STET PSD2 API

Documentation

Author: Robache Hervé

Date: 2018-04-10

Version: 1.3.0 (English)

Table of content

1. Introduction

1.1. Context

The revised Payment Service Directive (PSD2) points out some new roles providing services to a Payment Service User (PSU):

- Third Party Providers (TPP) which can be subdivided into three categories
  - Account Information Service Providers (AISP)
  - Payment Initiation Service Providers (PISP)
  - Payment Issuer Instrument Service Providers (PIISP)
- Account Servicing Payment Service Providers (ASPSP).

Each Member Country has to transpose the PSD2, within its own national law.

The PSD2 is completed by a set of documents provided by the European Banking Authority (EBA). Among these documents, the Regulatory Technical Standards (RTS) for Strong Customer Authentication (SCA) details some requirements, for instance on security principles: traceability, strong customer authentication…

1.2. Mission

STET has been mandated by its shareholders in order to design and provide an open API (Aka STET PSD2 API) that would specify the different interactions between TPPs and ASPSPs for carrying out the different use cases of PSD2. This API could be extended to other (non-PSD2) use cases in the future but this extension is not part of the mandate.

As the RTS for SCA are now finalised, this version of the API and its documentation takes into account the new constraints and rules that have been introduced.

This version also includes

- Items that have been identified and studied in common with the BERLIN GROUP, in a strategy of convergence of the different European API initiatives.
- Evolvements linked to the change requests that have been received after public release of STET PSD2 API V1.2.

The STET PSD2 API does not cover:

- Interactions between PSUs and TPP
- Interactions between PSUs and ASPSP
- Registration information management

The technical characteristics of this API are provided within a SWAGGER 2.0 file. The present document purpose is to provide extra-information on this API and to give some interaction samples.

1.3. Licence

This specification is published under the following licence

> “Creative Commons – Attribution 3.0 France (CC BY 3.0 FR)”

This work has been coordinated by STET with the following contributors:

- BNP Paribas
- Le Groupe BPCE
- Le Groupe Crédit Agricole
- La Banque Fédérative du Crédit Mutuel – CIC
- La Banque Postale
- La Société Générale
- La Caisse des Dépôts et Consignations
- Le Crédit Mutuel - ARKEA
- HSBC France
- L’OCBF

2. Business Model

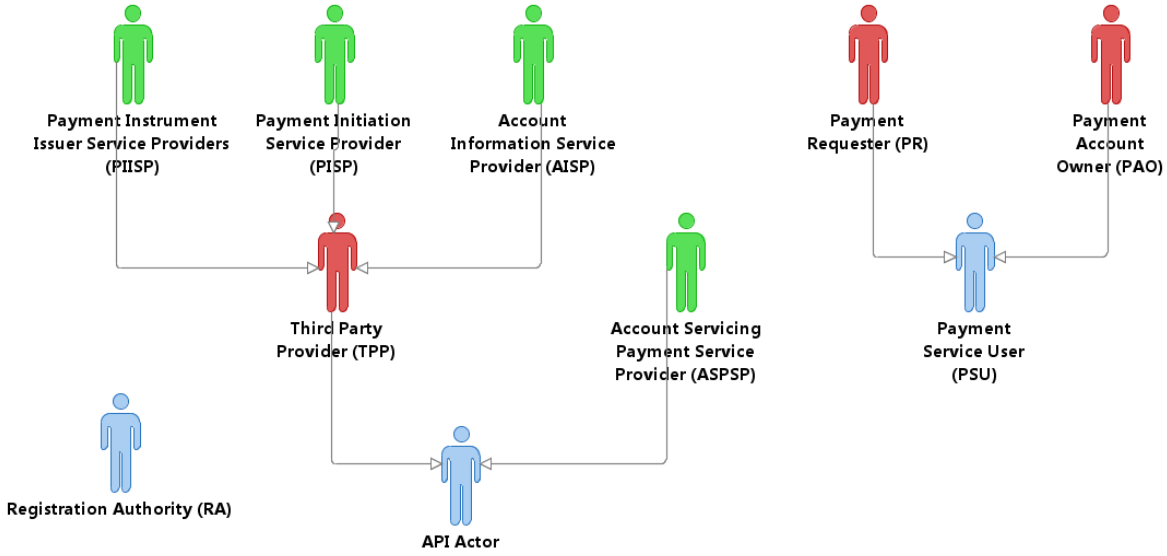
2.1. Actors and Roles

A PSD2 actor is either an entity or a physical person which can endorse one or several roles.

Most of the roles are defined in PSD2. However some extra-roles have been specified for the purpose of the STET PSD2 API during the analysis phase of the project.

Within the following diagram:

- Actors are cyan-coloured
- Pure PSD2 roles are green-coloured
- Specific STET PSD2 API roles are red-coloured



2.1.1. Payment Service User (PSU)

PSUs are the end-users of the services provided by TPPs and ASPSPs.

They are either physical persons or entities (organisations, companies, administrations…).

They do not interact directly with the STET PSD2 API.

A given PSU endorses at least one of the following roles:

- Payment Account Owner (PAO) for one or several accounts held by one or several ASPSPs.
- Payment Requester (PR) asking either for a payment or a coverage check.

2.1.2. API actors

2.1.2.1. Account Servicing Payment Service Provider (ASPSP)

These are Payment Service Providers (PSPs) which are in charge of holding bank accounts for their customers (PSU).

2.1.2.2. Third Party Provider (TPP)

These actors can intermediate between PSUs and ASPSPs, acting on behalf of a PAO or a PR.

On one hand, a given PAO may contract with a TPP in order to use the services provided by this TPP:

- Account Information Services (AISP role) will allow the PAO to get information, through a single interface, about all of his/her accounts, whatever the ASPSP holding this account.
- Payment Instrument Issuer Service (PIISP role) that will check the coverage of a given payment amount by the PSU's account.

On the other hand, a PR may also contract with a TPP that will provide the following services:

- Payment Initiation Services for requesting a Payment Request approval by the PSU and requesting the subsequent execution through a Credit Transfer (PISP role).

2.1.3. Registration Authorities (RA)

RAs are in charge of registering and overviewing the PSD2 actors.

The registration information is the foundation on which each actor can rely in order to know:

- Who is a given actor?
  - Identity
  - Contacts (business, legal, operational…)
  - Insurance coverage
  - Authentication media
    - X.509 certificates
    - Certification chain and services (revocation list, OCSP)
- For which roles this actor has been registered
  - AISP
  - PISP
  - PIISP
  - ASPSP
- Technical characteristics
  - APIs that are provided
  - URLs that are to be used, for test or live processing.

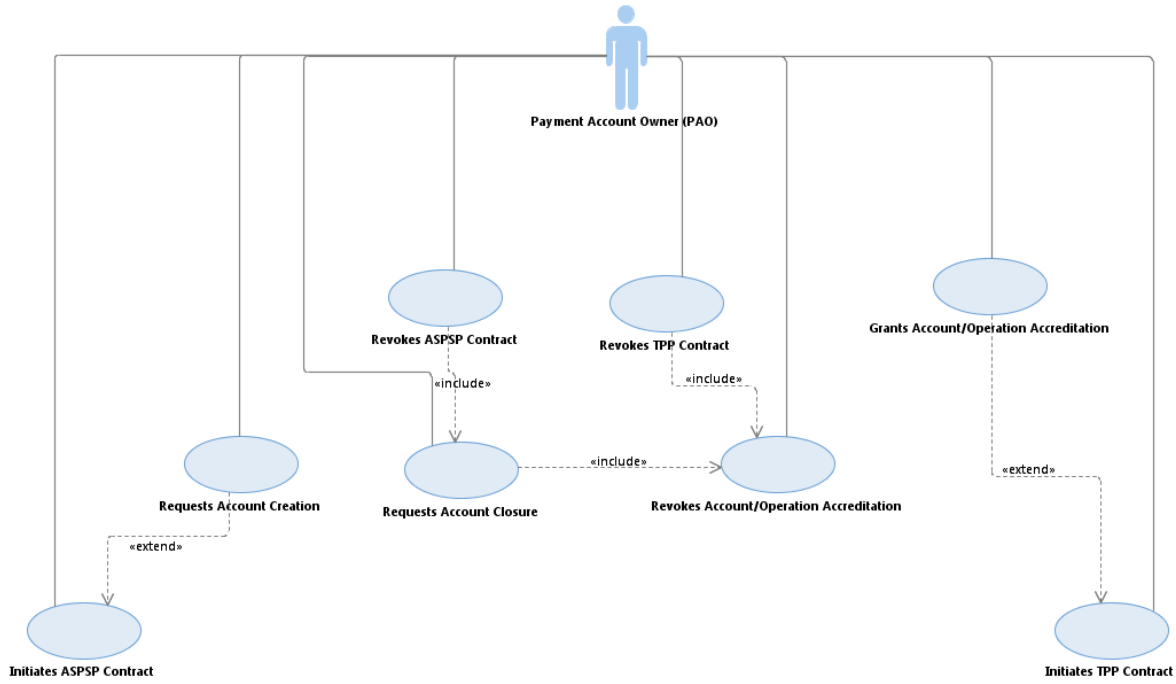
Registration Authorities must keep track of changes for each actor in order to recover the full history of the actor.

