THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

Joint Initiative on a PSD2 Compliant XS2A Interface

NextGenPSD2 XS2A Framework

Operational Rules

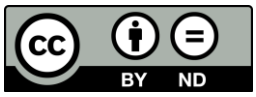
Version 1.0

08 February 2018

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 Background

With [PSD2] the European Union has published a new directive on payment services in the internal market. Among others [PSD2] contains regulations on new services to be operated by so called Third Party Payment Service Providers (TPP) on behalf of a Payment Service User (PSU). These new 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 on the Availability of Funds Service (FCS) to be used by a Payment Instrument Issuing Service Provider (PIISP) TPP as defined by article 65 of [PSD2].

To implement these new services (subject to PSU consent) a TPP needs to access the account of the PSU. The account is usually 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).

Responsibilities and rights of TPP and ASPSP concerning the interaction at the XS2A interface are defined and regulated by [PSD2]. In addition, more detailed requirements for the implementation and operation of the XS2A interface are defined by [EBA-RTS].

1.2 Task

The Joint Initiative has prepared a specification of an XS2A interface which

- supports the new services defined by [PSD2],
- enables an ASPSP to implement an XS2A interface compliant with the requirements of [PSD2] and [EBA-RTS] by an ASPSP, and
- can in future be extended to support further value-added services beyond the scope of [PSD2].

1.3 Limits

The Joint Initiative only specified the XS2A interface which is to be provided by an ASPSP and to be used by a TPP. It is not giving guidance on the overall PSD2 compliance of the ASPSP implementation e.g. regarding the supported authentication method.

Although the overall scope of PSD2 work includes further interfaces, these interfaces are not part of the work of the Joint Initiative. For this reason the following interfaces are not considered further in this document:

- Interface PSU – TPP for the interaction of the PSU with the TPP.
- Interface PSU – ASPSP for executing online banking transactions.
- Interface TPP – QTSP for request and delivery of the qualified certificates the TPP needs to identify itself at the XS2A interface of an ASPSP.
- Interface ASPSP – QTSP used by the ASPSP to request status information from the QTSP about the qualified certificates of a TPP.
- Interface TPP – national authority of the home Member State of the TPP for the authorisation of the TPP.
- Interface QTSP – national authority of the home Member State of a TPP for the exchange of information about the authorisation status of the TPP.

In future there may be national or international registries containing information about ASPSP and/or TPP. However, these registries are not considered further in this document. The XS2A interface specified by the Joint Initiative will work without these registries.

1.4 Documents

The document at hand gives an overview of the PSD2 compliant XS2A interface specified by the Joint Initiative. The document furthermore contains basic rules to be observed by an ASPSP when providing an interface and rules to be observed by a TPP when using an interface based on the specifications of the Joint Initiative.

The technical specification of the XS2A interface in form of an API specification is not part of this document. Please refer to the corresponding Implementation Guidelines [XS2A-ImplG] for this technical specification.

1.5 Document History

Version	Change/Note	Approved
0.99	Market consultation draft of the Berlin Group XS2A Interface Framework	NextGenPSD2 Taskforce, 27 September 2017
1.0	Version 1.0 for publication. Takes into account the results of the market consultation and the final EBA-RTS on SCA and CSC.	NextGenPSD2 Taskforce, 08 February 2018

2 Services and variants of the XS2A interface

2.1 Scope of the XS2A interface

The work of the Joint Initiative is limited to the specification of the XS2A interface. The following figure shows the (logical) location of this interface:

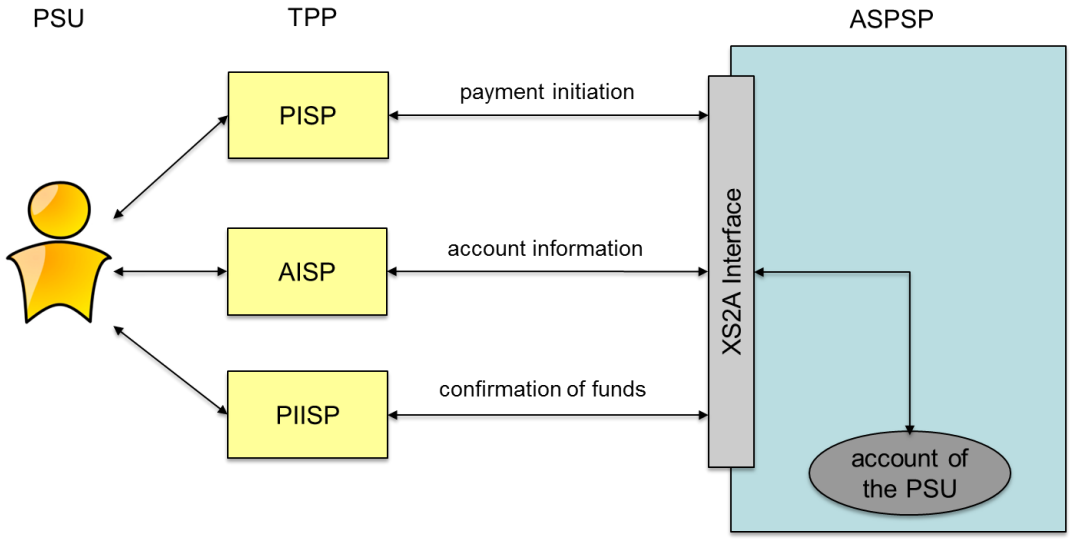


Figure 1: XS2A interface

An ASPSP can use this specification to implement the PSD2 compliant XS2A interface necessary to allow a TPP access to accounts managed by the ASPSP. The TPP can use the specification to implement its accesses to the accounts managed by an ASPSP.

Please note: The interface between the TPP and the PSU is not within the scope of this specification.

2.2 Services of the XS2A interface

The XS2A interface supports different services. 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 which extended service it wants to support in its implementation of the XS2A interface in accordance with its own market needs.

2.2.1 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 comply with the requirements 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 comply with the requirements defined by article 67 of [PSD2].
Fund confirmation service	FCS	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 comply with the requirements defined by article 65 of [PSD2].

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

For each of these core services, the specification [XS2A-ImplG] of the Joint Initiative defines a set of request/response messages and the corresponding data elements. These messages and data elements are exchanged between the TPP and the ASPSP at the 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.

2.2.2 Extended services

The necessary set of request/response messages and the corresponding data elements for extended services can be specified either by

- the Joint Initiative as part of a future new release of the specification [XS2A-ImplG],
- a group of interested ASPSPs or
- a single 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.

2.3 Variants of the XS2A interface

[XS2A-ImplG] specifies 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 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 sub-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 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:

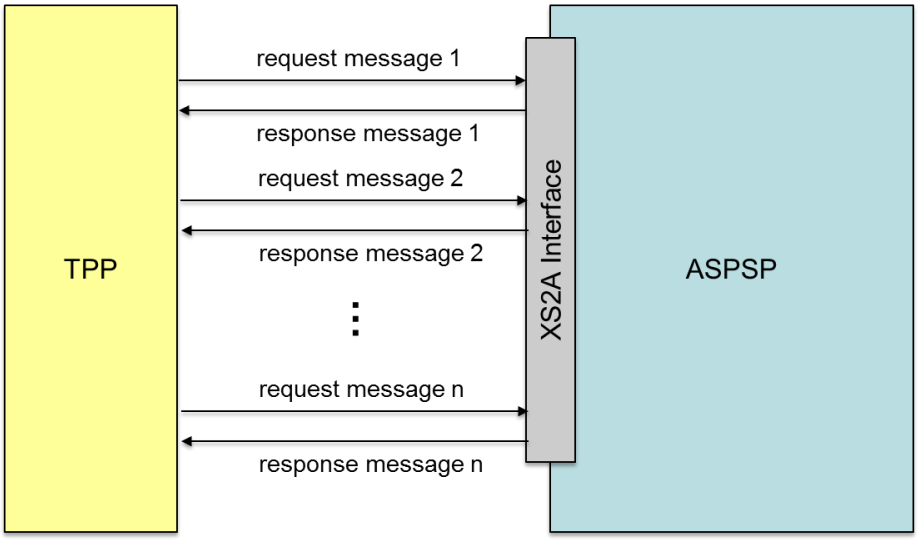


Figure 2: Interaction of TPP and ASPSP at the XS2A interface

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 fund confirmation service (FCS) 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 transaction 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 [EBA-RTS].

- The ASPSP shall respond to incoming requests of any TPP without discrimination in compliance with the requirements from [PSD2] and [EBA-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 [EBA-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 Use cases supported for the core services

The current version of the XS2A interface specification supports the following use cases for the core services:

Use case	Service	Role of the TPP	Support optional	PSU directly involved
Initiation of a single payment	Payment initiation service	PISP	no	yes
Initiation of a future dated single payment	Payment initiation service	PISP	yes	yes
Initiation of a multiple/bulk payment	Payment initiation service	PISP	yes	yes
Initiation of a recurring payment	Payment initiation service	PISP	yes	yes
Establish account information consent	Account information service	AISP	yes	yes
Get list of reachable accounts	Account information service	AISP	yes	no
Get account details of the list of accessible accounts	Account Information service	AISP	no	no
Get balances for a given account	Account information service	AISP	no	no
Get transaction information for a given account	Account information service	AISP	no	no
Get a confirmation on the availability of funds	Funds confirmation service	PIISP	no	no

Table 2: Use cases for the core services

Each use case belongs to one of the core services. A TPP may only execute a transaction according to a use case if it holds the corresponding role indicated in the column "Role of the TPP".

In addition, the XS2A interface will support technical use cases within the RESTful API approach which are not necessarily used within the above mentioned use cases, e.g. to read

details on consent objects or other created resources. Further details on the technical use cases will be defined in [XS2A-ImplG].

Not all of the above use cases have to be supported at the XS2A interface of an ASPSP. If a use case is marked as optional in the column "Support optional" the ASPSP is free to decide whether or not to support this use case at its XS2A interface.

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

If a transaction based on a use case requires direct involvement of a PSU, strong customer authentication of the PSU may be necessary. Please refer to 5.5 for details about strong customer authentication. One of the purposes of a strong customer authentication is to prove that the transaction is executed with the consent of the PSU.

If a transaction is based on a use case that 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 transaction. A longer time period may elapse between the PSU giving the consent and the actual execution of the transaction by the TPP. The steps necessary for giving and proving the consent of the PSU depend on the use case and will be explained in the following sections and in section 5.4.

