however will not be covered by the scope of this document
b) The interfaces implemented by ASPSPs must be compliant with PSD2, the Payment Services Act and related acts, in particular the RTSs
c) The TPP must be registered in at least one register of the European Union Member State in the role it intends to play during the PolishAPI standard-based communication
d) The TPP must have a valid certificate used for identification in the XS2A interface obtained from a qualified provider of trust services and meeting the requirements of the Electronic Identification and Trust Services Act. The certificate should additionally meet the requirements defined in the RTSs and in the ETSI technical specification (TS 119 495)

1.4.3 PSU Authentication Mechanisms

The PolishAPI Standard allows the PSU authentication mechanisms as listed below. The ASPSP may freely select the authentication method. The selection made should be compliant with the regulations in force.

1.4.3.1 Authentication Mechanism on the ASPSP's Side

The PolishAPI Standard allows the use of a mechanism of ASPSP-side authentication, which assumes a redirection to the ASPSP's website during the execution of the AIS, PIS and CAF services. This means that the PSU's authentication and authorisation data are given exclusively at the ASPSP's website. The PSU is authenticated in the ASPSP's interface.

1.4.3.2 Authentication Mechanism in an External Authorisation Tool (Decoupled)

The PolishAPI Standard allows the use of an authentication mechanism using an external authorization tool during the performance of the AIS, PIS and CAF services. The mechanism of authentication in an external authorisation tool has been presented at a high level in the diagram below. Detailed concerning its use will be supplemented in the next version of this document.

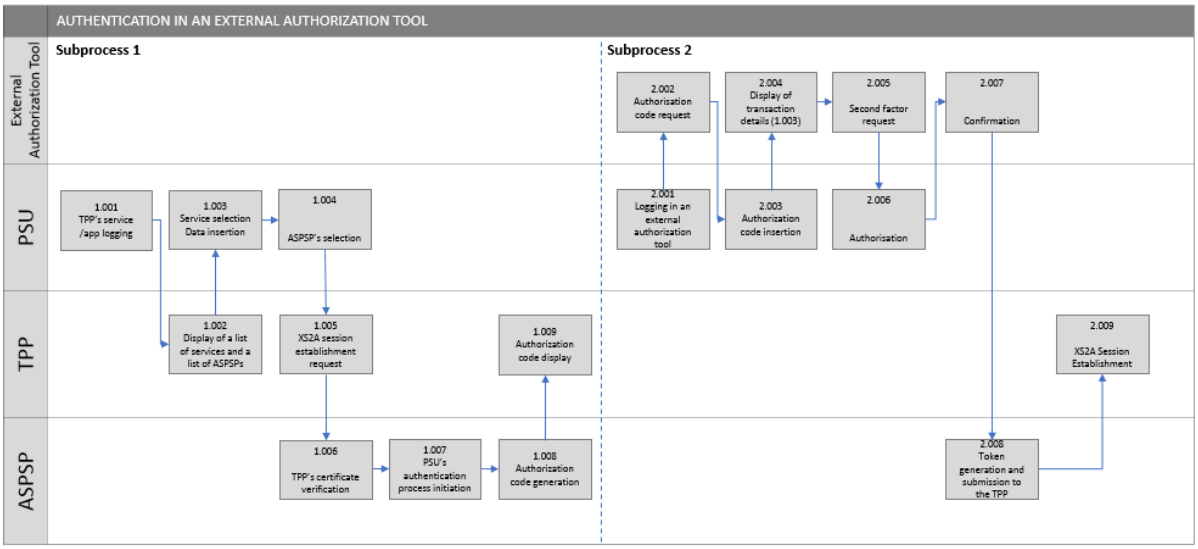


Figure 3: Authentication in an external authorization tool

1.4.3.3 Other Authentication Mechanisms

The standard may contain a description of other mechanisms of authentication which meet the regulatory requirements and requirements agreed during the work of the project group. They will be published in subsequent versions of this document.

1.4.4 Management of PSU's Consents for the Performance of Services by a TPP

Pursuant to PSD2, the TPP may perform services for a PSU only upon his/her consent and within the scope covered by such consent. The PolishAPI standard defines the framework of consent grant and revocation by PSUs.

1.4.4.1 Process of Granting Consent by PSU to Effect the PIS Service

It is assumed that the payment initialization process performance will be in each case related to the grant of consent by the PSU within the framework of the TPP interface.

1.4.4.1.1 Option in case the authentication mechanism on the ASPSP's side is used

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to TPP to provide the PIS service
- 004 / PSU completes the transfer form, which should contain at least the information indicated in Chapter 3.1.3 of this specification: 'List of Fields Required by the ASPSP in the Compliance Scope'
- 005 / TPP transfers the payment initiation request to the ASPSP and a redirection is made to the ASPSP's domain in order to authenticate the PSU
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP sends a PSU authentication request
- 008 / Authentication
- 009 / ASPSP presents the PSU a list of payment account from which a payment transaction may be initiated to select from
- 010 / PSU selects one account from the list. and accepts the transaction
- 011 / ASPSP generates and sends to the PSU an additional authorization element (e.g. OTP) – provided that it is required in accordance with the regulations in force
- 012 / PSU authorises the transaction using the method applied in relations with the ASPSP (the PSU has an option to refuse authorisation, which results in the fact that the payment transaction is not effected)
- 013 / ASPSP performs the request and then a redirection is made to the TPP's domain

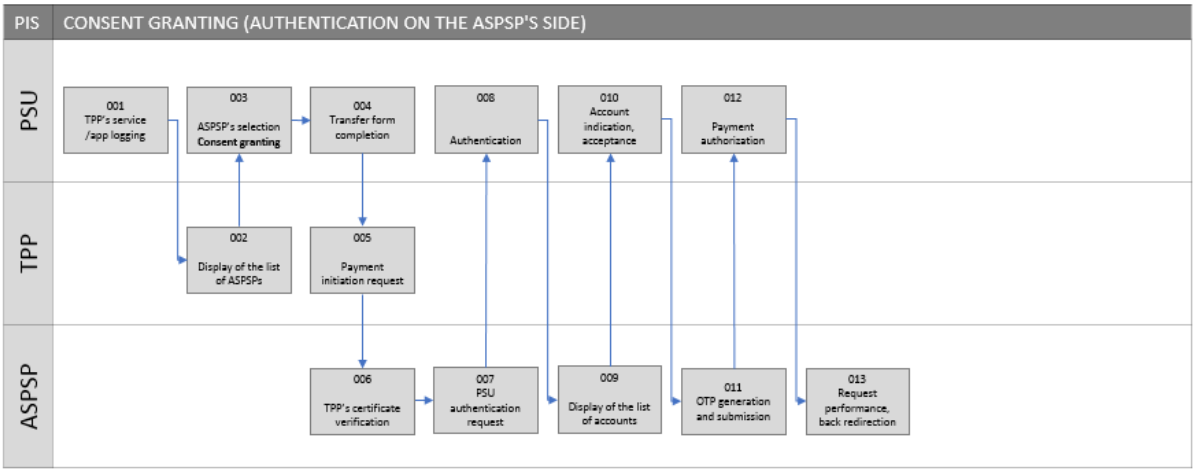


Figure 4: PIS. Consent grant (authentication on the ASPSP's side)

1.4.4.1.2 Option in case an authentication mechanism in an external authorization mechanism is used

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to TPP to provide the PIS service

- 004 / PSU completes the transfer form, which should contain at least the information indicated in Chapter 3.1.3 of this specification: 'List of Fields Required by the ASPSP in the Compliance Scope' (specifying, without limitation, the number of account from which the payment is to be initiated)
- 005 / TPP transfers the payment initiation request to the ASPSP
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP initiates the process of PSU's authentication
- 008 / TPP transfers the authentication request to the PSU
- 009 / Authentication in an external authorisation tool (cf. item 1.4.3.2)
- 010 / The external authorization tool displays the payment details and the PSU accepts the transaction
- 011 / ASPSP generates and sends to the PSU an additional authorization element (e.g. OTP) – provided that it is required in accordance with the regulations in force
- 012 / PSU authorises the transaction (PSU has an option to refuse authorisation, which results in the fact that the payment transaction is not effected)
- 013 / ASPSP performs the request

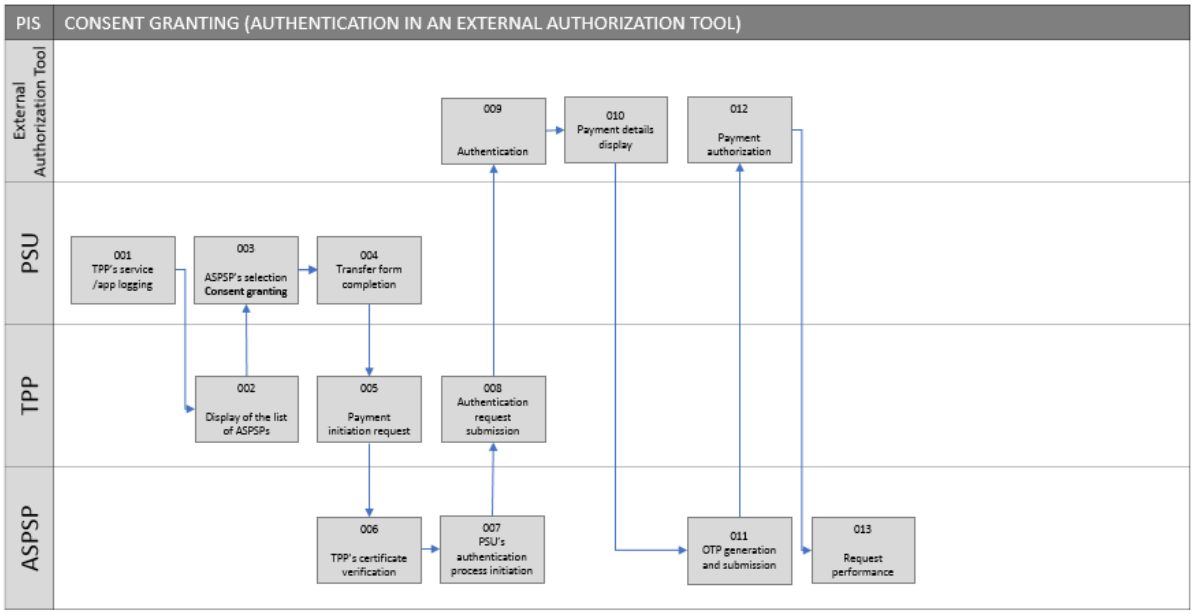


Figure 5: PIS. Grant of consent (authentication in an external authorization tool)

1.4.4.2 Process of Granting Consent by PSU to Effect the AIS Service

In this Chapter, the term 'consent' refers exclusively to the provision of the AIS service and means the grant of consent for the service without indicating specific accounts (in case of an option with a retrieval of a list of accounts) or with an indication of the same (in case of an option with a manual account number insertion). This process is always linked with the strong customer authentication (SCA).

Determination of access parameters (in case of an option with a retrieval of a list of accounts) means each operation on specific accounts within the limits of the consent to effect the AIS services, including:

- indication of a specific account
- change of parameters for a specific account (e.g. date of access)
- withdrawal of indication of a specific account or
- withdrawal of consent

These operations do not require the strong customer authentication (SCA).

The standard allows two processes of granting a consent for the AIS service (in options allowing the authentication on the ASPSP's side and in an external authorisation tool) as described in items from 1.4.4.2.1 to 1.4.4.2.4. The ASPSP may implement one process or both.

1.4.4.2.1 Grant of consent with a manual insertion of the account number in case of authentication on the ASPSP's side

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to the given TPP to provide the account information service concerning an account maintained by the given ASPSP
- 004 / PSU inserts the account number and defines the scope of access
- 005 / TPP sends a token request to the ASPSP
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP sends a PSU authentication request
- 008 / SCA authentication
- 009 / ASPSP gives the TPP an access token (containing information about the scope of access), in case of AIS a multiple one with a refresh token

In case the account number or one of the many account numbers inserted is incorrect or when an access to the given account cannot be given, error message 400 will be returned.

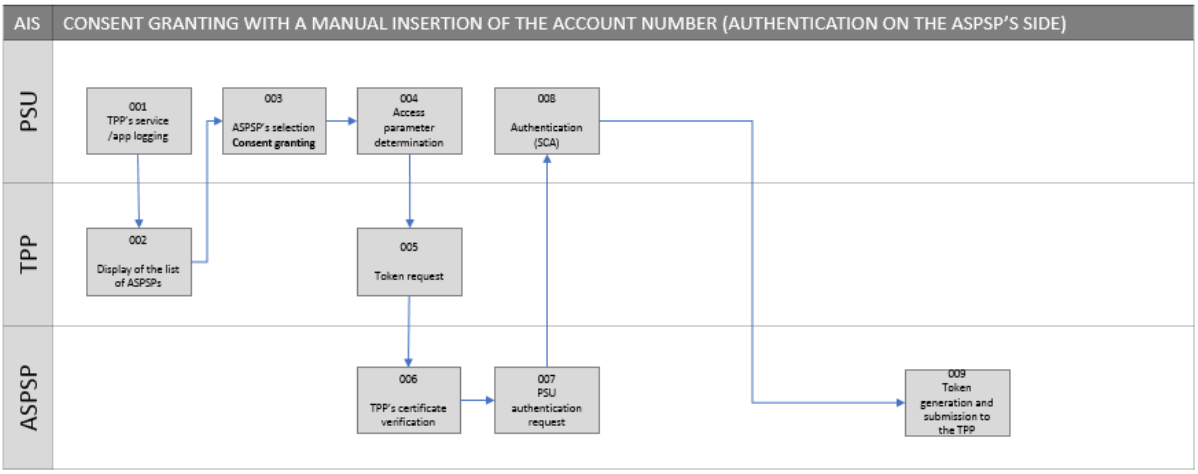


Figure 6: AIS. Grant of consent with a manual insertion of the account number (authentication on the ASPSP's side)

1.4.4.2.2 Grant of consent with a manual insertion of the account number in case of authentication in an external authorization tool

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to the given TPP to provide the account information service concerning an account maintained by the given ASPSP
- 004 / PSU inserts the account number and defines the scope of access
- 005 / TPP sends a token request to the ASPSP
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP initiates the process of PSU's authentication

- 008 / TPP transfers the authentication request to the PSU
- 009 / SCA authentication in an external authorisation tool (cf. item 1.4.3.2)
- 010 / ASPSP gives the TPP an access token (containing information about the scope of access), in case of AIS a multiple one with a refresh token

In case the account number or one of the many account numbers inserted is incorrect or when an access to the given account cannot be given, error message 400 will be returned.