2.2. Use cases

Some of the use cases that are listed below are directly implemented by the STET PSD2 API, for they rely on interactions between TPPs and ASPSPs.

Other uses cases are tagged as “NON-API” and are only described for global understanding purpose.

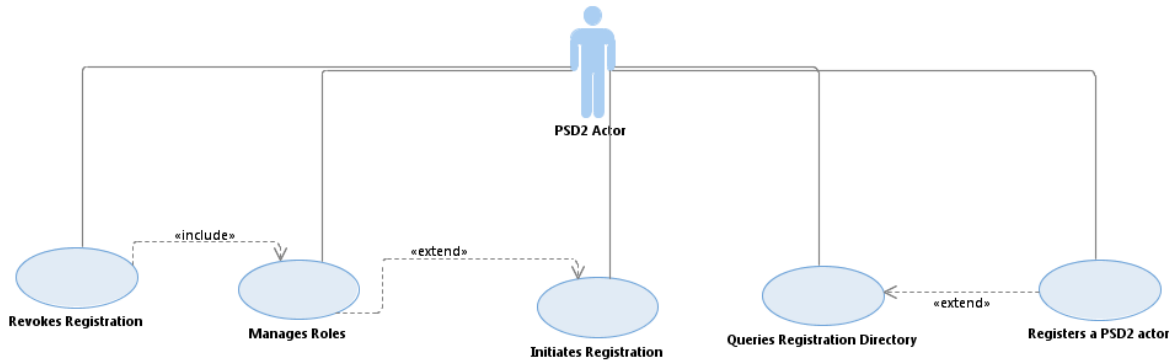
2.2.1. PAO uses cases (NON-API)



USE CASE (PAO)	DESCRIPTION	INTERACTIONS
Initiates ASPSP Contract	The user contracts with an ASPSP in order to use its services. This use case is likely extended by one or more occurrences of the “Requests Account Creation” use case	ASPSP
Requests Account Creation	The user asks the ASPSP to open a new payment account Requires a contract between the PAO and the ASPSP	ASPSP
Requests Account Closure	The user asks the ASPSP to close an existing payment account This use case includes the “revokes Account/Operation Accreditation” use case for all operations on this account and for all granted TPP.	ASPSP TPP (indirectly)
Revokes ASPSP Contract	The user revokes the contract with the ASPSP This use case includes the “Requests Account Closure” use case for each account that is held by the ASPSP. This use case includes the “Revokes Account/Operation Accreditation” use case for all operations on each of these accounts and for all granted TPP.	ASPSP TPP (indirectly)

USE CASE (PAO)	DESCRIPTION	INTERACTIONS
Initiates TPP Contract	The user contracts with a TPP having AISP and/or PIISP roles in order to use its service This use case is likely extended by one or more occurrences of the “Grants Account/Operation Accreditation” use case	TPP
Grants Account/Operation accreditation	The user allows the TPP to access a given set of operations on one of his/her payment accounts. Requires a contract between the PAO and the ASPSP, a contract between the PAO and the TPP and the registration of this PAO-TPP relationship by the ASPSP. Requires also that the capture and the execution of the accreditation are handled by the ASPSP or the TPP (PSU choice).	ASPSP TPP
Revokes Account/Operation accreditation	The user asks the ASPSP to revoke the TPP access for a given set of operations on a given PAO account Requires that the capture and the execution of the revocation are handled by the ASPSP or the TPP (PSU choice).	ASPSP TPP
Revokes TPP Contract	The user revokes the contract with the TPP. This use case includes the “Revokes Account/Operation Accreditation” for all grants given to the TPP, whatever the ASPSP. Since this cannot be automated, it is the PAO’s duty to initiate all the relevant revocations with each ASPSP.	TPP ASPSP

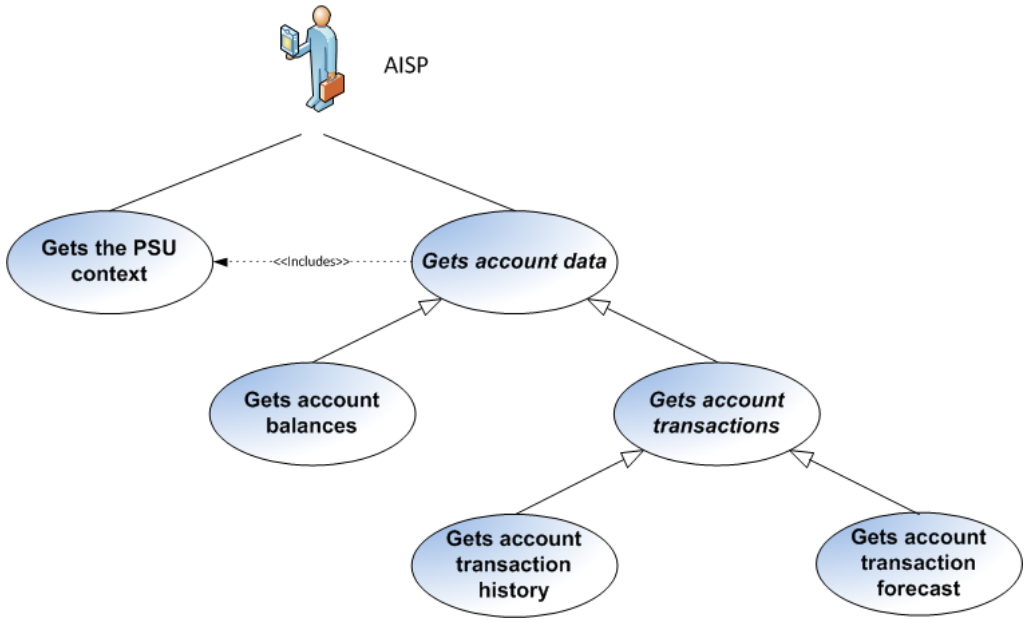
2.2.2. Registration use cases (NON-API)



USE CASE (PSD2 ACTOR)	DESCRIPTION	INTERACTIONS
Initiates Registration	The user asks the RA for registration. This use case is likely extended by one or more occurrences of the “Manages Roles” use cases	RA other actors (indirectly)
Manages Roles	The user asks the RA to be referenced for a given set of roles. This use case can be replayed in order to reference or dereference any role.	RA other actors (indirectly)

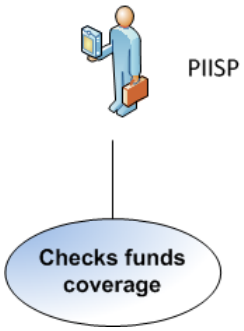
USE CASE (PSD2 ACTOR)	DESCRIPTION	INTERACTIONS
Revokes registration	The user informs the RA that its registration is to be cancelled	RA other actors (indirectly)
Queries Registration Directory	The user queries the RA directory in order to get data on other PSD2 actors: roles, certificates…	RA other actors (indirectly)
Registers a PSD2 actor	The user registers a given PSD2 actor into its own Directory	None