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 use cases, 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 Use case: Initiation of a single payment

Transactions according to this use case 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 transaction 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 transaction 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:

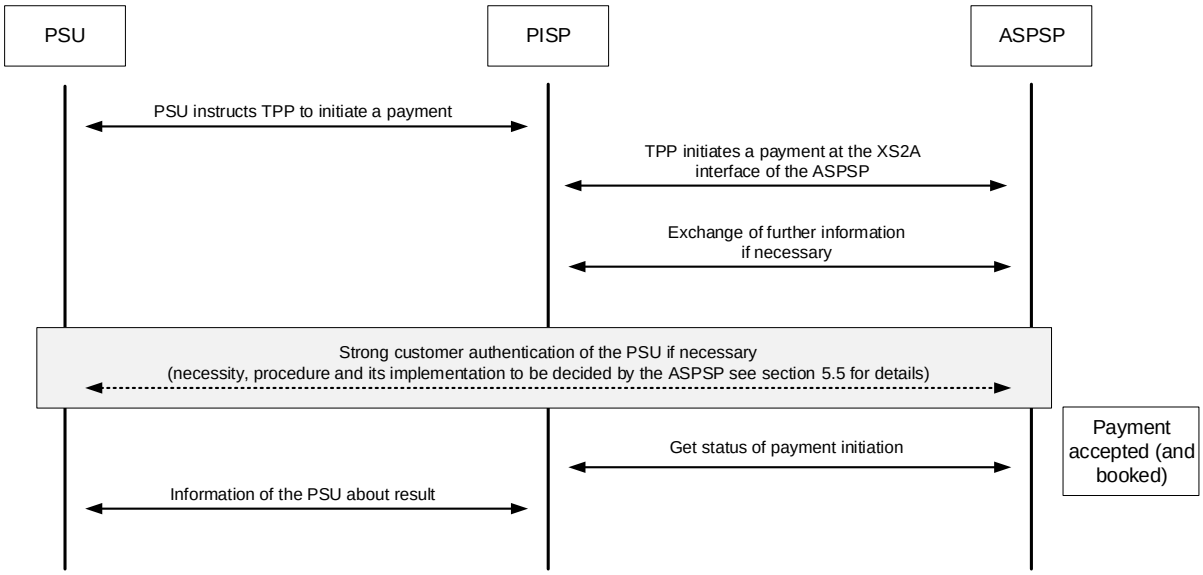


Figure 3: Use case Initiation of a single payment

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 Use case: Initiation of a future dated single payment

Thbe 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:

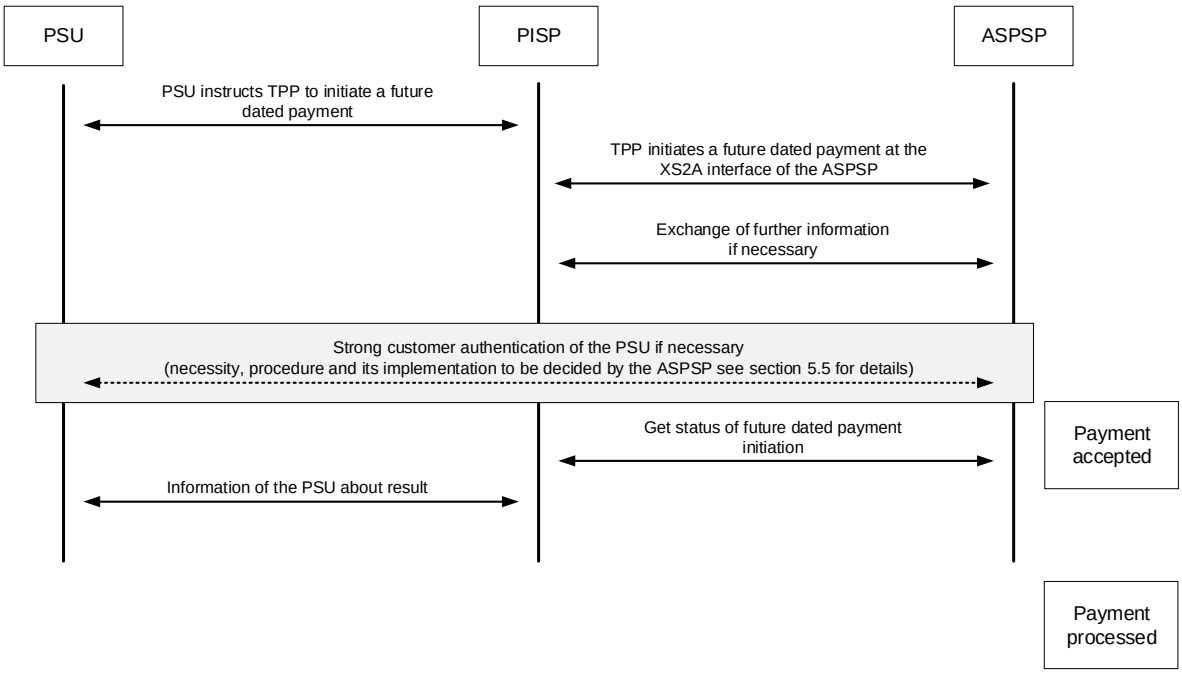


Figure 4: Use case Initiation of a future dated payment

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 Use case: Initiation of a multiple/bulk payment

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. The collecting of the several payments may be performed in the interface between PSU and TPP.

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

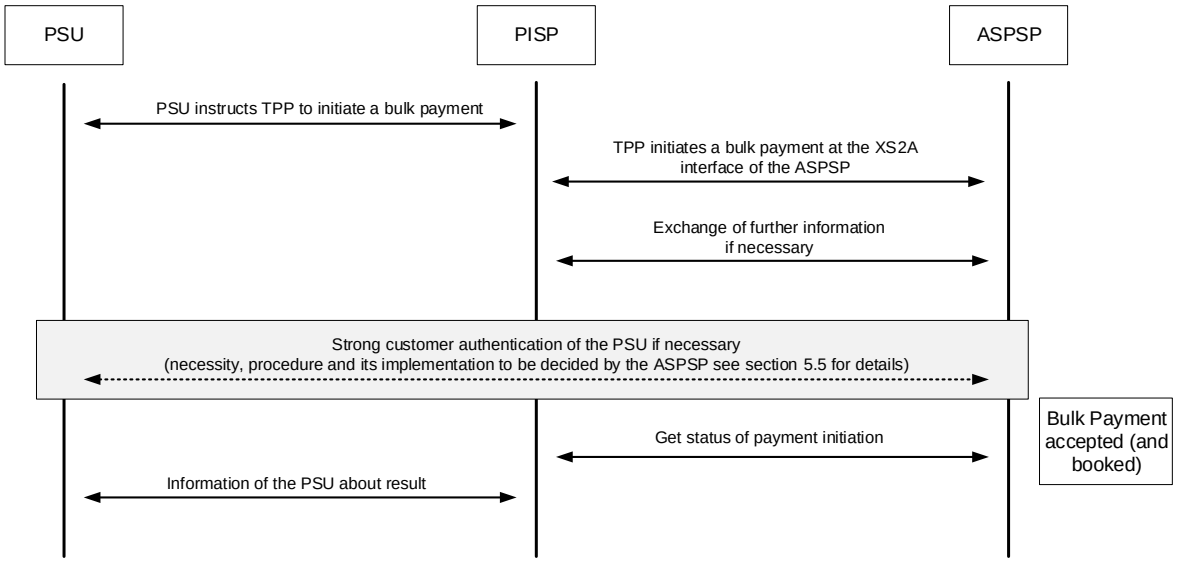


Figure 5: Use case Initiation of a bulk payment

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 Use case: Initiation of a recurring payment

The initiation of a recurring payment is realised in the XS2A interface by 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.

This specific payment initiation needs to be authorised by the PSU with a SCA.

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

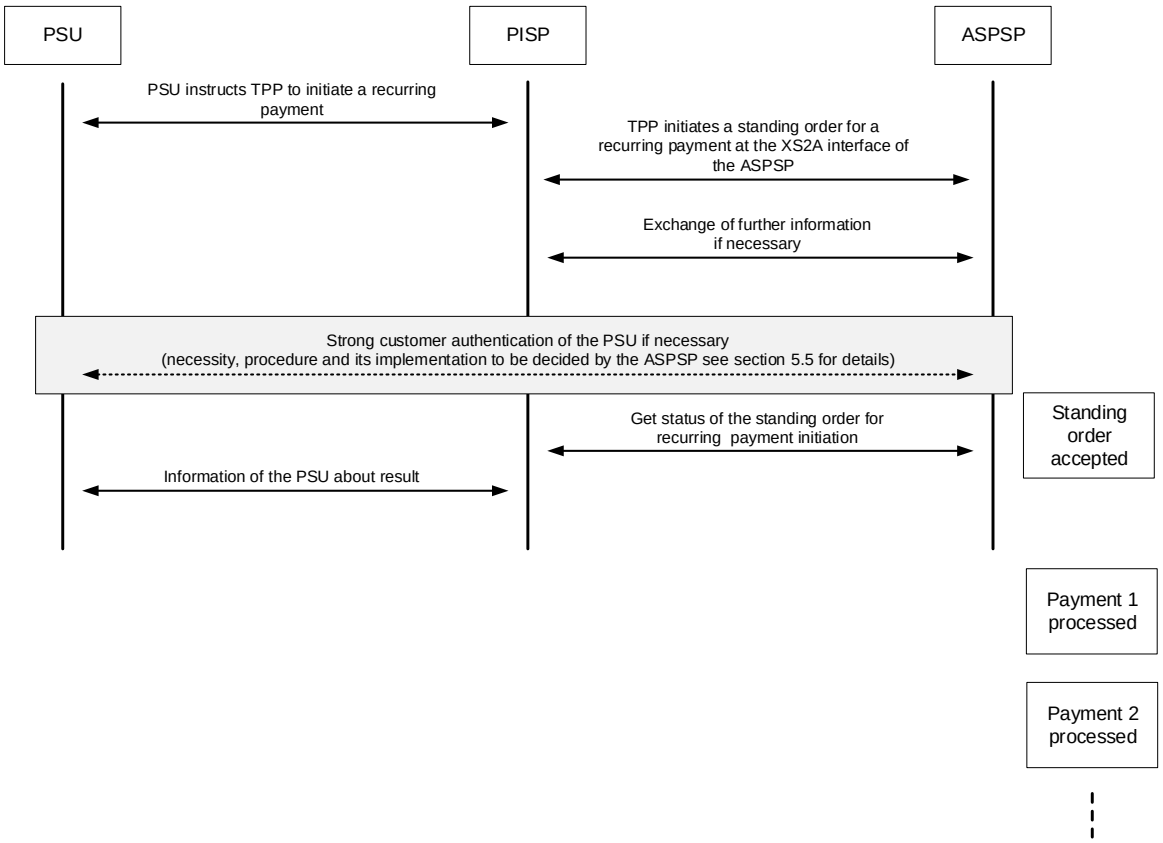


Figure 6: Use case Initiation of a standing order for recurring payments

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.

