THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

NextGenPSD2 XS2A Framework

Implementation Guidelines

Extended Services

Multiple Consents Service

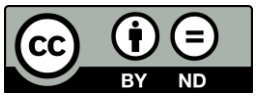
Version 1.0

30 October 2020

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

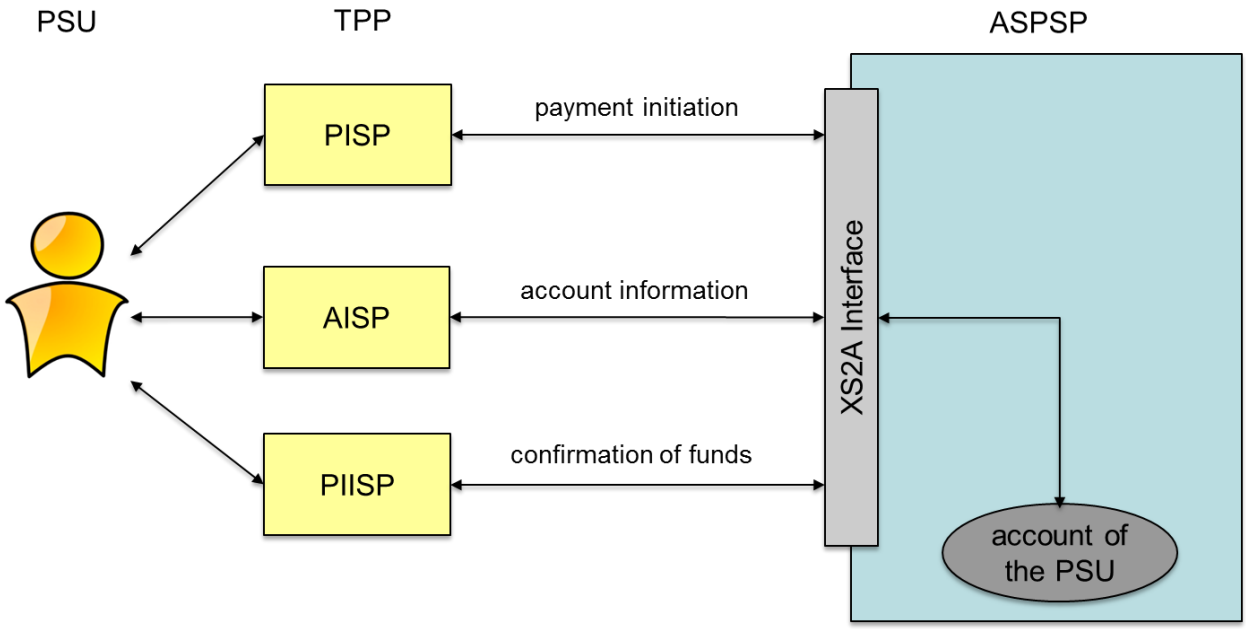
1.1 Background

With [PSD2] the European Union has published a new directive on payment services in the internal market. Member States had to adopt this directive into their national law until 13th of January 2018.

Among others [PSD2] contains regulations of 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 of the Availability of Funds service to be used by Payment Instrument Issuing Service Provider (PIISP) TPP as defined by article 65 of [PSD2].

For operating the new services a TPP needs to access the account of the PSU which is usually managed by another PSP called the Account Servicing Payment Service Provider (ASPSP). As shown in the following figure, an ASPSP has to provide an interface (called "PSD2 compliant Access to Account Interface" or short "XS2A Interface") to its systems to be used by a TPP for necessary accesses regulated by [PSD2]:



Further requirements on the implementation and usage of this interface are defined by a Regulatory Technical Standard (short RTS) from the European Banking Authority (short EBA), published in the Official Journal of the European Commission.

One of these requirements for the ASPSP is to provide an access to account information data once the consent of the PSU is provided. Additional requirements apply e.g. regarding to 4 times a day access without PSU involvement as well as for recurring accesses to account information where the PSU is directly involved. The NextGenPSD2 Taskforce has developed a consent API which can in detail specify the nature and scope of the TPP access to account information. After authorisation by the PSU, this results in a consent token which is then used for getting access to the accounts by the TPPs and which might be used by the ASPSP to control the access of the TPP, e.g. regarding the 4 times a day access without PSU involvement. Following the NextGenPSD2 Framework, a PSU can always have only one recurring consent agreed with a TPP within an ASPSP system – if a new recurring consent is submitted and authorised for this PSU/TPP combination, as it is needed e.g. for supporting the 90 days rule for account information access, then the old consent token is automatically invalidated.

TPPs might be challenged by this in a situation where they are offering AIS services to different subsystems or to other companies under regulation of civil law. The existing modelling mandates them to be aware of the PSU identity and to aggregate the PSU related consent details from different sources within their system or from companies they have got a cooperation with. This is part of the consent management obligation which is between PSU and TPP, following [EBA-RTS].