2.2.3. AISP use cases



USE CASE (AISP)	DESCRIPTION	INTERACTIONS
Gets the PSU Context	The user queries the ASPSP in order to get - the PSU accounts it is allowed to access - the operations it is allowed to process on each PSU account	ASPSP
Gets Account Data	*This use case is abstract. Its purpose is to stress that the "Gets the PSU Context" is a prerequisite for all other use cases on a given account*	*none*
Gets Account Balance	The user queries the ASPSP in order to get the balance on one given account. The ASPSP can provide several balance computing's (Instant Balance, Accounting Balance…), each balance type being specified with an explicit label.	ASPSP
Gets List of Transactions	This use case is abstract and can be seen as the common interface for the two following uses-cases.	ASPSP
Gets Account Transaction History	The user queries the ASPSP in order to get all the transactions that have been committed to one given PSU account within a given range of value dates.	ASPSP
Gets Account Transaction Forecast	The user queries the ASPSP in order to get all the transactions that are known by the ASPSP to be committed to a given PSU account	ASPSP

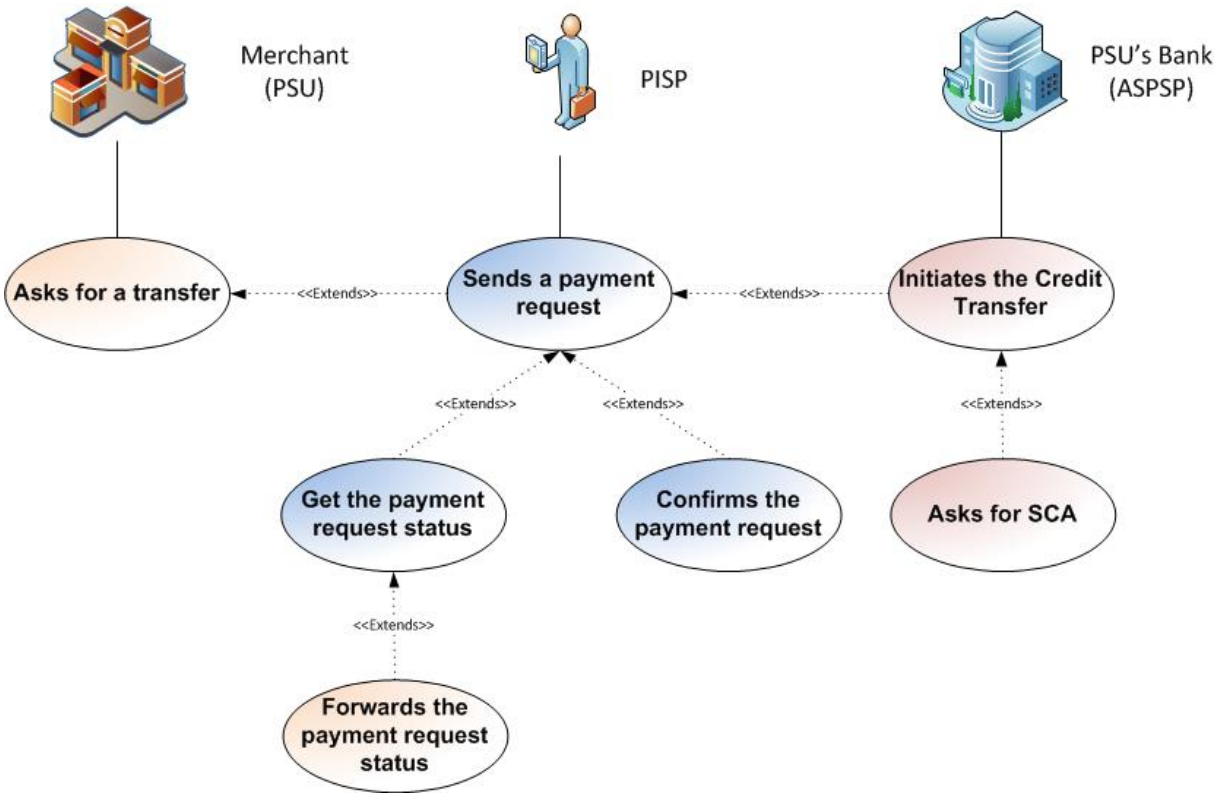
2.2.4. PIISP use cases



USE CASE (PIISP)	DESCRIPTION	INTERACTIONS
Checks Funds Coverage	The user queries the ASPSP in order to check if a given transaction amount can be covered by one given PSU account	ASPSP

2.2.5. PISP uses cases

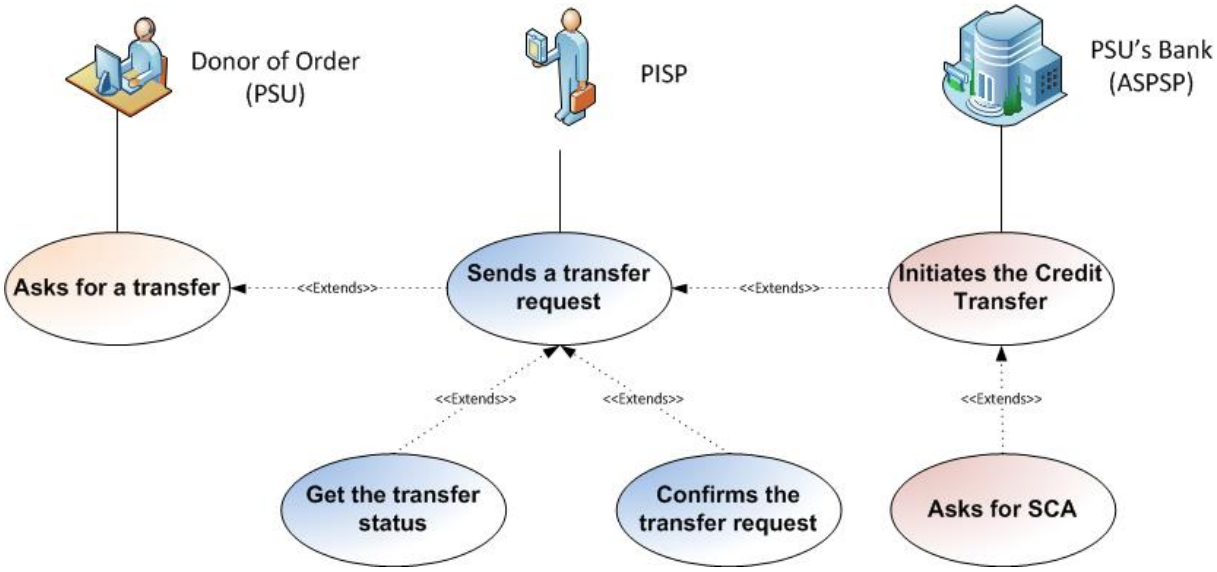
2.2.5.1. Payment Request on behalf of a Merchant



USE CASE (PISP)	DESCRIPTION	INTERACTIONS
Sends a Payment Request	The user sends to the ASPSP all the information needed to initiate a Payment from one PAO account (debtor) to one PR account (creditor)	ASPSP
Confirms the Payment Request	The user confirms the Payment Request to the ASPSP and might forward a PSU authentication factor so that the ASPSP can complete the Strong Customer Authentication and initiate the subsequent Credit Transfer	ASPSP
Gets the Payment Request status	The user gets the status of the Payment Request from the ASPSP.	ASPSP
Forwards the Payment Request status to the Creditor (Non-API)	The user informs the PR of the status of the Payment Request	PR (Creditor)

USE CASE (ASPSP)	DESCRIPTION	INTERACTIONS
Asks for SCA (Non-API)	Provided the Payment Request is valid, the user asks the PAO in order to get the SCA and consent to the relevant Payment Request	PSU
Initiates the Credit Transfer (Non-API)	Provided the PAO has given his/her consent, the ASPSP initiates the relevant Credit Transfer.	PR's ASPSP (Creditor Agent)

2.2.5.2. Transfer Request on a behalf of a Donor of Order



USE CASE (PISP)	DESCRIPTION	INTERACTIONS
Sends a Transfer Request	The user sends to the ASPSP all the information needed to initiate a Transfer from one PAO account (debtor) to one PR account (creditor)	ASPSP
Confirms the Transfer Request	The user confirms the Transfer Request to the ASPSP and might forward a PSU authentication factor so that the ASPSP can complete the Strong Customer Authentication and initiate the subsequent Credit Transfer	ASPSP
Gets the Payment Request status	The user gets the status of the Transfer Request from the ASPSP.	ASPSP

USE CASE (ASPSP)	DESCRIPTION	INTERACTIONS
Asks for SCA (Non-API)	Provided the Transfer Request is valid, the user asks the PAO in order to get the SCA and consent to the relevant Transfer Request	PSU
Initiates the Credit Transfer (Non-API)	Provided the PAO has given his/her consent, the ASPSP initiates the relevant Credit Transfer.	Beneficiary's ASPSP (Creditor Agent)

3. Prerequisites and technical details

3.1. Actors registration

PSD2 actors must be registered by a registration authority. The information that has been collected must be accessible to other actors in order to provide trust and interoperability.

