PSD2 API Solution - Documentation of the DKB Specific Methods and Workflows

Addressees:

Business Analysts, Project Managers, Developers, Architects, IT

Autor Alexander Kuhn

Version 1.00

Datum 13.06.2019

Versionshistorie

Version	Änderungsgrund	Datum	Autor	Status
1.00		23.04.2019	A. Kuhn	

Inhaltsverzeichnis

1. Introduction

For the implementation of the **PSD2 XS2A** (Access to Account) interface of the **DKB (**Deutsche Kreditbank) the procedure according to the Berlin Group Standard V1.3 was chosen. The PSD2 XS2A API (**PSD2 API Solution**) is provided by **CREALOGIX AG**. The corresponding MVP (Minimum Viable Product) approach is described in detail in the TPP documentation (PSD2 API Solution - Documentation for TPPs) including all standard business transactions and technical information. However, some features of the Berlin Group standard have not been implemented or have been implemented differently. Reasons are the technical design of the interface itself, for which DKB uses the **FinTS** access variant (similar to the **DKB Online Banking**) and DKB-internal decisions. An explanation of the special features can be found in the following chapters. Additionally, this document lists the supported DKB products and methods, which are available for **AISP** (Payment Initiation Service Provider), **PISP** (Payment Initiation Service Provider) and **PIIS** (Payment Instrument Issuing Service Provider) via the XS2A interface.

All PSD2 relevant features and functions will be available at the latest to **14.June 2019**. Thus, the DKB can apply for the exemption from the contingency measures according to **RTS Art. 33(6)**. However, a fallback concept can be found in the document 'Contingency Measures'.

2. Strong Customer Authentication (SCA)

A SCA is required for the PreAuth of the PSU and for the authorization of AIS consents and PIS payments.

2.1 PreAuth

A TPP-controlled pre-step authentication is used to enable access to the system. In the preAuth a SCA is **always** required, i.e. the PSU has to authenticate (login + password) and authorize (TAN) the access to its DKB online banking account before the XS2A interface can be used. For Payment Initiation Services (PIS), Account Information Services (AIS) and Fund Confirmation Services (FCS) the preAuth has to be the first step. After the successful authentication of a PSU in the preAuth, an access token is generated which can be used at the XS2A interface afterwards.

The required, separate API calls for the PreAuth are described in the TPP documentation (and PreAuth documentation). The OAuth method(s) for the SCA are:

- **Embedded Approach**: The PSU has to enter his login data at the TPP (Third Party Provider). The TPP is responsible to send the credentials (including the TAN) via API to the ASPSP.
- **Redirect Approach** (*in a later release(!)*): PSU enters its credentials directly at the OAuth server. The TPP has to provide a redirect URL and the TAN is recorded via the OAuth Server.

2.2 SCA TAN

During the SCA, the PSU has to authorize an action with its 2nd factor. (The 1st factor are the PSUs DKB credentials.) Therefore, the DKB offers following TAN methods:

2nd Factor	PSU Requirements	Description
TAN2Go	Mobile Device , DKB TAN2Go App	The PSU gets a one-time password (OTP/TAN) pushed into the DKB TAN2Go App. The PSU needs to provide the TAN in the TPP page and the TPP send it via the API to the ASPSP (embedded).
ChipTAN (manual)	ChipTAN Generator DKB-Banking-Card / Girocard	The PSU receives a one-time password (OTP/TAN) on the 'TAN-Generator'. The PSU needs to provide the TAN in the TPP page and the TPP sends it via the API to the ASPSP (embedded).

In development: Additional 2nd factor methods

2nd Factor	PSU Requirements	Description
Device-binding (for mobile banking)	'bonded' Mobile Device, DKB Banking App	The PSU can register one mobile device via the DKB Banking App. After that, the 'bonded' device of the PSU can be used as 2nd factor. A one-time password (OTP/TAN) is not required.
Push Message (for web banking)	'bonded' Mobile Device DKB Banking App	For Web Banking the PSU can also use its 'bonded' device as 2nd factor. After login (1st factor) a Push Message is sent to the DKB Banking App (on the 'bonded' device) and the PSU has to confirm the login by accepting the Push Message. A one-time password (OTP/TAN) is not required.

The DKB customer (PSU) can choose one or several of these TAN methods at DKB. The available 2nd factor methods for a PSU are reported to the TPP via the XS2A API. The TAN must be transmitted to the API within 5 minutes.

2.3 SCA Exemptions

The derogation provided in Article 10 of the RTS has **not** been implemented. Thus, a PSU must authorise itself using SCA for each login (PreAuth). This corresponds to the regular behaviour of DKB online banking.

Whitelisting, low-value transaction and transaction risk analysis (Article 13, a5 and 16 of the RTS) are also not supported in the first approach of the XS2A interface.

