Sopra Financial Technology

Sparda XS2A-API

OAuth Beschreibung

Version 3.0.3, 23.08.2021

Inhalt

1 Zusammenfassung

Dieses Dokument beschreibt die Sparda XS2A-API. Es basiert auf dem **NextGenPSD2 Framework Version 1.3.3**, welches von der Berlin Group bereitgestellt wird.

2 OAuth2-Protokoll (Autorisierung + Token)

Um Konto- oder Payment-Daten abfragen zu können, ist ein gültiger Access-Token notwendig. Die Realisierung wird grundlegend auf Basis des OAuth2-Protokolls der Berlin-Group-Spezifikation durchgeführt.

2.1 Autorisierung

Sie erhalten den Autorisierungscode, wenn Sie über die XS2A-API einen Consent oder ein Payment anlegen bzw. löschen. In der Response des jeweiligen Aufrufs erhalten Sie einen Link, mittels dem Sie den Kunden an den Identity Provider (IDP) weiterleiten.

2.1.1 Request

Aufruf der XS2A –API über z.B.:

- POST https://api.sparda.de/xs2a/3.0.0/v1/consents
- POST https://api.sparda.de/xs2a/3.0.0/v1/payments/sepa-credit-transfers
- DELETE https://api.sparda.de./xs2a/3.0.0/v1/payments/sepa-credit-transfers

Wichtig ist, dass Sie bei dem Request in dem Customer Header „X-BIC“ die BIC des Kunden mitgeben, um in der Response die richtige Instituts-URL für den IDP zu erhalten.

Sollte Ihnen bei der Erstellung eines PIS-Request die IBAN des Kunden nicht bekannt sein, können Sie diese auch weglassen. Dem Kunden wird dann am IDP die IBAN seines Zahlungsverkehrskontos angezeigt. Falls der Kunde mehr als ein Zahlungsverkehrskonto haben sollte, bekommt der Kunde eine Liste mit allen IBANs der Zahlungsverkehrskonten angezeigt und kann dort die richtige IBAN auswählen.

Beispiel:

```
curl --location --request POST
'https://api.sparda.de/xs2a/3.0.0/v1/consents' \

--header 'X-Request-ID: 74cef646-39fd-4640-988c-422870ce6b4a' \
--header 'Accept: application/json' \
--header 'Content-Type: application/json' \
--header 'PSU-IP-Address: 192.168.1.2' \
--header 'TPP-Redirect-URI: https://tppapi.sopra-ft.com' \
```

```
--header 'TPP-Nok-Redirect-URI: https://tppapi.sopra-ft.com' \
--header 'X-BIC: GENODEF1S06' \

--data-raw '{
    "access": {
      "allPsd2": "allAccounts"
    },
    "recurringIndicator": true,
    "validUntil": "2021-12-31",
    "frequencyPerDay": 4
}'
```

2.1.2 Response

Die Response aus dem API-Call wird folgendermaßen aussehen:

Beispiel:

```
{
    "consentStatus": "received",
    "consentId":
"lHxpyGplqaUKd-RdXFuuWsoyl4Gm-WsVt9UMk5a-if1enq-N38DMVOiHJH2Kh1biMaK3A41L
EI6-AQr7NTEPlneGDd8_WXXE6Y4C13Cr9H8=_=_psGLvQpt9Q",
    "_links": {
        "scaRedirect": {
            "href":
"https://idp.sparda-n.de/oauth2/authorize?bic=GENODEF1S06&client_id=PSDDE
-BAFIN-1923678&redirect_uri=https://tppapi.sopra-ft.com&response_type=cod
e&scope=AIS:tx-b6129fab4a076263f31e659ce5f88ffff6b8743b4d2ffd678b97a2eedd
4d8d9d&code_challenge_method=S256&code_challenge={code_challenge}"
        },
        "self": {
            "href":
"https://api.sparda.de/xs2a/3.0.0/v1/consents/lHxpyGplqaUKd-RdXFuuWsoyl4G
m-WsVt9UMk5a-if1enq-N38DMVOiHJH2Kh1biMaK3A41LEI6-AQr7NTEPlneGDd8_WXXE6Y4C
13Cr9H8=_=_psGLvQpt9Q"
        },
        "status": {
            "href":
"https://api.sparda.de/xs2a/3.0.0/v1/consents/lHxpyGplqaUKd-RdXFuuWsoyl4G
m-WsVt9UMk5a-if1enq-N38DMVOiHJH2Kh1biMaK3A41LEI6-AQr7NTEPlneGDd8_WXXE6Y4C
13Cr9H8=_=_psGLvQpt9Q/status"
        },
        "scaStatus": {
            "href":
"https://api.sparda.de/xs2a/3.0.0/v1/consents/lHxpyGplqaUKd-RdXFuuWsoyl4G
m-WsVt9UMk5a-if1enq-N38DMVOiHJH2Kh1biMaK3A41LEI6-AQr7NTEPlneGDd8_WXXE6Y4C
13Cr9H8=_=_psGLvQpt9Q/authorisations/133aade3-1ca4-4839-93f6-
520ef3d52274"
        }
    }
}
```