A non-registered actor cannot interact with another actor.

Each actor must be provided with at least one X.509 certificate, for TLS 1.2 purpose, delivered by a registered Qualified Certification Service Providers (QTSP).

3.2. Cross-Authentication and Data Encryption

The STET PSD2 API relies on TLS 1.2 protocol in order to get cross-authentication between actors. Moreover, this protocol also ensures data confidentiality during their transport on the network.

Whenever a TPP connects as a client to an ASPSP API service, it will check the ASPSP server certificate and present its own qualified certificate (QWAC) respecting the ETSI/TS119495 Technical Specification. In case of authentication failure, on one side or the other, the connection must be closed.

No additional encrypting or authenticating feature is required.

3.3. Strong Customer Authentication (SCA)

Three different approaches can be used by a TPP to allow the Strong Customer Authentication by the ASPSP. These three approaches rely on a PSU identification that must be relevant to the ASPSP (National identifier or Bank customer identifier).

These three approaches are implemented in different ways, depending on the relevant use case:

- either during the authorisation process (cf. § 3.4), mostly for AISP and PIISP use cases
- or during the consent management process, for instance in case of Payment Request (cf. § 4.5)

3.3.1. Redirect Approach

Through the Redirect approach, the PSU authentication process is fully processed by the ASPSP.

In order to allow this, the TPP has to redirect the PSU to the ASPSP authentication service, meaning the PSU will leave temporarily the TPP interface for authenticating towards the ASPSP interface.

The TPP might have already captured a PSU identifier that can be handled by the ASPSP for unambiguously recognizing the PSU. In this case this identifier might be forwarded through the redirection.

After finalisation of the authentication, the ASPSP redirects the PSU back to the TPP interface.

3.3.2. Decoupled approach

Through the Decoupled approach, the PSU authentication process is fully processed by the ASPSP.

In order to allow this the TPP has to capture a PSU identifier that can be handled by the ASPSP for unambiguously recognizing the PSU, and to forward this identifier to the ASPSP.

Based on this identifier, the ASPSP will trigger a Strong Customer Authentication through a decoupled device or application, meaning that the PSU will not leave the TPP interface during the authentication process.

3.3.3. Embedded approach

Through the Embedded approach, the PSU authentication process involves the TPP that will forward one or two authentication factor, these factors being:

- One “Knowledge” factor, e.g. an unlock PIN known by the PSU
- One “Possession” factor, e.g.
    - a One-Time Password sent by the ASPSP on a separate device or application owned by the PSU
    - a response to a challenge sent by the ASPSP on a separate device or application owned by the PSU

3.4. Authorization

3.4.1. Levels of authorization

The following levels of authorization may be checked and combined in order to compute the effective rights granted to the TPP:

AUTHORIZATION LEVEL	DESCRIPTION
Authorization by TPP role	Once the TPP has been registered for a given role, it can call any of the PSD2 features provided by an ASPSP through the STET PSD2 API for this role.
Authorization by TPP-ASPSP agreement	The TPP can call any of the additional (non PSD2) features provided by an ASPSP through the STET PSD2 API, provided there is a bilateral agreement to use these features.
Authorization by TPP-PSU agreement	If the PSU has contracted with a TPP, he/she must - Give a list of the ASPSPs that it allows the TPP to access - Process an SCA against each of those relevant ASPSPs that will further allow the TPP to access the PSU data.
Authorization by PSU context	The PSU is able to specify his/her PSU context detailing, for each of its relevant accounts: - If this account will be accessible or not by the TPP - Which features can be used by the TPP The PSU can modify at any time his/her PSU context.

3.4.2. AISP and PIISP authorization levels

Since a TPP is acting on behalf of a PSU being a PAO, the PSD2 use cases that are linked with AISP and PIISP roles require the following authorization levels:

- Authorization by Role
- Authorization by TPP-PSU agreement
- Authorization by PSU context

3.4.2.1. List of the relevant ASPSPs

When contracting with a TPP, the PSU will provide a list of the ASPSPs that it allows the TPP to access. This list may not be exhaustive and so may not include some of the PSU's ASPSPs.

3.4.2.2. Registration of the TPP-PSU agreement by each ASPSP

This registration is due to enable the further access of the TPP to the PSU's data that is hosted by a given ASPSP by providing the TPP with an OAUTH2 access token.

AISP scope

The OAUTH2 scope requested by an AISP can be one of the following values:

- “aisp”
- “aisp extended_transaction_history”

The first scope value allows the AISP accessing all accessible accounts and data allowed by the PSU until expiration of the by-law specified delay between two SCAs. However, the value does not allow requesting an extended transaction history, i.e. history including transactions older than 90 days.

The second scope value allows the AISP accessing all accessible accounts and data allowed by the PSU until expiration of the by-law specified delay between two SCAs. It also allows requesting an extended transaction history.

However this “aisp extended_transaction_history” scope will be restricted to “aisp” by the ASPSP during the first token refresh. Thus:

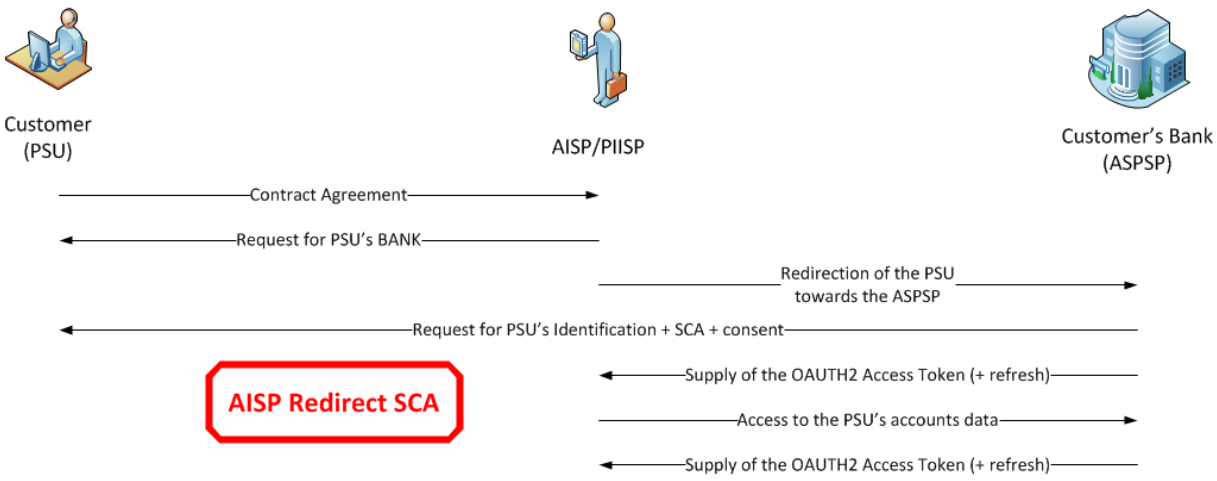
- The AISP will be able to ask for an extended transaction history with the very first access token retrieved after a token request. So, In this case a single SCA will be required and used to get the token and to ask for an extended transaction history.
- Any further extended transaction history request will be considered as out of scope (cf. § 3.4.2.3)

PIISP scope

The OAUTH2 scope requested by a PIISP can only be “piisp”.

