THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

Joint Initiative on a PSD2 Compliant XS2A Interface

NextGenPSD2 XS2A Framework

Security Bulletin

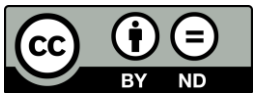
Version 1.1

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

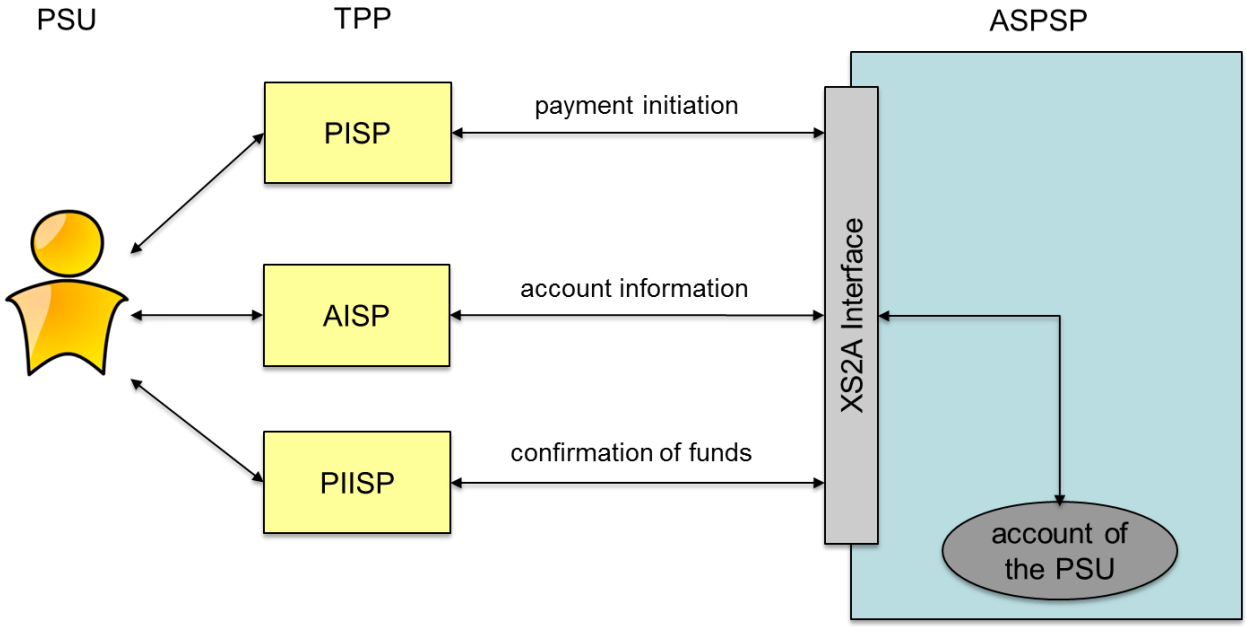
1 Introduction

1.1 Background

The Berlin Group started to publish its XS2A Framework in Version 1.3 on 15 October 2018 with later updates on the Implementation Guidelines leading to a Sub Version 1.3.4 on 5 July 2019, to a Sub Version 1.3.6 on 3 February 2020 and to a Sub Version 1.3.8 on 30 October 2020. This framework consists of the two Documents

- [XS2A OR]: Operational Rules and
- [XS2A IG]: Implementation Guidelines.

The following account access services are covered by this framework:



Every XS2A interface might be affected by potential fraud and attacks, like the ASPSP online channels itself. ASPSPs have evolved several mitigation measures to counter attacks in their online channels.

The NextGenPSD2 XS2A Implementation Guidelines foresee the support of several mitigation measures to counter fraud in line with the corresponding requirements of [EBA-RTS]. Many of these mitigation measures are related to processing of SCA methods or SCA exemption processing. These measures might further depend on the chosen SCA Approach of the ASPSP, i.e. the choice between an

- Embedded SCA Approach,
- Decoupled SCA Approach,

- Redirect SCA Approach, or the
- Integrated OAuth SCA Approach,

as defined in [XS2A IG].

