THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

openFinance API Framework

XS2A API as PSD2 Interface

Operational Rules

Version 2.0

31 October 2025

License Notice

This Specification has been prepared by the Participants of the Joint Initiative pan-European PSD2-Interface Interoperability* (hereafter: Joint Initiative). This Specification is published by the Berlin Group under the following license conditions:

- "Creative Commons Attribution-NoDerivatives 4.0 International Public License"

  

  This means that the Specification can be copied and redistributed in any medium or format for any purpose, even commercially, and when shared, that appropriate credit must be given, a link to the license must be provided, and indicated if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. In addition, if you remix, transform, or build upon the Specification, you may not distribute the modified Specification.

- Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Berlin Group or any contributor to the Specification is not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.

- The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import (parts of) the Specification.

---

* The 'Joint Initiative pan-European PSD2-Interface Interoperability' brings together participants of the Berlin Group with additional European banks (ASPSPs), banking associations, payment associations, payment schemes and interbank processors.

Contents

1 Introduction

1.1 From Core XS2A Interface to openFinance API

With [PSD2] the European Union has published a directive on payment services in the internal market. Among others [PSD2] contains regulations on services to be operated by so called Third Party Payment Service Providers (TPP) on behalf of a Payment Service User (PSU). These services are

- Payment Initiation Service (PIS) to be operated by a Payment Initiation Service Provider (PISP) TPP as defined by article 66 of [PSD2],
- Account Information Service (AIS) to be operated by an Account Information Service Provider (AISP) TPP as defined by article 67 of [PSD2], and
- Confirmation of Funds Service (COF) to be used by a Payment Instrument Issuing Service Provider (PIISP) TPP as defined by article 65 of [PSD2].

To implement these services (subject to PSU consent) a TPP needs to access the account of the PSU. The account is managed by another PSP called the Account Servicing Payment Service Provider (ASPSP). To support the TPP in accessing the accounts managed by an ASPSP, each ASPSP has to provide an "access to account interface" (XS2A interface). Such an interface has been defined in the Berlin Group NextGenPSD2 XS2A Framework.

This XS2A Framework is now extended to extended services and developed into a Version 2 API family. This interface is addressed in the following as **openFinance API**. This openFinance API differs from the XS2A interface in several dimensions:

- The extended services might not rely anymore solely on PSD2.
- Other important regulatory frameworks which apply are e.g. GDPR.
- The openFinance API can address different types of **API Clients** as access clients, e.g. TPPs regulated by an NCA according to PSD2, or corporates not regulated by an NCA.
- The extended services might require contracts between the access client and the ASPSP.
- While the client identification at the openFinance API can still be based on eIDAS certificates, they do not need to be necessarily PSD2 compliant eIDAS certificates.
- The extended services might require e.g. the direct involvement of the access client's bank for KYC processes.

Note: The notions of API Client and ASPSP are used because of the technical standardisation perspective of the openFinance API. These terms are analogous to "asset broker" and "asset holder" resp. in the work of the ERPB on a SEPA API access scheme.

Note: In implementations, the API services of several ASPSPs might be provided on an aggregation platform. Such platforms will be addressed in the openFinance API Framework as "API provider".

The following account access methods are covered by this framework:

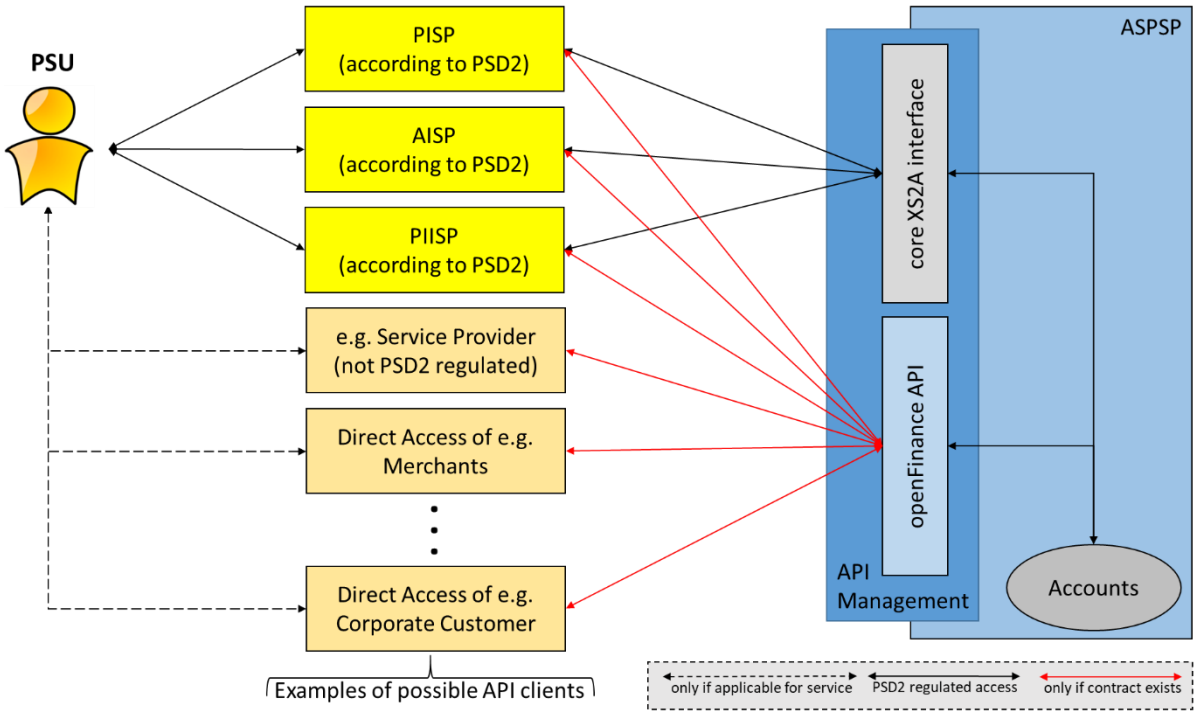

Figure 1: Core XS2A interface and openFinance API

1.2 Core Compliance Services: XS2A API within the openFinance API Framework

The openFinance API Framework as displayed above can of course still be restricted to an **XS2A API** which is fulfilling core PSD2 compliant services accessible for all related and licensed TPPs, while sharing new architecture items and/or data modelling with the full openFinance API Framework.

This document covers the service definitions for the PSD2 compliance related part of the openFinance API Framework. Please note that this document is based on security measures and protocol functions as defined in the framework document [oFA-PFSM] and strongly relies on the basic framework foundation described in [oFA-OR-FW].

1.3 Document Structure

This document specifies the core XS2A API Services within the openFinance API Framework in detail:

- The core services and variants of the XS2A interface in Section 2,
- A description of the actors which access the XS2A interface directly and their respective roles in section 3,
- A detailed list of the services which are supported for the core services, including whether they are optional or mandatory by the [PSD2] in section 104,
- The key concepts which are specific for core services of the XS2A interface in section 5,
- The operational rules the services have to follow in section 6, and
- The message and data model in section 7.

1.4 Document History

Version	Change/Note	Approved
2.0	First released version of the operational rules of the V2 consent API	

Remark for Future: Please note that the Berlin Group openFinance API Framework is still under constant development. Technical issues, which are already in discussion within the Berlin Group openFinance working structure are mentioned in this document by "Remark for Future" to make the reader aware of upcoming potential changes.

2 Services and variants of the XS2A interface

2.1 Services of the XS2A interface

It is distinguished between core services and extended services. According to PSD2 requirements an ASPSP must support all core services at its XS2A interface. The ASPSP is free to decide if and if so which extended service it wants to support in its implementation of the XS2A interface in accordance with its own market needs.

2.1.1 Core services

Every implementation of the XS2A interface based on the specification of the Joint Initiative shall support the following core services:

Service	Abbr.	Usage
Payment initiation service	PIS	This service may be used by a PISP to initiate a single payment on behalf of a PSU using a given account of that PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service are defined by article 66 of [PSD2].
Account information service	AIS	This service may be used by an AISP to request information about the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service are defined by article 67 of [PSD2].
Fund confirmation service	COF	This service may be used by a PIISP to request a confirmation of the availability of specific funds on the account of a PSU. The account is managed by the ASPSP providing the XS2A Interface. Functionality and restrictions of this service are defined by article 65 of [PSD2].

Table 1: Core services to be supported by the XS2A interface

For each of these core services, different variants of these services can be distinguished. In earlier versions of the operational rules of services accessible at the XS2A interface, these service variants were called "use cases". For standardisation purposes of the framework documentation for version 2.x, they are now referred to as **API Services** in this document.

The implementation guidelines [oFA-IG-Com] define for each API Service a set of request/response messages and the corresponding data elements in detail. These messages and data elements are exchanged between the TPP and the ASPSP at the XS2A interface. The supported set of API services may vary between different ASPSP. See section 4 for a list of all API Services at the XS2A interface and the distinction if the service mandatory or optional for the ASPSP's implementation at its XS2A interface .

A TPP which has the necessary authorisation and role (see section 3) can use these services to access the XS2A interface of an ASPSP. No further contractual relationship between the TPP and the ASPSP is needed.

2.1.2 Extended services

The necessary set of request/response messages and the corresponding data elements for extended services can be specified and implemented at the ASPSP's XS2A interface at the discretion of the ASPSP.