Im Redirect-Link ist noch die code_challenge zu befüllen. Alle anderen Daten können so übernommen werden.

Nach dem Aufruf des IDP-Links gibt der Kunde im Login-Formular der entsprechenden Sparda-Bank seine Online-Banking-Credentials ein. Anschließend wird er bei korrekter Eingabe zur starken Kundenauthentifizierung weitergeleitet.

Ist diese starke Kundenauthentifizierung erfolgreich, wird der Kunde mittels der Redirect-URI in Ihre Anwendung zurückgeleitet – gleichzeitig wird der Autorisierungscode an die URI angehängt. Dies kann wie folgt aussehen:

https://tppapi.sopra-ft.com/?code=tac-4a8a7d21cad5664cb3158ed87fe3b0f3fda253269f71cb16484cd0660ff871d5

2.2 Neuen Access-Token abrufen

Um den besagten Access-Token vom IDP zu erhalten, muss ein POST-Request an den IDP an die Adresse https://idp.sparda.de/oauth2/token gesendet werden. Diese Adresse ist nur mit einem gültigen eIDAS-Zertifikat erreichbar. Der Request tauscht den erhaltenen Autorisierungscode gegen einen Access-Token und einen Refresh-Token aus.

2.2.1 Request

Der Request enthält folgende Parameter:

Parameter	Pflicht	Beschreibung	Beispiel
grant_type	ja	„authorization_code“ muss hier angegeben werden	authorization_code
client_id	ja	Eindeutiger TPP-Identifier – entspricht dem *organizationIdentifier* aus dem eIDAS-Zertifikat	PSDDE-BAFIN-1923678
redirect_uri	ja	die exakte TPP-URI an die der User Agent nach der Autorisierung weitergeleitet wurde – URI muss also mit der redirect_uri aus der Autorisierung übereinstimmen	https://tppapp.sopra-ft.com
code	ja	Autorisierungscode aus der Autorisierung	tac-4a8a7d21cad5664cb3158ed87fe3b0f3fda253269f71cb16484cd0660ff871d5
code_verifier	ja	vom TPP-Client generierter „code_verifier“ (PKCE für OAuth 2.0) – muss mit dem „code_challenge“ aus Autorisierung zusammenpassen (PKCE-Standard) - RegEx für „code_verifier“: [\w\-\._~]{44,127}	thisisfinallyavalidcodeverifieraslongasthedistancetothemoon

Beispiel:

```
curl --location --request POST 'https://idp.sparda.de/oauth2/token' \

--header 'Content-Type: application/x-www-form-urlencoded' \

--data-urlencode 'grant_type=authorization_code' \
--data-urlencode
'code=tac-4a8a7d21cad5664cb3158ed87fe3b0f3fda253269f71cb16484cd0660ff871d
5' \
--data-urlencode 'redirect_uri=https://tppapi.sopra-ft.com' \
--data-urlencode 'client_id=PSDDE-BAFIN-1923678' \
--data-urlencode
'code_verifier=thisisfinallyavalidcodeverifieraslongasthedistancetothemoo
n'
```

2.2.2 Response

Die Response enthält sowohl den notwendigen Access-Token als auch einen Refresh-Token.