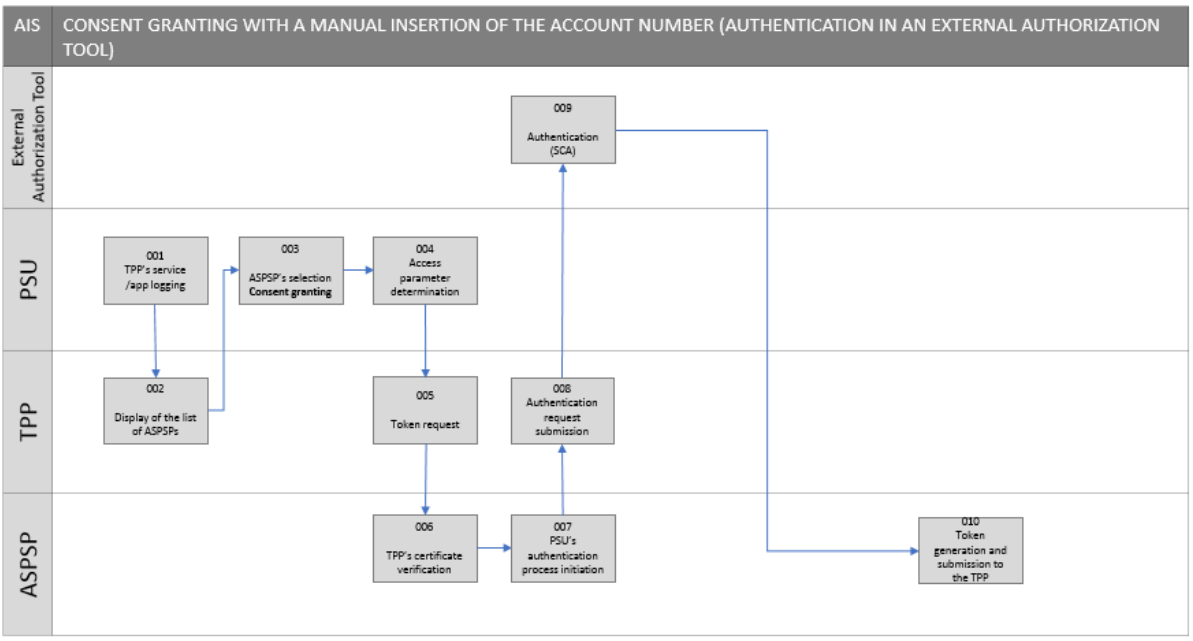


Figure 7: AIS. Grant of consent with a manual insertion of the account number (authentication in an external authorization tool)

1.4.4.2.3 Grant of consent with an account list retrieval in case of authentication on the ASPSP's side

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to the given TPP to provide the account information service concerning an account maintained by the given ASPSP
- 004 / TPP sends a token request to the ASPSP
- 005 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 006 / ASPSP sends a PSU authentication request
- 007 / SCA authentication
- 008 / ASPSP transfers the access token to the TPP
- 009 / TPP sends a request to the ASPSP for a transfer of the PSU's account list (together with an access token)
- 010 / ASPSP gives the TPP a list of PSU's accounts (a full or a partially masked account number + product name + account type)
- 011 / TPP displays a list of accounts
- 012 / PSU indicates an account (or accounts) in order to determine the scope of access
- 013 / PSU determines the access parameters
- 014 / TPP sends a token exchange request to the ASPSP (for a token containing access details)
- 015 / ASPSP verifies the identity of the TPP and the PSU (on the basis of the first access token)

- 016 / ASPSP gives the TPP a new access token (containing information about the scope of access), in case of AIS a multiple one with a refresh token

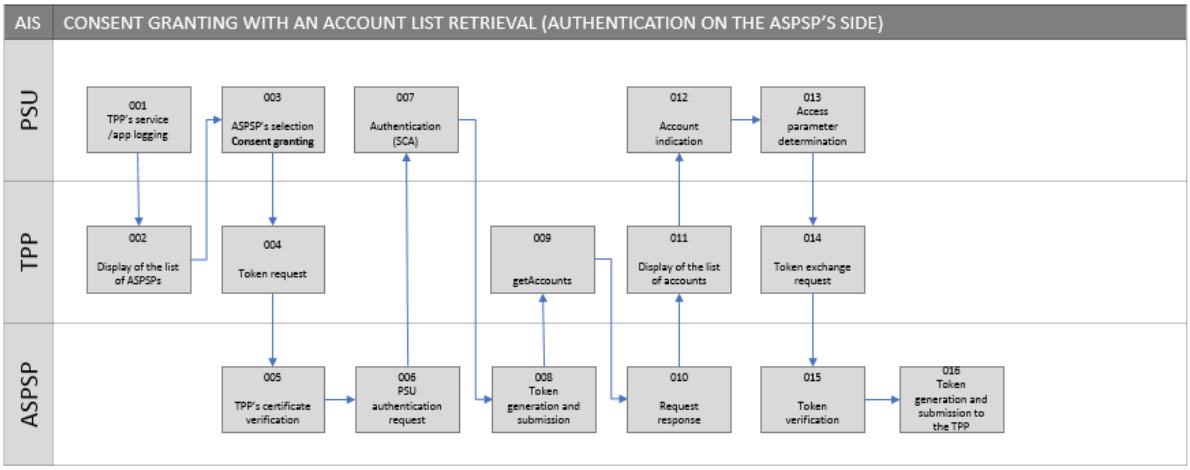


Figure 8: AIS. Grant of consent with an account list retrieval (authentication on the ASPSP's side)

1.4.4.2.4 Grant of consent with an account list retrieval in case of authentication in an external authorization tool

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays the list of ASPSPs
- 003 / PSU selects an ASPSP from the list and grants a consent to the given TPP to provide the account information service concerning an account maintained by the given ASPSP
- 004 / TPP sends a token request to the ASPSP
- 005 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 006 / ASPSP initiates the process of PSU's authentication
- 007 / TPP transfers the authentication request to the PSU
- 008 / SCA authentication in an external authorisation tool (cf. item 1.4.3.2)
- 009 / ASPSP transfers the access token to the TPP
- 010 / TPP sends a request to the ASPSP for a transfer of the PSU's account list (together with an access token)
- 011 / ASPSP gives the TPP a list of PSU's accounts (a full or a partially masked account number + product name + account type)
- 012 / TPP displays a list of accounts
- 013 / PSU indicates an account (or accounts) in order to determine the scope of access
- 014 / PSU determines the access parameters
- 015 / TPP sends a token exchange request to the ASPSP (for a token containing access details)
- 016 / ASPSP verifies the identity of the TPP and the PSU (on the basis of the first access token)
- 017 / ASPSP gives the TPP a new access token (containing information about the scope of access), in case of AIS a multiple one with a refresh token

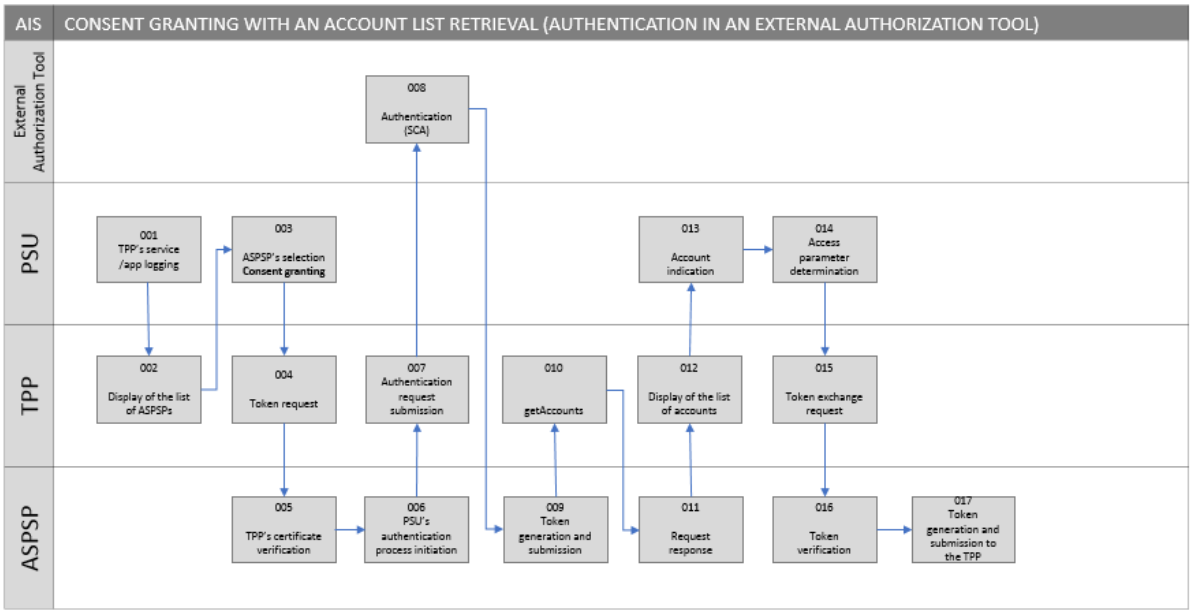


Figure 9: AIS. Grant of consent with an account list retrieval (authentication in an external authorization tool)

1.4.4.2.5 Access parameter edition

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays a list of consents
- 003 / PSU selects a specific consent from the list of consents within the framework of which the changes will be made
- 004 / PSU introduces the changes within the framework of the consent (edits the access parameters)
- 005 / TPP sends a token exchange request to the ASPSP
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP verifies the token related to the consent
- 008 / ASPSP generates an access token and transfers it to the TPP

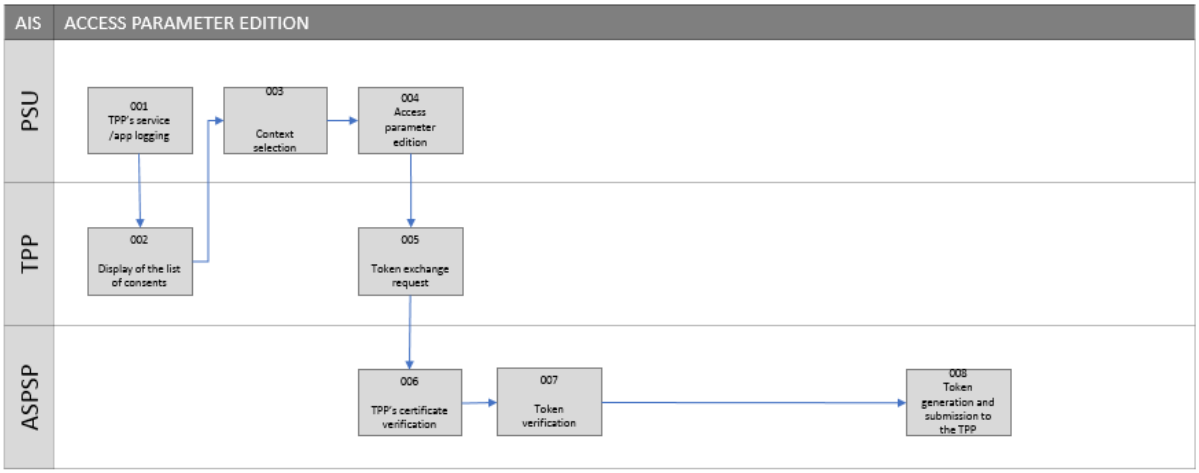


Figure 10: AIS. Access parameter edition

1.4.4.2.6 Withdrawal of consent

- 001 / PSU initiates the process in the TPP's interface
- 002 / TPP displays a list of consents
- 003 / PSU selects a specific consent from the list of consents within the framework of which the changes will be made
- 004 / PSU withdraws the consent for the AIS service
- 005 / TPP sends a token revocation request to the ASPSP
- 006 / ASPSP verifies the TPP's identify on the basis of a certificate (or also on the basis of the register of TPPs)
- 007 / ASPSP invalidates the token related to the consent

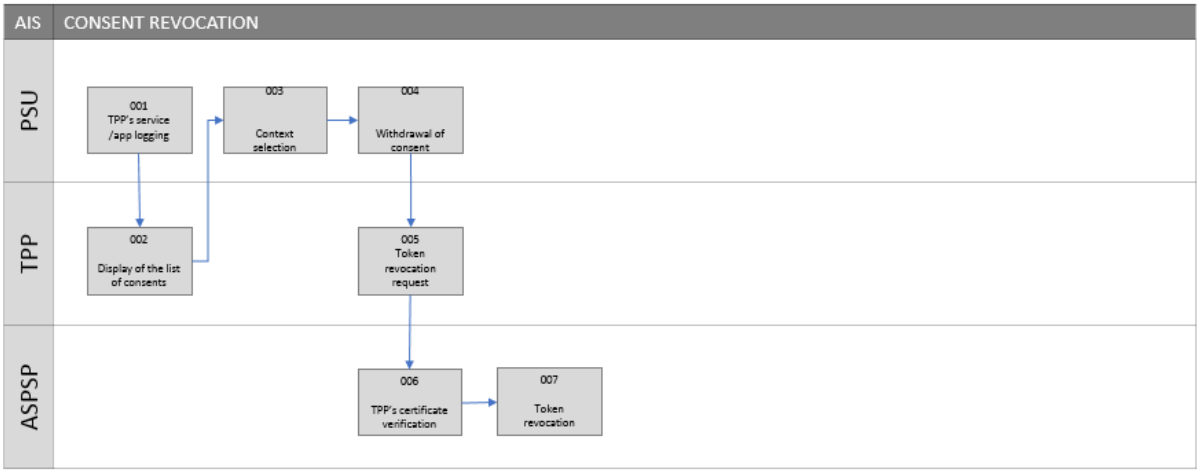


Figure 11: AIS. Withdrawal of consent

1.4.4.3 Process of Granting Consent by PSU to Effect the CAF Service

The process of the PSU's granting a consent for the ASPSP to effect the CAF service will be developed in the next version of this document. For the purposes of the current version, it is assumed that the request within the CAF service is made exclusively in the situation when the consent has been made previously.

1.4.5 Application of the Strong Customer Authentication (SCA) Mechanism

ASPSPs use any given strong PSU authentication system (SCA) they selected and the PolishAPI standard does not define and does not recommend any way in which this procedure may be conducted. Furthermore, the decision to release a given transaction from the SCA procedure remains in the exclusive competence of the ASPSP.

1.4.6 Provision of Services within the Compliance Scope

Each ASPSP is obliged to make available the services from the Compliance Scope pursuant to PSD2 and the 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.

1.4.7 Provision of Services within the Premium Scope

Each ASPSP takes the decisions on making available the services within the Premium Scope and, in case of a decision to start offering them, determines the extent of such services independently. The performance of services within the Premium Scope will not require a contractual relation between the ASPSP and the TPP.

1.5 Development of the PolishAPI Standard

Currently, the PolishAPI standard defines the Compliance Scope of the AIS, PIS and CAF services. A permanent development of the standard in response to regulatory, technological and business changes on the Polish and European market is assumed. The changes will be published as subsequent versions of the PolishAPI standard specification.

