



Berlin Group NextGen PSD2

Changelog

PSD2 Compliance Berlin Group - Changelog

1.12.0

- [PSD2 Compliance Berlin Group - Changelog](#)
 - [Introduction](#)
 - [Account Information Service - AIS](#)
 - [Card Information Service - CIS](#)
 - [Service-Tpp-Management - Exclusive tpp onboarding feature](#)
 - [Service-Tpp-Management - Exclusive tpp update feature](#)
 - [UI-Backoffice - Exclusive tpp onboarding module](#)
 - [UI-Backoffice - Environment Configuration](#)

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.

Account Information Service - AIS

The following changes have been done for the AIS flow:

- For `allAccess` attributes in consent model, i.e. `availableAccounts`, `availableAccountsWithBalance`, `allPsd2 =>>` values can be either `allAccounts` or `allAccountsWithOwnerName`. In previous releases, we have been supporting a different value i.e. `all-accounts` which is not compliant. `all-accounts` is still supported for backward compatibility and will be removed in upcoming releases.

The previous version of access:

```
"access" : {  
  "availableAccounts": "all-accounts"  
}
```

The current version of Access field

```
"access" : {
  "availableAccounts": "allAccounts"
}
```

Endpoints

The below endpoint is affected:

- **POST /consents**

Typ send post consent for all Access

POST data:

```
{
  "validUntil" : "2020-09-26",
  "frequencyPerDay" : 1,
  "recurringIndicator" : true,
  "combinedServiceIndicator" : false,
  "access" : {
    "availableAccounts": "allAccounts"
  }
}
```

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/5fd70426a

```

```

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

```

Service-Tpp-Management - Exclusive tpp onboarding feature

A new feature has been introduced in *service-tpp-management*, **Exclusive TPP onboarding**. Exclusive tpps are the super set of the existing tpps having some extra privilege and information, depicting the nature of these tpps.

- A new field *TppAdditionalInformation* has been added in the Tpp model to capture this extra information. The structure of *TppAdditionalInformation* is as follows-