Redirect Approach for AISP and PIISP

The registration process relies on an OAUTH2 sequence for obtaining an Authorization Code Grant (cf. https://tools.ietf.org/html/rfc6749#section-4.1) and can be summarized through the following steps.



- The PSU specifies, to the TPP, the identity of one of its ASPSPs
- The TPP initiates the OAUTH2 sequence by redirecting the PSU to the relevant ASPSP's authorization infrastructure, through the following URL pattern and parameters

```
GET /authorize?response_type=code&client_id={clientId}&redirect_uri={redirectUrl}&scope={scope}[&state={state}]
```

NAME		DATA	TYPE AND CONSTRAINS
response_type	[1..1]	Expected type of token	String[10] Must be valued with "code"
client_id	[1..1]	TPP identification	String[34] must be equal to the OrganizationIdentifier part of the Distinguished Name of the eIDAS certificate, according to ETSI specification
redirect_uri	[0..1]	Call-back URL of the TPP	String[140]
scope	[0..1]	Specifies the generic accreditations that both the PSU and the TPP agreed on: - For AISP o aisp o extended_transaction_history - for PIISP o piisp.	String[140] Space delimited roles list.
state	[0..1]	Internal state that can be used by the TPP for context management.	String[34]

- The ASPSP
  - Identifies and authenticates the PSU
  - Computes the relevant TPP checks (roles, validity, non-revocation…)

- Afterwards, the ASPSP redirects the PSU to the TPP, using the previously given call-back URL (redirect_uri) and the following parameters:

NAME		DATA	TYPE AND CONSTRAINS
code	[1..1]	Short-time code to use in order to get the access token	String[34]
state	[0..1]	Internal state if provided by the TPP	String[34]

- In order to get the access token, the TPP is now able to call, through a POST request, the ASPSP's authorization infrastructure with the following parameters.

NAME		DATA	TYPE AND CONSTRAINS
grant_type	[1..1]	Requested authorization type	String[34] Must be valued with "authorization_code"
code	[1..1]	Short-time code previously provided by the ASPSP	String[34]

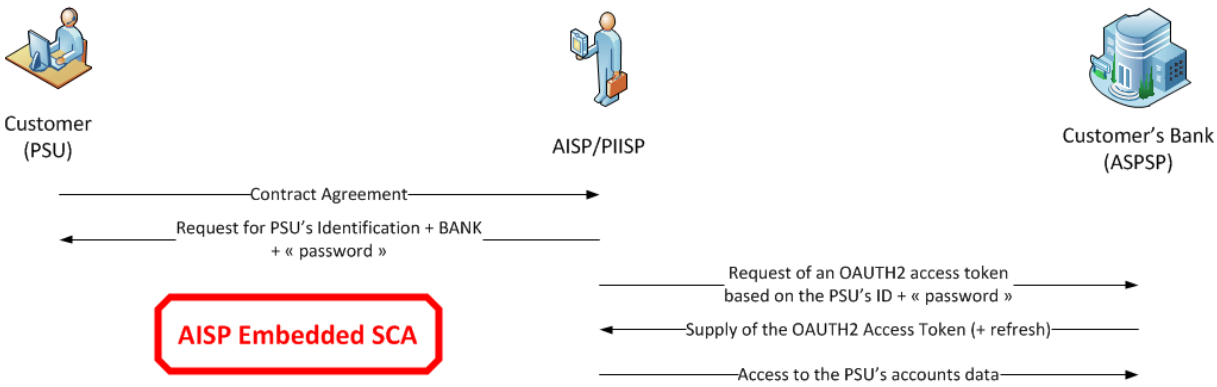
NAME		DATA	TYPE AND CONSTRAINS
redirect_uri	[1..1]	Call-back URL of the TPP	String[140] Must be equal to the one provided during the authorization code request
client_id	[1..1]	TPP identification.	String[34] must be equal to the OrganizationIdentifier part of the Distinguished Name of the eIDAS certificate, according to ETSI specification

- The ASPSP
  - Identifies and authenticates the TPP through the presented X.509 certificate
  - Computes the relevant TPP checks (roles, validity, non-revocation…)
- The ASPSP answers through a HTTP200 (OK) response that embeds the following data.

NAME		DATA	TYPE AND CONSTRAINS
access_token	[1..1]	Access token provided by the ASPSP to the TPP.	String[140]
token_type	[1..1]	Type of the provided access token (“Bearer” or “MAC”)	String[10] Must be values with “Bearer”
expires_in	[0..1]	Token lifetime, in seconds. The token can be used several times as far as it is not expired.	Numeric
refresh_token	[0..1]	Refresh token that can be used for a future token renewal request.	String[140]

Embedded Approach

The registration process relies on an OAUTH2 sequence for obtaining a Resource Owner Password Grant (cf. https://tools.ietf.org/html/rfc6749#section-4.3) and can be summarized through the following steps.



- The PSU specifies, to the TPP, the identity of one of his/her ASPSPs and provides him with

- His/her identifier against the ASPSP services
- A “password” that is the result of a Strong Customer Authentication applied to the PSU by the ASPSP.

- The TPP initiates the OAUTH2 sequence by sending the following request directly to the ASPSP’s Authorisation Service.

```
POST /token HTTP/1.1
    Host: server.example.com
    Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
    Content-Type: application/x-www-form-urlencoded

    grant_type=password&username=johndoe&password=A3ddj3w
```

NAME		DATA	TYPE AND CONSTRAINS
grant_type	[1..1]	type of requested grant	String[10] Must be valued with “password”
username	[1..1]	PSU identification	String[34]
password	[1..1]	PSU “password”	String[20] Result of the concatenation of a “knowledge factor” and a “possession” factor

scope	[0..1]	Specifies the generic accreditations that both the PSU and the TPP agreed on:
		- For AISP
		  ○ aisp
		  ○ extended_transaction_history
		- for PIISP
		  ○ piisp.
			String[140]
			Space delimited roles list.

- The ASPSP
  - Identifies and authenticates the TPP through the presented X.509 certificate
  - Computes the relevant TPP checks (roles, validity, non-revocation…)
- The ASPSP checks the identifier of the PSU and parse the “password” in order to retrieve and check the “Knowledge” factor and the “Possession” factor, thus processing the SCA.
- In case of successful SCA, the ASPSP answers through a HTTP200 (OK) response that embeds the following data.

NAME		DATA	TYPE AND CONSTRAINS
access_token	[1..1]	Access token provided by the ASPSP to the TPP.	String[140]
token_type	[1..1]	Type of the provided access token (“Bearer” or “MAC”)	String[10] Must be values with “Bearer”
expires_in	[0..1]	Token lifetime, in seconds. The token can be used several times as far as it is not expired.	Numeric
refresh_token	[0..1]	Refresh token that can be used for a future token renewal request.	String[140]

3.4.2.3. Use of the access token

The access token must be used within each request within the “Authorization” header, prefixed by the token type “Bearer”.

If the access token is expired, the request will be rejected with HTTP400 with an error equal to “invalid_token” and the request can be replayed once the access token has been refreshed.

If the access token scope cannot cover the request (case of extended transaction history request for instance):

- The request will be rejected with HTTP403 with an error equal to “insufficient_scope”
- The refresh token will be revoked so the request could be replayed once a new token, having the right scope, would have been requested and provided.
- The new refresh token will be valid up to 90 days.

3.4.2.4. Refreshing the Access Token

According to the RFC 6749 (cf. https://tools.ietf.org/html/rfc6749#section-6), the Refresh Token can be used by the TPP in order to get a refreshed Access Token by the following request.

```
POST /token HTTP/1.1
    Host: server.example.com
    Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW
    Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token&refresh_token=tGzv3JOkF0XG5Qx2TlKWIA
```

NAME		DATA	TYPE AND CONSTRAINS
grant_type	[1..1]		Must be valued with “refresh_token”
refresh_token	[1..1]	Value of the provided refresh token	
scope	[0..1]	Specifies the generic accreditations that both the PSU and the TPP agreed on: “aisp” or “piisp”. “extended_transaction_history” is not allowed in this case.	String[140] Space delimited roles list.