4.5 Use case: Establish account information consent

A TPP may execute transactions according to this use case to receive the right to execute further transactions according to the other use cases of the account information service. Subject to consent of the PSU, the TPP can obtain the following rights for transactions (of the account information service):

- Get the list of reachable accounts of the PSU once.
- Get the balances for a list of accounts once or multiple times.
- Get payment transaction information for a list of accounts once or multiple times.

If the TPP is granted the right to access balance or payment transaction information for certain accounts, this will include automatically the right to retrieve detailed information about the related payment accounts.

If the TPP is granted the right to execute a transaction multiple times, the validity period of the right in days or the maximal period offered by the ASPSP are defined. It is furthermore possible to define the permitted frequency of corresponding transactions (per day). The requirements of [PSD2] and [EBA-RTS] shall be observed during the entire validity period granted and for the allowed frequency of transactions.

The ASPSP can offer optionally that the TPP submits only the account information type which has been agreed on between TPP and PSU. The ASPSP then will involve the PSU into the selection of the corresponding accounts. This option is not supported in the embedded SCA approach, cp. section 5.5.

Remark: Please note that while e.g. the consent is established to get account information for a list of accounts, the actual technical transaction to retrieve the account data might be applicable only per a specific account, cp. Section 4.6 to Section 4.9.

In case of multicurrency accounts, the account access can be granted on multicurrency account level as well as on sub-account level. The TPP is steering this by submitting the corresponding request, addressing the multicurrency account or sub-account level.

While the transaction 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. However, the TPP has to inform the PSU clearly about the rights for which the PSU has to confirm its consent.

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

Subject to the decision of the ASPSP, strong customer authentication of the PSU may be necessary.

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

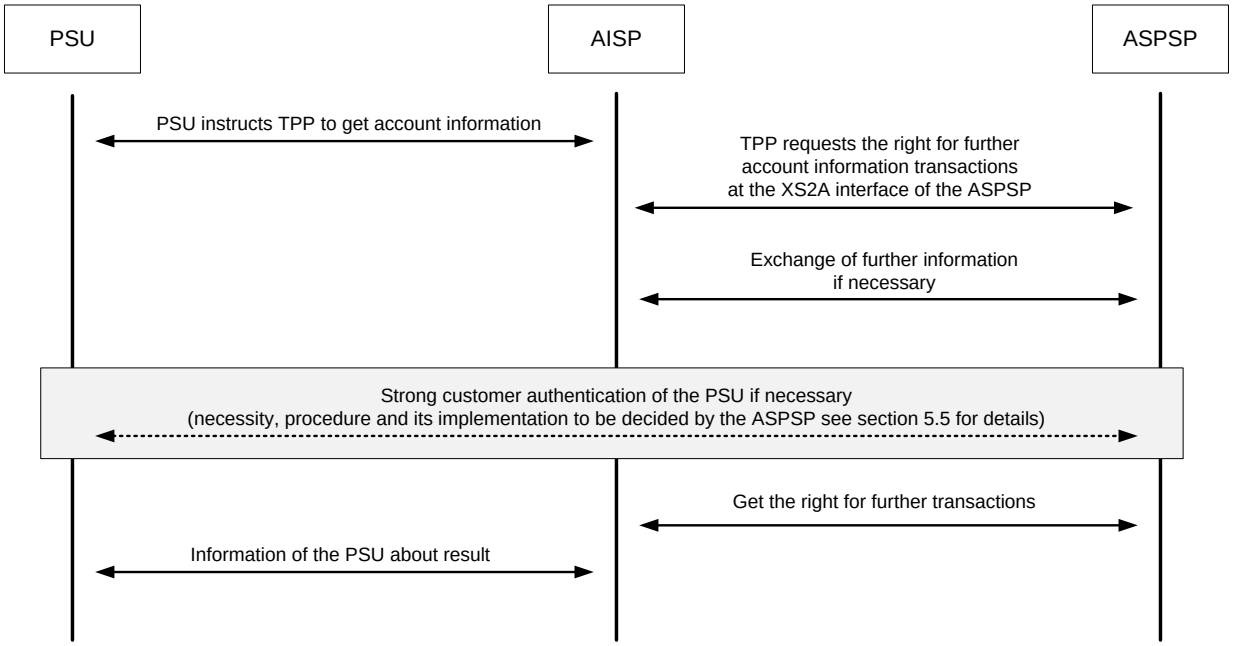


Figure 7: Use case Establish account information consent

4.6 Use case: Get list of reachable accounts

The support of this use case at the XS2A interface is optional for an ASPSP.

Transactions according to this use case can be used by a TPP to receive a list of reachable accounts of a PSU managed by the ASPSP. The term reachable 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 reachable at the XS2A interface.

As a result of this transaction 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 transaction based on the use case 'Establish account information consent', the TPP can use the obtained account numbers to receive further information about the accounts in additional transactions of the account information service.

The transaction 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 transaction.

The ASPSP will reject the transaction 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 transaction if the TPP does not have the necessary rights for this transaction type from a previous transaction according to the use case 'Establish account information consent'.

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

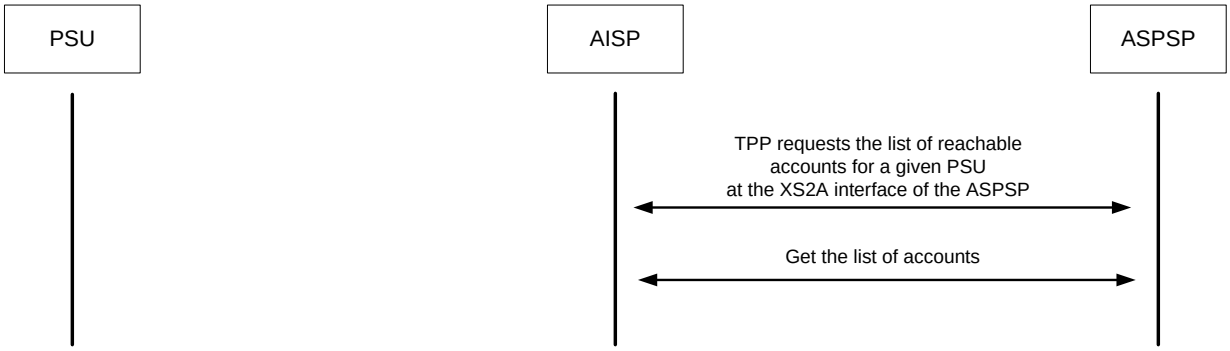


Figure 8: Use case Get list of reachable accounts

4.7 Use case: Get account details of a list of accessible accounts

Transactions according to this use case can be used 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 transactions.

Details of these accounts 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 transaction 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 transaction.

The ASPSP will reject the transaction 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 transaction if the TPP does not have the necessary rights for this transaction type from a previous transaction according to the use case 'Establish account information consent'.

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

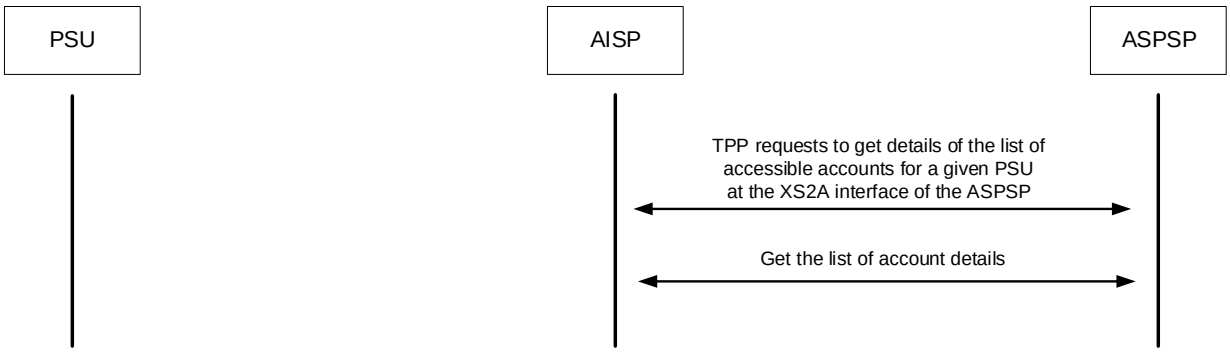


Figure 9: Use case Get account details of a list of accessible accounts

4.8 Use case: Get balances for a given account

The TPP can use transactions according to this use case 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 transaction, 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 transaction 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 transaction at the XS2A interface is initiated by the TPP. The transaction 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 transaction.

The ASPSP will reject the transaction 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 transaction if the TPP has not been granted the necessary rights for this transaction type during a previous transaction according to the use case Establish account information consent.

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

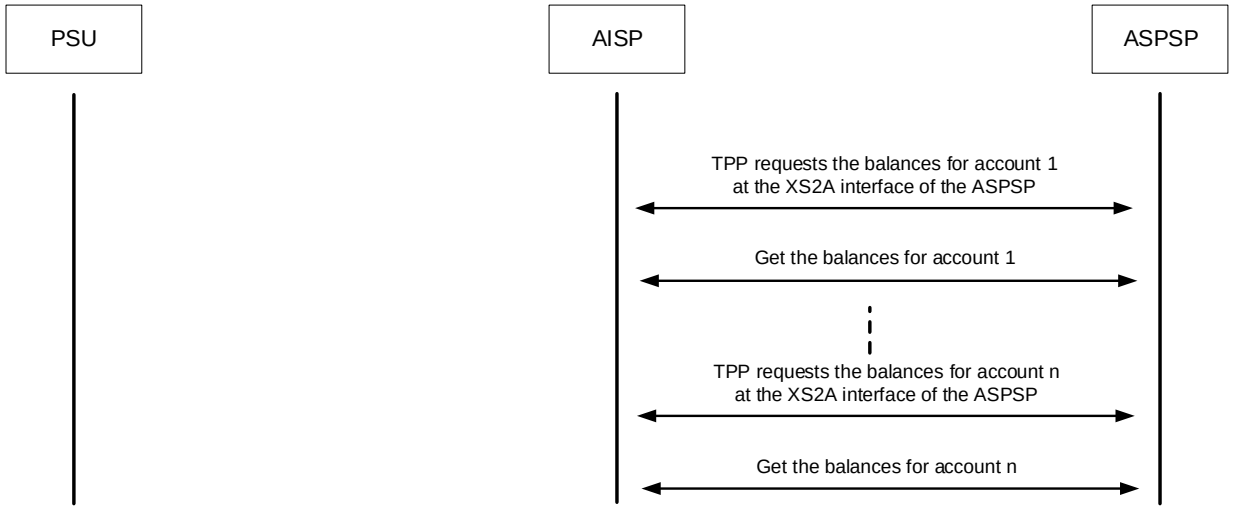


Figure 10: Use case Get balances for a given list of accounts

4.9 Use case: Get transaction information for a given account

The TPP can use transactions according to this use case 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 use case “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 transaction of a 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 transaction 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 transaction.