```
{
  ...
  "tppAdditionalInformation" : {
    "unlimitedAccess" : true/false,
    "tppType" : "PREMIUM/COMPLIANCE",
    "partnerName" : "Payconiq/psd2"
  }
}
```

- A new endpoint `POST /tpps/exclusive` for the creation of these exclusive tpps has been implemented.

Service-Tpp-Management - Exclusive tpp update feature

A new feature has been introduced in *service-tpp-management*, **Exclusive TPP update**. Once an exclusive tpp has been onboarded it can also be updated via the UI- backoffice application.

- A new endpoint `PUT /tpps/exclusive/{id}` for updating an exclusive tpp has been implemented which is exposed for a Back Office User.

UI-Backoffice - Exclusive tpp onboarding module

A new features has been introduced in ui-backoffice, **Exclusive tpp onboarding module**. A new module having all the details of an exclusive tpp has been created. A *Back Office User* can perform the following actions on this module-

- *Back Office User* can create a new exclusive tpp.
- *Back Office User* can view the list of created exclusive tpps.
- *Back Office User* can search the exclusive tpp by its name.
- *Back Office User* can update the exclusive tpp.
- *Back Office User* can view the orderbook of an exclusive tpp.

Note: For more details about the above feature check [here](#).

UI-Backoffice - Environment Configuration

Below environment configuration is marked as deprecated, for latest UI-Backoffice environment configuration please refer to readme of backoffice:

Field	Type	Description	Example
production	boolean	true if the environment is a prod environment (no debug traces and better perfs)	true
Settings section			
settings.pagination	number	Define the page size of each micro-service call	50
settings.aspsp_url_disable_regex_check	boolean	Define if the redirect urls of a TPP need to be verified by an exact URL regex. We can disable this behavior putting this var to true. - In SBX environments, true by default. - In UAT environments, false by default	true
settings.tpp_redirect_url_disable_regex_check	boolean	Define if the PSD2 standard urls of an ASPSP need to be verified by an exact URL regex. We can	true

		disable this behavior putting this var to true. - In SBX environments, true by default.- In UAT environments, false by default.	
Api subsection			
settings.api.host	string	Api host url	https://
settings.api.key	string	Api key define for this application (can be found in API Portal)	d30e19f8ea6
settings.api.port	string	Allow to define a X-SBS-ENV-PORT to use Kubernetes namespace.	30201
Auth subsection			
settings.auth.client_id	string	Client id of the application used to get Basic authorization in 64base.	argent
settings.auth.password	string	Secret of the application used to get Basic authorization in 64base.	uKPtk
OpenId subsection			
settings.openid.authority	string	OpenId authority url	https://

settings.openid.realm	string	OpenId realm	realms
settings.openid.client_id	string	OpenId client id	test-ar
settings.openid.response_type	string	OpenId response type	code i
settings.openid.root	string	OpenId root url when redirect (url of the backoffice application)	https://
settings.openid.scope	string	OpenId scope (data present in the OpenId token)	openic
i18n subsection			
settings.language.default	string	Default language	en
settings.language.list	array	Array of languages can be used in the application. Each item of the list need to have : id: Identifier of the language label: Display label of the language icons: Codes ISO on 2 char for the language (display the flags of the language)	[{ "id" "icons" "Franç
URIs subsection (exposed in API Portal)			
settings.uris.aspsps	string	ASPSP management	/partic manag

		exposed URI	
settings.uris.auth	string	Server external auth exposed URI	/auth
settings.uris.consent	string	Customer consent exposed URI	/partic manag
settings.uris.events	string	Orderbook exposed URI	/event
settings.uris.tpps	string	TPP Management exposed URI	/partic manag
settings.uris.psus	string	User roles exposed URI	/party-
settings.uris.regulatedEntities	string	Regulated entities from external registry exposed URI	/obe-r
PSD2 Standards List			
settings.psd2_standards	array	Array of PSD2 standards names allowed to use in the application (select box)	['berli
Modules activated			
settings.modules.actasaspp	boolean	Allow to enable or disable the Act as ASPSP module (true = enabled, false = disabled).Need to be true for now.	true
settings.modules.actastpp	boolean	Allow to enable	true

		or disable the Act as TPP module (true = enabled, false = disabled).Need to be true for now.	
settings.modules.preta	boolean	Allow to enable or disable the PRETA module (true = enabled, false = disabled).	false
Access Control List			
settings.acl.actasaspsp_consents_view settings.acl.actasaspsp_consents_delete settings.acl.actasaspsp_psus_search settings.acl.actasaspsp_psus_auditbook settings.acl.actasaspsp_tpps_create settings.acl.actasaspsp_tpps_edit settings.acl.actasaspsp_tpps_details settings.acl.actasaspsp_tpps_auditbook settings.acl.actastpp_aspsps_create settings.acl.actastpp_aspsps_edit settings.acl.actastpp_aspsps_details settings.acl.preta_regulatedEntities_details	array	Array of roles that can access to this action (the values of the array need to be define in Keycloak roles. By default, they are this roles available: 'admin', 'tpp-manager', 'viewer').	['adm
Security session			
settings.security.idle_max_duration_seconds	number	Duration from which the user is considered inactive (without action on his part). Triggers an inactivity notification.	240
settings.security.idle_countdown_seconds	number	Duration of the inactivity notification. At the end of this	60

		period, the user is disconnected.	
settings.security.failure_tentatives	number	The application can try to get a DXP token 5 times in a row. If it fails 5 times, it stop trying.	5
Notification system			
settings.notification.timeout_interval_seconds	number	Duration of the error / warning notifications. 0 = infinity / user action needed to close the notification.	0
External registry			
settings.external_registry.operated_countries	array	Operated countries about the aspsp	['BE', ']
settings.external_registry.accreditations_mapping.AIS	string	Mapping between the external registry AIS accreditations and tpp management AIS accreditations	AIS
settings.external_registry.accreditations_mapping.CIS	string	Mapping between the external registry CIS accreditations and tpp management CIS accreditations	CBPII

settings.external_registry.accreditations_mapping.PIS	string	Mapping between the external registry PIS accreditations and tpp management PIS accreditations	PIS
---	--------	--	-----