- The ASPSP
    - Identifies and authenticates the TPP through the presented X.509 certificate
    - Computes the relevant TPP checks (roles, validity, non-revocation…)
- The ASPSP answers through a HTTP200 (OK) response that embeds the following data.

NAME		DATA	TYPE AND CONSTRAINS
access_token	[1..1]	Access token provided by the ASPSP to the TPP.	String[140]
token_type	[1..1]	Type of the provided access token (“Bearer” or “MAC”)	String[10] Must be values with “Bearer”

NAME		DATA	TYPE AND CONSTRAINS
expires_in	[0..1]	Token lifetime, in seconds. The token can be used several times as far as it is not expired.	Numeric
refresh_token	[0..1]	Refresh token that can be replace the previous refresh token.	String[140]

If the refresh token has been revoked, the request will be rejected with HTTP400 and an error equal to “invalid grant”.

3.4.2.5. Refresh Token Revocation

The refresh token provided to an AISP is de facto revoked by the ASPSP

- After timeout of the by-law specified delay between two SCAs.
- After reject of a request for insufficient scope in order to allow the AISP to request another token with the desired scope.

The TPP is also able to ask for the revocation of the refresh token, according to RFC 7009 (cf. https://tools.ietf.org/html/rfc7009) through the following request.

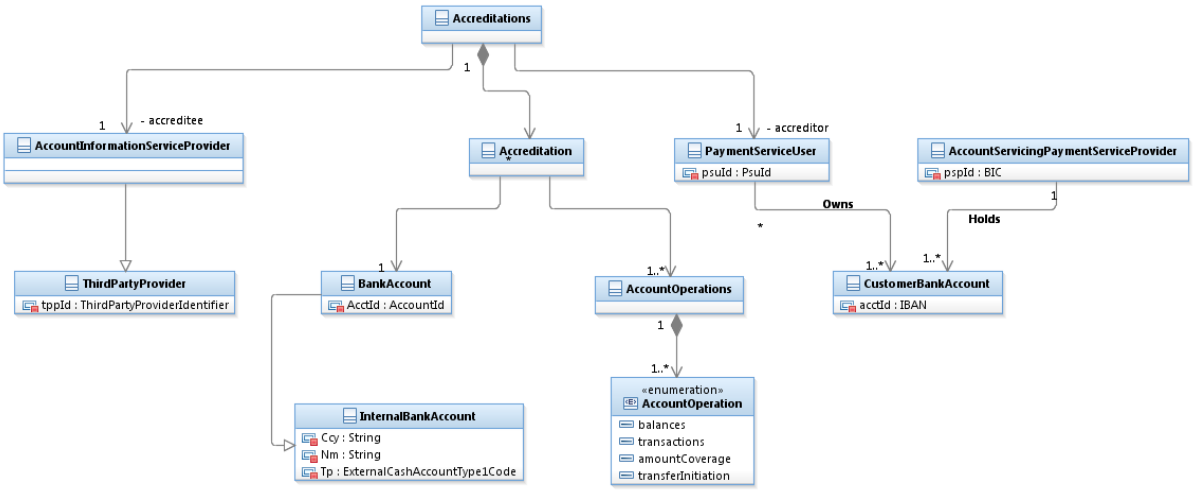
```
POST /revoke HTTP/1.1
    Host: server.example.com
    Content-Type: application/x-www-form-urlencoded
    Authorization: Basic czZCaGRSa3F0MzpnWDFmQmF0M2JW

    token=45ghiukldjahdnhzdauz&token_type_hint=refresh_token
```

NAME		DATA	TYPE AND CONSTRAINS
token	[1..1]	Token to be revoked by the ASPSP.	String[140]
token_type_hint	[0..1]	Information about the type of token to be revoked	Must be values with “refresh_token”

3.4.2.6. PSU context model

The PSU context can be seen as a collection of individual accreditations.



This collection is specific to a given PSU, a given TPP and a given ASPSP.

Each single accreditation relies on a specific account that is owned by the PSU and is held by the ASPSP. It specifies which pieces of data (transactions, balances) the TPP is allowed to carry out on this account.

The PSU can choose to manage this context with the AISP, or with the ASPSP, by using one of the following consent management models.

PSU context managed with the AISP

In this model, the AISP is responsible of

- The capture of the PSU choices:
    - The PSU specifies to the AISP which account and piece of data should be accessed or not.
    - At any time, the PSU can edit his/her consent choices
- The execution of the PSU choices: The AISP has the responsibility to respect the PSU choices and not to access any data that it has not been granted for;

Thus in this model, the ASPSP might not have any clue about the PSU's choices and thus could be unable to check the legitimacy of the AISP's requests.

However, the AISP must keep the ASPSP informed that this consent management model is applied by setting a [PSU-Account-Consent-Responsibility] HTTP Header to the "BY-AISP" value in each of its API request.

If this header value is set to “BY-ASPSP”, the second consent management model is applied.

PSU context managed with the ASPSP

In this model, the ASPSP is responsible of

- The capture of the PSU choices:
    - The PSU specifies to the ASPSP which account and piece of data should be accessed or not by the AISP.
    - By default, without any explicit specification by the PSU, all available payment accounts and pieces of data will be made accessible to the AISP.
    - At any time, the PSU can edit his/her consent choices. A PSU is also able to anticipate his/her consent choices, prior to any contract with an AISP, if a given ASPSP provides such OPT-OUT services.
- The execution of the PSU choices: The ASPSP must check the legitimacy of each of the AISP’s requests against the consent choices of the PSU

The AISP will then get from the ASPSP the map of all accessible accounts and pieces of data.

3.4.3. PISP authorization levels

3.4.3.1. General rules

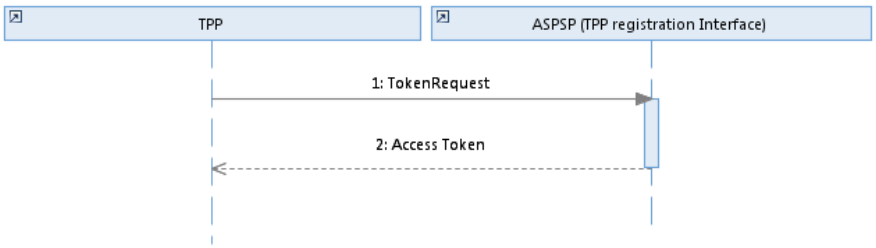
For Payment Request on behalf of a Merchant and Transfer Request on behalf of a Donor of Order, the law requires a SCA, unless exemption cases. This SCA will embed the PSU’s consent to the subsequent Credit Transfer.

That for, the PSD2 use cases that are linked with the PISP role only require an “Authorization by Role” authorization level for accessing the ASPSP API services.

However, It must be noticed that a PAO may ask to be placed under an OPT-OUT statement by its ASPSPs, avoiding any incoming Payment Request to be processed on its accounts.

3.4.3.2. Registration of the TPP access

The registration of the TPP by the ASPSP relies on an OAUTH2 sequence for obtaining a Client Credential (cf. https://tools.ietf.org/html/rfc6749#section-4.1) and can be summarized through the following steps.



- The TPP sends directly, through a POST request, its access token request to the ASPSP authorization infrastructure with the following URL pattern and parameters

```
GET /token?grant_type=client_credentials&scope={scope}
```

NAME		DATA	TYPE AND CONSTRAINS
grant_type	[1..1]	Requested authorization type	String[34] Must be valued with "client_credentials"
scope	[0..1]	Specifies the generic accreditations that both the PSU and the TPP agreed on: PISP.	String[140] Space delimited roles list. Default value is "PISP"

- The ASPSP
  - Identifies and authenticates the TPP through the presented X.509 certificate
  - Computes the relevant TPP checks (roles, validity, non-revocation…)
- The ASPSP answers through a HTTP200 (OK) response that embeds the following data.