An ASPSP supporting extended services at its XS2A interface may limit access to these extended services to a special group of TPPs. If requested by the ASPSP a contractual relationship regulating the usage of the extended service shall be established between the ASPSP and the TPP.

There is a well-established standard for premium services which are specified and implemented at the openFinance API of an ASPSP. An introduction to this is given by [oFA Intro] which extends to the Operational Rules for the respective extended services. This is not further elaborated here.

2.2 Variants of the XS2A interface

[oFA-IG-Com] and [oFA-OR-FW] specify variants for most of the services. For one single service, different variants can distinguish between

- additional requirements for the identification of the TPP,
- the approach to executing strong customer authentication (if needed),
- the API Services supported at the XS2A interface (see section 4),
- the products to be supported as part of the service (for example for the payment initiation service the products SCT, SCT Inst, domestic payment etc.),
- the data elements needed as part of a service (for example structured or unstructured remittance information as part of a SCT payment),
- etc.

Further, the exact scope and functionality of the PSD2 core services might depend further on

- the functionality offered by the ASPSP in the online banking web frontend or
- requirements set by national legal provisions in the context of PSD2.

For that reason, some API Services will be set as an optional support on ASPSP side in this framework, e.g. bulk payments, recurring payments or future dated payments within the payment initiation service.

If different variants of a service or optional sub-services and functionality are specified the ASPSP decides which of these variants and/or sub-services resp. functionality are supported/required by its XS2A interface. The ASPSP shall inform the TPP about the variants supported/required by its XS2A interface as part of the interface documentation. The ASPSP may use a standardising APIs for implementation parameters chosen by the ASPSP to offer implementation details to the API Client in a compact and machine readable way. For further information on this, see [oFA Disc].

The TPP must use the service variant selected by the ASPSP to access the XS2A interface of the ASPSP.

3 Actors and roles

3.1 The actors

Only the following two actors are considered to be active at the XS2A interface:

- **ASPSP:** Provides an XS2A interface to the TPP. Receives request messages at its XS2A interface and sends corresponding response messages to the TPP.
- **TPP:** Executes services defined by [PSD2] on behalf of a PSU. If necessary for the service the TPP may access the account(s) of the PSU managed by an ASPSP via the XS2A interface. The TPP sends request messages to the XS2A interface of the ASPSP and receives corresponding response messages from that ASPSP.

The following figure shows the interaction of the TPP and the ASPSP at the XS2A Interface:

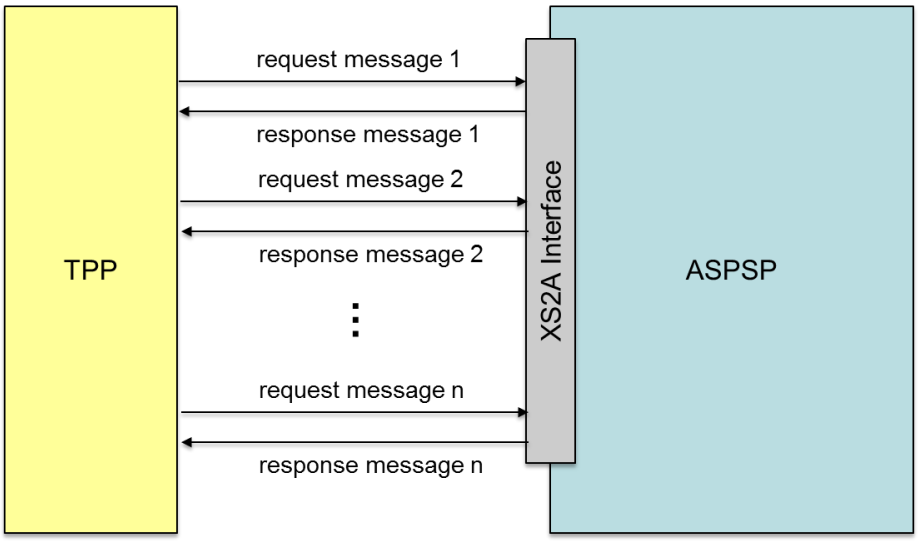

Figure 2: Interaction of TPP and ASPSP at the XS2A interface

Please note:

- An ASPSP can also act as a TPP by taking one of the roles of a TPP (see section 3.2). In that case the ASPSP can offer the services defined by [PSD2] to a PSU and can access the XS2A Interface of another ASPSP.

- Apart from these two active actors at the XS2A interface, the PSU is another crucial actor for the execution of PSD2 related services:

  PSU: The PSU implicitly or explicitly instructs the TPP to perform a PSD2 service towards its ASPSP. The PSU can be a natural or legal person. Please note that in the related data model used for the XS2A specification, the PSU-ID will always refer to a natural person, e.g. a corporate's employee in the case where the PSU is a legal person. The data model is extended by using in addition corporate identifications where needed.

- Apart from its essential role for the overall concept, the PSU is not an active actor at the XS2A interface. A PSU never directly accesses the XS2A interface of an ASPSP.

3.2 The roles of a TPP

For a TPP as an actor at the XS2A interface, it has to be distinguished between the following roles:

- **PISP:** Payment Initiation Service Provider – TPP accessing the XS2A interface of an ASPSP while executing a payment initiation service (PIS) according to article 66 of [PSD2].

- **AISP:** Account Information Service Provider – TPP accessing the XS2A interface of an ASPSP while executing an account information service (AIS) according to article 67 of [PSD2].

- **PIISP:** Payment Instrument Issuing Service Provider – TPP accessing the XS2A interface of an ASPSP while executing a confirmation of funds service (COF) according to article 65 of [PSD2].

A TPP may have different roles if it has the necessary authorisations from the corresponding competent authority of its home Member State. The TPP shall only execute one of its roles per service at the XS2A Interface, i.e. for all request messages used to execute a single service.

3.3 Minimum requirements for the actors

The actors actively involved in the usage of an XS2A interface have to comply at least with the following minimum requirements:

3.3.1 ASPSP

An organisation acting as ASPSP at the XS2A interface provided by the Joint Initiative has to comply at least with the following requirements:

- The ASPSP shall implement at least one XS2A interface according to the specifications provided by the Joint Initiative. Please note: An ASPSP may of course also support other [PSD2]-compliant interfaces. The possibility of having additional interfaces is not considered further in this document.
- To operate its XS2A interface the ASPSP shall comply with the obligations defined by [PSD2] and [RTS].
- The ASPSP shall respond to incoming requests of any TPP without discrimination in compliance with the requirements from [PSD2] and [RTS] provided that the TPP can be identified correctly and has the correct role corresponding to the service it wants to execute.

3.3.2 TPP

An organisation acting as TPP at the XS2A interface provided by the Joint Initiative shall comply at least with the following requirements:

- The TPP shall be authorised by the competent authority of its home Member State according to [PSD2].
- This authorisation must be valid (i.e. it has not been withdrawn).
- The TPP shall obtain the qualified certificates to be used for its identification at the XS2A interface from a Trust Service Provider with a qualified status (QTSP) compliant with [eIDAS]. These certificates have to comply with the additional requirements defined by [RTS] and the technical specification [TS 119 495] of ETSI.
    - If a TPP can act using different roles, each role shall be listed in its qualified certificate.
    - The TPP shall cease to use a qualified certificate as soon as the necessary authorisation has been withdrawn according to [PSD2].
- The TPP shall access the XS2A interface of an ASPSP according to the applicable specifications.
- For each access to the XS2A interface of an ASPSP the TPP shall identify itself towards the ASPSP as required by the specification of the XS2A interface.

4 API Services supported for the core services

The current version of the XS2A interface specification supports the following API Services:

API Service	Service Type	Role of the TPP	Support optional	PSU directly involved
Initiation of a single payment	PIS	PISP	no	yes
Initiation of a single future dated payment	XDPIS	PISP	yes	yes
Initiation of a bulk payment	BPIS	PISP	yes	yes
Initiation of a recurring payment	RPIS	PISP	yes	yes
Cancellation of payments	PIS, XDPIS, BPIS, RPIS	PISP	yes	yes
Establish consent on account information	CONS-AIS	AISP	no	yes
Get list of addressable accounts	AIS-PAY	AISP	yes	no
Get account details of the list of accessible accounts	AIS-PAY	AISP	no	no
Get balances for a given account	AIS-PAY	AISP	no	no
Get transaction information for a given account	AIS-PAY	AISP	no	no
Get card account details of the list of accessible card accounts	XAIS-CA	AISP	yes	no
Get balances for a given card account	XAIS-CA	AISP	yes	no

API Service	Service Type	Role of the TPP	Support optional	PSU directly involved
Get transaction information for a given card account	XAIS-CA	AISP	yes	no
Grouping services to signing baskets	SGNB	PISP / AISP	yes	yes
Get a confirmation of funds	COF	PIISP	no	no

Table 2: API Services for the core services

Note: In this document, it is differentiated between addressable accounts and accessible accounts. An account of a PSU is defined to be addressable if said account is open for access through the XS2A API according to the PSD2. In contrast, for an accessible account, the PSU has to give explicit consent to at least one of the defined account information types.

With the exception of the API Service “Grouping services to signing baskets” each service belongs to one of the core services. A TPP may only execute an API Service if it holds the corresponding role indicated in the column "Role of the TPP".