The ASPSP will reject the transaction 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 transaction if the TPP has not been granted the necessary rights for this transaction type during a previous transaction according to the use case Establish account information consent.

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

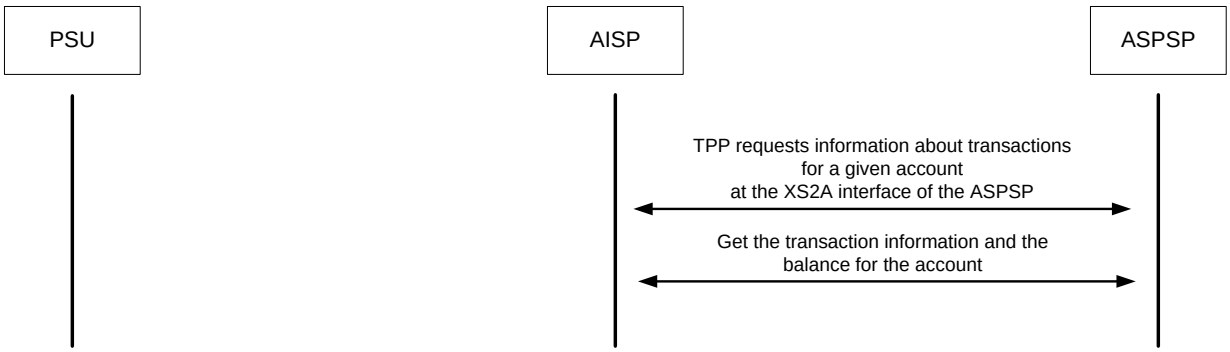


Figure 11: Use case Get payment transaction information for a given account

4.10 Use case: Get confirmation on the availability of funds

The TPP can use transactions according to this use case 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 transaction 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 transaction. The document at hand does not cover the interface between the PSU and the ASPSP required for the exchange of information.

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

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

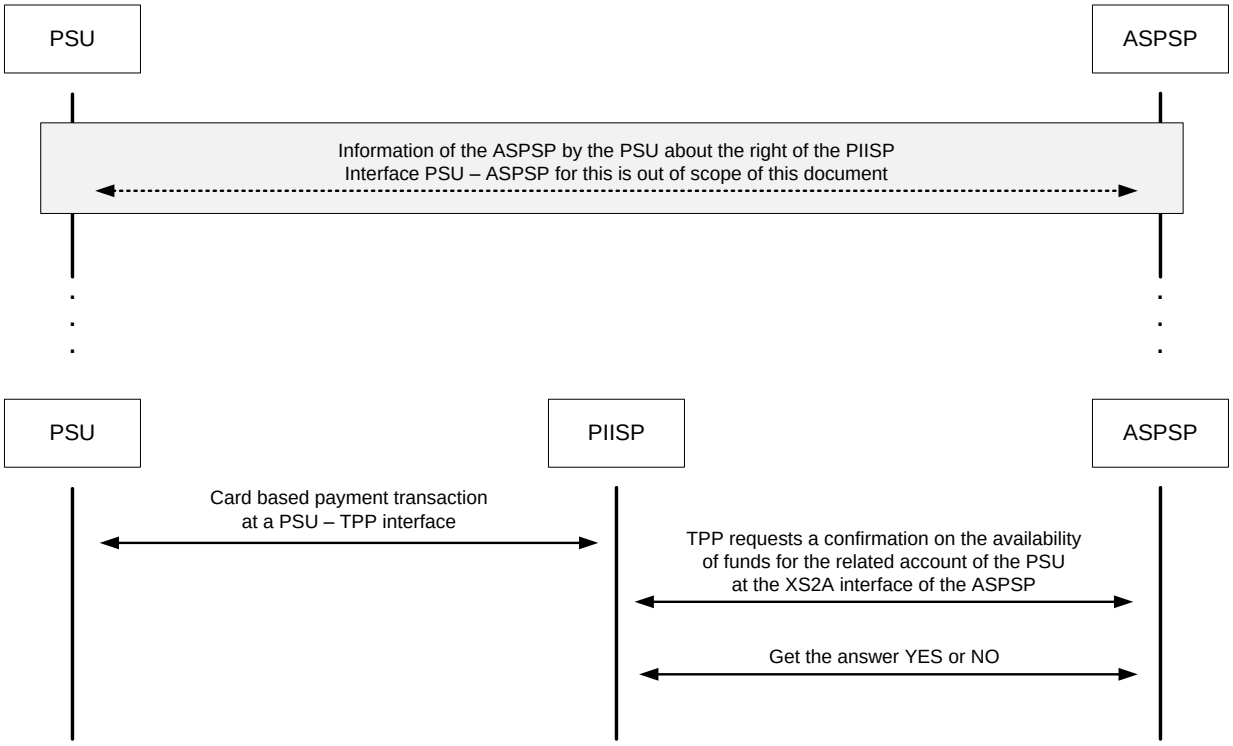


Figure 12: Use case Get the confirmation on the availability of funds

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 transaction according to this use case. 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 [XS2A-ImplG].

5.1 Layers of the interface

The specification of the XS2A interface distinguishes between the transport layer and the application layer:

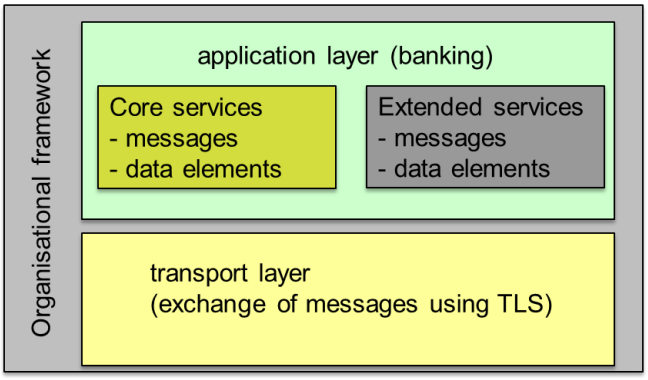


Figure 13: Layers of the XS2A interface

Among other things, the organisational framework contains rules and processes for the change management and for the further development of the standard. This framework is developed by the Berlin Group and is not covered in this document.

5.1.1 Application layer

The services of the XS2A interface are specified by defining messages and data elements which are exchanged between TPP and ASPSP. The set of all messages and all data elements defines the application layer of the XS2A interface. The messages at the application layer are implemented using a REST API approach.

5.1.2 Transport layer

The transport layer defines the technical exchange of the messages between TPP and ASPSP over the internet.

The communication between the TPP and the ASPSP is always secured by a TLS-connection. This TLS-connection is set up and controlled by the TPP. It is not necessary to set up a new TLS-connection for each transaction: However, the ASPSP may terminate an existing TLS-connection if this is required by its security setting.

For the exchange of the messages the protocol http (https) is used.

Version 1.2 or higher will be used for TLS and version 1.1 or higher will be used for http. Further refinement is defined in [XS2A-ImplG].

5.2 Messages – transactions – sessions

Messages, transactions and sessions are basic concepts of the XS2A interface specification and of the execution of processes at the XS2A interface according to the services supported by the XS2A interface. The following sections contain a short overview of how these terms are used in the XS2A interface specification.

5.2.1 Message at the XS2A interface

A message is the basic building block for the execution of processes at the XS2A interface. Messages are defined by a set of parameters (i.e. data elements) which are transported when the sending party sends a message to the receiving party.

It is distinguished between request messages and response messages. For the current version of the XS2A interface a request message is always sent by a TPP to the ASPSP using the XS2A interface of the ASPSP. After executing an incoming request message the ASPSP will send the corresponding response message to the TPP.

For the implementation of an XS2A interface each request message will be executed using either POST, GET, PUT or DELETE http methods. Every response message will be executed as a http response.

5.2.2 Transaction at the XS2A interface

A transaction at the XS2A interface is defined as the set of all messages that must be exchanged between TPP and ASPSP to execute one of the following business transactions according to the use cases defined in section 4:

- Payment initiation transaction: Initiation of a single payment from a given payer's account to a given payee's account according to the use case defined in section 4.1.

- Payment initiation transaction: Initiation of a future dated single payment from a given payer's account to a given payee's account according to the use case defined in section 4.2.

- Payment initiation transaction: Initiation of a bulk/multiple payment from a given payer's account to several given payee’s accounts according to the use case defined in section 4.3.

- Payment initiation transaction: Initiation of a recurring payment via a standing order from a given payer's account to a given payee's account with a defined frequency and duration according to the use case defined in section 4.4.

- Establish account information consent transaction: obtain the right to execute further transactions of the account information service according to the use case defined in section 4.5.

- Get list of reachable accounts transaction: Receive a list of reachable accounts for a given PSU according to the use case defined in section 4.6.

- Get account details transaction: Receive detailed information for the list of accessible accounts according to the use case defined in section 4.7

- Get balances transaction: Receive the balances for a list of given accounts according to the use case defined in section 4.8.

- Get account information transaction: Receive a list of account transaction information for a given account according to the use case defined in section 4.9.

- Confirmation of funds transaction: Receive confirmation of the availability of funds for a specific amount and a given account according to the use case defined by section 4.10.

Any transaction is initiated by the TPP who sends one of the following messages to the XS2A interface of the ASPSP:

- Payment initiation request message to start a new "Payment initiation transaction" related to single payments, future dated single payments, bulk/multiple payments or recurring payments by standing orders.

- Account information consent request message to start a new "Establish account information consent transaction".

- Read account data request message to start a new "Get list of accounts transaction", a "Get account details of the accessible accounts", a new "Get balances transaction" or a new "Get account information transaction". The type of transaction to be started by this request message is determined by the parameters of that message.

- Confirmation of funds request message to start a new confirmation of funds transaction.

Every transaction at the XS2A interface belongs to one of the services supported by the XS2A interface as defined in section 4. It is not possible to mix different services in one single transaction. A TPP may only start a new transaction at the XS2A interface if it has the necessary role for this service as defined in Table 2 at the beginning of section 4.