NAME		DATA	TYPE AND CONSTRAINS
access_token	[1..1]	Access token provided by the ASPSP to the TPP.	String[140]
token_type	[1..1]	Type of the provided access token ("Bearer" or "MAC")	String[10] Must be values with "Bearer"
expires_in	[0..1]	Token lifetime, in seconds. The token can be used several times as far as it is not expired.	Numeric

The access token must be used within each request within the "Authorization" header, prefixed by the token type "Bearer".

If the access token is expired, the request will be rejected with HTTP400 with an error equal to "invalid_token" and the request can be replayed once a new client credentials token has been requested and provided.

3.5. Applicative authentication

Each request sent by the TPP has to be signed using http-signature mechanism which is specified by the following IETF draft-paper:

- https://datatracker.ietf.org/doc/draft-cavage-http-signatures/

The way it should be implemented is the following

- Computing a SHA256 digest of the HTTP body and adding this digest as an extra HTTP header.
- Using a specific Qualified Certificate (QSealC), respecting the ETSI/TS119495 Technical Specification, in order to apply a RSA-SHA256 signature on
    - all headers that are present in the HTTP request, including the previously computed digest
    - on the specific “(request-target)” field which if specified by the IETF draft-paper
- Adding this signature within an extra HTTP header embedding
    - The key identifier which must specify the way to get the relevant qualified certificate
    - The algorithm that has been used
    - The list of headers that have been signed
    - The signature itself.

In case of absent or invalid signature, the request will be rejected with HTTP400.

3.6. Fraud detection oriented information

Whenever the TPP is able to provide the information relating to its connection with the PSU, the following extra HTTP-headers must be set within the HTTP request in order to allow the ASPSP to integrate this information into its own fraud detection process.

Moreover these headers can be considered as proof of the PSU being connected.

DATA	COMMENT	EXTRA HTTP HEADER
IP Address of the PSU terminal when connecting to the TPP	In regards with GDPR rules, this must be subject to PSU's consent	PSU-IP-Address
IP Port of the PSU terminal when connecting to the TPP		PSU-IP-Port
HTTP Method used for the most relevant PSU's terminal request to the TTP		PSU-HTTP-Method
Timestamp of the most relevant PSU's terminal request to the TTP		PSU-Date
"User-Agent" header field sent by the PSU terminal when connecting to the TPP		PSU-User-Agent
"Referer" header field sent by the PSU terminal when connecting to the TPP		PSU-Referer
"Accept" header field sent by the PSU terminal when connecting to the TPP		PSU-Accept
"Accept-Charset" header field sent by the PSU terminal when connecting to the TPP		PSU-Accept-Charset
"Accept-Encoding" header field sent by the PSU terminal when connecting to the TPP		PSU-Accept-Encoding
"Accept-Language" header field sent by the PSU terminal when connecting to the TPP		PSU-Accept-Language

3.7. Specific HTTP messages to be used

MESSAGE	HTTP CODE	SIGNIFIANCE
FORMAT_ERROR	400	Format of certain request fields are not matching the XS2A requirements. An explicit path to the corresponding field might be added in the return message.
RESOURCE_UNKNOWN	404	If ressourceId in path
PERIOD_INVALID	400	Requested time period out of bound.
ACCESS_EXCEEDED	429	The access on the account has been exceeding the consented multiplicity per day.
REQUESTED_FORMATS _INVALID	406	The requested formats in the Accept header entry are not matching the formats offered by the ASPSP.

3.8. STET PSD2 API technical summary

TOPIC	CHOICE	COMMENT
Access network	Internet	
Network protocol	HTTP 1.1 (Minimum)	
Data encryption **Cross-authentication**	TLS 1.2	Could be enforced through STS and/or PFS
Authorization protocol	OAUTH2	One of the following token modes - Authorization Code Grant (AISP, PIISP) - Client credential (PISP)
Applicative protocol	REST	In respect of the Richardson Maturity Model, on level three in order to provide HYPERMEDIA links.
Applicative authentication	http-signature	Notice this is actually an IETF draft, waiting for approval and so subject to some modifications. https://datatracker.ietf.org/doc/draft-cavage-http-signatures/
PSU Strong Customer Authentication approaches	REDIRECT, DECOUPLED or EMBEDDED	
Data format	JSON/UTF8	With use of ISO20022 based data structures
Technical documentation	SWAGGER 2.0	

4. Functional model

The functional model focuses on the business and functional processes.

Further details are specified within the applicative model which is provided through a SWAGGER 2.0 file and some log examples that illustrate relevant use cases (cf. § 5 and further) on these topics:

- Technical data formats
- Error cases
- HYPERMEDIA links

4.1. Retrieval of the PSU accounts (AISP)

4.1.1. Prerequisites

- The TPP has been registered by the Registration Authority for the AISP role.
- The TPP and the PSU have a contract that has been enrolled by the ASPSP
    - At this step, the ASPSP has delivered an OAUTH2 “Authorization Code” or “Resource Owner Password” access token to the TPP (cf. § 3.4.2).
- The PSU has chosen to manage the accessibility on his/her individual accounts, with the AISP or with the ASPSP.
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its OAUTH2 “Authorization Code” or “Resource Owner Password” access token which allows the ASPSP to identify the relevant PSU and retrieve the linked PSU context (cf. § 3.4.2) if any.

4.1.2. Business flow

The TPP sends a request to the ASPSP for retrieving the list of the PSU accounts.

The ASPSP retrieves the relevant PSU accounts and builds the answer as an accounts list. The result may be subject to pagination in order to avoid an excessive result set.

Each account will be provided with its characteristics, a balance report and the list of functionalities that have been granted by the PSU to the TPP.

4.1.3. Request content

The API entry point is GET /accounts

The only information provided by the TPP through its request is the OAUTH2 “Authorization Code” or “Resource Owner Password” access token.

4.1.4. Response content (if no error)

The ASPSP provides the following data:

FIELD	MULT.	DESC.
accounts	[1..1]	List of PSU account that are made available to the TPP
accounts	[0..*]	PSU account that is made available to the TPP
accounts.resourceId	[1..1]	Identification of the account as defined as a resource by the ASPSP
accounts.bicFi	[0..1]	ISO20022: Code allocated to a financial institution by the ISO 9362 Registration Authority as described in ISO 9362 "Banking - Banking telecommunication messages - Business identification code (BIC)".
accounts.accountId	[0..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
accounts.accountId.iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
accounts.accountId.other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
accounts.accountId.other.identification	[1..1]	API: alias of an account
accounts.accountId.other.schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
accounts.accountId.other.issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
accounts.name	[1..1]	Label of the PSU account In case of a delayed debit card transaction set, the name shall specify the holder name and the imputation date
accounts.details	[0..1]	Specifications that might be provided by the ASPSP - characteristics of the account - characteristics of the relevant card
accounts.linkedAccount	[0..1]	Case of a set of pending card transactions, the APSP will provide the relevant cash account the card is set up on.
accounts.usage	[0..1]	Specifies the usage of the account - PRIV: private personal account - ORGA: professional account
accounts.cashAccountType	[1..1]	Specifies the type of the account - CACC: Cash account
accounts.product	[0..1]	Product Name of the Bank for this account, proprietary definition
accounts.currency	[1..1]	Currency used for the account

FIELD	MULT.	DESC.
balances	[0..1]	list of balances provided by the ASPSP
[1..*]	[1..*]	Structure of an account balance
name	[1..1]	Label of the balance
balanceAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
balanceType	[1..1]	Type of balance - CLBD: (ISO20022 ClosingBooked) Accounting Balance - XPCD: (ISO20022 Expected) Instant Balance - VALU: Value-date balance - OTHR: Other Balance
lastChangeDateTime	[0..1]	Timestamp of the last change of the balance amount
referenceDate	[0..1]	Reference date for the balance
lastCommittedTransaction	[0..1]	Identification of the last committed transaction. This is actually useful for instant balance.
psuStatus	[0..1]	Relationship between the PSU and the account - Account Holder - Co-account Holder - Attorney
_links	[1..1]	links that can be used for further navigation when browsing Account Information at one account level - balances: link to the balances of a given account - transactions: link to the transactions of a given account
balances	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
transactions	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
_links	[1..1]	Links that can be used for further navigation when browsing Account Information at top level - self: link to the list of all available accounts
self	[1..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
first	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
last	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
next	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
prev	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

So, for each account, the ASPSP might also provide

- A balance report

- some hyperlinks in order to specify which further actions can be performed on each account if allowed by the PSU:
    - balance (getting the balances)
    - transactions (getting the transactions).