In addition, the XS2A interface will support technical services within the RESTful API approach which are not necessarily used within the above mentioned API Services, e.g. to read details on consent objects or other created resources. Further details on the technical services will be defined in [oFA-IG-Com].

Not all of the above API Services have to be supported at the XS2A interface of an ASPSP. If it is marked as optional in the column "Support optional" the ASPSP is free to decide whether or not to support this API Service at its XS2A interface. Of course the ASPSP has to respect requirements of the European and national regulations by its decision. In general, an ASPSP should support all API Services at its XS2A interface that it also supports at its online interfaces used directly by the PSU.

The execution of any service at the XS2A interface is subject to the consent of the PSU. Some API Services require direct involvement of the PSU while others do not. This is specified in column "PSU directly involved".

If an API Service requires direct involvement of a PSU, strong customer authentication (SCA) of the PSU may be necessary. The process of a strong customer authentication and its different variants is explained in detail in [oFA-OR-FW], the technical details of this are given in [oFA-PFSM]. For the explicit usage of SCA in the scenarios of this document, please refer to [oFA-IG-Com] as well. One of the purposes of a strong customer authentication is to prove that the service is executed with the consent of the PSU.

If an API Service does not require direct involvement of the PSU, strong customer authentication is not possible. In this case the PSU has to give consent by other means prior to the service. A longer time period may elapse between the PSU giving the consent and the actual execution of the service by the TPP. The steps necessary for giving and proving the consent of the PSU depend on the API Service and will be explained in the following sections and in section 5.2.

The account information services can deal with regular payment accounts with one account currency and with multicurrency accounts:

Definition: A multicurrency account is a payment account which is a collection of different sub-accounts which are all addressed by the same account identifier like an IBAN by e.g. payment initiating parties. The sub-accounts are legally different accounts and all differ in their currency, balances and transactions. An account identifier like an IBAN together with a currency always addresses uniquely a sub-account of a multicurrency account.

In the below API Services, it is mentioned when it makes a difference if a regular payment account, a multicurrency account or a sub-account of a multicurrency account is addressed.

4.1 API Service: Initiation of a single payment

The support of this API Service at the XS2A interface is mandatory.

This API Service can be used to initiate a single payment in form of a credit transfer from an account of the PSU to an account of the payee. Debit payments are not supported in the first version of the specification but may be specified in a later stage as extended service.

While the service at the XS2A interface is initiated by the TPP, it must first be initiated by the PSU at the PSU – TPP interface. The PSU – TPP interface is not within the scope of this document.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role PISP.

Subject to the decision of the ASPSP, strong customer authentication of the PSU has to be executed.

The following figure shows only the very top level information flow:

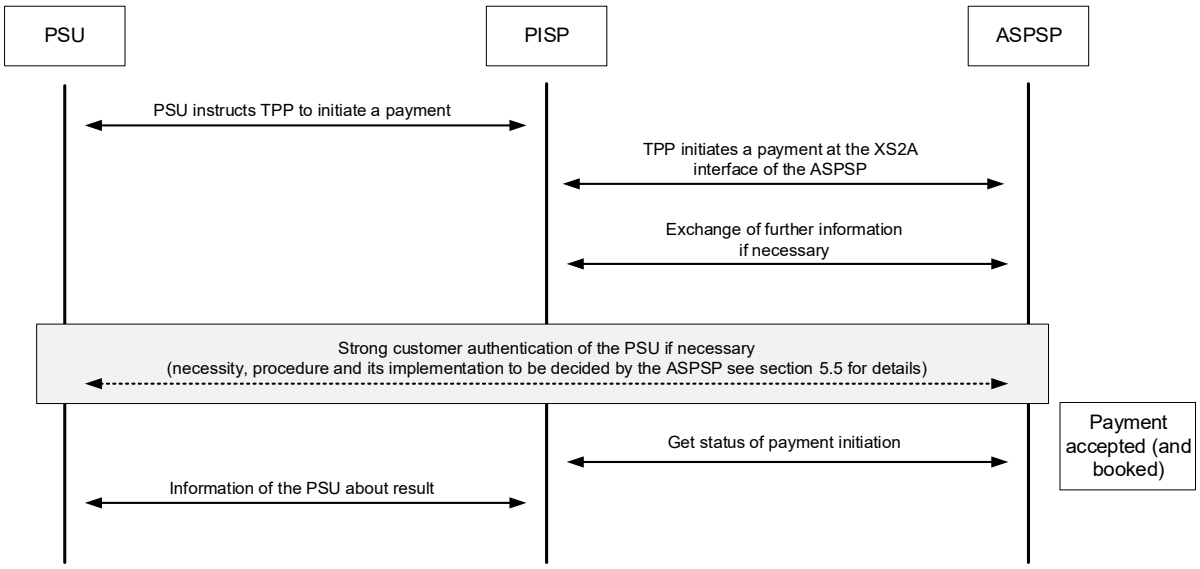

Figure 3: API Service Initiation of a single payment

Remark: It depends on the booking system of the bank whether the payment is booked directly after the acceptance of the payment initiation (real-time booking banks) or later (batch booking banks).

4.2 API Service: Initiation of a single future dated payment

The support of this API Service at the XS2A interface is optional for an ASPSP.

This API Service can be used to initiate a single payment in form of a credit transfer which has to be processed by the ASPSP at a given date in the future. The following holds:

- The PSU has to initiate this service at the PSU – TPP interface.
- The ASPSP will reject the service if the TPP cannot be identified at the XS2A interface and/or if it does not have the role PISP.
- Subject to the decision of the ASPSP, strong customer authentication of the PSU has to be executed.

The following figure shows only the very top level information flow of an initiation of a future dated payment. The only difference to the initiation of a regular payment is that the booking is in the future:

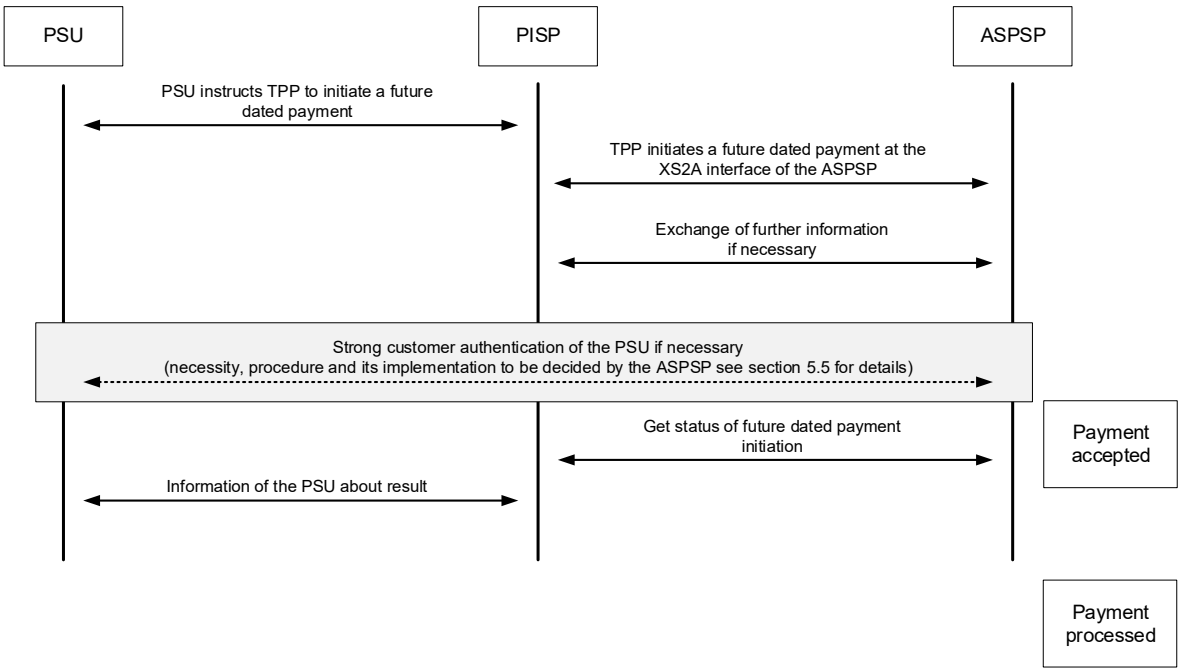

Figure 4: API Service Initiation of a future dated payment

Remark: The processing, i.e. the actual booking of the payment will be analogous to the processing of future dated payments as initiated in the client interface of the ASPSP.

4.3 API Service: Initiation of a bulk payment

The support of this API Service at the XS2A interface is optional for an ASPSP.

Multiple payments, where a PSU first collects several payments and then performs a SCA to authorise the collection (bulk) of these payments is always realised as a bulk payment initiation in the XS2A interface. For a bulk payment all collected payments shall be based on the same payment product and initiated from the same debtor account of the PSU. The collection of several payments to a bulk payment may be performed in the interface between PSU and TPP. The following holds:

- The PSU has to initiate this service at the PSU – TPP interface.
- The ASPSP will reject the service if the TPP cannot be identified at the XS2A interface and/or if it does not have the role PISP.
- Subject to the decision of the ASPSP, strong customer authentication of the PSU has to be executed.