2 Glossary of Terms used in the Document

Account Information Service (AIS) – as defined in Art. 66 of PSD2.

Account Information Service Provider (AISP) – TPPs using the XS2A interface to access information about the PSU's payment account.

Confirmation of the Availability of Funds (CAF) – a service defined in Art. 65 of PSD2.

European Banking Authority (EBA) – the European Banking Authority.

ETSI – European Telecommunication Standardisation Institute.

OAuth2 – Oauth2 is an open authorisation standard. It allows users to share their private resources (e.g. pictures, films, contacts) stored at a given site with another party without a necessity to fathom the complexities of authorisation, usually providing the user name and a token (one-time passwords).

Payment Initiation Service Provider (PISP) – TPPs using the XS2A interface to initiate the a payment transaction debited to the PSU's account.

Payment Initiation Services (PIS) – as defined in Art. 67 of PSD2.

Payment Instrument Issuer Service Provider (PIISP) – TPPs using the XS2A interface to confirm the availability at the PSU's payment account of an amount necessary to effect the payment transaction performed on the basis of an instrument issued by the PIISP.

Payment Services Directive (PSD) – Directive 2007/64/EC of the European Parliament and of the Council on payment services in the internal market.

Payment Services Directive 2 (PSD2) – Directive 2015/2366 of the European Parliament and of the Council on payment services in the internal market and repealing Directive 2007/64/EC.

Payment Services User (PSU) – natural or legal person making use of a payment service in the capacity of either payer or payee, or both.

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

Regulatory Technical Standard (RTS) – Commission Delegated Regulation (EU) No. 2018/389 of 27 November 2017 supplementing Directive (EU) 2015/2366 of the European Parliament and of the Council with regard to regulatory technical standards for strong customer authentication and common and secure open standards of communication.

Revised Payment Services Directive (PSD2) – Directive (EU) 2015/2366 of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (revised payment services directive).

Strong Customer Authentication (SCA) - means an authentication based on the use of two or more elements (components) categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.

Swagger – is an open source software which helps design, build, document and consume the RESTful Web services.

TS 119 495 – draft (v. 0.0.3) of a technical specification of the standard concerning the qualified certificate profile for the needs of the Payment Services Directive (Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificate Profiles and TSP Policy Requirements under the Payment Services Directive 2015/2366/EU), published in January 2018.

Granting Consent – a process in result of which the PSU grants TPP consent to access his/her account held by the ASPSP in order to effect a service, including the AIS, PIS and CAF services.

Authentication – a process in result of which the ASPSP verifies the PSU's identity.

Payment Services Act – Polish Payment Services Act of 19 August 2011.

XS2A (Access to Account) – access to payment accounts used to perform AIS, PIS, CAF and other services effected as part of the PolishAPI.

Premium Scope of the AIS, PIS and CAF services **–** services exceeding the requirements laid down in PSD2.

Compliance Scope of the AIS, PIS and CAF services **–** services required by PSD2.

3 Business Definition of the Compliance Scope Services

3.1 Business Definition of the Compliance Scope for the PIS Service

The Payment transaction initiation service within the Compliance Scope consists in making available by the ASPSP of a possibility to initiate a payment from the payment account by the PSU via a TPP who acts as a PISP after obtaining prior consent from the PSU as appropriate.

3.1.1 Types of Transactions within the Compliance Scope

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:

a) The payment is a bank transfer
b) The payment is a single transfer
c) The payment is a transfer with the current date
d) The payment is a transfer made to an IBAN number (NRB number in case of ASPSPs operating in Poland), including a transfer to a Polish tax office
e) If it is a domestic transfer, it is settled using one of the following systems (depending on which of the systems is supported by the ASPSP):
    a. Elixir,
    b. Express Elixir,
    c. SORBNET2,
    d. Blue Cash.
f) If the payment is a foreign transfer, it is settled in one of the systems listed below:
    a. SWIFT
    b. SEPA
    c. TARGET
g) It is available in the online interface of the given ASPSP
h) The PSU will complete all the data required to order a transfer (the ASPSP will not provide support in the form of dictionaries, dropdown lists or other creators) or in case of the process described in item 1.4.4.1.1 all the data save the number of the account from which the payment will be initiated.

The data given by the TPP in the transfer order should not be modified by the PSU in the ASPSP's domain. Each ASPSP is obliged to make available the services from the Compliance Scope pursuant to PSD2 and the 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.

3.1.2 Information about the Transaction Status

As part of the message exchange in the PIS service within the Compliance Scope, the ASPSP will immediately advise the TPP about the order acceptance or rejection. Additionally, the TPP will be able to retrieve information about the payment status using the getPayment method with an option to enquire about the status of many payments (getMultiplePayments), provided the ASPSP offers such a functionality. The ASPSP will have an optional possibility to transfer to the TPP (asynchronous) information about the payment status using the /v1.0/accounts/v1.0/paymentCallBack method.

The following statuses are defined:

a) Submitted
b) Pending
c) Rejected

d) Done

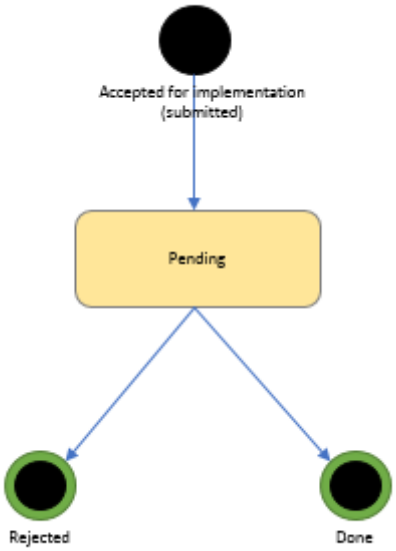


Figure 12: Diagram of payment statuses

3.1.3 List of Fields Required by the ASPSP in the Compliance Scope

In order to initiate the PIS service payment transaction within the Compliance Scope correctly, the ASPSP may request from the PSU, via the TPP (PISP), that the following fields be completed with transaction order data. Each ASPSP may expect the PSU to transfer another set of data via the TPP.

With reference to foreign transfers, the use of particular fields will be optional, depending on the functionalities supported by the given ASPSPs. The ASPSP will effect the payments on condition that the payment will be initiated as appropriate by the TPP, i.e. appropriate fields with appropriate content are submitted.

Mandatory fields defining the TPP:

a) TPP's name

3.1.3.1 National transfer

FIELD NAME	COMMENTS
Address of the transfer payee	
Order date	
Effective date of the transfer	
Transfer amount	
Name of the transfer sender	Sender's name completed by the ASPSP in order to avoid a situation when the transfer order coming from the ASPSP contains data other than data of the holder of the account debited.
Name of the transfer payee	

Transfer sender's account number	It may be specified by the TPP, however the PSU should have an option to select the account to be debited after redirection to the ASPSP.
Transfer payee's account number	
Transfer description field	
Urgency mode	ExpressD0, StandardD1
Transfer type (system)	In case of a domestic transfer: Elixir, ExpressElixir, Sorbnet, BlueCash, Internal
Currency	In case the field is empty, the ASPSP will make the transfer in the account currency.
Hold	Bool type field (default value false), owing to which the client will be able to make an explicit wish to make a block (in case of, e.g. a payment order on a free day)

3.1.3.2 Domestic transfers to tax authorities / customs authorities in Poland

FIELD NAME	COMMENTS
Address of the transfer payee	
Data of the authorities	
Order date	
Effective date of the transfer	
Payer's ID	
Liability ID	
Transfer amount	
Name of payer	Sender's name completed by the ASPSP in order to avoid a situation when the transfer order coming from the ASPSP contains data other than data of the holder of the account debited.
Period number	
Transfer sender's account number	It may be specified by the TPP, however the PSU should have an option to select the account to be debited after redirection to the ASPSP.
Transfer payee's account number	
Form symbol	
Period type	
Transfer type	Constant value – transfer to the tax office
Urgency mode	ExpressD0, StandardD1
Transfer execution mode (system)	Standard (Elixir), express (ExpressElixir)
Currency	
Hold	Bool type field (default value false), owing to which the client will be able to make an explicit wish to make a block (in case of, e.g. a payment order on a free day)

3.1.3.3 EEA foreign transfer

FIELD NAME	COMMENTS
Address of the transfer payee	
Transfer amount	
Name of the payee's bank	
Name of the transfer sender	Sender's name completed by the ASPSP in order to avoid a situation when the transfer order coming from the ASPSP contains data other than data of the holder of the account debited.
Name of the transfer payee	
Transfer sender's account number	It may be specified by the TPP, however the PSU should have an option to select the account to be debited after redirection to the ASPSP.
Transfer payee's account number	
Transfer description field	
Residence status	
Transfer execution mode	Standard, express
Transfer type (system)	SEPA, Instant SEPA, Target
Currency	Constant value - EUR
Hold	Bool type field (default value false), owing to which the client will be able to make an explicit wish to make a block (in case of, e.g. a payment order on a free day)

3.1.3.4 Foreign transfer other than EEA

FIELD NAME	COMMENTS
Transfer sender's account number	Sender's name completed by the ASPSP in order to avoid a situation when the transfer order coming from the ASPSP contains data other than data of the holder of the account debited.
Transfer payee's account number	
Name of the transfer sender	Sender's name completed by the ASPSP in order to avoid a situation when the transfer order coming from the ASPSP contains data other than data of the holder of the account debited.
Name of the transfer payee	
Address of the transfer payee	
Transfer description field	
Transfer amount	
Currency	
BIC/SWIFT of the payee's bank	
Country of the payee's bank	
Name of the payee's bank	

Address of the payee's bank	
Residence status	
Cost clause	
Transfer execution mode	Standard, urgent, express
Transfer type (system)	SWIFT
Hold	Bool type field (default value false), owing to which the client will be able to make an explicit wish to make a block (in case of, e.g. a payment order on a free day)

3.1.4 Diagrams of Requests under the PIS Service within the Compliance Scope

The diagram was presented in Use Case #1 in Chapter 4.

3.1.5 Authorisation of a payment transaction initiated by means of a PIS service

The ASPSP provides a possibility to authorise a payment transaction ordered by the PSU under a payment initiation service within the understanding of the Payment Services Act (PSA), irrespective of the authorisation method and its complexity. The authorisation method is selected by the ASPSP.

3.2 Business Definition of the Compliance Scope for the AIS Service

The account information service within the Compliance Scope consists in making available by the ASPSP of data concerning the transaction history and selected information about the payment account to which the PSU has an active on-line access. The access is granted to a TPP acting as an AISP after a prior acquisition of consent as appropriate from the PSU. 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) The transaction booking date (as per the indicated specific booking date and within the specified range of dates)
b) The transaction amount
c) The payment account debits and credits

3.2.1 Definition of a Payment Account

This service is provided only for payment accounts to which the given PSU has an on-line access. The account must meet all of the following cumulative conditions:

a) It is an account held for one or more users which is used to effect payment transactions (as per the definition laid down in the PSA)
b) The PSU has an on-line access to the account

3.2.2 Frequency of Requests within the Compliance Scope

As part of the AIS service within the Compliance Scope, the TPP (AISP) may request that the ASPSP sent a payment account history and selected information about the payment account:

a) Up to 4 times within a 24 hour time span from the first request in case when the data collection is not initiated at the PSU's request via the TPP (AISP), but by TPP (AISP) on the basis of consent provided earlier by the PSU;
b) In each instance when the request is initiated directly by PSU via the intermediation of the TPP (AISP).

A higher frequency of requests in case when the data collection is not initiated at the PSU's request via the TPP (AISP) but by the TPP (AISP) on basis of consent expressed earlier by the PSU may be allowed with regard to the AIS service only in the Premium Scope and is subject to separate bilateral arrangements by and between the ASPSP and the TPP (AISP).

3.2.3 Scope of Information concerning the Payment Account History within the Compliance Scope

Within the Compliance Scope, the AIS service comprises the provision to the PSU, together with data filtering mechanisms (including transaction history date scopes), of all available on-line account history of transactions booked, pending and rejected at the given payment account and blocked funds, which are visible to the PSU in the APSPS's on-line channel. Whereby, a pending transaction means a transaction that is not booked, not modifiable and which influences the available funds (available balance).

3.2.4 List of Fields Required by the ASPSP in the Compliance Scope

In response to the request sent by the TPP (AISP), the ASPSP sends information from the following fields.

FIELD NAME	COMMENT
Account number	Account number
Account currency	For each payment account
Given names and surname / Name and address of the PSU	Given name for a natural person and a business name for a legal person
Available funds	Funds available in the account currency - after the transaction
Transaction identifier	Unique identifier of the given transaction as assigned by the ASPSP
Amount in original currency	For each account history transaction
Book balance of the account	Book balance of the account - after the transaction
Account type	E.g. account for the consumer / business account + product reference, e.g. account, credit card, savings account, etc.
Transaction date	For each account history transaction
Amount	For each account history transaction
Sender's account number	For each account history transaction
Payee's account number	For each account history transaction
Description	For each account history transaction
Title	For each account history transaction
Transaction status	For each account history transaction
Transaction type	Credit/debit transaction. For each account history transaction
Currency of original transaction	For each account history transaction
Account type name (defined by the ASPSP)	Product's commercial name
Data of the tax office	Only for transfers to tax authorities / customs authorities in Poland
Book date	For each account history transaction
Exchange rate date	For each account history transaction
TPP's Transaction ID	Unique ID of the given transaction as assigned by the TPP
Payer's ID	Only for transfers to tax authorities / customs authorities in Poland
Liability ID	Only for transfers to tax authorities / customs authorities in Poland
Transaction exchange rate	For each account history transaction
Period number	Only for transfers to tax authorities / customs authorities in Poland
Payee's account virtual number	For each account history transaction
Year	Only for transfers to tax authorities / customs authorities in Poland

Form symbol	Only for transfers to tax authorities / customs authorities in Poland
Period type	Only for transfers to tax authorities / customs authorities in Poland
Payment type	Only for transfers to tax authorities / customs authorities in Poland
Unique ID of the payment instrument by which the transaction was effected	E.g. payment card number (masked, as per the data presentation in the ASPSP's online interface)
Type of operation	For each account history transaction
Account balance after the transaction	For each account history transaction
Payment ID type	Only for transfers to tax authorities / customs authorities in Poland
Name and address of the incoming transfer payee	For each incoming transfer transaction at the account history
Name and address of the outgoing transfer payee	For each outgoing transfer transaction at the account history
Address of the payee's bank	For foreign transfers only
Code of the payee's bank	For foreign transfers only
Name of the payee's bank	For foreign transfers only
BIC/SWIFT of the payee's bank	For foreign transfers only
Name and address of the incoming transfer sender	For each incoming transfer transaction at the account history
Name and address of the outgoing transfer sender	For each outgoing transfer transaction at the account history
Account name as defined by the client	Provided the Bank makes available such a service
Transaction originator	In case of transactions originated by people other than the account holder (given name and surname)
TPP's name	In case of transactions initiated as part of the PIS service
MCC	Code for each transaction / operation made using the card

The fields described in the table above 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). To the scope of data concerning the account and transactions, each ASPSP may add additional fields, taking advantage for this purpose of the auxData type Map field within the AccountInfo, TransactionInfo, TransactionHoldInfo, TransactionPendingInfo and TransactionRejectedInfo structures.