This item is addressed in the following extension of the AIS protocol. The intention is, that the ASPSP might offer the TPP to provide multiple recurring consents for the same PSU.

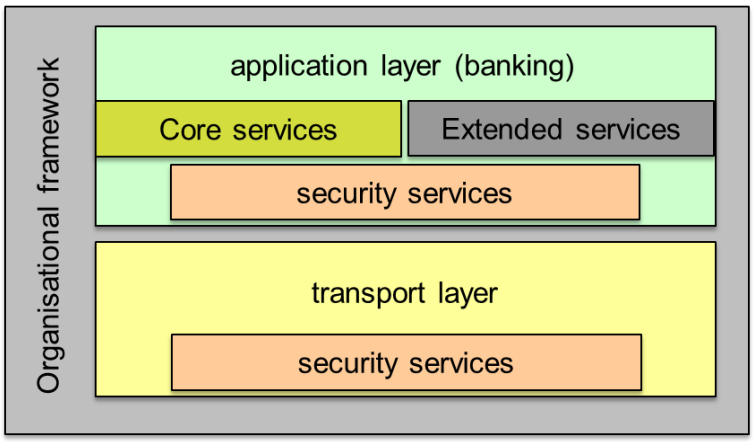
1.2 XS2A Interface Specification

This document is an extension of the NextGenPSD2 XS2A Specification which defines a standard for an XS2A Interface and by this reaching interoperability of the interfaces of ASPSPs at least for the core services defined by [PSD2].

The XS2A Interface is designed as a B2B interface between a TPP server and the ASPSP server. For the time being, the protocol defined in this document is a pure client-server protocol, assuming the TPP server being the client, i.e. all API calls are initiated by the TPP. In future steps, this protocol might be extended to a server-server protocol, where also the ASPSP initiates API calls towards the TPP.

The Interoperability Framework defines operational rules, requirements on the data model and a process description in [XS2A-OR].

This document details the standard in defining messages and detailed data structures for **extended services** of the XS2A Interface. For the specification the two layers shown in the following figure are distinguished:



This document now describes how the existing services for account information can be extended to allow the TPP to submit several recurring consent requests with potential difference in consent AIS scope for the same PSU which will then grant recurring access of the TPP to the PSU's data at the same time.

This document makes no assumption on the fact whether ASPSPs might mandate a contract between TPP and ASPSP to use this extended service. In some countries this service might also be mandated by NCAs.

Remark for Future: Please note that the Berlin Group NextGenPSD2 XS2A interface is still under constant development. Technical issues, which are already in discussion within the Berlin Group NextGenPSD2 working structure are mentioned in this document by "Remark for Future" to make the reader aware of upcoming potential changes.

1.3 Document History

Version	Change/Note	Approved
1.0	Initial Version	NextGenPSD2 TF 2020-10-30

2 Character Sets and Notations

For definition on character Sets and Notations as well as for request and response notations refer to Chapter 2 of [XS2A-IG].

3 Transport Layer

For details on the transport Layer, please refer to Chapter 3 in [XS2A-IG].

4 Application Layer: Guiding Principles

The following extension will define requirements on the requests for the ASPSP how to support the Multiple Consents Service. No new message types are defined for this service.

4.1 Signing Messages at Application Layer

The ASPSP may require the TPP to sign request messages in general for using the XS2A Interface. This requirement shall be stated in the ASPSP documentation. The signing requirements are defined in [XS2A-IG].

There is no specific signing requirement resulting from the Multiple Consent Service.

4.2 API Access Methods

No additional API access methods are defined for the Multiple Consent Service.

4.3 Multiple Consents within Establishing a Consent

When using the Establish Consent Account Information Request as defined in [XS2A-IG] to establish a recurring access, there will be no impact on the status of other consent tokens related to the PSU involved, in contrast to definitions on side effects in [XS2A-IG].

The ASPSP shall inform the TPP about the support of the Multiple Consent Service within the response message.

4.4 Multiple Consents within Read Account Information

Once a consent token is activated for a PSU through the establish consent process, it might be used until the end of the pre-defined validity period, if not cancelled by the TPP or the PSU directly.

If another consent token is activated for the same PSU by the same TPP before the end of the pre-defined validity period within the XS2A interface via another establish consent process, then there is no effect on the existing consent token within the Multiple Consent Service.

In this case both tokens can be used until the validity period of the corresponding token or until cancellation of the token by the TPP or the PSU.

4.5 Additional Error Information

No specific addition error information is needed for this extended service.

4.6 Status Information

Status Information for the AIS within the Establish Consent Process

No specific status information needed for this extended service.

5 Extensions of Existing Message Types

The following changes and extensions are applied to the messages as defined in [XS2A-IG].

5.1 Extension to the Account Information Consent Request

5.1.1 Extension for the Detailed Consent Model

In the definitions of the Account Information Consent Request for dedicated accounts as defined in Section 6.3.1.1 of [XS2A-IG] the following changes apply (marked with yellow colour):

Call

```
POST /v1/consents
```

Creates an account information consent resource at the ASPSP regarding access to accounts specified in this request.