The following figure shows only the very top level information flow of a bulk payment initiation:

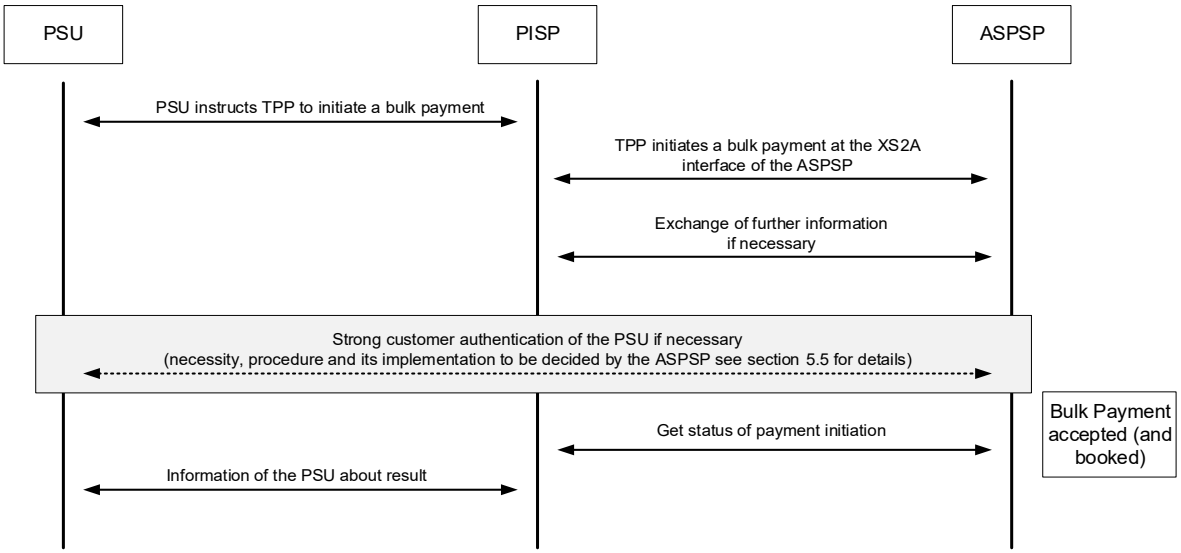

Figure 5: API Service Initiation of a bulk payment

Remark: The same remark as on the time of booking applies as for the initiation of a single payment. Please note that the bulk payment can also contain single future dated payment if the ASPSP supports this function. The booking then is divided in several sub-steps accordingly.

4.4 API Service: Initiation of a recurring payment

The support of this API Service at the XS2A interface is optional for an ASPSP.

The initiation of a recurring payment is realised in the XS2A interface as the initiation of a corresponding standing order, as it is supported today by ASPSP in the client interface. The TPP can initiate a single payment together with administrative information about the frequency and duration of the recurring payments. The duration can be infinite. The following holds:

- The PSU has to initiate this service at the PSU – TPP interface.
- The ASPSP will reject the service if the TPP cannot be identified at the XS2A interface and/or if it does not have the role PISP.
- Strong customer authentication of the PSU has to be executed.

The following figure shows only the very top level information flow of an initiation of a standing order for a recurring payment:

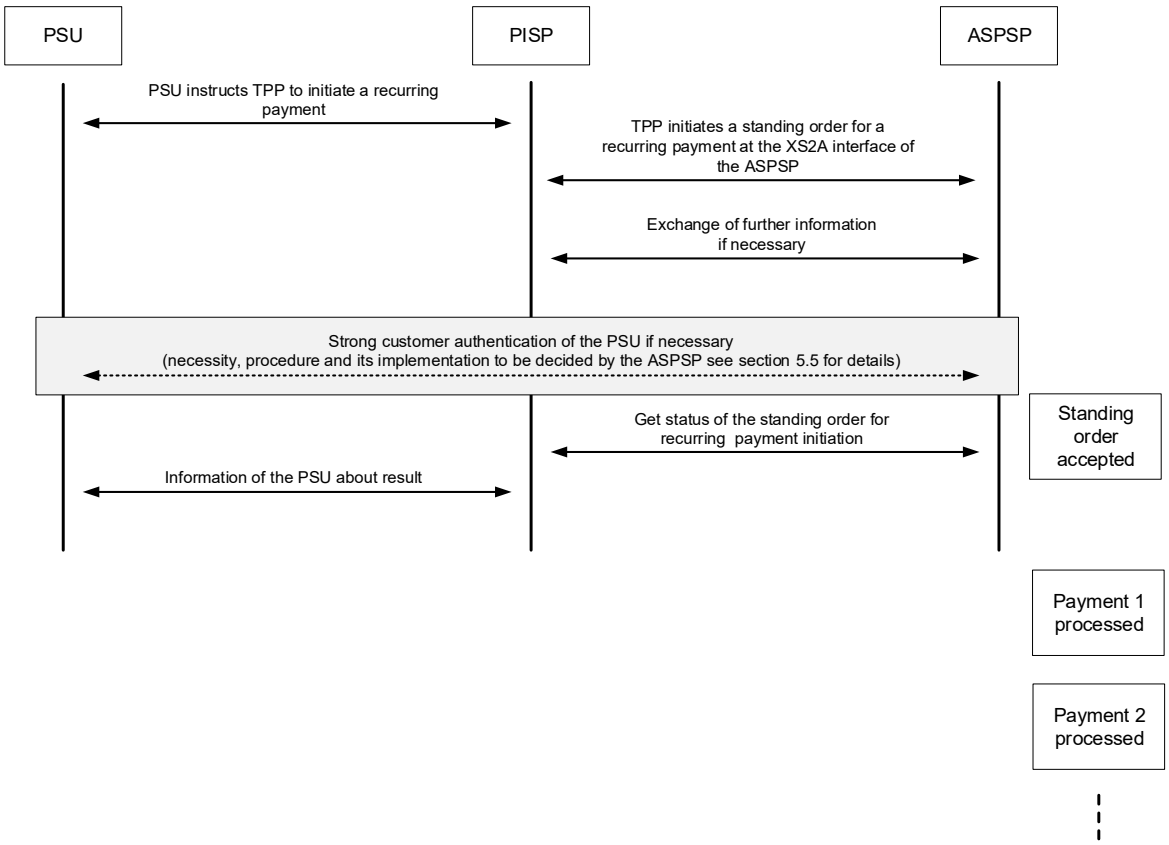

Figure 6: API Service Initiation of a standing order for recurring payments

Remark: The processing, i.e. the actual booking of the recurring payments will be analogous to the processing of recurring payments as initiated by a corresponding standing order in the client interface of the ASPSP, i.e.

- the execution of the following payments is determined by the frequency and validity submitted as part of the initiation of the recurring payment,
- a following payment (belonging to the recurring payment) is only executed if sufficient funds are available at the time of booking, and
- no reporting about the execution of following payments (belonging to the recurring payment) is given at the XS2A interface.

4.5 API Service: Cancellation of payments

The support of this API Service at the XS2A interface is optional.

A TPP uses this API Service to cancel a (still pending) payment, which has been initiated by him before. Only future dated payments and recurring payments may be cancelled by this API Service. The following holds:

- The PSU has to initiate this service at the PSU – TPP interface.
- The ASPSP will reject the service if the TPP cannot be identified at the XS2A interface and/or if it does not have the role PISP.
- Subject to the decision of the ASPSP, strong customer authentication of the PSU has to be executed.

If the initiated payment has been a bulk payment according to section 4.3, the cancellation will affect all included payments. It is not possible to cancel a single payment which has been initiated as part of a bulk payment.

The following figure shows only the very top level information flow of a cancellation of a payment:

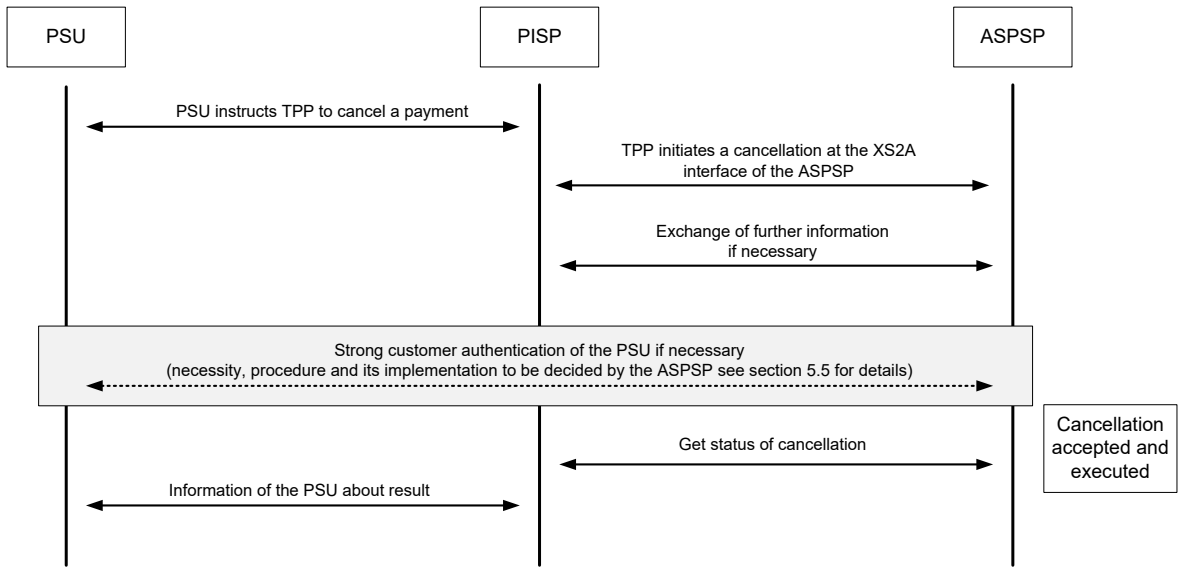

Figure 7: API Service Cancellation of a payment

Remark: It is up to the ASPSP to decide if a given payment can still be cancelled or not.