The list of fields made available when the ASPSP allows the use of the account list retrieval within the process of granting consent for the AIS or PIS services.

FIELD NAME	**COMMENT**
Account number	Account number in a masked form, only the 2 first and last 4 digits of the account number visible without masking, according to the ASPSP's decision
Account type name (defined by the Bank)	Product's commercial name
Account type	E.g. account for the consumer / business account + product reference, e.g. account, credit card, savings account, etc.

3.2.5 Diagrams of Requests under the AIS Service within the Compliance Scope

The diagram was presented in Use Case #2 in Chapter 4.

3.3 Business Definition of the Compliance Scope for the CAF Service

The service of confirmation of funds at the payer's payment account in an amount sufficient to effect the payment transaction within the Compliance Scope consists in sending a request by the TPP acting

as a PIISP to the ASPSP for a confirmation whether or not the PSU's payment account has funds in the amount as determined in the request on the basis of consent granted earlier by the PSU. In response, the ASPSP sends a message in the form of 'YES' or 'NO'.

3.3.1 List of Fields Required by the ASPSP in the Compliance Scope

In order to support a request concerning a conformation of funds at the payer's payment account in an amount sufficient to effect a CAF payment transaction within the Compliance Scope correctly, the ASPSP may request from the PSU, via the TPP (PIISP), that the following fields be completed with transaction order data. Details concerning the fields are defined in Chapter 5.7 Canonical Data Model.

FIELD NAME	REQUIRED	COMMENTS
Identifier of account the request concerns	X	Account previously connected with the payment instrument on the basis of consent granted by the PSU.
Amount	X	
Currency	X	Currency of transaction

3.3.2 Diagrams of Requests under the CAF Service within the Compliance Scope

The diagram was presented in Use Case #3 in Chapter 4.

4 Sample Use Cases

The current PolishAPI standard version described the manner of performance of XS2A interface-based transactions within the Compliance Scope as defined in Chapter 3 hereof and the TPP may participate in such transactions in one of the roles defined.

Examples illustrating the use of particular services were presented in this chapter. Their aim is only to illustrate the steps for particular services and should not be treated as an exhaustive list of admissible use cases.

4.1 Use Case #1: initiation of a single payment by the PISP (PIS)

The use of a PIS service within the Compliance Scope as presented in this Use Case consists in the initiation by the TPP acting as a PISP of a payment transaction debited to the PSU's payment account held by the ASPSP on the basis of applicable provisions of the Payment Services Act. The ASPSP may reject the transaction if the TPP (PISP) has not been identified as an entity authorised to effect a PIS service.

4.1.1 Single payment initiation by the PISP using a mechanism of ASPSP-side authentication

The diagram below concerns the processes described in Chapter 1.4.4.1.1 (Process of Granting Consent by PSU to Effect the PIS Service – Authentication on the ASPSP's Side) and 3.1.2 (Information about the Transaction Status).

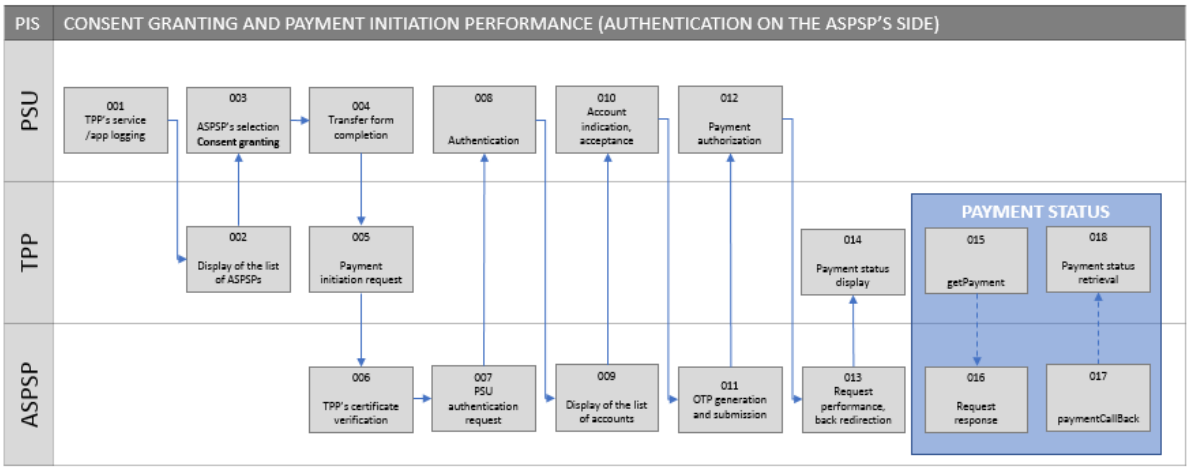


Figure 13: PIS / Grant of consent and performance of payment initiation and payment status retrieval

4.1.2 Single payment initiation by the PISP using an authentication mechanism in an external authorization tool

The diagram below concerns the processes described in Chapter 1.4.4.1.2 (Process of Granting Consent by PSU to Effect the PIS Service – Authentication in An External Authorization Tool) and 3.1.2 (Information about the Transaction Status).

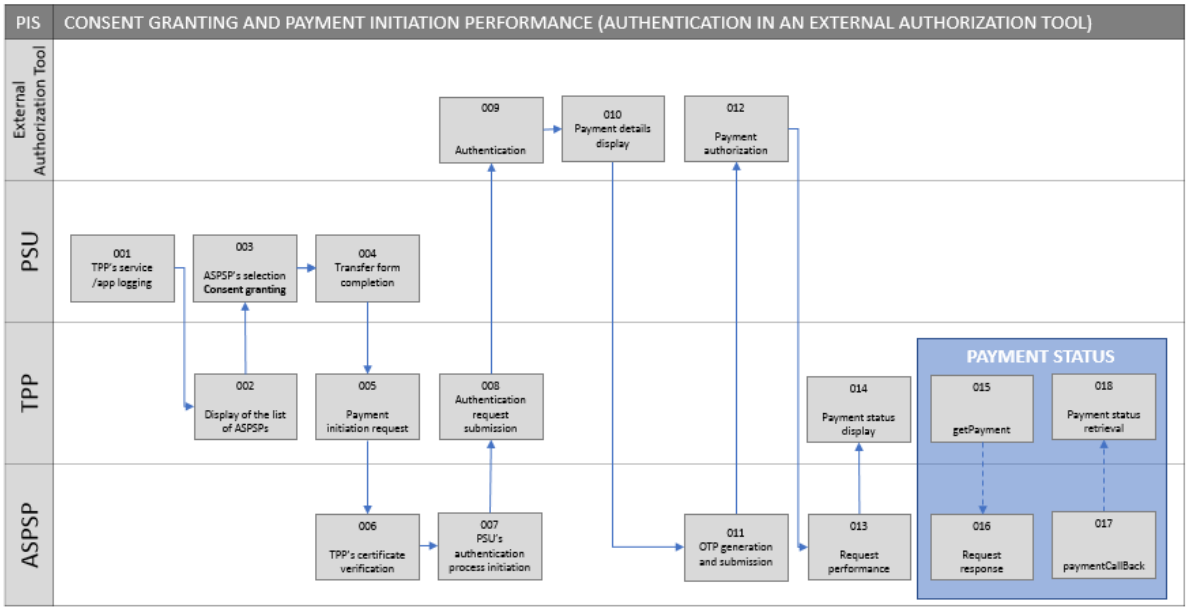


Figure 14: PIS / Grant of consent and performance of payment initiation (authentication in an external authorization tool) and payment status retrieval

4.2 Use Case #2: payment account information display by the AISP (AIS)

The use of an AIS service within the Compliance Scope as presented in this Use Case consists in the acquisition by the TPP acting as an AISP of information about the PSU's payment account held by the ASPSP on the basis of applicable provisions of the Payment Services Act.

The process of granting consent to use the AIS service has been described in Chapter 1.4.4.2. The Case described below assumes that the PSU granted AISP his/her consent to collect a defined scope of data. A request is initiated by the AISP on behalf of the PSU.

This process has been presented at a high level in the diagram below.

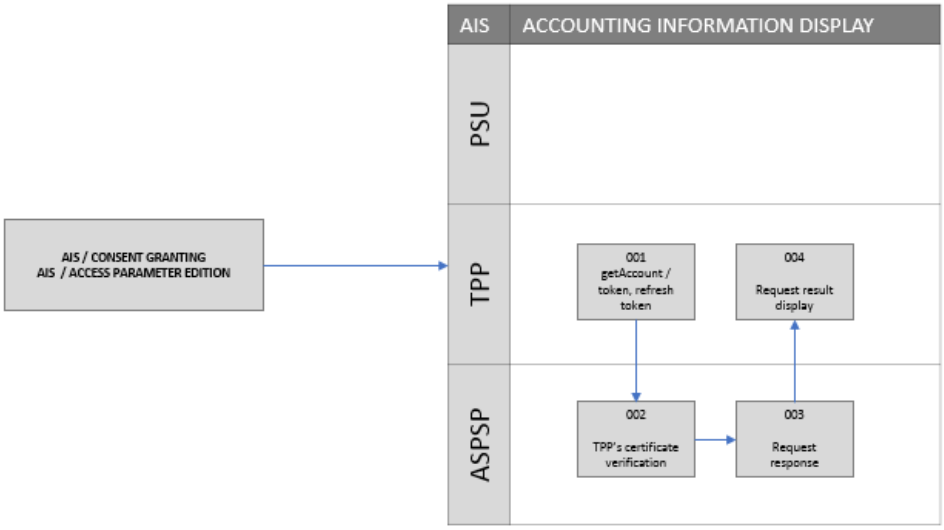


Figure 15: AIS / Payment account information display by the AISP

4.3 Use Case #3: request for confirmation of funds by a PIISP (CAF)

The use of an CAF service within the Compliance Scope as presented in this Use Case consists in the initiation by the TPP acting as an PIISP of a request for availability of funds in the transaction amount at the PSU's payment account on the basis of applicable provisions of the Payment Services Act.

The PSU must previously indicate to the PIISP a payment account that will be verified in each case in terms of funds availability and grants his/her consent for the ASPSP holding the given payment account to answer such requests. The PSU initiates a business process requiring a verification whether or not the payment account previously indicated by the PSU has funds available in the amount equal at least to the requested amount. In order to effect the service, the PIISP establishes an XS2A session with ASPSP, sends a request and receives a 'YES' or 'NO' answer.

This process has been presented at a high level in the diagram below.

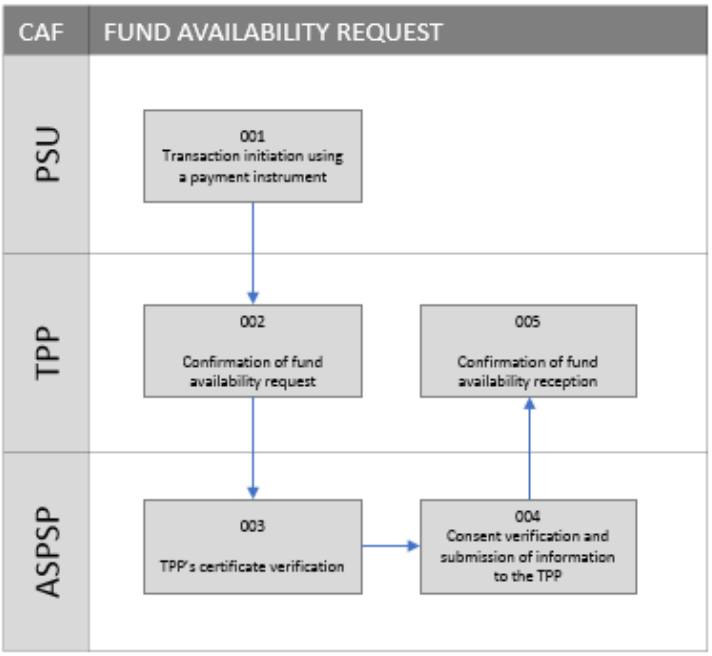


Figure 16: Figure 16: CAF / Request for confirmation of funds

This process may be used to, for example, authorise a transaction effected by payment instruments not linked to the payment account held by the instrument issuer.

5 PolishAPI Technical Specification

5.1 Technical Assumptions

The table below presents the technical assumptions made for the PolishAPI:

No.	Assumption	Description	Justification
1	Direct TPP-ASPSP communication	In the basic variant of the PolishAPI the TPP and the ASPSP communicate with each other directly.	The peer-to-peer architecture used increases the safety and efficiency as well as allows the avoidance of a single point of failure.
2	Role of the PSD2 HUB	In case the ASPSP uses the services of a PSD2 HUB, it is neutral for the TPP. The PSD2 HUB presents itself using the ASPSP's certificate, from the TPP's perspective, there is no difference whether it gets connected with the PSD2 HUB or directly with the ASPSP.	Efficient and Safe API and PolishAPI Standard Implementation.
3	The TPP-ASPSP communication is a server-server one	No direct communication of the client's device (e.g. a mobile app) with the ASPSP's PolishAPI servers is allowed. The TPP should be legally obliged to secure the access keys (so-called access certificate). In particular, the access certificates may not be installed in mobile apps made available to the PSUs)	
4	Separation of the client's consent step from the operation performance step	The client's consent for the service step will be effected using the OAuth2 standard and will be separate from the performance of the operation itself. One of the effects will be the fact that the consent in itself will not entail any financial consequences.	Flexibility in the implementation of new services, including the Premium Services.
5	Scope of the PolishAPI	The scope of the PolishAPI specifies the following: - way of granting consent for the performance by the TPP of an operation on behalf of the customer - scope of operations and rights - URL where the given service is available - standard scope of parameters per service - security mechanisms - communication principles - error handling The PolishAPI does not specify the following	The RTS make the scope of functionality and the scope of data dependent on the scope of functionality made available in the Internet banking, which is different for each ASPSP

		- full scope of functionalities to be made available by the ASPSP as well as the information as to which ones of them will not be within the Compliance Service - full specification of fields per service for each ASPSP	

5.2 XS2A Session Establishment

The XS2A communications session comprises enquiries and answers in the communication between the TPP and the ASPSP as part of the operations under the account information service, the payment initiation service and the request concerning available funds service made after the TPP has been identified. In particular, it may comprise the authentication by the PSU during that session.