Beispiel:

```
{
    "access_token": "tat-
568bc4701722b480739a957ffec1f1da19e603dde17911ffc43f552e8ed8f48b",
    "refresh_token": "trt-
945cfc9677c6a5533f7c1ed89c886fa8bc95b103a37397200a17c378b522338a",
    "scope": "AIS:tx-
b6129fab4a076263f31e659ce5f88ffff6b8743b4d2ffd678b97a2eedd4d8d9d",
    "token_type": "Bearer",
    "expires_in": 300
}
```

2.3 Access-Token refreshen

Ein Access-Token ist maximal 5 Minuten gültig. Nach dieser Zeit kann mit diesem Token kein Aufruf mehr gegen die XS2A-API durchgeführt werden.

Mit Hilfe des zusätzlich erhaltenen Refresh-Token kann jedoch ein neuer Access-Token generiert werden.

Hierfür ist erneut ein Request gegen https://idp.sparda.de/oauth2/token durchzuführen.

2.3.1 Request

Der Request enthält folgende Parameter:

Parameter	Pflicht	Beschreibung	Beispiel
grant_type	ja	„refresh_token“ muss hier angegeben werden	refresh_token
client_id	ja	Eindeutiger TPP-Identifier – entspricht dem *organizationIdentifier* aus dem eIDAS-Zertifikat	PSDDE-BAFIN-1923678
refresh_token	ja	es muss der Refresh-Token übergeben werden, der gleichzeitig mit dem abgelaufenen Access-Token ausgegeben wurde	trt-945cfc9677c6a5533f7c1ed89c886fa8bc95b103a37397200a17c378b522338a

Beispiel:

```
curl --location --request POST 'https://idp.sparda.de/oauth2/token' \

--header 'Content-Type: application/x-www-form-urlencoded' \
--header 'X-BIC: GENODEF1S06' \

--data-urlencode 'grant_type=refresh_token' \
--data-urlencode
'refresh_token=trt-945cfc9677c6a5533f7c1ed89c886fa8bc95b103a37397200a17c3
78b522338a' \
--data-urlencode 'client_id=PSDDE-BAFIN-1923678'
```

2.3.2 Response

Die Response enthält einen neuen Access-Token und einen neuen Refresh-Token.

Beispiel:

```
{
    "access_token": "tat-
2c4958882aad89ce289ac0066d1b8fca176e0ead220203df7a7854a5f5d0fba7",
    "refresh_token": "trt-
8f3245b08e011e02bc84febeb3e08a378c2a8a8f67e077bd99ce9daaabebae87",
    "scope": "AIS:tx-
b6129fab4a076263f31e659ce5f88ffff6b8743b4d2ffd678b97a2eedd4d8d9d",
    "token_type": "Bearer",
    "expires_in": 299
}
```

3 OAuth2 Fehlermeldung

Im Fehlerfall wird anstatt des Autorisierungscodes die Fehlermeldung an die Redirect URI angehängt.

Aufbau der Fehlermeldung:

Parameter	Pflicht	Inhalt	Beschreibung
error	ja	Invalid_request unauthorized_client access_denied unsupported_response_type invalid_scope server_error temporarily_unavailable business_error	Fehlerkategorie
error description	nein	Text	Text der Fehlermeldung
error_code	nein	Nummer	Nummer der Fehlermeldung

Beispiel einer Fehlermeldung:

https://tppapp.sopra-ft.com/?error=invalid_request&error_description=Kunden-Authentifizierung+fehlgeschlagen

4 Changelog XS2A-API

Für Version 1.0.0 wurden die folgenden Änderungen am **NextGenPSD2 Framework Version 1.3.3** (bereitgestellt durch die Berlin Group) durchgeführt

- Endpunkte für Signing Baskets entfernt
- Endpunkte für Common Payments entfernt
- Bulk Payments entfernt
- Endpunkte für POST/PUT authorisation entfernt
- CAMT/PAIN/XML Format entfernt
- Endpunkte für Card Accounts entfernt
- alle Payment-Produkte bis auf sepa-credit-transfers entfernt
- allgemeine Beschreibung an die Sparda/SFT Bestimmungen angepasst
- POST/GET-Aufrufe für single und periodic-payment aufgeteilt