4.6 API Service: Establish consent on account information

The support of this API Service at the XS2A interface is mandatory.

A TPP may use this API Service to receive the right to execute other account information services in the future without involving the PSU. The TPP may request consent for cards or for payment accounts. Among other parameters, the level of detail accessible for the API Client, as well as a validity period for which the consent may be used and a maximum frequency per day must be fixed within this request. It is possible for the API Client to request a one-time access or a recurring access to the account information.

For the core services, the requirements of [PSD2] and [RTS] shall be observed during the entire validity period granted and for the allowed frequency of services. For the extended services, this is at the discretion of the ASPSP.

The establish consent on account information service is explained in detail in [oFA-OR-CO].

Remark: Please note that while e.g. the consent is established to get account information for a list of accounts, the actual technical service to retrieve the account data might be applicable only per a specific account, cp. Section 4.7 to Section 4.10.

4.7 API Service: Get list of addressable accounts

The support of this API Service at the XS2A interface is optional for an ASPSP.

This API Service can be used by a TPP to receive a list of addressable accounts of a PSU managed by the ASPSP. The term addressable accounts shall refer to online accessible payment accounts (according to article 65, 66, 67 of [PSD2]). ASPSPs support a large variety of account models. The ASPSP shall decide (in compliance with PSD2) what accounts have to be treated as online accessible payment accounts and must therefore be addressable at the XS2A interface.

As a result of this service type, the TPP will receive a list of account numbers. No further information about the accounts is returned. If the TPP has been granted the right to receive further information in the context of a previous "Establish consent on account information" service request, the TPP can use the obtained account numbers to receive further information about the accounts in additional services of the account information service.

The service at the XS2A interface is initiated by the TPP. It does not have to be initiated by the PSU at the PSU – TPP interface previously. However, the PSU must still have granted its consent during a previous service.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role AISP. The ASPSP will also reject the service if the TPP does not have the necessary rights for this service type, i.e. no pre-existing consent as a result from a "Establish consent on account information" can be proven.

The following figure shows only the very top level information flow:

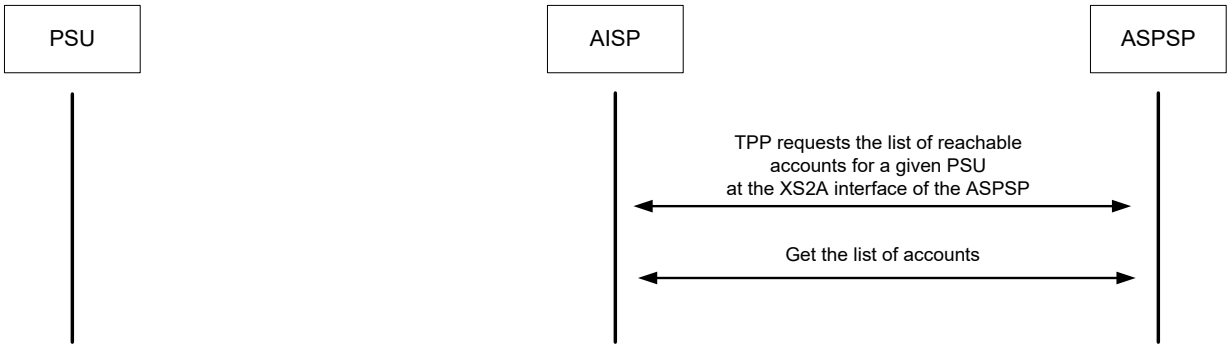

Figure 8: API Service Get list of addressable accounts

4.8 API Service: Get account details of a list of accessible accounts

The support of this API Service at the XS2A interface is mandatory.

This API Service allows the TPP to retrieve detailed information about all accounts of a PSU accessible to this TPP. **Accessible accounts** are defined as those accounts of a PSU for which a consent has been granted to the TPP to access these accounts for balances or transaction information.

Details of these accounts to be delivered as the result of this service can be

- hyperlinks to account information resources associated with these accounts,
- alias identifiers under which these accounts are addressable,
- types and names of the accounts and
- the (booking) balance of the accounts if required as an additional data element and if the right has been granted to the TPP.

The service at the XS2A interface is initiated by the TPP. It does not have to be initiated by the PSU at the PSU – TPP interface previously. However, the PSU must still have granted its consent during a previous service.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role AISP.

The ASPSP will also reject the service request if the TPP does not have the necessary rights for this service type, i.e. no pre-existing consent as a result from a "Establish consent on account information" can be proven.

The following figure shows only the very top level information flow:

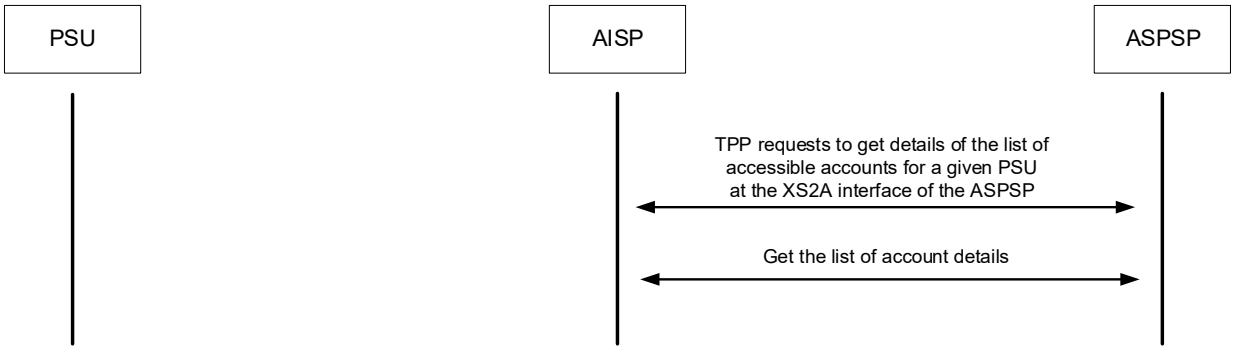

Figure 9: API Service Get account details of a list of accessible accounts

4.9 API Service: Get balances for a given account

The support of this API Service at the XS2A interface is mandatory.

The TPP can use this API Service to receive the balances for a given account. As a result the TPP will receive detailed balances for the account identified in the request of this service, besides booked balances this can be e.g. authorised or intermediary balances, depending on the implementation of the ASPSP. No further information about transactions of the accounts will be returned.

If the PSU has granted access to balances of several accounts, then a corresponding service has to be submitted for each account separately.

Please note that in case of a multicurrency account a list of all balances of the existing sub-accounts in the related currencies is returned to a corresponding request, if account information is granted on multicurrency account level.

The service at the XS2A interface is initiated by the TPP. The service does not have to be initiated by the PSU at the PSU – TPP interface previously. However, the PSU must still have granted its consent during a previous service.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role AISP.

The ASPSP will also reject the service if the TPP can not prove to possess the necessary rights for this service type gained during a previous "Establish account information consent" service.

The following figure shows only the very top level information flow:

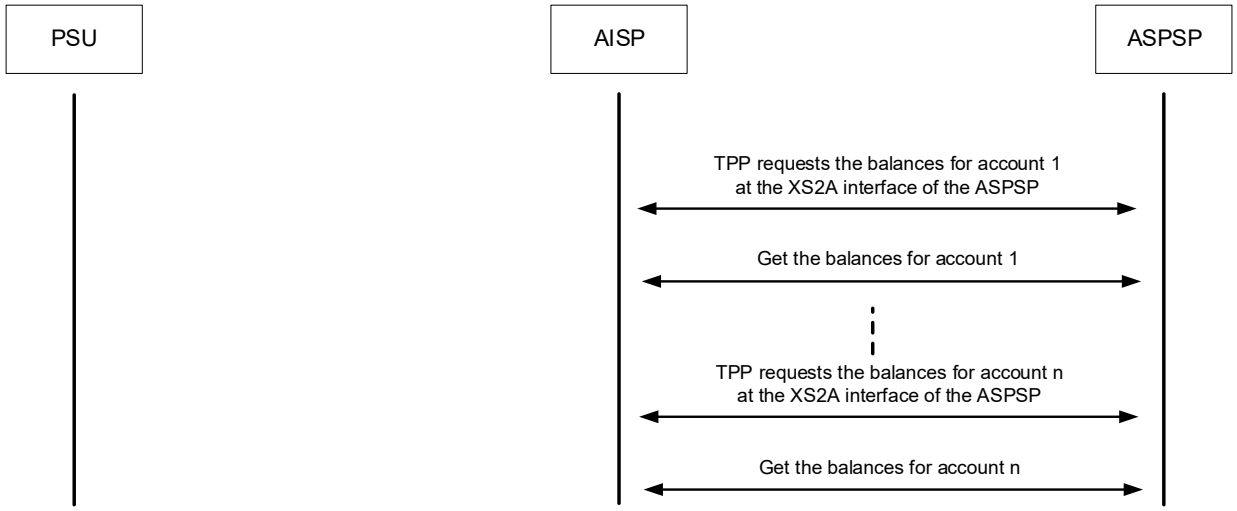

Figure 10: API Service Get balances for a given list of accounts

4.10 API Service: Get transaction information for a given account

The support of this API Service at the XS2A interface is mandatory.