The XS2A sessions established between a TPP and an ASPSP must meet the following conditions without limitation:

a) 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 – within the understanding of Art. 4 of the RTS, which shall be changed at the next step into a proper access token in accordance with the OAuth 2.0 protocol.
b) The state parameter must be unique for each authorisation process effected by the given TPP
c) It is suggested that the authorisation code on the ASPSP's server side and the access token were the object ID 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
d) Together with the access token, also the scope parameter is transferred to the TPP (the same as in the request or limited by the user during the authorisation)
e) The PSU's authentication may take place in accordance with the methods listed in Chapter 1.4.3. of this document

The diagram of the XS2A session establishment process flow is presented below.

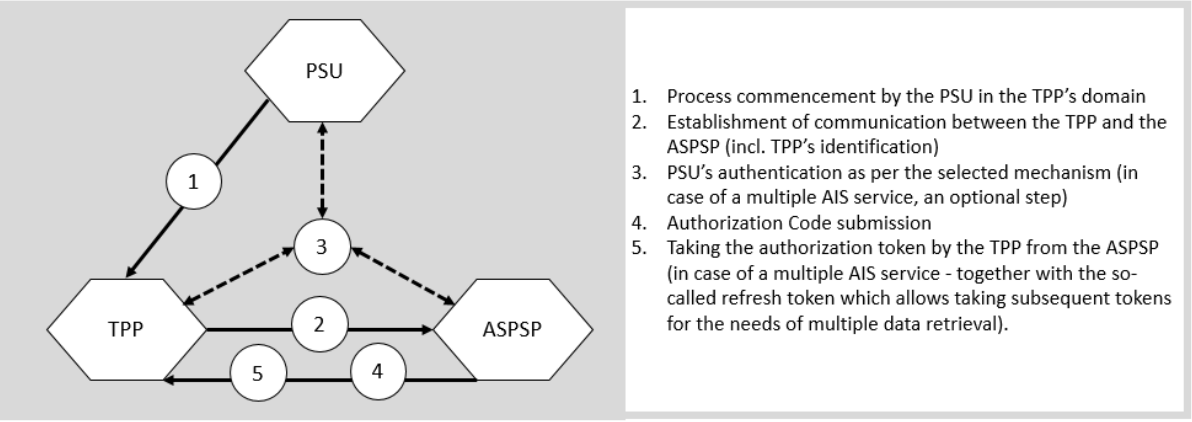


Figure 17: Multilayer XS2A session establishment diagram

Each transaction under the AIS, PIS and CAF service should be effected as part of a dedicated separate XS2A communications session, whereby for the AIS service it is admissible to use the same session for

a higher number of AIS operations maintaining the downtime time, after the expiration of which the PSU will be automatically logged out and the session will be terminated.

5.3 Definitions of token

For the AIS service:

Token – allows a multiple AIS calling for a maximum period of 90 days as per Article 10 of the RTS,

Refresh token – allows a new token taking (as per the OAuth 2.0 Authorization Framework, 1.5 Refresh token: https://tools.ietf.org/html/rfc6749#page-10).

For the PIS service:

Token – [in the authentication mechanism on the ASPSP's side] allows one-time calling of the initiation service and multiple calling of the service requesting a payment status for a period of time as defined by the ASPSP (e.g. 3 days). The token is invalidated upon the return of an irreversible payment status of 'done' or "rejected'. The above assumption is independent from the user (PSU) authorisation and authentication model, a one-time consent means a one-time transfer and the token will allow payment status requests for a defined period of time. The payment initiation option by calling dedicated services will be allowed for in the token definition after PSU authentication mechanisms other than on the ASPSP's side are supplemented in subsequent versions of the specification.

5.4 Mutual Authentication of the TPP and the ASPSP

The mutual authentication of the TPP and the ASPSP takes place on the basis of the X.509v3 certificates issued by a trusted third party. A trusted third party may by, in particular, an institution performing the role of the Identity Hub. It may also be any other party offering a trust-based relationship based on public key infrastructure mechanisms.

All operations consisting in the flows specified and described in the standard are possible only in a situation of a correct authentication in a process that comprises a mutual authentication of the server and the client (mutual authentication).

A description of the public key infrastructure used for the needs of authentication of parties (TPP, ASPSP, PISP) is not a part of the PolishAPI standard. It should be described in separate documents (working standards), taking into account the structure of trust relation between the certification institutions and the interoperability of the PolishAPI with other solutions of this type in place in other countries.

5.5 Communication Protocol

HTTP /2 or HTTP 1.1, secured by SSL/TLS (version) with certificate-based client authentication (Mutual authentication) will be used as the communication protocol. Due to the requirement to ensure non-repudiation (request and response signing), only the POST method will be used in the http communication.

5.6 Resource Name Diagram

The PolishAPI services will be made available under addresses compliant with the following model:

```
https://{DNS domain}/{v{Resource version number 1}/{Resource name 1}}/.../v{Resource version number n}/{Resource name n}
```


Field description:

a) DNS domain/address – where the ASPSP makes the PolishAPI services available (information made available in the PSD2 register)
b) Resource version number – number of the version according to PolishAPI specification (digit before the dot) and subsequent interface number within the given ASPSP (digit after the dot)
c) Resource name – number of the resource the request concerns; resources nesting routes, e.g. /v{version number of resource accounts}/accounts/v{number version of resource transactionsDone}/transactionsDone

5.7 Canonical Data Model

In order to unify the data types, a canonical data model was proposed as presented in the table below. A detailed model definition is given in Annex No. 1. The model documentation is provided in Annex No. 2.

Class Name	Designation
AccountIban	Account no
AccountInfo	Class of information about the account
AccountInfoRequest	Class of request concerning a single account
AccountResponse	Class of response to a request concerning the PSU's account
AccountsRequest	Class of request concerning accounts
AccountsResponse	Class of response to a request concerning many PSU's accounts
Address	Class containing data of a postal address
Bank	Class containing bank's data
BankAIS	Class containing bank's data used in AIS requests
ConfirmationOfFundsRequest	Class of request concerning the available funds at the account
ConfirmationOfFundsResponse	Class of response to a request concerning the available funds at the account
Error	Class of information containing data about the error returned
Map	Class of map <string, string>
NameAddress	Class containing the data of the name and address in the form of four data lines
PageInfo	Class containing data allowing the use of the paging mechanism
PaymentAddResponse	Class of response to the payment order
PaymentDomestic	Auxiliary class of standard domestic transfer
PaymentExpressDomesticAddRequest	Class of express domestic transfer
PaymentInfo	Class of information about the payment
PaymentRequest	Class of request concerning the payment status
PaymentResponse	Class of response to the payment request
PaymentStandardDomesticAddRequest	Class of request of a standard domestic transfer
PaymentStandardEEAAddRequest	Class of request of a SEPA foreign transfer
PaymentStandardNonEEAAddRequest	Class of request of a foreign transfer other than SEPA
PaymentStatus	Dictionary of payment statuses
PaymentTaxAddRequest	Class of request of a tax transfer
PaymentsRequest	Class of request concerning multiple payment status
PaymentsResponse	Class of response to a request concerning multiple payments
Payor	Class of information about the payer to the Social Insurance

	Institution (ZUS) and Tax Office
RecipientAIS	Class containing recipient's data used in AIS requests
RecipientPIS	Class containing recipient's data used in PIS requests
RecipientPISTax	Class containing recipient's data used in PIS requests for tax operations
RequestHeader	Class containing information about the PSU
ResponseAsync	Class of response to an asynchronous request
ResponseHeader	Class containing return metadata
SenderAIS	Class containing sender's data used in AIS requests
SenderPIS	Class containing sender's data used in PIS requests
TransactionDetailRequest	Class of request concerning a single transaction
TransactionDetailResponse	Class of response to a single transaction request
TransactionDoneInfoResponse	Class of response containing a list of transactions done
TransactionHoldInfoResponse	Class of response containing a list of transactions
TransactionInfo	Class describing the payment transaction booked
TransactionInfoBase	Base class describing a payment transaction
TransactionInfoCard	Class representing information about the card within the framework of a transaction
TransactionInfoRequest	Class of a request concerning transactions
TransactionInfoRequestBase	Base class for requests concerning transactions
TransactionInfoTax	Class of information given for a transfer to a tax office / customs authorities
TransactionInfoZUS	Class of information given for a transfer to the Social Insurance Institution (ZUS)
TransactionPendingInfo	Class describing the pending payment transaction
TransactionPendingInfoResponse	Class of response containing a list of pending transactions
TransactionRejectedInfo	Class describing a rejected payment transaction
TransactionRejectedInfoResponse	Class of response containing a list of rejected transactions
TransferData	Class containing transfer data

Pending transaction – a transaction that is not done (booked), not modifiable and which influences the available funds (available balance).

5.8 Operations

Due to the requirement to ensure non-repudiation in the http communication, only the POST method will be used as it allows the JWS Signature format signature. Within the operation, the context of a specific user is determined on the basis of an access token.

5.9 Sorting

The records returned are sorted chronologically (on a reversed basis).

5.10 Filtering

Filtering in the AIS service takes place after setting the appropriate properties in the TransactionInfoRequest class object:

a) transactionIdFrom -Transactions from the given transaction ID 'chronologically'

b) transactionDateFrom – initial transaction date of the data range requested
c) transactionDateTo – final transaction date of the data range requested
d) bookingDateFrom – initial booking date of the data range requested
e) bookingDateTo – final booking date of the data range requested
f) type – CREDIT or DEBIT
g) minAmount – minimum operation amount within the data range requested
h) maxAmount – maximum operation amount within the data range requested

5.11 Paging

Results of requests containing many records (where many is > 100) should be paged. Subsequent pages will be retrieved by setting the pageId attribute in the TransactionInfoRequest class. The pageId attribute should be set to the value returned in the PageInfo class of the previous request. Forward navigation - nextPage, backward navigation - previousPage. The number of records per page is defined by the perPage attribute in the TransactionInfoRequest class. The maximum settable value for the perPage parameter is suggested to be 100. Page numbers start from 1. Skipping the pageId parameter will return the first page.

5.12 Response Statuses

The technical statuses will be returned by the following http codes:

Status	Description
200 OK	The operation was successful
304 Not Modified	Used when the cache headers have been used
400 Bad Request	The request is syntactically incorrect
401 Unauthorized	Incorrectly authenticated user
403 Forbidden	Authorisation error (no rights to access the resource)
404 Not Found	Reference to a non-existing resource
405 Method Not Allowed	Use of an inappropriate method – the method used in the request is not allowed for the resource indicated (Only POST is used)
406 Not Acceptable	Incorrect Accept heading in the request (the server does not support it)
415 Unsupported Media Type	If an incorrect content type was set in the request
422 Unprocessable Entity	Validation error
429 Too Many Requests	Request rejected due to the fact that the maximum number of requests to access the resource has been exceeded

5.13 HTTP Headers

The following HTTP headers will be used in the requests:

Header	Type	Description
Authorization	String	Authentication header (used when sending a token). 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'.
Date	Date	Request timestamp in the RFC 5322 date and time format.
Accept	Content type	Should be set to application/json Otherwise the application should return 406 Not Acceptable HTTP.
Accept-Encoding	Gzip, deflate	The operation should support GZIP and DEFLATE coding, it may also return non-compressed data.

Accept-Language	'pl', 'en', etc.	Defined the preferred language in which the response is to be returned. The operation does not have to support this header
Accept-Charset	Charset type like 'UTF-8'	UTF-8
Content-Type	application/json	Should be set to application/json. Otherwise, the operation returns: 415 Unsupported Media Type HTTP status code
X-JWS-SIGNATURE	String	JWS Signature (Detached)

Response headers:

Header	Obligatory?	Description
Date	Yes	Timestamp on the basis of the GMT server time as per RFC 5322
Content-Type	Yes	application/json
Content-Encoding	Yes	GZIP or DEFLATE
Expires	No	Defines the cache policy for slowly varying objects e.g. Expires: Mon, 25 Jun 2012 21:31:12 GMT
Size	Yes	Response size in bytes
ETag	No	Resource version identifier
Last-Modified	No	Last resource modification date
X-JWS-SIGNATURE	Yes	JWS Signature (Detached)

5.14 Message format

The data exchange format will be JSON with the UTF-8 coding. All messages have a defined JSON schema draft #4. The parameter names will be saved camelCase.

5.15 Basic Data Formats

Format	JSON format	Description
Text	String	Text coded in UTF-8
Dates	String	Pursuant to ISO8601. Date and time will be represented in the form of YYYY-MM-DD to YYYY-MM-DDThh:mm:ss.ccczzzzzz with the mandatory specification of the time zone Designations: YYYY – year, MM – month, DD – day, hh – hour, mm – minute, ss – second, ccc – millisecond (optional) zzzzzz – e.g. +02:00 or Z to denote universal time For example: 2016-10-10T12:00:05.342+01:00
Amounts	String	Written as digits with a sign separating the integer part from the fractional part up to the second decimal place (the dot sign). In case of positive value, no additional signs are given. In case of negative value, the '-' sign is added before the number
Integer	Number	The integer numbers are represented without group separators
Real number	String	Real numbers are represented without group separators and with the '.' sign as a decimal separator
Country codes	String	In accordance with ISO 3166
Currencies	String	Currency symbols in accordance with ISO 4217
Account numbers	String	IBAN numbers in accordance with ISO 13616
Bank identifiers	String	Bank Identifier Codes (BIC) in accordance with ISO 9362

6 Security of information

This chapter presents general security requirements vital from the perspective of standard creation and its designing on the basis of the IT solution ecosystem compliant with the PolishAPI. Detailed security requirements comprising additionally the problems of security of PolishAPI-based system implementation, operation and maintenance will be described in a separate document and its development will be preceded by a preparation of a detailed risk model. In consequence, they will be an answer to specific identified threats, places where the threats may potentially materialise as well as the assessment of the level of materiality and probability and impact of the cases when such threats should materialise on the safety and operational continuity of the PolishAPI ecosystem.

Particular PolishAPI-based IT system components should have a clearly defined separation between the data layer, the controller's layer and the presentation layer. The components should be separated from each other by a defined security measures such as network segmentation or the firewall rules.

6.1 TPP's Authentication

Users must be properly authenticated before they are granted access to the API function so as to ensure a high level of protection both from an impersonation on the part of unauthorised users of lawful users and from an unauthorised escalation of the authorisation level by users having a legal access to the API. The authentication takes place on the basis of public key certificates during a TLS mutual authentication process (*server side* & *client side authentication*) via an https protocol.

Authentication errors must result on the denial of access to the API function.

The user and session authentication data as well as operation authentication tokens may not be transferred in the form of URI parameters.