The NextGenPSD2 Framework supports in addition to the different SCA Approaches as such the transport of major data as detectable in the PSU – TPP interface. This sort of PSU related device and interface data is used by ASPSPs already today in online channels for fraud detection.

Chapter 2 is explaining why this data was introduced into the Implementation Guidelines and how the absence of related data might lead to a higher risk score in the risk management systems of the ASPSPs. Thus, some of these mitigation measures are addressing the specific situation of introducing a Third Party Provider between the PSU and the ASPSP by forwarding PSU device or PSU –TPP interface related data to the ASPSP.

In [FAPI-CBPIA] specific attacks on redirect based protocols implemented within the PSD2 context have been published, where session fixation is addressed. The NextGenPSD2 TF has defined a specific mitigation measure in the NextGenPSD2 XS2A interface for session fixation in addition to mitigation measures defined in Section 2 applicable only in the SCA Redirect Approach and Integrated SCA OAuth Approach starting with version 1.3.6 of the XS2A Framework. This mitigation measure supports an authorization code as defined in the OAuth2 protocol generated during the SCA processing on the redirection authorisation page, which is then to be used in a subsequent authorisation confirmation step. This approach is sketched in Chapter 3 of this document. Depending on the ASPSP's requirements, this mitigation measure might already be implemented starting from version 1.3.4 of the Implementation Guidelines. In this case, this needs to be documented explicitly in the ASPSP's documentation.

1.2 Change Log

Version	Change/Note	Approved
1.0	Initial Version	6 November 2019
1.1	Adapted to the new version 1.3.6 and higher of [XS2A IG] in introduction and Section 3. Reference to the EBA Opinion on Obstacles added in Section 2.3 on the OAuth Pre-Step.	30 October 2020

2 Support of Existing Mitigation Measures

Already version 1.3.x of [XS2A IG] supports some (technical) mitigation measures which (by proper implementation) may support to minimise the chance of success of potential attacks at the XS2A interface. These are:

- Shortening the time frame for executing a necessary authentication of the PSU.
- Check and evaluate information known about the PSU/TPP interface.
- Execute an OAuth 2 pre-step.
- Accept only complete transactions at the XS2A interface.

Many attacks at online channels are based already today to some extent on social engineering. Technical parts of the attacks can only be successful if the attacked PSU cooperates due to his deception by a "convincing story" of the attacker. Due to the changing eco system for accessing accounts managed by an ASPSP (for initiating payments or for retrieving account information) these attacks might become more likely and PSU might become more easily vulnerable by such attacks. For this reason it is recommended that an ASPSP in addition to technical counter measures increases his efforts for informing and raising of the awareness of the PSU about potential attacks.

2.1 Shortening the time frame for authentication

For many attacks the attacker needs the cooperation of the attacked PSU, because the authentication of the PSU is a requirement for the transaction to be executed successfully. For this cooperation the attacker has to convince the PSU to execute the strong customer authentication within a time frame beginning with the start of the (either implicit or explicit) authorisation process for the transaction at the XS2A interface (see for example section 5.1 of [XS2A IG]) and ending after some interface specific time out. The duration of this time frame is determined by the ASPSP. By shortening this time frame the chances of success for the attacks is decreased.

2.2 Check and evaluate information about the PSU/TPP interface

Version 1.3.6 and higher of [XS2A IG] enables to include information about the PSU/TPP interface into request messages to be sent by the TPP to the XS2A interface. Parameters of the header may contain the following information:

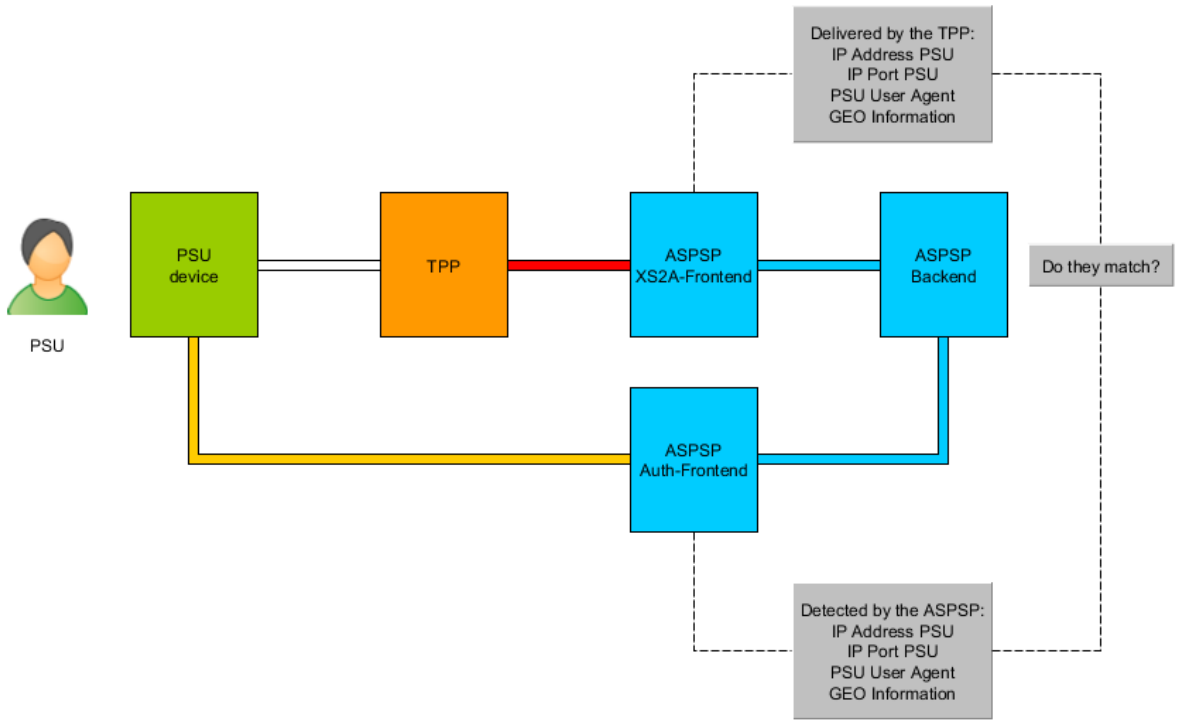
- IP address of the PSU for accessing the TPP.
- IP Port number of the PSU for accessing the TPP.
- Key information about the browser type and operating system used by the PSU to access the TPP.
- Device Identification.
- Information about the GEO location of the PSU while accessing the TPP.

See section 4.8 of [XS2A IG] for details.

The IP address of the PSU has to be delivered mandatorily by the TPP as part of the "Payment Initiation Request" and the "Establish Consent Request". For all other information it is optional to deliver these parameters. Also for other request messages it is optional to include this information. See section 5.2 (for payment initiation) and 6.2 (for account information) of [XS2A IG] for an overview of these header parameters.

This information about the PSU/TPP interface will be used by the ASPSP as input for his fraud detection and risk management systems. Some ASPSPs use this information also to exclude some authentication methods (for example some ASPSPs do not allow to receive an OTP by SMS on the same smartphone used also for the transaction itself). For this reason it is highly recommended that a TPP includes all of this information into his request messages. Missing information may result in an assessment of the user device as not useable for the authentication method or in a classification of the current transaction as a "higher risk transaction". By this the probability of a rejection of that transaction due to the result of fraud detection and/or risk management might be increased.

Transactions at the XS2A interface may include a redirection of the PSU to a frontend of the ASPSP. This is the case if the redirect approach or the integrated OAuth approach for executing a strong customer authentication is used. For these transactions the information about the PSU/TPP interface delivered by the TPP should be used by the ASPSP to detect possible attacks to the sessions used at the PSU/TPP interface and the PSU/ASPSP interface. The following picture shows the context:



By comparing the information about the PSU/TPP interface delivered by the TPP and the information about the PSU/ASPSP interface detected by the ASPSP itself, the possibility of the success of attacks as described in [FAPI-CBPIA] can be reduced.