The TPP can use this API Service to receive information about payment transactions of a specific account. As a result the TPP will receive information about all payment transactions executed during the time period indicated in the request. In addition, the ASPSP might return also the booking balance.

Note: Other balances will be provided in scope of the API Service “Get balance information for a given account”.

In addition, the ASPSP can optionally offer the service of a delta report. In this case, the ASPSP is delivering only the information about payment transaction since the last access of this TPP to this account information service or it is delivering the information about payment transaction starting with the next payment transaction with a given transaction identification.

In case of an addressed multicurrency account, the ASPSP shall deliver all payment transactions of all sub-accounts in the related currencies.

The service at the XS2A interface is initiated by the TPP. It does not have to be initiated by the PSU at the PSU – TPP interface previously. However, the PSU must still have granted its consent during a previous service.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role AISP.

The ASPSP will also reject the service if the TPP does not have the necessary rights for this service type, i.e. no pre-existing consent as a result from a "Establish consent on account information" can be proven.

The following figure shows only the very top level information flow:

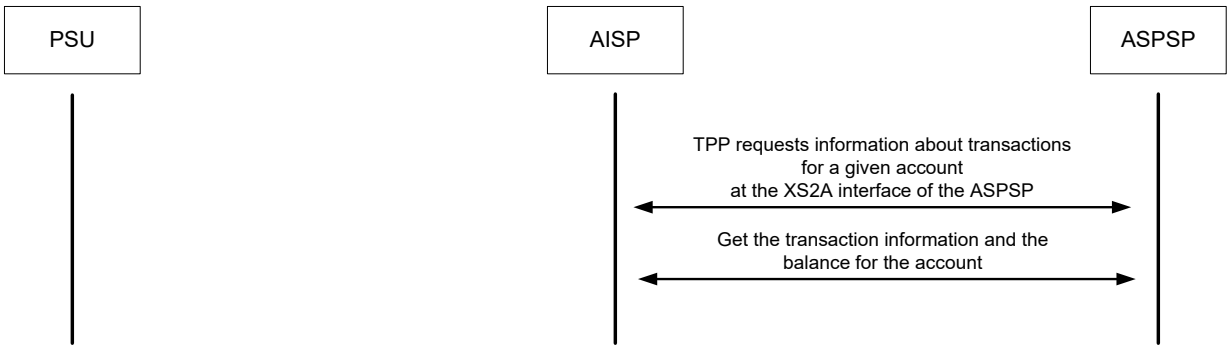

Figure 11: API Service Get payment transaction information for a given account

4.11 API Services with access to card accounts

Card accounts are defined as specific reconciliation accounts for credit cards. Some ASPSPs provide such accounts to aggregate reconciliation of transactions of several cards with the current account of the PSU.

The API Services

- Get card account details of the list of accessible card accounts,
- Get balances for a given card account, and
- Get transaction information for a given card account

are similar to the corresponding API Services with access to payment accounts.

All these API Services are optional.

4.12 API Service: Grouping requested services to signing baskets

The support of this API Service at the XS2A interface is optional for an ASPSP.

A TPP may use this API Service to bundle several services, which are already initiated but not yet authorised. Then the PSU may execute one single SCA the signing basket structure which then provides the consent for all entries simultaneously. This service is described in [oFA-OR-FW].

Remark: The steps for the authorisation of the PSU are not part of the API Service " Grouping services to signing baskets" but are necessary for executing the services contained in the

basket. Depending on the nature of the services contained in the basket it might be necessary to repeat the authorisation steps for other PSU (i. e. services with multilevel SCA).

4.13 API Service: Get confirmation of funds

The support of this API Service at the XS2A interface is mandatory.

The TPP can use services according to this API Service to receive confirmation about the availability of the requested funds on a specific account. As a result the TPP will only receive the answer YES or NO. No further information about the account will be returned.

While the service at the XS2A interface is initiated by the TPP, it must first be initiated by the PSU by means of an e.g. card based payment transaction at a PSU – TPP interface, for example at a checkout point. The PSU – TPP interface is not within the scope of this document.

According to article 65 of [PSD2] the PSU has to inform the ASPSP about its consent to a specific request of the TPP prior to the service. The document at hand does not cover the interface between the PSU and the ASPSP required for the exchange of this consent information.

The ASPSP will reject the service if the TPP cannot be identified correctly at the XS2A interface and/or if it does not have the role PIISP.

The ASPSP will also reject the service if the PSU has not previously informed the ASPSP about its consent to the corresponding service of the TPP.

The following figure shows only the very top level information flow:

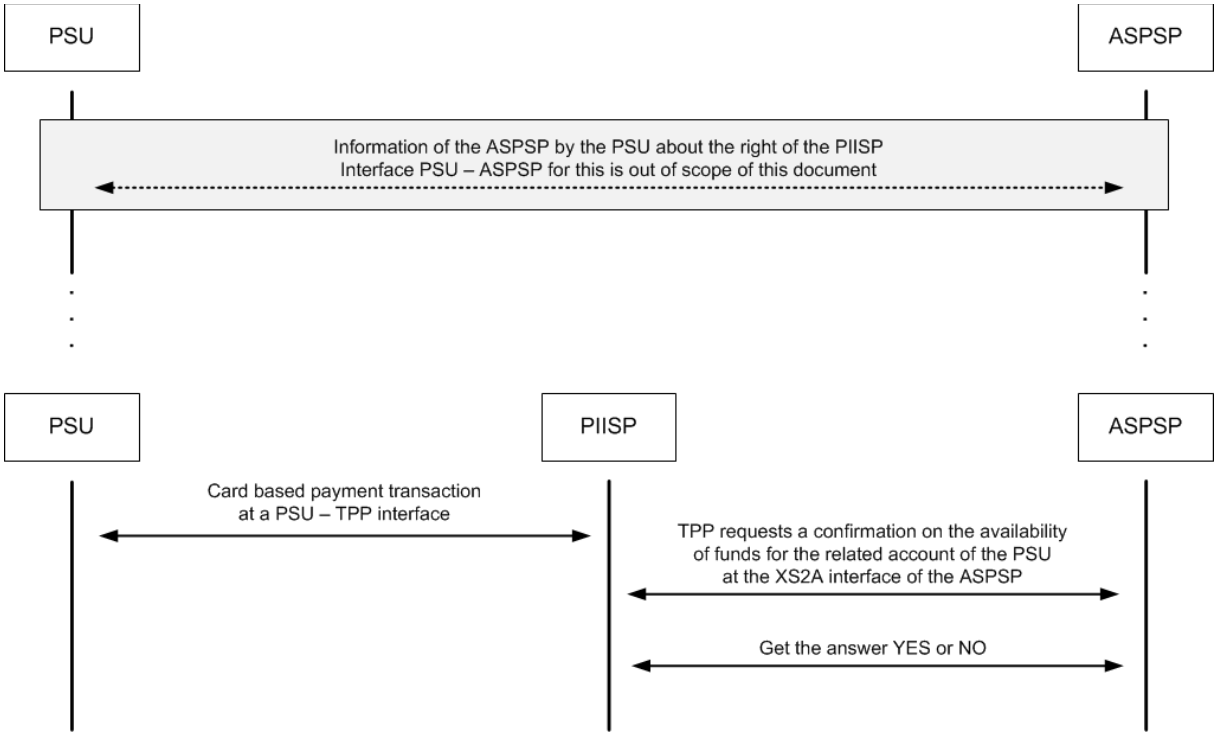

Figure 12: API Service Get the confirmation of funds

Note: The step "Information of the ASPSP by the PSU about the right of the PIISP" is included for information purposes only. It is not part of the service according to this API Service. The step has to be conducted only once for each PIISP.

5 Key concepts of the XS2A interface

This section contains an overview of the key concepts of an XS2A interface implemented according to the specification of the Joint Initiative. For the detailed specification please refer to the document [oFA-IG-Com].

5.1 Identification of the TPP at the XS2A interface

The following are requirements specific for the compliance services at the XS2A interface. They are mandated by the [PSD2] and are additional to the basic requirements given in Section 4.6 in [oFA-OR-FW].

The TPP needs a qualified certificate for website authentication (QWAC) for authentication at the transport layer and a qualified certificate for electronic seals (QSealC) for authentication at the application layer. These certificates have to be compliant with the requirements of the ETSI specification [TS 119 495]. Both certificates must be compliant with the additional requirements defined by [RTS] as well.

To execute a transaction as part of a service supported by the XS2A interface, the TPP has to be authorised to use the necessary role, i.e. PISP, AISP or PIISP. The verification of this role is part of the identification of the TPP. A TPP may have more than one role. All roles of the TPP must be listed in the qualified certificate that the TPP uses for identification at the XS2A interface.