5.2.3 Session at the XS2A interface

A session at the XS2A interface is defined as a set of transactions executed consecutively at the XS2A interface. Sessions can be used by an ASPSP for example to decide if strong customer authentication of the PSU is necessary as part of a transaction within the session.

Transactions belonging to different services may be mixed within a single session. This means that a TPP can, for example, request information about accounts of a PSU before initiating a payment on behalf of the PSU. It remains a prerequisite that the TPP holds all roles necessary to execute all transactions of the session. The roles of the TPP have to be included in the qualified certificate of the TPP.

The support of sessions at the XS2A interface is optional for an ASPSP. The ASPSP defines whether sessions are supported when implementing the XS2A interface. Whether or not sessions are supported will be stated in the documentation of XS2A interface provided by the ASPSP.

5.2.4 Example

The following figure gives an overview of the relation between messages, transactions and sessions at the XS2A interface:

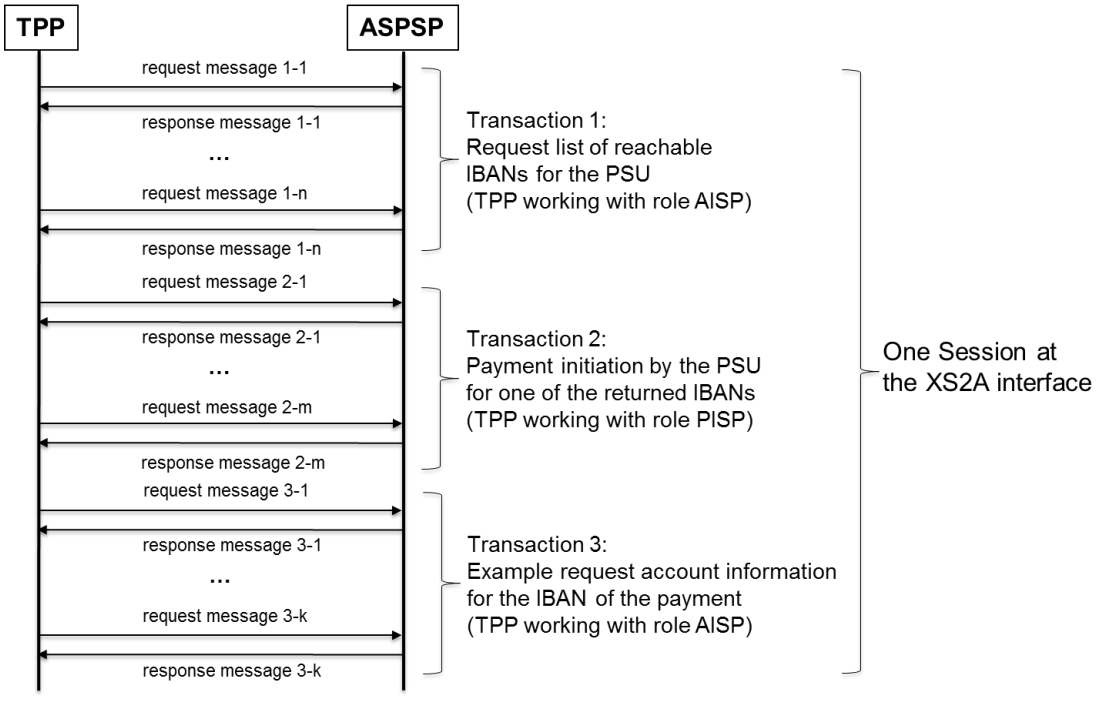


Figure 14: Example for the relationship message, transaction and session

In this example it is assumed that the TPP has already executed an "Establish account information consent transaction" beforehand in order to be granted the right to access the necessary rights needed for transaction 1 and transaction 3.

The transactions in the example belong to different services and are combined within one session. Please note that the TPP must have been authorised to use the role AISP as well as the role PISP. The role AISP is necessary for transactions 1 and 3, the role PISP is necessary for transaction 2.

Note that the concept of a session is an optional part of the XS2A interface framework. An ASPSP is free to decide whether or not to support sessions as part of its implementation of the XS2A interface. Whether or not sessions are supported will be stated in the documentation of XS2A interface provided by the ASPSP.

5.3 Identification of the TPP

A TPP may only access the XS2A interface of an ASPSP if the TPP identifies itself at the XS2A interface. According to [EBA-RTS] this identification requires a qualified certificate issued by a QTSP compliant with [eIDAS].

Clarification: The identification of the TPP towards the ASPSP is required in articles 65, 66 and 67 of [PSD2]. The TPP is defined as the PSP that has a direct relationship with the PSU for the execution of a transaction at the XS2A interface. A TPP may decide to use the support of a technical service provider(s) to access the XS2A interface of an ASPSP. However, it is still the TPP that has to be identified by the ASPSP, not the technical service provider(s), i.e. the certificates associated to the TPP have to be used when addressing the XS2A interface of the ASPSP.

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.

In the context of the identification of a TPP at the XS2A interface it is distinguished between two levels:

- Identification of the TPP at the transport layer.
- Identification of the TPP at the application layer.

The TPP must always be identified at the transport layer. Additional identification of the TPP at application level is only necessary if requested by the ASPSP. The ASPSP defines in its XS2A interface documentation if identification at the application level is necessary.

5.3.1 Identification of the TPP at transport layer

At the transport layer, the TPP is identified by means of the client authentication which is part of the TLS-connection setup between the TPP and the ASPSP.

For this identification the TPP needs a qualified certificate for website authentication according to section 8 of [eIDAS]. This certificate has to be compliant with the additional requirements defined by [EBA-RTS]. The profile of these certificates (QWAC profile) is specified by the technical specification [TS 119 495] of ETSI.

Clarification: If a TPP uses further technical service provider(s) to access the XS2A interface of an ASPSP the qualified certificate of the TPP must be used for the setup of the TLS-connection with the ASPSP. The certificate of a technical service provider(s) may not be used.

5.3.2 Identification of the TPP at application layer

To identify the TPP at the application layer, the TPP has to sign all messages to be sent to the ASPSP. The electronic seal (i.e. the electronic signature) and the certificate of the TPP have to be sent to the ASPSP as part of the message.

The electronic seal for a message shall be calculated based on the Internet standard for signing HTTP messages defined by the IETF Network Working Group.

The TPP needs a qualified certificate for electronic seals according to section 5 of [eIDAS] for identification. This certificate has to be compliant with the additional requirements defined by [EBA-RTS]. The profile of these certificates (QSealC profile) is specified by the technical specification [TS 119 495] of ETSI.

Clarification: If a TPP uses further technical service provider(s) to implement its accesses to the XS2A interface of an ASPSP the electronic seal shall be generated by the TPP and the qualified certificate of the TPP shall be sent to the ASPSP. The certificate of a technical service provider(s) may not be used.

5.4 Confirmation of the consent of the PSU

Each transaction at the XS2A interface is subject to the consent of the PSU. How consent of the PSU is confirmed during a transaction depends on the transaction type as shown in the following table:

Transaction	How the PSU grants consent	How consent of the PSU is verified
Payment initiation	Authentication of the PSU using strong customer authentication with dynamic linking to the transaction. In cases of an exemption of strong	Verification of the authenticity of the PSU and of the transaction by verification of the strong customer authentication. In cases of

Transaction	How the PSU grants consent	How consent of the PSU is verified
	customer authentication by other means to be decided by the ASPSP.	exemption to strong customer authentication by other means to be decided by the ASPSP.
Establish account information consent	Identifies itself as part of the transaction, 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 transaction.	Verifies the access token given to the TPP as result of a previously executed Establish account information consent transaction.
Get details of accessible accounts	Consent was granted during a previously executed Establish account information consent transaction.	Access token given to the TPP was verified as result of a previously executed Establish account information consent transaction.
Get balances	Consent was granted during a previously executed Establish account information consent transaction.	Access token given to the TPP was verified as result of a previously executed Establish account information consent transaction.
Get transaction list	Consent was granted during a previously executed Establish account information consent transaction.	The access token given to the TPP was verified as a result of a previously executed Establish account information consent transaction.
Confirmation of funds	The PSU has already informed the ASPSP about its consent using another interface. The PSU/ASPSP interface is not covered by this document.	Verification if the ASPSP has already been informed about the consent of the PSU.

Table 3: Consent of the PSU within transactions

A transaction at the XS2A interface may only be executed if the consent of the PSU can be confirmed. Otherwise the ASPSP will reject the transaction.

5.5 Strong customer authentication

Some of the following transactions require strong customer authentication (SCA) of the PSU at the XS2A interface as part of the transaction:

- Payment initiation transactions.
- Establish account information consent transactions.

Requirements for the application of SCA and possible exemptions are defined in article 97 of [PSD2] and chapter III of [EBA-RTS]. For each individual transaction the ASPSP has to decide if SCA has to be executed. This decision has to be compliant with the requirements defined by [PSD2] and [EBA-RTS].

If a SCA is necessary then it has to be decided on

- the procedure and
- the personalised security credentials

to be used by the PSU. If several SCA procedures are available for the PSU, then the ASPSP shall offer these procedure to TPP/PSU to choose between these procedures.

The specification of the Joint Initiative distinguishes the following four approaches to SCA as part of a transaction at the XS2A interface of an ASPSP:

- Redirect approach,
- OAuth2 approach,
- Decoupled approach and
- Embedded approach.

The ASPSP decides which of these approaches to SCA are supported by its XS2A interface implementation. The TPP can indicate in its first message of the Payment initiation or Establish consent information request whether the TPP prefers a redirect based SCA approach or not. In this context, also the OAuth2 approach is seen as a technically redirect based SCA approach. The ASPSP shall take this indication into account when deciding on the SCA approach to be performed.

The XS2A documentation of the ASPSP will provide the TPP with the necessary information. If SCA is necessary as part of a transaction the TPP has to use one of the approaches supported by the ASPSP.

Note: Currently, only the SCA of one PSU can be handled directly as part of the transaction at the XS2A interface. SCA for more than one PSU must be handled outside the XS2A interface. Future releases of this specification may support this approach for SCA (‘distributed approach’) at the XS2A interface.

Note: Currently, only the SCA as performed by the ASPSP is directly supported as part of the transaction at the XS2A interface. SCA method offered by PIS or AIS providers are not

yet explicitly supported by the XS2A interface. Future releases may support this approach for SCA ('delegated approach') at the XS2A interface.

5.5.1 SCA using the redirect approach

For the redirect approach the individual steps of the SCA are not executed at the XS2A interface, but directly between the PSU and the ASPSP. In this case, the PSU is redirected to a web interface of the ASPSP for authentication. Depending on the device used, the PSU may also be redirected to a special authentication app of the ASPSP (ref. next section).