Side Effects

When this Consent Request is a request where the "recurringIndicator" equals true, and if it exists already a former consent for recurring access on account information for the addressed PSU and potentially addressed corporate identification submitted by this TPP, then the former consent automatically expires as soon as the new consent request is authorised by the PSU.

There are no expiration side effects foreseen for Consent Requests where the "recurringIndicator" equals false.

The remark on side effects above does not apply within the Multiple Consent Service.

Query Parameters

No changes apply.

Request Header

No changes apply.

Request Body

No changes apply.

Response

Response Code

No changes apply.

Response Header

Attribute	Type	Condition	Description
Location	String	Mandatory	Location of the created resource.
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
ASPSP-Multiple-Consent-Support	Boolean	Conditional	true if the ASPSP supports the Multiple Consent Service. false if the ASPSP does not support the Multiple Consent Service. If not provided, this also implies that the ASPSP does not support the Multiple Consent Service.
ASPSP-SCA-Approach	String	Conditional	Possible values are: • EMBEDDED • DECOUPLED • REDIRECT OAuth will be subsumed by the constant value REDIRECT
ASPSP-Notification-Support	Boolean	Conditional	true if the ASPSP supports resource status notification services. false if the ASPSP supports resource status notification in general, but not for the current request. Not used, if resource status notification services are generally not supported by the ASPSP. Shall be supported if the ASPSP supports resource status notification services, see more details in the extended service definition [XS2A-RSNS].
ASPSP-Notification-Content	String	Conditional	The string has the form

Attribute	Type	Condition	Description
			status=X1, …, Xn where Xi is one of the constants SCA, PROCESS, LAST and where constants are not repeated. The usage of the constants supports the following semantics: SCA: Notification on every change of the scaStatus attribute for all related authorisation processes is provided by the ASPSP for the related resource. PROCESS: Notification on all changes of consentStatus or transactionStatus attributes is provided by the ASPSP for the related resource. LAST: Notification on the last consentStatus or transactionStatus as available in the XS2A interface is provided by the ASPSP for the related resource. This field must be provided if the ASPSP-Notification-Support =true. The ASPSP might consider the notification content as preferred by the TPP, but can also respond independently of the preferred request.

Response Body

No changes apply.

Example

Request

```
POST https://api.testbank.com/v1/consents
Content-Type:           application/json
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7756
PSU-IP-Address:         192.168.8.78
```

```
PSU-User-Agent:          Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
Date:                    Sun, 06 Aug 2017 15:05:37 GMT

{
  "access": {
      "balances": [
          { "iban": "DE40100100103307118608" },
          { "iban": "DE02100100109307118603",
            "currency": "USD"
          },
          { "iban": "DE67100100101306118605" }
        ],
      "transactions": [
          { "iban": "DE40100100103307118608" },
          { "maskedPan": "123456xxxxxx1234" }
        ]
    },
  "recurringIndicator": true,
  "validUntil": "2017-11-01",
  "frequencyPerDay": 4

}
```

Response in case *of a redirect*

```
HTTP/1.x 201 Created
X-Request-ID:            99391c7e-ad88-49ec-a2ad-99ddcb1f7721
ASPSP-Multiple-Consent: true
ASPSP-SCA-Approach:      REDIRECT
Date:                    Sun, 06 Aug 2017 15:05:47 GMT
Location:                "v1/consents/1234-wertiq-983"
Content-Type:            application/json

{
  "consentStatus": "received",
  "consentId": "1234-wertiq-983",
  "_links": {
    "scaRedirect": {"href": "https://www.testbank.com/authentication/1234-
wertiq-983"},
    "status": {"href": "/v1/consents/1234-wertiq-983/status"},
    "scaStatus": {"href": "v1/consents/1234-wertiq-983/
authorisations/123auth567"}
  }
}
```

5.1.2 Extensions for the Bank Offered and Global Consent Model

The same changes as above apply to the definitions of the Account Information Consent Request for bank offered and global consent models as defined in Section 6.3.1.2 of [XS2A-IG]. No explicit text is needed for this, since the call definitions in Section 6.3.1.2 of [XS2A-IG] just refer to the call definitions for the consent for dedicated accounts.

6 Extension of Complex Data Types

No extensions of complex data types needed for this service.

7 References

[XS2A-OR] NextGenPSD2 XS2A Framework, Operational Rules, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.0, published 08 February 2018

[XS2A-IG] NextGenPSD2 XS2A Framework, Implementation Guidelines, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3.8, published 30 October 2020

[XS2A-DP] NextGenPSD2 XS2A Framework, Domestic Payment Definitions, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, current version

[XS2A-RSNS] NextGenPSD2 XS2A Framework, Extended Services, Resource Status Notification Service, Version 1.0, 01 March 2019

[EBA-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, C(2017) 7782 final, published 13 March 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

[PSD2] Directive (EU) 2015/2366 of the European Parliament and of the Council on payment services in the internal market, published 23 December 2015