The ASPSP will reject the transaction if the TPP cannot be identified correctly at the XS2A interface and/or if the certificate used by the TPP to identify itself does not list the role required for this transaction.

5.2 Confirmation of the consent of the PSU

Each service at the XS2A interface is subject to the consent of the PSU. How consent of the PSU is confirmed during a service depends on the service type as shown in the following table. A service at the XS2A interface may only be executed if the consent of the PSU can be confirmed, otherwise the ASPSP will reject the service.

API Service	How the PSU grants consent	How consent of the PSU is verified
Payment initiation of - single payment, - future dated payment, - bulk payment, - recurring payment	Authentication of the PSU using strong customer authentication with dynamic linking to the service. In cases of an exemption of strong customer authentication by other means to be decided by the ASPSP.	Verification of the authenticity of the PSU and of the service by verification of the strong customer authentication. In cases of exemption to strong customer authentication by other means to be decided by the ASPSP.

API Service	How the PSU grants consent	How consent of the PSU is verified
Cancellation initiation	Depending on the regulations for this kind of services at the user interfaces offered by the ASPSP to the PSU directly.	Depending on the regulations for this kind of services at the user interfaces offered by the ASPSP to the PSU directly.
Establish account information consent	Identifies itself as part of the authorisation process, if necessary by strong customer authentication.	Verification of the identity of the PSU, if necessary by strong customer authentication.
Get list of accounts	Consent was granted during a previously executed Establish account information consent authorisation process	Verifies the access token given to the TPP as result of a previously executed Establish account information consent authorisation process.
Get details of accessible accounts - payment accounts, - card accounts	Consent was granted during a previously executed Establish account information consent authorisation process	Access token given to the TPP was verified as result of a previously executed Establish account information consent authorisation process.
Get balances for a given account - payment accounts, - card accounts	Consent was granted during a previously executed Establish account information consent authorisation process.	Access token given to the TPP was verified as result of a previously executed Establish account information consent authorisation process.
Get transaction information for a given account - payment accounts, - card accounts	Consent was granted during a previously executed Establish account information consent authorisation process.	The access token given to the TPP was verified as a result of a previously executed Establish account information consent authorisation process.
Establish signing basket	Authentication of the PSU using strong customer authentication (if necessary with dynamic linking). In cases of an exemption of strong customer authentication by other means to be decided by the ASPSP.	Verification of the authenticity of the PSU and of the service request by verification of the strong customer authentication. In cases of exemption to strong customer authentication by other means to be decided by the ASPSP.
Confirmation of funds	The PSU has already informed the ASPSP about its consent using another interface.	Verification if the ASPSP has already been informed about the consent of the PSU.

Table 3: Consent of the PSU

6 Operational rules

This section summarises the operational rules to be observed at the XS2A interface specifically, i.e. by each TPP accessing the XS2A interface and each ASPSP providing an XS2A interface which are particular to the compliance services. Not all of these rules are enforced by technical means of the XS2A interface. Further operational rules which apply for the ASPSP and the TPP in general are listed in [oFA-OR-FW].

The rules are given in alphabetic order. The order does not represent an order of importance.

6.1 Identification of the TPP and correct role

The TPP has to identify itself towards the ASPSP using a qualified certificate. The certificate of the TPP shall contain all roles the TPP is authorised to use.

The TPP has to use a qualified certificate within the setup of the TLS-connection with the ASPSP. For this the TPP has to use a qualified certificate for website authentication according to section 8 of [eIDAS].

If required by the ASPSP the TPP has to sign the request messages. The TPP has to use a qualified certificate for electronic seals according to section 5 of [eIDAS] for this purpose.

An ASPSP will reject any transaction at the XS2A interface if the TPP cannot be identified correctly, e.g. if the certificate is invalid, or if the TPP does not have the necessary role for the transaction, i.e. a TPP may execute payment initiation services if the TPP is certified to be a payment initiation service provider by its certificate, the same holds for account information services and payment instrument issuing services.

6.2 Non-Discrimination

An ASPSP has to respond to any incoming request message if the TPP can be identified correctly. It has to respond without any discrimination and applying the same service level offered to its own customer at the interfaces.

Article 68 of [PSD2] defines the only valid exceptions to this rule.

6.3 Payment Products

The portfolio of payment products to be supported in the XS2A interface for a PSU must fulfil the rules of non-discrimination as defined in [PSD2].

6.4 Revocation/cancellation of payment initiations

The ASPSP shall ensure that the possibility of the PSU to revoke payment initiations which are submitted via an PIS fulfils the legal requirements as defined in article 80 of [PSD2] and national law respectively.

Nevertheless, this framework allows the revocation of all future dated payments by the PSU directly between PSU and ASPSP. This applies to single future dated payments, future dated bulk payments and to recurring payments initiated by standing orders.

A future dated payment initiated by a TPP at the XS2A interface can also be cancelled before execution by the PSU by directly accessing the ASPSP.

A recurring payment initiated by a TPP at the XS2A interface can also be cancelled before execution by the PSU by directly accessing the ASPSP. It is also possible that the PSU changes parameters of the recurring payment such as frequency and validity or terminates the recurring payment finally by directly accessing the ASPSP.

6.5 Separation and combination of services

On the level of a single interaction of TPP and ASPSP, services are separated and cannot be combined.

A TPP may only use one role per API service. This role has to be confirmed by the certificate the TPP uses for identification.

The TPP may of course use different roles for different services. If supported by the XS2A interface of the ASPSP the TPP may use an exchange flow of request/response interactions at the XS2A interface to connect two (or more) consecutive services. The ASPSP will recognise the connection between the API services and will react accordingly. This allows to avoid unnecessary steps for the authentication of the PSU.

6.6 Validity of an service at the XS2A interface

One API service may consist of several request/response interactions between TPP and ASPSP. Between these request/response interactions some time is needed e.g. for PSU SCA interaction.

During the first request/response interaction, the ASPSP generates a new resource representing this initiated resource. The default validity time of this resource is 30 minutes. During this validity time, the TPP may address the resource of the ASPSP by means of requests permitted by this framework. An ASPSP may decide to set a different validity time for a resource.

6.7 Withdrawal of authorisation

The TPP shall cease to use its qualified certificate as soon its authorisation to act as a PISP, AISP and/or PIISP is withdrawn.

7 Message and data model

An abstract data model is presented for the usage of the XS2A Interface and the openFinance API in [oFA-OR-FW] and [oFA-IG-Com]. In this document only the differences and service-specifics for the compliance services are presented.

7.1 Protocol Level

For the request data on protocol level, the TPP requires a qualified certificate issued by a QTSP compliant with [eIDAS] according to [RTS] to identify itself at the XS2A interface. More precisely, it needs to use certificates based on qualified certificates for website authentication (QCWA) and on qualified certificates for electronic seals (QSealC). The TPP's role specified with this certificate must coincide with the role needed for service initiation, i.e. in order to initiate a payment service, the TPP must be a payment initiation service provider verified by its certificate, and the same holds for account initiation services and payment instrument issuing services accordingly. For the core services, the ASPSP is not allowed to deny the access of the TPP at its XS2A interface.

7.2 Payment Initiation related data model

Within the XS2A interface, a payment initiation transaction consists of at least the Payment Initiation Request and the Payment Initiation Response. Both, Payment Initiation Requests and Payment Initiation Responses belong to the category of Transaction Initiation messages, they are a Transaction Initiation Request resp. a Transaction Initiation Response. The data model for Transaction Initiation Requests and Responses are explained in detail in [oFA-OR-FW].

For the Decoupled, Redirect or Oauth2 SCA approach, there must be at least a second message pair payment Status Request and Payment Status Response to retrieve the information whether the SCA method was successful. In all cases, the ASPSP may ask the TPP to create/update the authorisation sub-resource created after the Payment Initiation Request with additional data via an Update Data request.

7.2.1 Payment Initiation Request Data on Protocol Level

Service specific parameters that might occur additionally to the parameters in a Transaction Initiation Request are the following:

- Rejection Preference Indicator (optional)

  The TPP can use this indicator to set a priority how the ASPSP shall act in case that not sufficient funds are available, indicating:

  - if a payment initiation shall be rejected by the ASPSP, or
  - if ASPSP shall deal with the payment initiation request as it would in its online channel (e.g. potentially waiting for a certain amount of time if funds arrive with which the initiation of the payment is possible).

- Payment Product (mandatory)

7.2.2 Payment Initiation Response Data on Protocol Level

Service specific parameters that might occur additionally to the parameters in a Transaction Initiation Response are the following:

- Transaction Fees and Transaction Fee Indicator (optional)

  Transports the total transaction fee relevant for the underlying payments (including currency conversion fees to the initiated transfer if applicable)

7.2.3 Payment Status Request

This request is used when a status of the payment is needed by the TPP, i.e. in the redirect, OAuth2, and decoupled SCA approach.

No specific data elements.

7.2.4 Payment Status Response

This response can contain several data elements in addition to the payment status. Details are defined in [oFA-IG-Com].

7.3 Account Information related data model

The AIS service in the XS2A interface is divided in two different steps, first the establishment of a consent and second the read data access as such. These two steps are implemented through different APIs, the /consents and the /accounts resp. /card-accounts APIs, cf. [oFA-IG-Com] and [oFA-CO]. The Establish Consent Request/Response messages are again Transaction Initiation Requests/Responses, respectively.