Once the PSU has been redirected to the ASPSP (app or web interface) the SCA of the PSU is executed step by step and directly between the ASPSP and the PSU. After completion of the SCA the PSU is redirected back to the TPP. The following figure shows the (much simplified) top level information flow for a payment initiation transaction with SCA based on the redirect approach:

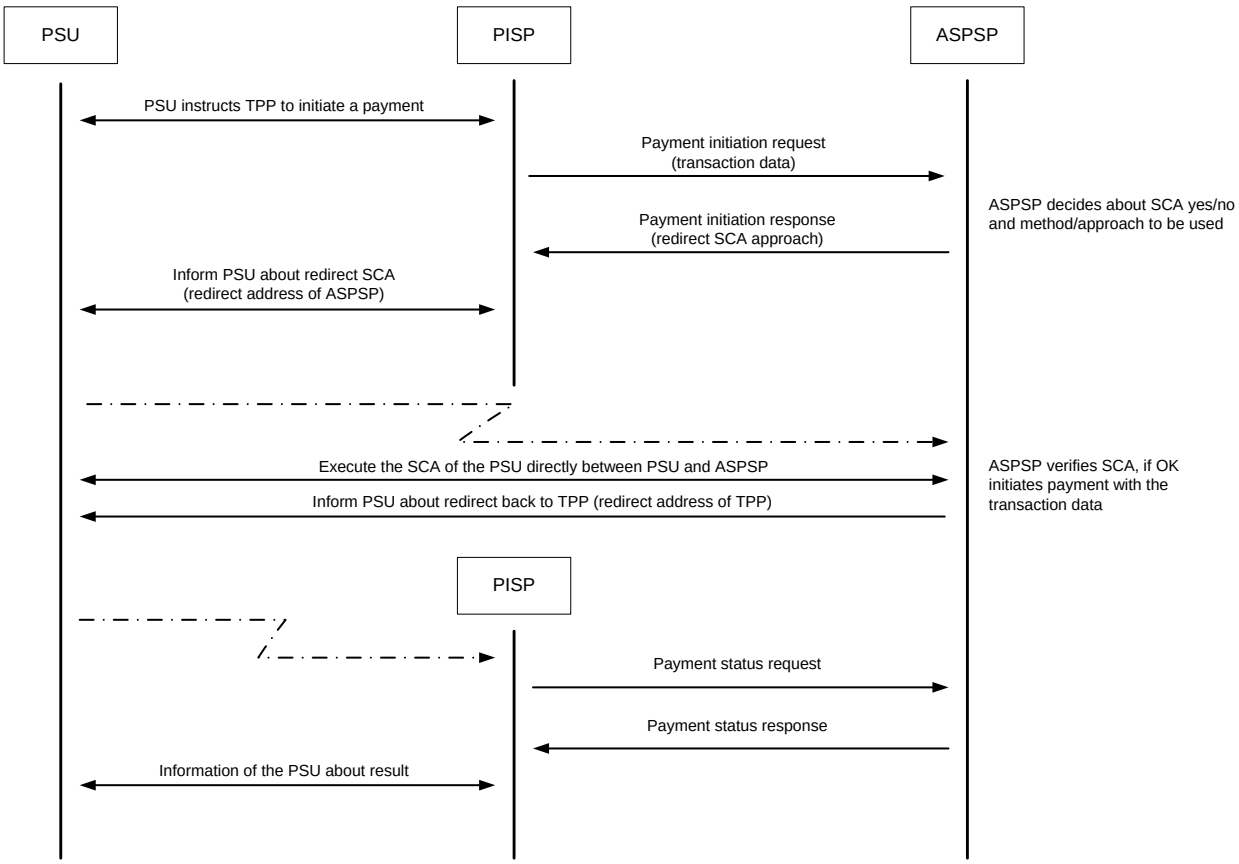


Figure 15: Redirect approach for SCA

When applying the redirect approach the TPP does not need detailed information about the individual steps of the SCA of the PSU. The redirect approach therefore allows the TPP to avoid the implementation of the different SCA methods at its PSU – TPP interface.

5.5.2 SCA using the OAuth2 approach

The transaction flow of the OAuth2 approach to SCA is similar to that of the redirect approach. The difference is that the redirection to the authentication server of the ASPSP is embedded into the OAuth2 protocol, where the "scope" attribute of the OAuth authorisation request is linked to the created payment initiation or consent resource. The access to the interface to retrieve the actual account datais then performed with using the access token delivered by the ASPSP's authentication server. The following figure shows the (much simplified) top level information flow for a payment initiation transaction with SCA based on the OAuth2 approach:

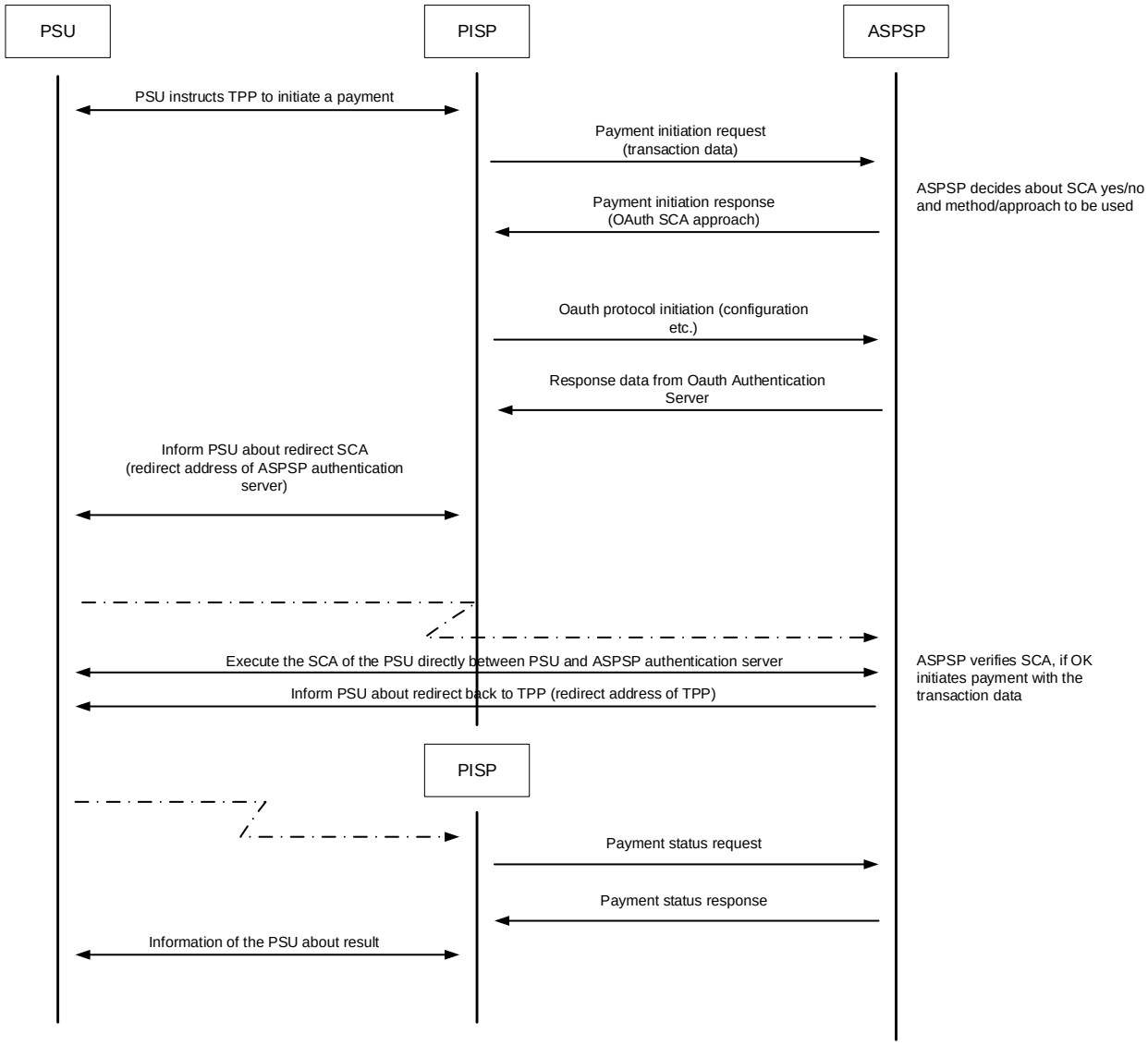


Figure 16: OAuth approach for SCA

When applying the OAuth SCA pproach the TPP does not need detailed information about the individual steps of the SCA of the PSU. The OAuth approach therefore allows the TPP to avoid the implementation of the different SCA methods at its PSU – TPP interface.

5.5.3 SCA using the decoupled approach

The transaction flow of the decoupled approach to SCA is similar to that of the redirect approach. The difference is that the ASPSP asks the PSU to authenticate e.g. by sending a push notification with payment transaction details to a dedicated mobile app or via any other application or device which is independent of the online banking frontend. In difference to the redirection flow, there is no impact on the PSU/TPP interface during the technical processing. The following figure shows the (much simplified) top level information flow for a payment initiation transaction with SCA based on the decoupled approach.