6.2 TPP's Authorisation

The TPP's authorisation must be based on the RBAC model (*Role Based Access Control*), where the level and scope of access to particular API resources depends on the role of the PolishAPI user.

The use of particular methods must be authorised so that the rights depended on the user's role. In particular, the level and scope of authorisation should be different for TPPs depending on the scope of their rights.

6.3 PSU's Authorisation for Operations made by a TPP

Irrespective of the PSU's authentication mechanism applied within the AIS/PIS/CAF services, it is assumed that the process will end by the issue by ASPSP of an Access Token (RFC 6749 - 1.4. Access Token) and, optionally, a Refresh Token (RFC 6749 - 1.5. Refresh Token). The operations are always requested by the TPP via a valid Access Token

6.4 Security in case of Mobile Apps

For security reasons in a model using the authentication mechanism on the ASPSP's side, the redirection to the ASPSP's site and back to the TPP's site will take place in the browser (browsers other than the system browse will not be allowed, the application of the WebView will not be allowed) and

not in the mobile app itself. The TPP may register the appropriate URL in the device's operating system so that after the redirection back to the TPP the mobile app be automatically resumed.

6.5 Data Validation and Integrity Assurance

The data must be subject to validation procedures in the context of variable types, the scope and the model of limit values. In particular, the structured JSON data must be parsed in accordance with the formal validation procedures, using a white list-based approach. The validation must also be made with regard to the Content-type and Accept (application/json) headers for the compliance of the header value with the actual text of the HTTP message.

During the validation, the digital signature in the header (X-JWS-SIGNATURE) must be validated in the context of the data received in the request.

In case of Content-type and Accept text validation errors, http message 406 should be returned (Not Acceptable).

Input data validation errors must be registered in logs.

The validation errors must be signalled by the HTTP 400 message (Bad Request) and the data must be rejected.

Not validated or incorrectly validated data must be rejected.

6.6 Cryptography

The communication using the PolishAPI must ensure a cryptographic security at two levels:

a) At the level of transmission via (https/TLS). The TLS connection parameter renegotiation must be made in a secure way in accordance with RFC 5746
b) At the message level, to ensure the non-repudiation, it is obligatory to use JSON Web Signature (JWS https://tools.ietf.org/html/rfc7515) the signature reference must be in the X-JWS-SIGNATURE header

Each TPP must have its own unique two pairs of keys (for transmission and for signature).

Separate certificates must be used to secure the transaction at the https level and at the JWS-SIGNATURE level. For https, the certificate must have an expanded key use (Client Authentication) for signature (Digital signature).

The certificates used to combine the transmission and the signature must be validated in terms of:

a) Validity (certificate validity date from and to)
b) No cancellation (crl/ocsp)
c) Path verification (https://tools.ietf.org/html/rfc4158)

Particularly sensitive information, including identification confirmations and authorization keys, may not be buffered or registered in logs.

Certificates should be issued taking into account the ETSI TS 119 495 specification.

6.7 Protection against API Abuse

The API implementation should take into account the mechanisms of protection against excessive requests from the part of the users (both authorised and unauthorised ones), in particular those generated on purpose with the intention to render the resource unavailable (DoS/DDoS), by an

application of mechanisms limiting the number of requests supported over a given time unit. The limit values should be determined after examination of the specific operational conditions. Limits of this kind should be parametrized. The count of the number of resource access requests should base on a key that unambiguously identifies the given TPP (the RequestHeader.tppID class) and the meters implemented per TPP on the server side. The limit excess must be signalled by HTTP message number 429 (Too Many Requests).

The security should be ensured on the basis of OWASP Guidelines - REST Security Cheat Sheet (https://www.owasp.org/index.php/REST_Security_Cheat_Sheet).

The limit control should be made 4 times a day. It should be noted that sending a request by the PSU resets the counter of requests sent by the TPP in the context of the given PSU.

6.8 Audit Information Logging

It is recommended that the time sources for all the parties using the PolishAPI should be synchronized in order to ensure that the log entries have the correct time stamp.

The key business operation logging should ensure non-repudiation and integrity of entries by using the data from JWS Signature.

A log should contain necessary information that will allow a precise time analysis in case of an incident so that it would be possible to combine particular entries into a single transaction. The element combining particular entries may be, for example, an abbreviation from the authorisation token.

7 Technical Description of the Authentication and Authorisation Process

7.1 Authentication Mechanism on the ASPSP's Side

In the model using the authentication mechanism on the ASPSP's side the process is based on the OAuth 2.0 Authorization Code protocol.

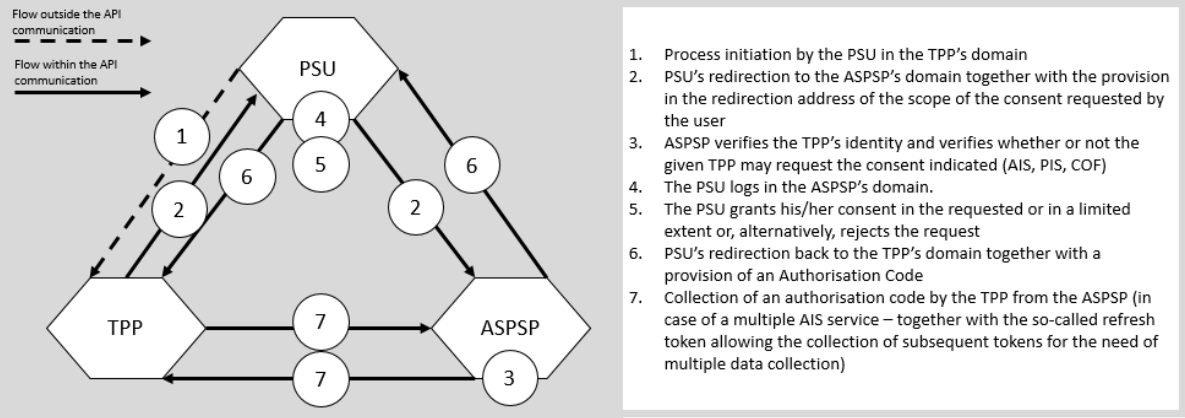


Figure 18: Authentication Mechanism on the ASPSP's Side

The process was described in RFC 6749 in Chapter 4.1. Authorization Code Grant

Below are described the steps and changes thereto implemented by the PolishAPI in relation with legal and security requirements

7.1.1 Redirection from the TPP to the ASPSP

As per RFC 4.1.1. The Authorization Request redirection comprises the following parameters

Parameter	Information if required in the PolishAPI	Comment
response_type	Required	'Code' value
client_id	Required	Pursuant to what is proposed by the Berliner Group, we use the following convention clientId=TPP.[CountryCode].[LicenseNumber]
redirect_uri	required	
scope	Required	
scope_details	Required	
state	Required	A random value unique for the TPP – protection against the Cross-Site Request Forgery attack

The scope_details parameter defines the time ranges, limitations and details of the given authorisation:

a) as to the scope of resources which are made available (e.g. a list of accounts)
b) time for which they are made available
c) limit of the number of uses
d) list of operations it concerns
e) selected operation parameters, e.g. length of back history, transfer parameters etc.

A specification of the scope_details parameter structure is given in Annexes No. 5 and No. 6.

The above parameters are sent by the PSU's browser as POST (due to the possible size of scope_details) in the JSON format - encoded and signed using the JSON Web Signature in accordance with RFC 7515

The *scope* parameter defines the access scopes (corresponding to particular resources (paths) of the specification:

- ais:accounts: Authorisation to effect AIS-Accounts
- ais:holds: Authorisation to effect AIS-Holds
- ais:transactionsDone: Authorisation to effect AIS-TransactionsDone
- ais:transactionsPending: Authorisation to effect AIS-TransactionsPending
- ais:transactionsRejected: Authorisation to effect AIS-TransactionsRejected
- ais:transationDetail: Authorisation to effect AIS-TransationDetail
- pis:multiplePayments: Authorisation to effect PIS-MultiplePayments
- pis:payment: Authorisation to effect PIS-Payment
- pis:domestic: Authorisation to effect PIS-Domestic
- pis:EEA: Authorisation to effect PIS-EEA
- pis:nonEEA: Authorisation to effect PIS-NonEEA
- pis:tax: Authorisation to effect PIS-Tax
- CAF:confirmationOfFunds: Authorisation to effect CAF-ConfirmationOfFunds

7.1.2 PSU's authentication and authorisation

Performance on the ASPSP's side

7.1.3 Reverse redirection of the PSU's browser to the TPP

In accordance with RFC 6749 4.1.2. Authorization Response

7.1.4 Token collection on the basis of the Authorization Code

In accordance with RFC 6749 4.1.3. Access Token Request token collection

Parameter	**Information if required in the PolishAPI**	**Comment**
grant_type	required	Value of the 'authorization_code'
Code	required	In accordance with the value given in step 7.1.3
redirect_uri	required	Value in accordance with the value in step 7.1.1
client_id	required	Pursuant to what is proposed by the Berliner Group, we use the following convention clientId=TPP.[CountryCode].[LicenseNumber]

The TPP's authentication takes place on the basis of a certificate used for the TLS connection

The data returned, except the data set foreseen in OAuth2 (RFC 5.1. Successful Response), should also contain the scope_details field with details of consents the PSU has agreed to give

Parameter	**Information if required in the PolishAPI**	**Comment**
access_token	required	

token_type	required	
expires_in	required	
refresh_token	optional	
scope	required	
scope_details	required	

7.1.5 Consent Withdrawal

The consent withdrawal is made using the /v1.0/accounts/v1.0/deleteConsent method

7.1.6 Use of the scope_details structure

- The one-time consent is supported using the scopeUsageLimit parameter.

7.1.7 Access token taking on the basis of the refresh token

As per RFC 6749.6. 'Refreshing an Access Token' after the access token has expired, the TPP may take a new Access Token using the refresh token (provided is has been issued). Such a situation will take place in case of a multiple AIS service and the CAF service.

Below is presented a TPP's request and a response from the ASPSP's server

Parameter	**Information if required in the PolishAPI**	**Comment**
grant_type	required	Value of 'refresh_token'
refresh_token	required	In accordance with the value provided by the ASPSP in step 7.1.4
scope	optional	The requested scope may not be larger than the one provided in step 7.1.4
scope_details	optional	The requested scope may not be larger than the one provided in step 7.1.4
is_user_session	optional	Defines whether or not the given session is related with an interaction with the PSU – true/false values. Expansion of the OAuth2 standard
user_ip	Required, if is_user_session=true	IP of the user's browser (information for fraud detection needs) Expansion of the OAuth2 standard
user_agent	Required, if is_user_session=true	Information concerning the version of the user's browser (information for fraud detection needs) Expansion of the OAuth2 standard

The response sent by the ASPSP is the same as in item 7.1.4

7.2 Other Authentication Mechanisms

This chapter will be supplemented at a later stage of work of the project group.

8 Technical description of the PIS Service

This chapter constitutes a summary of the API specification in the swagger format defined in Annex No. 1 and the documentation in the swagger-html2 format in Annex No. 2.

8.1 Diagram of Activity in the PIS Service

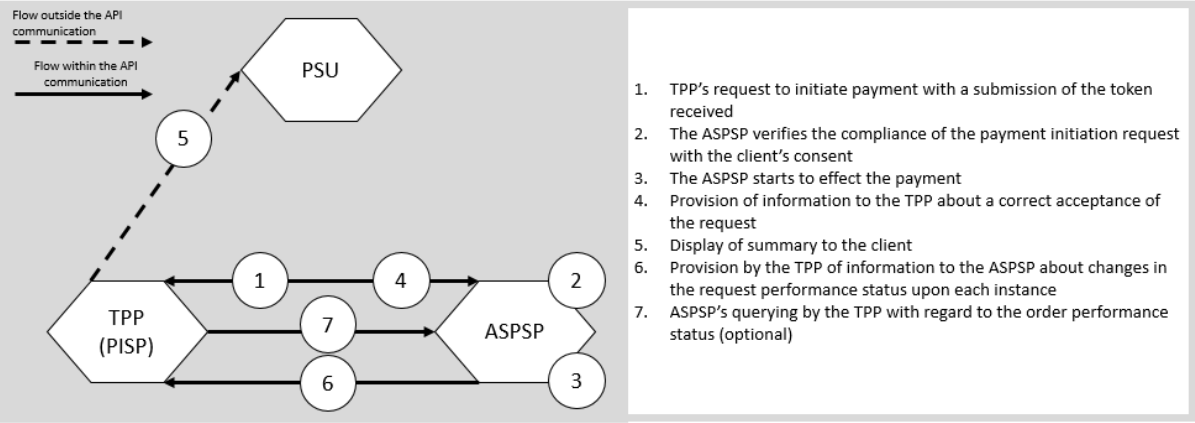


Figure 19: High-level diagram of activity in the PIS Service

8.2 Request Structure

The table below contains requests concerning the PIS service and a specification of classes of objects provided in the request and the response.

Resource (endpoint)	Description	KMD object class provided in the request and collected in the response
/payments/{version}/domestic	Initiates a domestic transfer	PaymentDomesticAddRequest/ PaymentAddResponse
/payments/{version}/ EEA	Initiates a SEPA foreign transfer	PaymentStandardEEAAddRequest/ PaymentAddResponse
/payments/{version}/ nonEEA	Initiates a non-SEPA foreign transfer	PaymentStandardNonEEAAddRequest/ PaymentAddResponse
/payments/{version}/ tax	Initiates a transfer to the tax office	PaymentTaxAddRequest/ PaymentAddResponse
/payments/{version}/ getPayment	Collects the transfer status	PaymentRequest/ PaymentResponse
/payments/{version}/ getMultiplePayments	Collects statuses of multiple payments. Calling does not require token reading.	PaymentsRequest/ PaymentResponse

8.3 Asynchronous PIS Service

The specification defines the CallBack interface, where the ASPSP informs the TPP about the transfer status change using the paymentCallBack method. The CallBack interface is defined in Annex No. 3.

The method used to secure the API is the 'apiKey' type (https://swagger.io/docs/specification/2-0/authentication/) and, additionally, the fingerprint of the TPP's server certificate used to make the

TLS connection of the CallBack - sent in the keyID parameter - is verified. In the PISs called, the TPP transfers the apiKey value and the callbackURL used in the CallBacks to the ASPSP.

9 Technical description of the AIS Service

This chapter constitutes a summary of the API specification in the swagger format defined in Annex No. 1 and the documentation in the swagger-html2 format in Annex No. 2.