7.3.1 Establish Consent

The message an data model for establish consent is specified in [oFA-CO] and explained in detail in [oFA-OR-CO].

Within this phase of the Account Information Service, the PSU is giving the consent to the AISP on the following parameters:

- the accounts accessible for the AIS,
- the type of Account Information Service to grant an access to (transaction list, list of standing orders, balances, list of addressable accounts, account details),
- whether this is a one-time access or a recurring one, and
- if it is a recurring access: the maximum frequency per day for accessing the information and its expiry date until which the access is granted.

The consent authorised by the PSU towards the ASPSP with an SCA and as a result of this process, a consent resource is created. The TPP can use this to retrieve the requested account information.

7.3.2 Read Account Data

Within the XS2A Interface a Get account information transaction is usually only one pair of a Get account information request and response. Only in cases, where the related account information is a payment transaction report, the content of the response might be paginated, or a link for a download of the data in a second step is provided.

The Get Account Information Request is addressing the related resource in the /accounts or /card-accounts API. The only common parameter for all defined types of account information is the following:

- Request Identification (mandatory)

  This is a unique ID generated by the API Client to identify individual request messages.

- Consent-ID (mandatory)

  The identification of the underlying consent resource.

- OAuth2 Access token (conditional)

  This is the access token resolving from an OAuth2 based authentication process.

- API Client electronical signature (conditional)

  Electronic signature is generated by the TPP following the definition in [oFA-PFSM] Section 6.2.2.2. Only to be delivered if mandated by the ASPSP.

- Further signature related data (conditional)

  In case the TPP has signed the request message, this contains the hash value calculated over the content of the body.

- PSU Context Data (used for the ASPSP's risk management, if not included in the message the ASPSP will take this into account in its risk management)

  - IP Address PSU (conditional)

    The IP address of the PSU, it is the IP address of the PSU, that was used by the PSU when actively requesting the service between PSU and API Client. If the PSU did not explicitly request the service, the IP address is not to be included.

  - PSU Device and Application Software Information (operating system, browser etc.) (optional),

  - GEO Location PSU (optional)

- PSU Account ID (conditional)

- PSU Involvement Indicator

  This indicator is not a parameter of the header or body of a request message itself, it only exists indirectly. The PSU's IP address is contained if and only if the request was actively initiated by the PSU. Thus, this data element indicates whether the PSU has initiated this request directly by a corresponding request on the PSU – TPP interface.

7.3.2.1 Get account details transaction

The related request message contains one additional parameter:

- With Balance Inidicator (optional)

  This data elements indicates that the TPP is requesting the ASPSP to show the booked balance together with the account details.

The related response contains only the account details like account identification, name as given by the PSU, account type and the hyperlinks to further account information resources as granted by the PSU.

7.3.2.2 Get balances transaction

The related request message addresses a dedicated account in the /accounts API. It contains no further parameter. The response returns at least the booking balance of the addressed account, in addition the ASPSP can deliver further balances as the intermediary or authorised balance.

In case of a multicurrency account, the response contains the related balances of all sub-accounts.

7.3.2.3 Get transaction information transaction

The related request message addresses a dedicated account and contains the following additional parameters:

- Acceptance Format Preference (mandatory)

  The TPP can define with this data element all format types of payment transaction reports which are supported of the camt.05x, JSON or MT94x formats and can define a preference on these formats.

- With Balance Indicator (optional)

  This data element indicates that the TPP is requesting the ASPSP to show the booked balance together with the payment transaction information.

- Delta Indicator (optional, but only to be used if supported by ASPSP)

  The TPP can indicate to receive only a delta report, either by

  - Transaction Identification (conditional, only use together with a positive Delta Indicator, but only to be used if supported by ASPSP).

    The referred transaction is the last transaction known by the TPP. The request is then only to receive all payment transactions booked after this payment transaction.

  - Booking status (mandatory)

    With the booking status, the TPP can ask for only booked or booked and pending payment transactions together. If supported by the ASPSP, the TPP can also ask only for the pending payment transactions.

  - Date From (conditional, is mandated if no Delta Indicator is set)

    If contained, the ASPSP is asked to report on all payment transactions starting with that booking date.

- Date To (optional)

  The ASPSP is asked to report on all payment transactions ending with that booking date.

The response will deliver the transaction lists of the addressed account following the request parameter settings.

If the addressed account is a multicurrency account, then all transactions retrieved from all sub-accounts are reported in their related currencies together.

7.4 Confirmation of Funds related data model

This service will be used by a payment service provider issuing card-based payment instruments (PIISP). According to article 65 1.(b) of [PSD2] the payer (PSU) has to give explicit consent to the ASPSP to respond to such a request.

The PSU has to inform the ASPSP before the first request of the PIISP can be answered by the ASPSP. As part of this initiation step the PSU has to inform the ASPSP about the ID-number of the card issued by the PIISP. In addition the PSU has to inform the ASPSP which of his payment accounts shall be "connected" to the card.

The XS2A interface will not be involved in executing the initiation step. In the following it is assumed that this initiation step has been executed and that the ASPSP has stored the ID-number of the card of the PSU and the "connected account".

7.4.1 Confirmation of Funds Request

- Request Identification (mandatory)

  This is a unique ID generated by the API Client to identify individual request messages.

- Consent-ID (conditional)

  The identification of the underlying consent resource.

- Further Signature related data (conditional)

  In case the TPP has signed the request message, this contains the hash value calculated over the content of the body.

- API Client Electronical Signature (conditional)

  Electronic signature is generated by the TPP following the definition in [oFA-PFSM] Section 6.2.2.2. Only to be delivered if mandated by the ASPSP

- Card Number of card issued by the PIISP (optional)

  Card number of the card issued by the PIISP, should be delivered if available.

- PSU Account (mandatory)

  The account number of the PSU

- Name Payee (optional)

  The merchant where the card is accepted as an information to the PSU.

- Instructed Amount

7.4.2 Confirmation of Funds Response

- Request Identification (mandatory)
- Funds Availability Indicator (mandatory)

  Indicator if sufficient funds are available at the time of the request

8 Annex

8.1 Glossary

AIS

Account Information Service according to article 4 (16) of [PSD2] and as regulated by article 67 of [PSD2].

AISP

Payment service provider offering an AIS to its customer. See article 4 (19) of [PSD2].

ASPSP

Account Servicing Payment Service Provider providing and maintain a payment account for a payer. See article 4 (17) of [PSD2].

PIISP

Payment Instrument Issuer Service Provider according to article 4 (14) and 45) of [PSD2]. A PIISP can use the service "Confirmation on the availability of funds" as regulated by article 65 of [PSD2].

PIS

Payment Initiation Service according to article 4 (15) of [PSD2] and as regulated by article 66 of [PSD2].

PISP

Payment service provider offering a PIS to its customer. See article 4 (18) of [PSD2].

PSP

Payment service provider according to article 4 (11) of [PSD2].

PSU

Payment Service User according to article 4 (10) of [PSD2].

QTSP

Qualified Trust Service Provider, e. g. a trust centre issuing qualified certificates

SCA

Strong Customer Authentication – authentication procedure based on two factors compliant with the requirements of [PSD2] and [RTS].

TPP

Third Party Provider – generic term for AISP/PIISP/PISP.

TSP/QTSP

Trust Service Provider according to [eIDAS]. Within the context of the XS2A interface specification only qualified TSPs (QTSPs) according to section 3 of [eIDAS] issuing qualified certificates for electronic seals and/or qualified certificates for website authentication which are compliant with the requirements of [RTS] are relevant.

XS2A interface

Access to account interface – interface provided by an ASPSP to TPP for accessing accounts.

8.2 References

[oFA-IG-Com] openFinance API Framework, Implementation Guidelines, Compliance Services, Version 2.4, 31 October 2025

[oFA-OR-CO] openFinance API Framework, Operational Rules, Consent API for V2, Version 2.0, 31 October 2025

[oFA-OR-FW] openFinance API Framework, Operational Rules, Basic Operational Rules of the Framework, Version 2.0, 31 October 2025

[oFA-CO] openFinance API Framework, Implementation Guidelines, Consent API for V2, Version 2.2, 31 October 2025

[oFA-PFSM] openFinance API Framework, Implementation Guidelines for Protocol Functions and Security Measures, Version 2.3, 31 October 2025

[oFA Disc] openFinance API Framework, Implementation Guidelines, Discovery Services, Version 1.1, 24 January 2025

[oFA Intro] openFinance API Framework, A Guide to Version 2.2, 31 July 2025

[RTS] Commission Delegated Regulation (EU) 2018/389 of 27 November 2017 supplementing Directive 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, L69/23, Official Journal of the European Union, 13.03.2018

[eIDAS] Regulation (EU) No 910/2014 of the European Parliament and of the Council on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market, 23 July 2014, published 28 August 2014

[TS 119 495] ETSI TS 119 495, Electronic Signatures and Infrastructures (ESI); Sector Specific Requirements; Qualified Certificates Profiles and TSP Policy Requirements under the Payment Service Directive 2015/2366/EU, V1.5.1 (2021-04)

[PSD2] Directive (EU) 2015/2366 of the European Parliament and of the Council on Payment Services in the Internal Market, published 25 November 2016

8.3 List of figures

8.4 List of tables