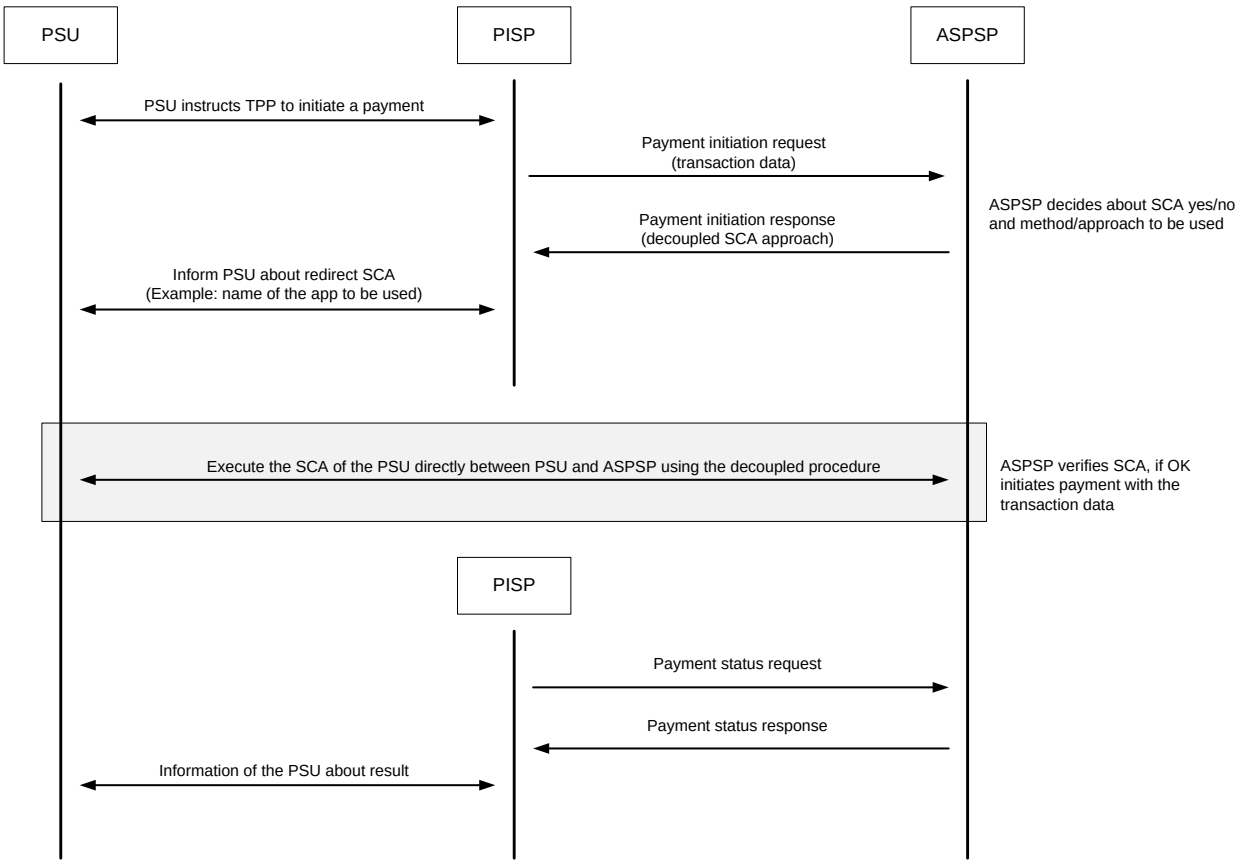


Figure 17: Decoupled approach for SCA

Just as for the redirect approach, the TPP does not need to have detailed knowledge about the individual steps of the SCA when applying the decoupled approach. The decoupled approach therefore allows the TPP to avoid the implementation of the different SCA methods at its PSU – TPP interface.

5.5.4 SCA using the embedded approach

When applying the embedded approach the SCA of the PSU is executed entirely as part of the transaction at the XS2A interface. The following figure shows the (much simplified) top level information flow for a payment initiation transaction with SCA based on the embedded approach. Basis for this example is a SCA method based on a static password of the PSU (as element of knowledge) and a dynamic one-time password (OTP) calculated by the PSU, for example using a smart card (as element of possession).

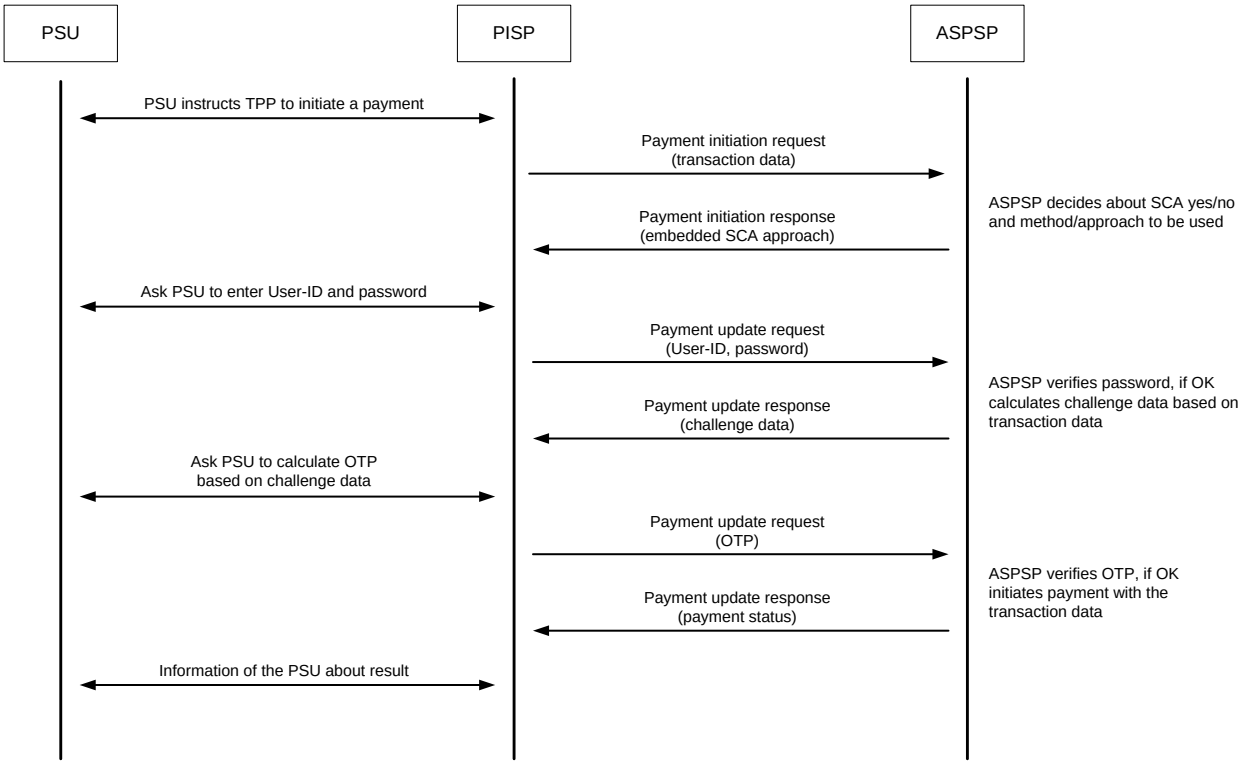


Figure 18: Embedded approach for SCA

Again, the interface PSU – TPP is not covered by this document. When using the embedded approach the TPP has to know how to inform the PSU about the different steps of the SCA (in contrast to the redirect or decoupled approach). In particular the TPP has to provide a means of displaying the challenge data to the PSU since the PSU needs this data to calculate the OTP. Depending on the ASPSP there is a large number of possible methods for this, for example the display of an animated graphic or the display of a black and white or coloured matrix code. The XS2A interface documentation of the respective ASPSP will contain a specification of the steps of the SCA methods. The challenge data sent by the ASPSP will contain an identification of the SCA method to be used.

5.6 OAuth2 as a pre-step for PSU authentication

The XS2A interface supports in addition to the use of OAuth2 as an integrated SCA approach as described in section 5.5.2 also the use of OAuth2 as a pre-step to deliver an access token for a PSU without already dealing with functional consent. This access token in this case only encapsulates the PSU identification as such and can be used in the embedded or decoupled SCA approach for PIS or AIS services. The related OAuth2 protocol in this case shall do without the redirect authorisation process.

6 Operational rules

This section summarises the operational rules to be observed by each TPP accessing the XS2A interface and each ASPSP providing an XS2A interface. Not all of these rules are enforced by technical means of the XS2A interface.

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

6.1 Coding of business data

For a payment initiation transaction the ASPSP may support the coding of the payment data using XML or using JSON or both. If XML is supported the payment data has to be coded as pain.001 message and the transaction status response will be coded as pain.002 message. If JSON is supported the payment data has to be transferred as JSON structure to be defined by the Implementation Guidelines [XS2A-ImplG].

For the reading of account information the ASPSP shall support one or more of the following coding of the account data to be delivered:

- camt.05x,
- JSON,
- MT94x.

The JSON structure to be used for transferring the account information will be defined by the Implementation Guidelines [XS2A-ImplG].

In any case it is up to the ASPSP to decide what kind of coding will be supported for payment data and for account information at its XS2A interface. The ASPSP will inform the TPP about its decision as part of the documentation of its XS2A interface.

6.2 Consent of the PSU

A TPP may execute a transaction at the XS2A interface of an ASPSP if it has the necessary consent of the PSU. The consent will be authorised by the PSU towards the ASPSP by performing a SCA procedure. In cases of exemptions, alternative authentication procedures might be agreed between PSU and ASPSP and might be integrated into the consent authorisation flow.

An ASPSP will reject any transaction at the XS2A interface if the consent of the PSU cannot be proven.

6.3 Currency of transactions

The specification of the XS2A interface does not make any provisions concerning the currency of transactions (only relevant for the services PIS and FCS).

6.4 Decision about strong customer authentication

The ASPSP has to decide

- if SCA has to be executed as part of a transaction at the XS2A interface,
- which method and personalised credentials have to be used for SCA, where the PSU will be involved in a selection process if several SCA procedures are available, and
- which approach has to be used for executing SCA, taking into account the redirection preference of the TPP.

The TPP has to follow the decision of the ASPSP.

6.5 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.

6.6 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.

6.7 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].

6.8 Revocation 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 payment and recurring payments initiated by standing orders.

6.9 Separation and combination of services

On the level of a single transaction, services are separated and cannot be combined.

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

The TPP may of course use different roles for different transactions. If supported by the XS2A interface of the ASPSP the TPP may use a session at the XS2A interface to connect two (or more) consecutive transactions. The ASPSP will recognise the connection between the transactions belonging to a session and will react accordingly. This allows to avoid unnecessary steps for the authentication of the PSU.

6.10 Validity of transactions

One XS2A transaction 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 transaction. 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.

6.11 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

In the following, an abstract data model is presented for the usage of the XS2A Interface. This model is further refined in [XS2A-ImplG].

7.1 Protocol Level

The following data elements are used independently of the semantic of the related messages, building an abstract basic protocol level.

7.1.1 Request Data on Protocol Level

The following protocol level data is defined for all request messages:

- Transaction Identification (Mandatory)

  This is an ID generated by the TPP to identify the transaction as defined by section 5.2.2 uniquely. It is used e.g. for dispute management.

- Request Identification (Mandatory)

  This is a unique ID generated by the TPP to identify individual request messages. It is used to solve e.g. operational issues.

- Request Timestamp (Mandatory)

  Each request of a transaction contains a standard http timestamp indicating the current processing time of the request.

- TPP Certificate Data (conditional)

  The qualified certificate of the TPP according to article 29 of [EBA-RTS]. Only to be delivered if mandated by the ASPSP for the case that the request message has to be signed by the TPP.

- Payload Hash (conditional)

  A hash over the content of the http request.