9.1 Diagram of Activity in the AI Service

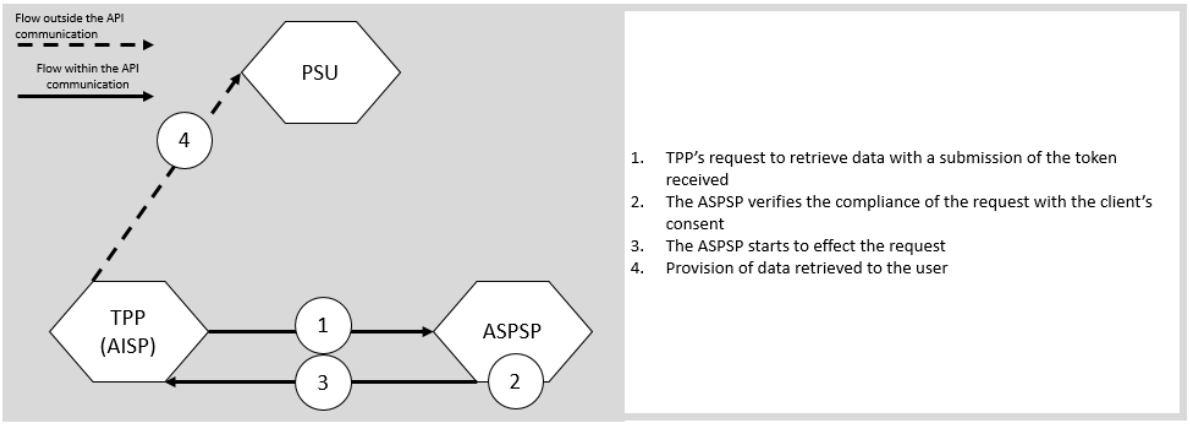


Figure 20: High-level diagram of activity in the AIS Service

9.2 Structure of the AIS Request

The table below contains requests concerning the AIS service and a specification of classes of objects provided in the request and the response.

Resource (endpoint)	**Description**	**KMD object class provided in the request and collected in the response**
/accounts/{version}/deleteConsent	Deletes/invalidates the consent	DeleteConsentRequest/ string
/accounts/{version}/getAccounts	Collects all accounts of the PSU	AccountsRequest/ AccountsResponse
/accounts/{version}/getAccount	Collects a single payment account	AccountInfoRequest/ AccountInfo
/accounts/{version}/getTransactionsDone	Collects all transactions made at the account	TransactionInfoRequest/ TransactionDoneInfoResponse
/accounts/{version}/getTransactionsPending	Collects all pending transactions at the account	TransactionInfoRequest/ TransactionPendingInfoResponse
/accounts/{version}/getTransactionsRejected	Collects all rejected transactions at the account	TransactionInfoRequest/ TransactionRejectedInfoResponse
/accounts/{version}/getHolds	Collects all account holds	TransactionInfoRequest/ TransactionHoldInfoResponse
/accounts/{version}/getTransationDetail	Collects data of a single transaction/hold	TransactionDetailRequest/ TransactionDetailResponse

9.3 Asynchronous AIS Service

The asynchronous method calling as a CallBack, where the TPP sends the operation request to the ASPSP together with a return address, will be defined in the subsequent version of the PolishAPI standard.

10 Technical Description of the CAF Service

This chapter constitutes a summary of the API specification in the swagger format defined in Annex No. 1 and the documentation in the swagger-html2 format in Annex No. 2.

10.1 Diagram of Activity in the CAF Service

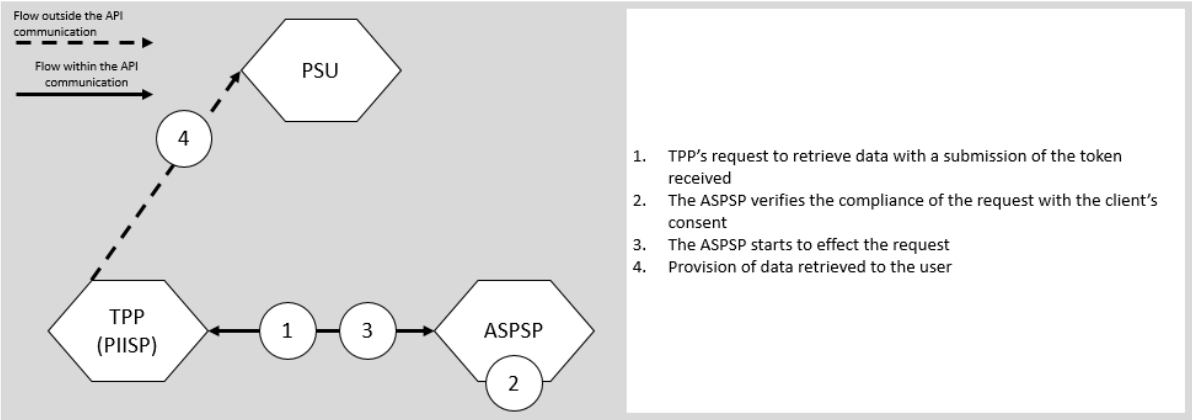


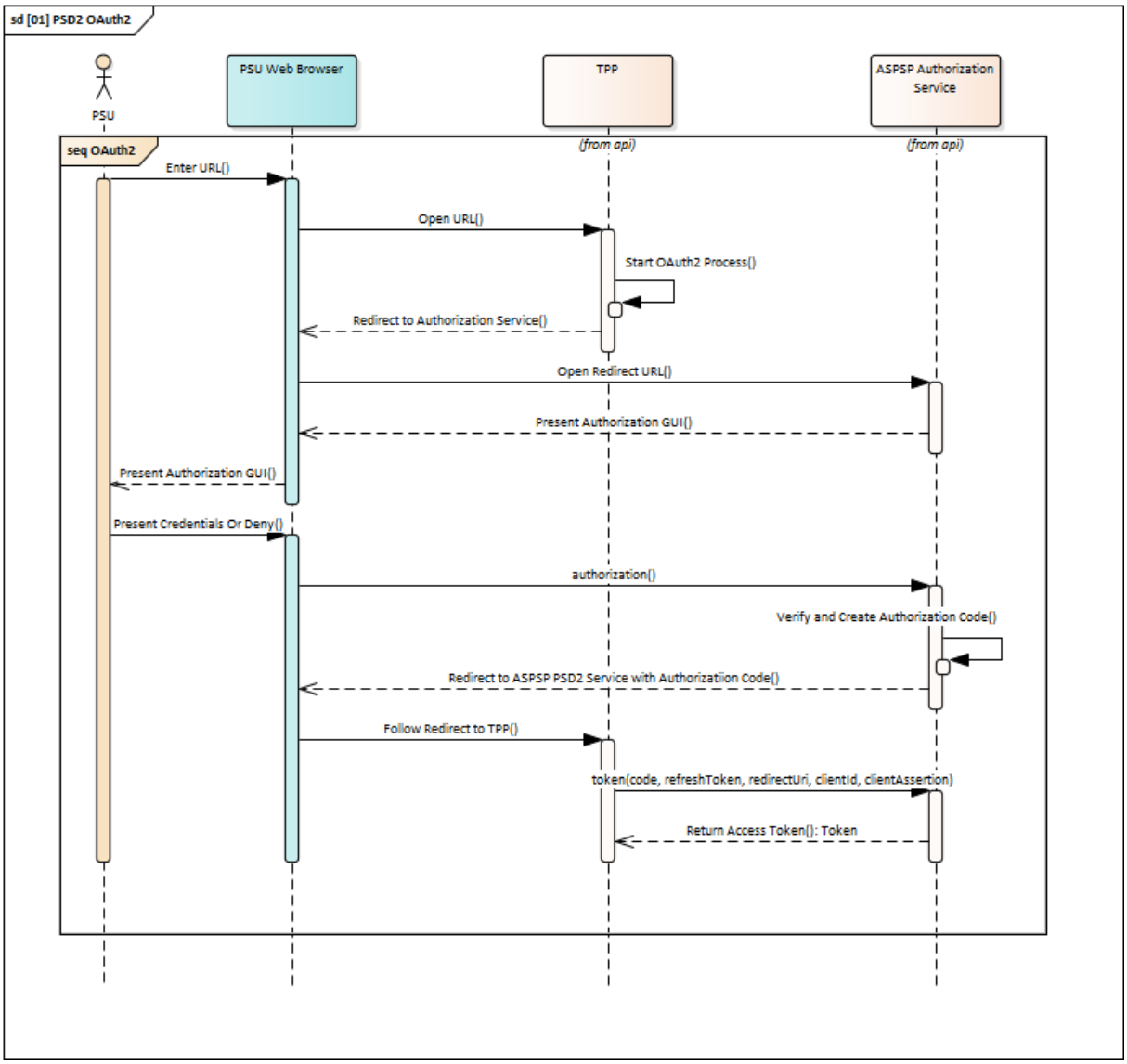
Figure 21: High-level diagram of activity in the CAF Service

10.2 Request Structure (including a description of fields and information if required)

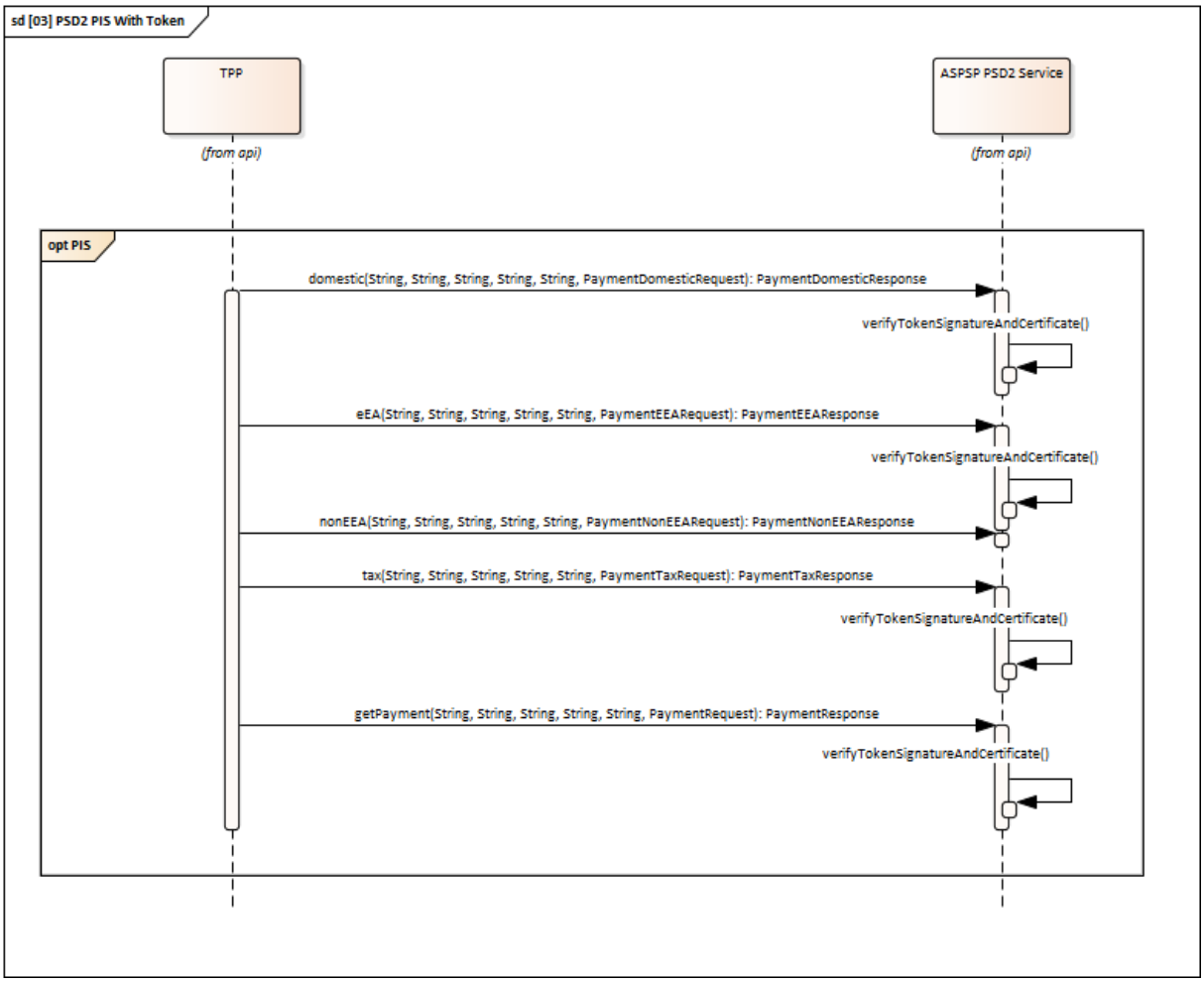
Resource (endpoint)	**Description**	**KMD object class provided in the request and collected in the response**
/confirmation/{version}/getConfirmationOfFunds	Confirmation of fund availability	confirmationOfFundsRequest/ confirmationOfFundsResponse