2.3 OAuth 2 Pre-Step

The NextGenPSD2 Interface allows the ASPSP to define an OAuth2 Pre-Step. Depending on the detailed definition of this Pre-Step, another mitigation measure is defined to counter potential attacks on the NextGenPSD2 protocol. Since this pre-step is not further detailed within [XS2A IG], this mitigation measure is not further detailed in this document neither.

Remark: When implementing the OAuth pre-step, the requirements on e.g. registration steps or no mandatory two SCA usage in specific PIS only scenarios as defined by [EBA-OP2] should be recognized by the ASPSP.

2.4 Complete transactions for submission at the XS2A interface

Further measures should be taken by an ASPSP to complicate the automated generation of mass attacks according to the attack scenario described in [FAPI-CBPIA]. For example if the PSU ID and/or the account number of the attacked PSU are not already demanded as part of the submission of a transaction at the XS2A interface of the ASPSP, the attacker can generate much more easily a fraudulent transaction and submit this at the XS2A interface, hoping that the PSU will provide the missing information (as part of the authorisation process) and after that will authorise the transaction. In this case the attacker can generate and submit a huge number of fraudulent transactions automatically, hoping that at least some of the attacked PSUs might complete and authorise some of these transactions. To avoid this kind of automated attacks transactions should be determined as completely as possible as part of their submission at the XS2A interface.

3 Additional Mitigation Measure (Authorization Code)

Starting with version 1.3.6 of [XS2A IG] the NextGenPSD2 Framework supports further mitigation measures specifically against the attack for redirect based SCA architectures described in [FAPI-CBPIA]. This solution is following the solution proposal as defined in OAuth2 using an access token resp. a confirmation code for a confirmation command of the TPP after the transaction has been authorized by the PSU via a redirection to the ASPSP authentication server. This solution is available for the Integrated OAuth NextGenPSD2 Interface solution as well as for a plain redirect SCA approach. As part of this solution the ASPSP informs the TPP about the extended process step by providing an additional hyperlink with tag "confirmation" together with either the hyplink with tag "scaOAuth" or "redirect".

The change to the other flows is that instead of the TPP sending a Payment Status Request Message (GET command on status resource), the TPP will need to send a Transaction Confirmation Request Message (PUT command with an access token to the authorisation resource), as shown in the following flows.

The functional difference of the two solutions is that the payment will not be executed by the ASPSP in the new solution as long as the Transaction Confirmation Request Message has not been performed.

Starting with version 1.3.6 of [XS2A IG] the transaction flow including the Transaction Confirmation Request Message is already described in the Implementation Guidelines. For details see

Section in [XS2A IG]	Transaction flow
5.1.2	Redirect SCA approach: Explicit start of the authorisation process with confirmation code
5.1.4	Redirect SCA approach: Implicit start of the authorisation process with confirmation code
5.1.6	OAuth2 SCA approach: Implicit start of the authorisation process

Starting with version 1.3.6 of [XS2A IG] the necessary technical enhancements to support this solution (e.g. new hyperlinks at several responses, a new Confirmation of Authorisation request in Section 7.6) are described in the Implementation Guidelines.

4 References

[XS2A-OR] NextGenPSD2 XS2A Framework, Operational Rules, The Berlin Group Joint Initiative on a PSD2 Compliant XS2A Interface, version 1.3, published 21 December 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

[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

[EBA-OP2] Opinion of the European Banking Authority on obstacles under Article 32(3) of the RTS on SCA and CSC, EBA/OP/2020/10, published 4 June 2020

[FAPI-CBPIA] OpenID Foundation, Financial-grade API (FAPI) Working Group, Cross-Browser Payment Initiation Attack, https://bitbucket.org/openid/fapi/src/master/TR-Cross_browser_payment_initiation_attack.md, 3.01.2019

[OA-SecTop] OAuth 2.0 Security Best Current Practice draft-ietf-oauth-security-topics-13, Lodderstedt et al., 8 July 2019, https://tools.ietf.org/html/draft-ietf-oauth-security-topics-13