- TPP Electronic Signature (conditional)

  Electronic signature generated by the TPP over a.o. the payload hash following the definition in [XS2A-ImplG]. The corresponding public key is part of the qualified certificate of the TPP according to article 29 of [EBA-RTS]. Only to be delivered if mandated by the ASPSP for the case that the request message has to be signed by the TPP.

Further technical data like resource IDs and interface versions etc. are determined by the API structure and defined in detail in the [XS2A-ImplG].

7.1.2 Response Data on Protocol Level

The following data is defined for all XS2A Interface Responses for handling messages.

- Resource ID (conditional)

  This is a unique ID generated by the ASPSP after the first transaction related request of a TPP of a payment initiation transaction or an establish consent transaction. This payment or consent resource ID is transmitted to the TPP within the first response. The token shall be used by the TPP for all subsequent requests within a transaction lifecycle. The ASPSP is free to define the token and its security features.

- Transaction Status (conditional)

  This is the status of a transaction on the ASPSP side. This transaction status is referring to a created resource like a payment initiation or a consent resource. This transaction status is used in response messages only where a transaction status is explicitly requested by the TPP, where the whole resource is addressed or where the resource is updated with data.

- Response Code

  The response code is a http code on transport level indicating a correct processing, session re-routing to another site or processing errors. In [XS2A-ImplG], a complete set of processing error codes is defined in detail.

- Hyperlinks for next transaction steps, e.g.

  - Hyperlink to the payment initiation or consent resource with different semantics like "update_psu_identification", "update_psu_authentication", "authorise_transaction" or "status".

  - Redirect URL ASPSP (conditional, only in case of Redirect Approach)

- PSU Message Information (optional)

  This data element contains a message, which is to be displayed to the PSU by the TPP.

- TPP Message Information (optional)

  This data element contains a message code and optionally open text information from the ASPSP to the TPP. It can be used by the ASPSP e.g. in exception

situations to deliver detailed error information and additional information to the TPP.

7.2 PIS related data model

Within the XS2A Interface, a payment initiation transaction consists of at least the Payment Initiation Request and the Payment Initiation Response. For the Decoupled, Redirect SCA Approach 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 update the payment initiation resource created after the Payment Initiation Request with additional data via an Update Data Request.

In case of the Embedded SCA Approach, a dedicated message pair consists of the Transaction Authorisation Request and the Transaction Authorisation Response for processing PSU credentials directly within the XS2A interface. This message pair is conditional, depending on the result of the ASPSP's risk management on SCA necessity. It can be repeated in case of a non-successful SCA of the PSU.

7.2.1 Payment Initiation Request

In the following, a minimum set of requirements on the Payment Initiation Request is defined. These requirements are independent of the encoding.

7.2.1.1 PSU Data

- PSU Identification (conditional, only if mandated by parameters published by the ASPSP)
- PSU Corporate Identification and Type (conditional, only if mandated by parameters published by the ASPSP and only if PSU is a corporate)
- PSU Risk Management Data. If not included in the message the ASPSP will take this into account in its risk management.
  - IP Address PSU (mandatory)
  - PSU Device and Application Software Information (operating system, browser etc.) (optional),
  - GEO Location PSU (optional)

7.2.1.2 TPP relevant data

- Redirect Preferred Indicator (optional)

  With this indicator, the TPP can set its priority for a re-direct based SCA Approach (Redirect SCA Approach or OAuth2 SCA Approach) vs. a SCA Approach without

a re-direction to a bank site (Embedded SCA Approach or Decoupled SCA Approach, depending on the authentication method).

- Redirect URL-TPP (conditional, only mandated if the Redirect Preferred Indicator equals true or if this Indicator is not contained)

  This data element defines an URL to which the ASPSP shall redirect the PSU browser session once the SCA on bank websites is performed.

7.2.1.3 Payment Related Data

The payload data of the Payment Initiation Request consist of all payment related data of the payment initiation. This data varies for different payment products. In [XS2A-ImplG] data definitions for

- SCT
- SCT INST
- SEPA Fast Payment (Target 2)
- Cross-currency credit transfer
- Some Domestic Credit Transfer Services in non-euro currency

are defined in detail.

Remark: Rules on more complex corporate payments will not be considered. These payments will be supported only for initiating corporate formats for TPPs published already today by ASPSPs.

7.2.2 Update PSU Data Request

This request is used when the Payment Initiation Response or an Update PSU Data Response is indicating that the underlying payment initiation resource needs to be updated by certain PSU related data. The sort of data is directly addressed by semantic hyperlinks contained in the related response message. The following data can be addressed:

- PSU Identification (conditional, if not yet submitted within the Payment Initiation Request)
- Corporate Identification (conditional, if not yet submitted within the Payment Initiation Request, if the PSU is corporate and if mandated by parameters published by the ASPSP)
- PSU Password (conditional)

- Authentication Method Choice (conditional, if ASPSP supports several SCA methods for the corresponding PSU)

- Proprietary Data (conditional, if correspondingly documented by the ASPSP)

7.2.3 Payment Initiation or Update PSU Data Response

- Available Authentication Methods, if the ASPSP supports several SCA methods for the corresponding PSU

- Challenge Data (conditional, used only for the Embedded SCA Approach and depending on the risk management of the ASPSP, and in rare cases also for the first authentication of the PSU via a password)

  The challenge data contain

  - challenge data if required by the SCA method,

  - formatting information for the PSU Authentication Data within the Transaction Authorisation Request,

  - additional information for the background of the SCA usage or in rare cases also for password usage (e.g. to type in certain digits of a secret)

7.2.4 Transaction Authorisation Request

This message is used only in case of the Embedded SCA Approach and when an authorisation of the initiated payment by a SCA method is needed.

- PSU Authentication Data (mandatory)

  Data submitted by the PSU to authorise the transaction when performing a SCA method. This is e.g. an OTP or an electronic signature.

7.2.5 Transaction Authorisation Response

This message has no additional data elements.

7.2.6 Payment Status Request

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

No specific data elements.

7.2.7 Payment Status Response

This message can contain several data elements in addition to the transaction status, specifically when an XML based transaction status message is supported. Details are defined in the [XS2A-ImplG].

7.3 AIS 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.

Remark: These two steps are implemented through different APIs – the /consents and the /accounts resp. /card-accounts APIs, cp. [XS2A-ImplG], Section 6.

7.3.1 Establish consent transaction

Within the XS2A Interface, an Establish consent transaction always starts with the Establish Consent Request and the Establish Consent Response. For the Decoupled, Redirect or OAuth2 SCA Approach, there must be at least a second message pair Consent Status Request and Consent Status Response within the XS2A interface to retrieve the information whether the SCA method was successful. In all cases, the ASPSP may ask the TPP to update the consent resource created after the Establish Consent Request with additional data via an Update Data Request.

In case of the Embedded SCA Approach, a dedicated message pair consists of the Transaction Authorisation Request and the Transaction Authorisation Response for processing PSU credentials directly within the XS2A interface. This message pair is conditional, depending on the result of the ASPSP's risk management on SCA necessity. It can be repeated in case of a non-successful SCA of the PSU.

7.3.1.1 Establish Consent Request

7.3.1.1.1 PSU Data

- PSU Identification (conditional, only if mandated by parameters published by the ASPSP)
- PSU Corporate Identification and Type (conditional, only if mandated by parameters published by the ASPSP and only if PSU is a corporate)
- PSU Risk Management Data. If not included in the message the ASPSP will take this into account in its risk management.
    - IP Address PSU (mandatory)
    - PSU Device and Application Software Information (operating system, browser etc.) (optional),

- GEO Location PSU (optional)

7.3.1.1.2 TPP data

- Redirect Preferred Indicator (optional)

  With this indicator, the TPP can set its priority for a re-direct based SCA Approach (Redirect SCA Approach or OAuth2 SCA Approach) vs. a SCA Approach without a re-direction to a bank site (Embedded SCA Approach or Decoupled SCA Approach, depending on the authentication method).

- Redirect URL-TPP (conditional, only mandated if the Redirect Preferred Indicator equals true or if this Indicator is not contained)

  This data element defines an URL to which the ASPSP shall redirect the PSU browser session once the SCA on bank websites is performed.

7.3.1.1.3 Consent Data

- Account Access (mandatory)

  This is a data structure describing the requested access on the PSU accounts. This data structure will refer different account information types like account details, balances and payment transaction information. The TPP then can address for all of these account information types the exact list of accounts.

  In addition, the ASPSP can optionally offer to support the submission of the requested account information types without addressing specific accounts. The ASPSP then will

  - either agree with the PSU within a Redirect SCA Approach or OAuth2 SCA Approach on possible restrictions of these account accesses to certain of the PSU accounts
  - or grant access to all available payment accounts of the PSU.

- Validity (mandatory)

  The end date of the validity of the consent. This is restricted by [EBA-RTS] to maximal 90 days. For a consent for a one off access, the current date is to be used.

- Access Frequency (mandatory)

  Maximal access to the account within this consent per day and without PSU involvement.

- Combined Service Indicator (mandatory)

This data element is indicating whether the consent shall also allow to submit payments within the same session, such that a new PSU authentication e.g with a password is not needed during the related Payment initiation transaction.

7.3.1.2 Establish Consent Response, Update Data Request and Update Data Response

The process of authorising a consent is analogous to the process of authorising a payment initiation, cp. Sections 7.2.2 and 7.2.3.

7.3.1.3 Consent Status Request and Response

This request is used, when a status of the authentication of the PSU is needed by the TPP, e.g.. in the Redirect, OAuth2 or decoupled SCA Approach. This request can be sent as long as the resource is accessible.

No specific data elements in request or response.

7.3.1.4 Consent Details Request and Response

This request is addressed on a created resource and requesting to retrieve the details of the consent resource. This request can be sent as long as the resource is accessible. This request might be needed for the TPP if the PSU has withdrawn the consent (partially or implicitly) via the PSU ASPSP interface. The request contains no specific data elements.

The corresponding response contains in its payload the current consent object, the detailed data structure is defined in [XS2A-ImplG].

7.3.2 Get account information transaction

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:

- 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.

- PSU Involvement Indicator

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 PIIS 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

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

- Name Payee (optional)
- Instructed Amount

7.4.2 Confirmation of Funds Response

- Funds Availability Indicator

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 [EBA-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 [EBA-RTS] are relevant.

XS2A interface

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

8.2 References

[XS2A-ImplG] NextGenPSD2 XS2A Framework, Implementation Guidelines, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.0, published 08 February 2018

[EBA-RTS] Commission Delegated Regulation (EU) No …/.. of XXX 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, C(2017) 7782 final, published 27 November 2017

[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] Draft 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, V0.0.3 (2018-01)

[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