3. Account Information Service (AIS)

3.1 Create Consent

Account information can only be requested after a consent has been created. The SCA used for PreAuth is **not** sufficient to authorize a consent. A 'second' TAN is required for the creation of a consent. Here again the embedded approach is used. (*In a later release*, the redirect approach will be offered, too.)

After the PSU has created a consent for an account, the TPP receives a consentId. **In general,** the consentId is valid **without limitation**, i.e. it can be used to receive account information for the related account in this and the following sessions. The creation of a new consent is not required because a SCA is performed during the PreAuth.

A consent can become invalid, if:

- the PSU, TPP or ASPSP (DKB) revokes the consent.
- the consent was created for a specific period of time (validUntil).

3.2 Get Account Information

After the creation of the consent, the consentId is used as header to access the associated account and read account list, read account details, read account balances and read transactions. For each new session, a PreAuth (with SCA) has to be performed.

3.3 Get Account Information Older 90 Days

Since the PreAuth (with SCA) is used for each login, no additional SCA is required for querying transactions older than 90 days. Thus, the user can work more efficiently within the application.

3.4 Account Retrievals 4 Times / Day

In accordance with BerlinGroup specifications, the interface has an integrated counting function that limits access to account data (here: transactions and balances) without customer involvement to a maximum of four queries per 24 hours. Please note that access without PSU is **not possible** due to the SCA rule described above.

4. Payment Initiation Service (PIS)

4.1 Payment SCA

To confirm payments, a SCA takes place for each transaction. The SCA used for PreAuth is **not** sufficient to authorize a payment. A second, **dynamic linked** TAN is required for the authorization of a payment. Here again the embedded approach is used. (*In a later release*, the redirect approach will be offered, too.) As with all SCA procedures used by the DKB, the TAN must have been transmitted to the API within 5 minutes.

After the authorization of a payment, the API responds if the payment was **accepted or declined**, similar to the DKB Online Banking. It is not possible to send an automated confirmation that the payment was booked successfully because of the DKB **batch-booking** approach.

4.2 Payment Products

Description	Characteristic	Decision
Supported Single Payment products	sepa-credit-transfers	YES
	instant-sepa-credit-transfers	NO
	target-2-payments	NO
	cross-border-credit-transfers	YES
Supported Bulk Payment products	sepa-credit-transfers	NO
	instant-sepa-credit-transfers	NO
	target-2-payments	NO
	cross-border-credit-transfers	NO
Supported Periodic Payment products	sepa-credit-transfers	YES
	instant-sepa-credit-transfers	NO
	target-2-payments	NO
	cross-border-credit-transfers	YES

4.3 Payment Services

Description	Code	Characteristic	Decision
Standing order (Dauerauftrag)	HKCDB	Standing order status	YES
	HKCDE	Standing order create	YES
	HKCDL	Standing order delete	YES
	HKCDN	Standing order change	NO
	HKCDU	Standing order suspend	NO
Scheduled transfer (Terminüberweisung)	HKCSB	Scheduled transfer status	YES
	HKCSE	Scheduled transfer create	YES
	HKCSL	Scheduled transfer delete	YES
	HKCSA	Scheduled transfer change	NO

Moreover, it is not possible for the PSU to identify the TPP as the creator or initiator of the orders by means of a bank statement. The TPP is requested to provide the customer with the relevant information.

5. Fund Confirmation Service (FCS)

5.1 FCS Consent

FCS consents will be created by ASPSP (DKB) as suggested from Berlin Group. The TPP has to ask the PSU (DKB customer) to establish a FCS consent at the DKB. The PSU has to inform DKB with TPP registration number (which is part of the QWAC), the card number of the issued card (if available) and the account that should be linked to the FCS consent. After the creation of the consent, the TPP can check if enough funds are available on the related account.

Note: DKB would like to establish the "Extended value add services" of the Berlin Group in a further release. Then it should be possible to create a FCS consent via the TPP webpage, in a similar way like an AIS consent.

5.2 Fund Confirmation

Before the fund confirmation check a PreAuth (with SCA) is required. The ASPSP (DKB) checks if the certificate is valid and if a consent for the requested account exists.

The amount provided in this query or used for the evaluation corresponds to the regular account balance. Reserved amounts and the credit line are **not** included in the check.

6. Miscellaneous

6.1 Password Reset

The TPP Documentation describes the sign-in and sign-up processes for the WSO2 API Management Store in detail. It also contains the function for resetting the TPP password for the store. Alternatively, the TPP support is available.

6.2 Service Information

Technical support is available from Mo - Fr (9 a.m. to 5 p.m.) through our service provider Crealogix.

Contact:

E-Mail: kundenportal@crealogix.com

Hotline: +49 900-1352991 (1.49 € per minute).