11 Diagrams of Sequences for the PSD2 Interface Method Calls (PL)

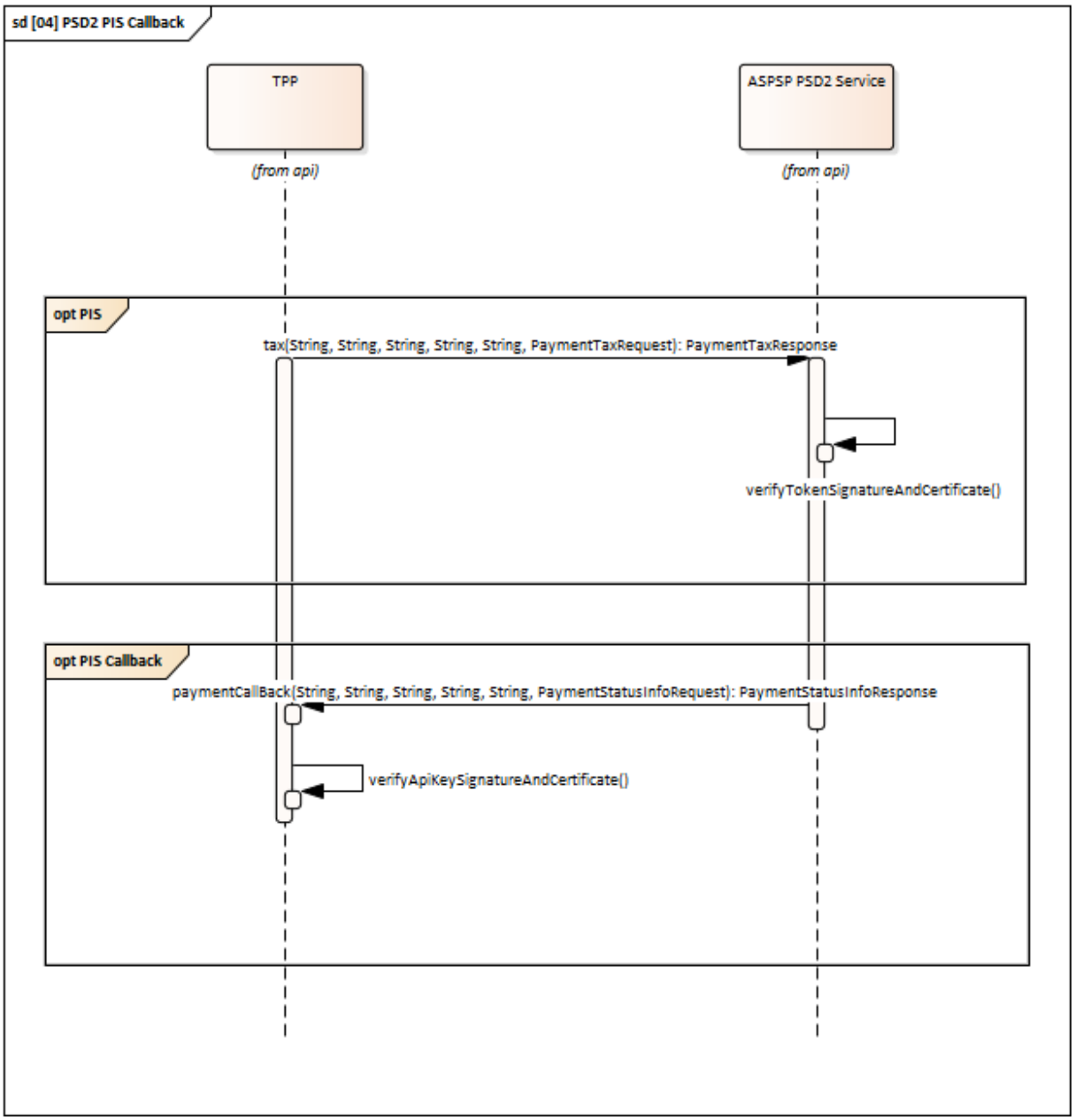
11.1 OAuth2 authorization



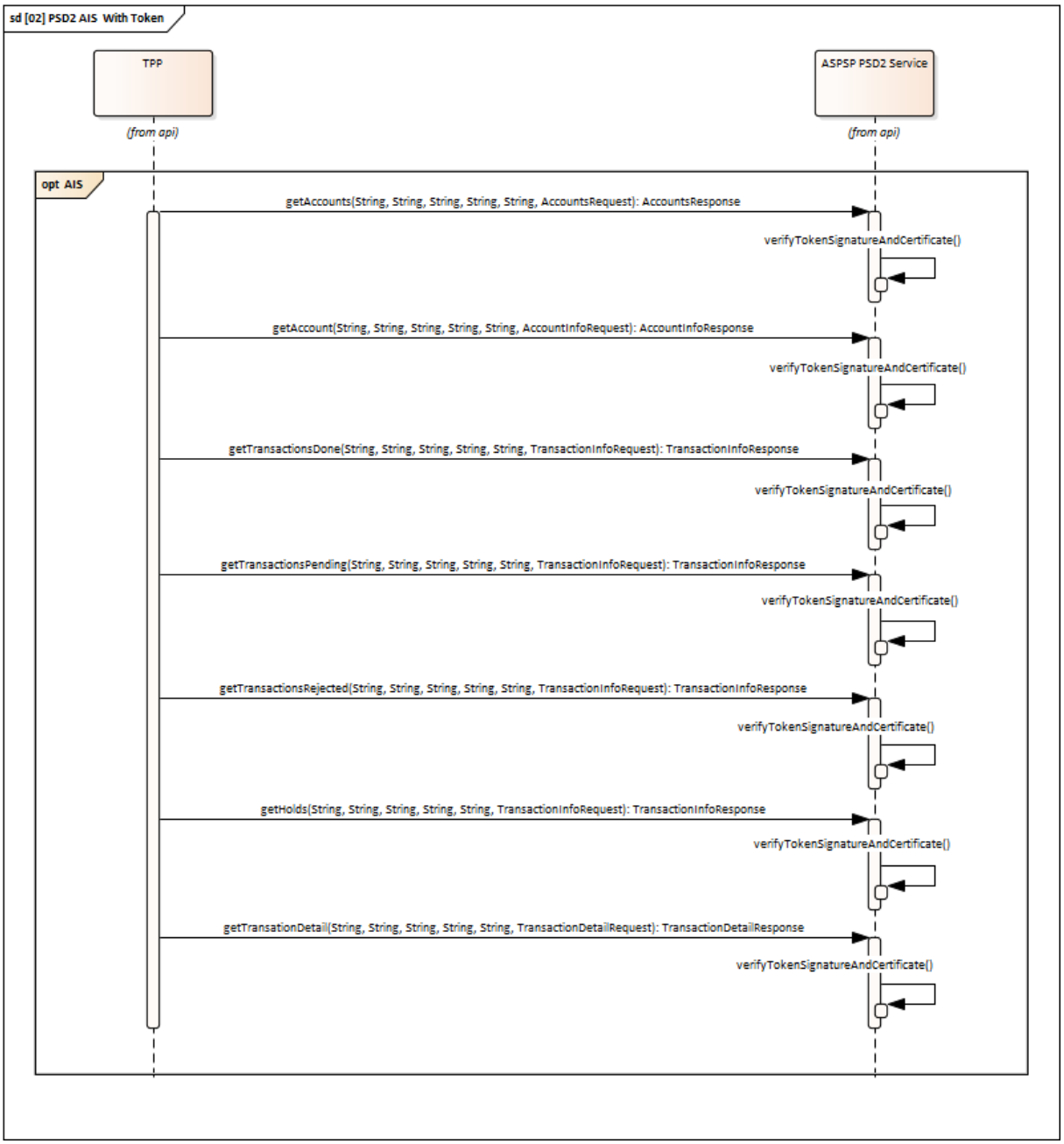
11.2 PIS calls with OAuth2 authorization



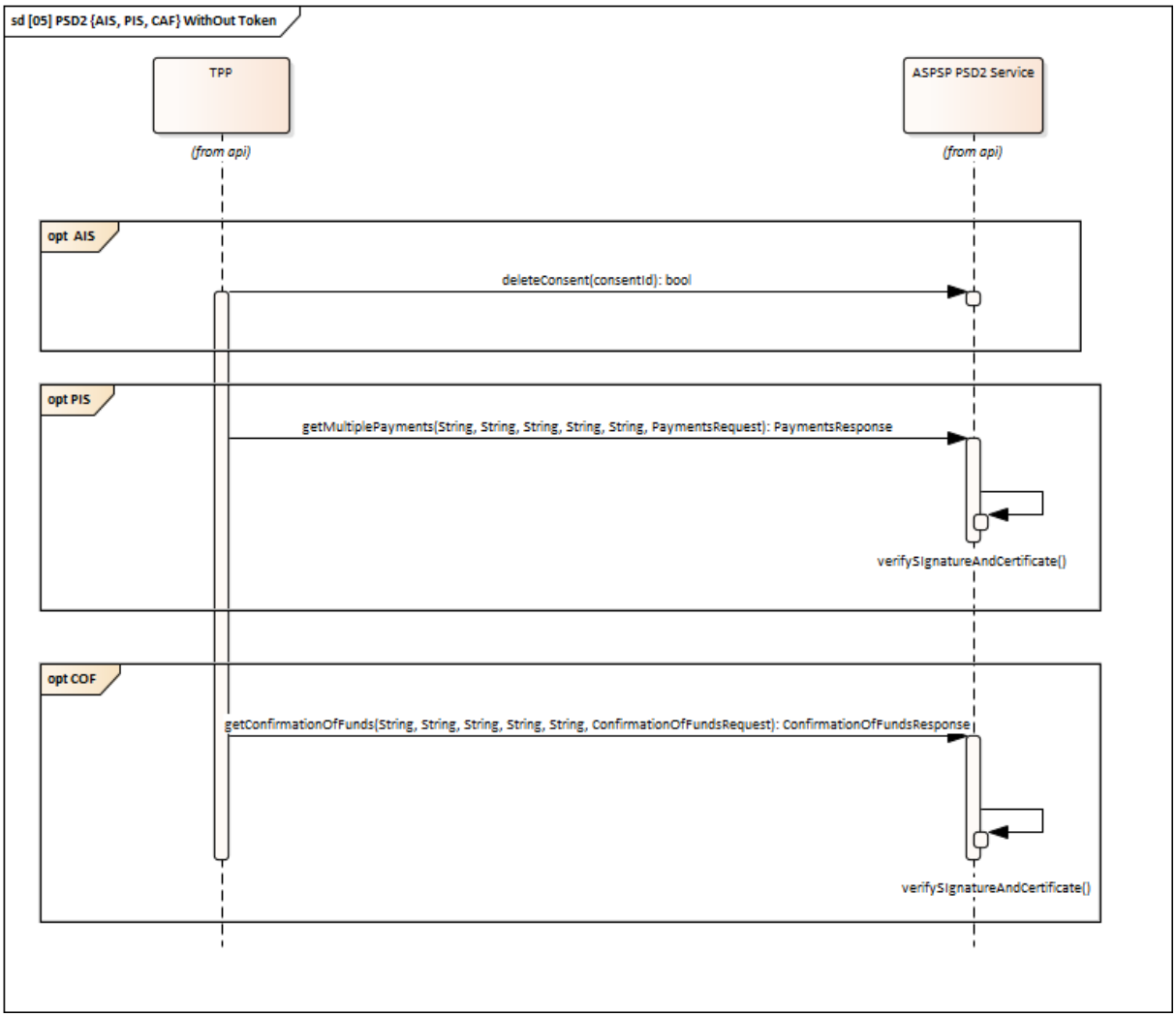
11.3 Callback PIS calls



11.4 AIS calls with OAuth2 authorization



11.5 AIS, PIS, CAF calls without OAuth2 authorization



12 Error codes

Stage	Error	HTTP code	How supported
Redirection of the client to the ASPSP's domain together with a provision in the redirection address of parameters of the initiated payment	Provision of incorrect parameters	400	Reverse redirection of the client to the TPP's domain and process abortion (pursuant to RFC6749 4.1.2.1)
The ASPSP verifies the TPP's identity in the Identity Hub and verifies whether or not the given TPP may request the consents indicated (AIS or PIS)	Incorrect verification of the TPP's identity	401	Display of a message to the user
	Incorrect verification of the TPP's licence (e.g. only AIS)	403	Reverse redirection of the client to the TPP's domain and process abortion (pursuant to RFC6749 4.1.2.1)
The client logs in the ASPSP's domain	Incorrect logging - 1 time	401	Waiting for a correct client logging
	Multiple incorrect logging	401	Waiting for a correct client logging
	No service activation by the TPP (opt-out)	403	Reverse redirection of the client to the TPP's domain and process abortion (pursuant to RFC6749 4.1.2.1)
	No funds	422	Reverse redirection of the client to the TPP's domain and process abortion (appropriate error code returned when requesting a payment service)
The client expresses the consent in the requested or limited scope or else rejects the request	Request rejection by the client	403	Reverse redirection of the client to the TPP's domain and process abortion (pursuant to RFC6749 4.1.2.1)
	Incorrect authorisation by the client	403	Reverse redirection of the client to the TPP's domain and process abortion (pursuant to RFC6749 4.1.2.1)
Reverse redirection of the client to the TPP's domain	The client's end device shutdown before the redirection	-	The TPP has an option to complete the operation by taking the token using contextId
Authorisation token taking from the ASPSP by the TPP	Unknown TPP	401	Process abortion without the request being admitted
	Incorrect token request parameters	400	Process abortion without the request being admitted

	Communication with the ASPSP impossible	-	Process abortion without the request being admitted
The ASPSP verifies the compliance of the payment initiation request with the client's consent	No compliance with the consent granted	401	Process abortion without the request being admitted
	Limit of requests for the desired service has been exceeded	429	Process abortion without the request being admitted
The ASPSP starts to effect the payment	No funds	422	End of process (error code returned)
Provision of information to the TPP about a correct acceptance of the request	Communication with the TPP impossible	-	Message renewal x3 Failure information Possibility to repeat all messages
Provision by the TPP of information to the ASPSP about changes in the request performance status	Communication with the TPP impossible	-	Message renewal x3 Failure information Possibility to repeat all messages
The ASPSP verifies the compliance of the payment account data request with the client's consent	No compliance with the consent granted	403	End of process
ASPSP receives a request	Access to the service blocked by the ASPSP	403	End of process
ASPSP receives a request	Access to the service blocked by the PSU	403	End of process

12.1 Error codes for the HTTP 403 response code

Code	Message
1	Incorrect verification of TPP licenses
2	No activation of TPP services
3	Rejection of the request by the client
4	Incorrect authorization by the client
5	Non-compliance with the consent given
6	Access to the service blocked by ASPSP
7	Access to the website blocked by the PSU
8	Blocked TPP's access to bank services by the bank
9	Blocked TPP's access to bank services by the client

13 Standard Implementation Recommendations

13.1 Timeout Support

Due to the timeout type events which may occur during the http request processing, the ASPSP must ensure uniqueness verification at the server layer at the requestId level. Having identified a non-uniqueness of the request, the ASPSP returns the 400.1 error (Request repeated).

The recommended timeout value is 30 seconds.

13.2 TPP verification

The TPP authentication should be made based on the communications certificate (SSL) and signature certificate (jws), with a simultaneous verification whether or not the certificates correspond to the TPP's ID (tppId) in the ASPSP's database. The tppId value is determined by the ASPSP during the TPP registration; the suggested value is TPP's EUNIP .

13.3 Oauth2

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 an incorrect URL address which may be submitted by an untrusted party.

13.4 Fraud Prevention

In order to prevent potential frauds, a dedicated RequestHeader Class was implemented which is provided in each request and contains the following information about the PSU: IP address and userAgent. The structure will be useful for the ASPSP during the implementation of security mechanisms.

Additionally, it is recommended that the entities participating in the project exchanged information about suspected unauthorised transactions/compromised IPs etc.

14 List of Annexes

Annex No. 1: The RESTfull api interface definition file in the swagger format: ‘2.0’ - PolishAPI-ver1.0.0.yaml

Annex No. 2: The SDK RESTfull api documentation in the swagger-html2 format - PolishAPI-ver1.0.0.html

Annex No. 3: The RESTfull api callback interface definition file in the swagger format: "2.0" - PolishAPI-CallBack-ver1.0.0.yaml

Annex No. 4: The SDK RESTfull api callback interface documentation in the swagger-html2 format - PolishAPI-CallBack-ver1.0.0.html

Annex No. 5: The scope_details definition file - OAuth2 interface extensions in the form json/scheme - PolishAPI-scope_details-ver1.0.0.json

Annex No. 6: The SDK scope_details documentation - OAuth2 interface extensions in the swagger-html2 format - PolishAPI- scope_details -ver1.0.0.html

