



Berlin Group NextGenPSD2

Changelog

PSD2 Compliance Berlin Group - Changelog 1.12.0

- PSD2 Compliance Berlin Group - Changelog
 - Introduction
 - Card Information Service - CIS
 - Handle whitespaces in IBAN and BBAN for AIS, PIS And CIS
 - Addition of transactionDate in GET /transactions response
 - Support of RSASSA-PSS signature scheme for request signature

Introduction

The updated version published is following the international Berlin Group NextGenPSD2 standard, version 1.3. Please note that the version in the URL will not change, the "v1" will be kept in all existing URLs.

Card Information Service - CIS

The following changes have been done for the CIS flow:

- Managing funds-confirmation with correct token checks. There were few incorrect error codes for CIS and CIS consent flow in the solution and in this release we have made corrections for them.
- *CIS*: **consent-id** header is not matching with the token's security data.

The below endpoint is affected:

- **POST /funds-confirmations**

eg

```
HTTP/1.1 400 Bad Request
Date: Mon, 14 Dec 2020 06:18:02 GMT
Content-Type: application/json
X-Request-Id: 957a3005-c81e-4df1-8aec-a40f7685ff09
location: /funds-confirmations/
```

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "CONSENT_UNKNOWN",
      "text": "The Consent-ID header does not match any active consent for the
TPP"
    }
  ]
}
```

- *CIS Consent*: **consent-id** in path doesn't exist at **ASPSP** side for **GET** and **DELETE** endpoints.

The below endpoint is affected:

- **GET /consents/confirmation-of-funds/{consent-id}**

eg

```
HTTP/1.1 403 Forbidden
Date: Mon, 14 Dec 2020 06:18:02 GMT
Content-Type: application/json
X-Request-Id: 957a3005-c81e-4df1-8aec-a40f7685ff09
location: /funds-confirmations-consents/5f6a0ee35069197acb467616
```

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "CONSENT_UNKNOWN",
      "text": "Consent id does not exist"
    }
  ]
}
```

- *CIS Consent* : when `authorisationId` is invalid for `/consents/{consentId}/authorisations/{authorisationId}`.

The below endpoint is affected:

- **GET /consents/confirmation-of-funds/{consent-id}/authorisations/ABC_XYZ**

eg

```
HTTP/1.1 403 Forbidden
Date: Mon, 14 Dec 2020 06:18:02 GMT
Content-Type: application/json
X-Request-Id: 957a3005-c81e-4df1-8aec-a40f7685ff09
location: /funds-confirmations-consents/5fd7042543e832694ef17c34/authorisations/ABC_XYZ
```

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "RESOURCE_UNKNOWN",
      "text": "Invalid identifier format for resource id"
    }
  ]
}
```

```
]
}
```

- *CIS Consent* : when `consentId` is not matching with the authorisation resourceId of provided `authorisationId` in `/consents/{consentId}/authorisations/{authorisationId}`.

The below endpoint is affected:

- **GET /consents/confirmation-of-funds/{consent-id}/authorisations/{authorisationId}**

eg

```
HTTP/1.1 403 Forbidden
Date: Mon, 14 Dec 2020 06:18:02 GMT
Content-Type: application/json
X-Request-Id: 957a3005-c81e-4df1-8aec-a40f7685ff09
location: /funds-confirmations-
consents/5fd6fa6b43e832694ef17bf0/authorisations/5fd70426ae383d15b807ad6d
```

```
{
  "tppMessages": [
    {
      "category": "ERROR",
      "code": "RESOURCE_UNKNOWN",
      "text": "The addressed resource is unknown relative to the TPP"
    }
  ]
}
```

Handle whitespaces in IBAN and BBAN for AIS, PIS And CIS

In this patch, we have handled managing of whitespaces for IBAN/BBAN before it's used to make any call to banks.

Note: No extra property has been added for this.

Addition of transactionDate in GET /transactions response

- In the response of GET /transactions, a new field `transactionDate` has been added. This field is *The Date when the actual transaction was initiated by a third party at ASPSP.*

The example structure of new transaction is as follows-

```
{
  ...
  "booked": [
    {
```

```

    "bookingDate": "2021-05-17",
    "valueDate": "2021-05-18",
    "transactionDate": "2021-05-18",
    "transactionAmount": {
      "amount": "1.00",
      "currency":
    }
    ...
  }
  ]
...
}

```

Support of RSASSA-PSS signature scheme for request signature

In this release we have provided support for **RSASSA-PSS** signature scheme using SHA512 as hash algorithm and MGF1 (with SHA512) as mask generation function i.e., "SHA512withRSAandMGF1"

Now TPP can use **SHA512withRSAandMGF1** algorithm in request signature header if **RSASSA_PSS** signature algorithm is used in QSeal certificate

Note: Supported signature algorithms are: rsa-sha256, rsa-sha512, SHA512withRSAandMGF1.