4.2. Retrieval of an account balances report (AISP)

4.2.1. Prerequisites

- The TPP has been registered by the Registration Authority for the AISP role
- The TPP and the PSU have a contract that has been enrolled by the ASPSP
    - At this step, the ASPSP has delivered an OAUTH2 “Authorization Code” or “Resource Owner Password” access token to the TPP (cf. § 3.4.2).
- The PSU has chosen to manage the accessibility on his/her individual accounts, with the AISP or with the ASPSP.
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its OAUTH2 “Authorization Code” or “Resource Owner Password” access token which allows the ASPSP to identify the relevant PSU and retrieve the linked PSU context (cf. § 3.4.2) if any.
- The TPP has previously retrieved the list of available accounts for the PSU

4.2.2. Business flow

The AISP requests the ASPSP on one of the PSU’s accounts.

The ASPSP answers by providing a balance-report on this account. The balance-report is a list of balances that shall at least include the accounting balance.

4.2.3. Request content

The API entry point is GET /accounts/{accountId}/balances

The AISP provides through its request:

- The OAUTH2 “Authorization Code” or “Resource Owner Password” access token.
- The resource Id of the relevant account, as retrieved from the list of the PSU’s accounts (cf. § 4.1).

4.2.4. Response content (if no error)

The balance-report provides the following data.

FIELD	MULT.	DESC.
balances	[1..1]	List of account balances
	[1..*]	Structure of an account balance
name	[1..1]	Label of the balance
balanceAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used

FIELD	MULT.	DESC.
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
balanceType	[1..1]	Type of balance - CLBD: (ISO20022 ClosingBooked) Accounting Balance - XPCD: (ISO20022 Expected) Instant Balance - VALU: Value-date balance - OTHR: Other Balance
lastChangeDateTime	[0..1]	Timestamp of the last change of the balance amount
referenceDate	[0..1]	Reference date for the balance
lastCommittedTransaction	[0..1]	Identification of the last committed transaction. This is actually useful for instant balance.
_links	[1..1]	links that can be used for further navigation when browsing Account Information at one account level - self: link to the balances of a given account - parent-list: link to the list of all available accounts - transactions: link to the transactions of a given account
self	[1..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
parent-list	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
transactions	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.3. Retrieval of an account transaction set (AISP)

4.3.1. Prerequisites

- The TPP has been registered by the Registration Authority for the AISP role
- The TPP and the PSU have a contract that has been enrolled by the ASPSP
    - At this step, the ASPSP has delivered an OAUTH2 “Authorization Code” or “Resource Owner Password” access token to the TPP (cf. § 3.4.2).
- The PSU has chosen to manage the accessibility on his/her individual accounts, with the AISP or with the ASPSP.
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its OAUTH2 “Authorization Code” or “Resource Owner Password” access token which allows the ASPSP to identify the relevant PSU and retrieve the linked PSU context (cf. § 3.4.2) is any.
- The TPP has previously retrieved the list of available accounts for the PSU

4.3.2. Business flow

The AISP requests the ASPSP on one of the PSU’s accounts. It may specify some selection criteria.

The ASPSP answers by a set of transactions that matches the query. The result may be subject to pagination in order to avoid an excessive result set.

4.3.3. Request content

The API entry point is GET /accounts/{accountId}/transactions

The AISP provides through its request:

- The “OAUTH2 “Authorization Code” or “Resource Owner Password” access token.
- The resource Id of the relevant account, as retrieved from the list of the PSU’s accounts (cf. § 4.1)
- the following optional selection criteria:

FIELD	MULT.	DESC.
dateTo	[0..1]	Inclusive minimal imputation date of the transactions. Transactions having an imputation date equal to this parameter are included within the result.
dateFrom	[0..1]	Exclusive maximal imputation date of the transactions. Transactions having an imputation date equal to this parameter are not included within the result.
afterEntryReference	[0..1]	Specifies the value on which the result has to be computed. Only the transaction having a technical identification greater than this value must be included within the result

4.3.4. Response content (if no error)

The transaction set embeds for each transaction the following data.

FIELD	MULT.	DESC.
transactions	[1..1]	List of transactions
	[0..*]	structure of a transaction
resourceId	[0..1]	Identification of the transaction as defined as a resource by the ASPSP
entryReference	[0..1]	Technical incremental identification of the transaction.
transactionAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
creditDebitIndicator	[1..1]	Accounting flow of the transaction - CRDT: Credit type transaction - DBIT: Debit type transaction
status	[1..1]	Type of Transaction - BOOK: (ISO20022 ClosingBooked) Accounted transaction - PDNG: (ISO20022 Expected) Instant Balance Transaction - OTHR: Other
bookingDate	[1..1]	Booking date of the transaction on the account
remittanceInformation	[1..1]	ISO20022: Information supplied to enable the matching of an entry with the items that the transfer is intended to settle, such as commercial invoices in an accounts' receivable system. API: Only one occurrence is allowed
	[0..1]	Relevant information to the transaction
_links	[1..1]	links that can be used for further navigation when browsing Account Information at one account level - self: link to the transactions of a given account - parent-list: link to the list of all available accounts - balances: link to the balances of a given account - first: link to the first page of the transactions result - last: link to the last page of the transactions result - next: link to the next page of the transactions result - prev: link to the previous page of the transactions result
self	[1..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
parent-list	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
balances	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
first	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
last	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
next	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
prev	[0..1]	hypertext reference
href	[1..1]	URI to be used

FIELD	MULT.	DESC.
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.4. Request for payment coverage check (PIISP)

4.4.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PIISP role
- The TPP and the PSU have a contract that has been registered by the ASPSP
    - At this step, the ASPSP has delivered an OAUTH2 “Authorization Code” or “Resource Owner Password” access token to the TPP (cf. § 3.4.2).
- The PSU has chosen to manage the accessibility on his/her individual accounts, with the AISP or with the ASPSP.
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its OAUTH2 “Authorization Code” or “Resource Owner Password” access token which allows the ASPSP to identify the relevant PSU and retrieve the linked PSU context (cf. § 3.4.2) if any.

4.4.2. Business flow

The PIISP requests the ASPSP for a payment coverage check against either a bank account or a card primary identifier.

4.4.3. Request content

The API entry point is POST /funds-confirmations

The PIISP provides the following data to the ASPSP:

- The OAUTH2 “Authorization Code” or “Resource Owner Password” access token.
- The following additional parameters.

FIELD	MULT.	DESC.
paymentCoverage	[1..1]	Payment coverage request structure. The request must rely either on a cash account or a payment card.
paymentCoverageRequestId	[1..1]	Identification of the payment Coverage Request
payee	[0..1]	The merchant where the card is accepted as an information to the PSU.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
accountId	[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.

FIELD	MULT.	DESC.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties

4.4.4. Response content (no error)

The result is given by the ASPSP through a structure embedding:

- The processed request
- The result of the processing, being “true” if the coverage has been successfully checked or false if not.

FIELD	MULT.	DESC.
request	[1..1]	Payment coverage request structure. The request must rely either on a cash account or a payment card.
paymentCoverageRequestId	[1..1]	Identification of the payment Coverage Request
payee	[0..1]	The merchant where the card is accepted as information to the PSU.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
accountId	[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.

			iban		[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
			other		[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
				identification	[1..1]	API: alias of an account
				schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
				issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
	result				[1..1]	Result of the coverage check : - true: the payment can be covered - false: the payment cannot be covered
	_links				[1..1]	links that can be used for further navigation to post another coverage request.
		self			[1..1]	hypertext reference
			href		[1..1]	URI to be used
			templated		[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.5. Payment initiation on behalf of a merchant (PISP)

4.5.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PISP role
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.5.2. Business flow

4.5.2.1. Common flow

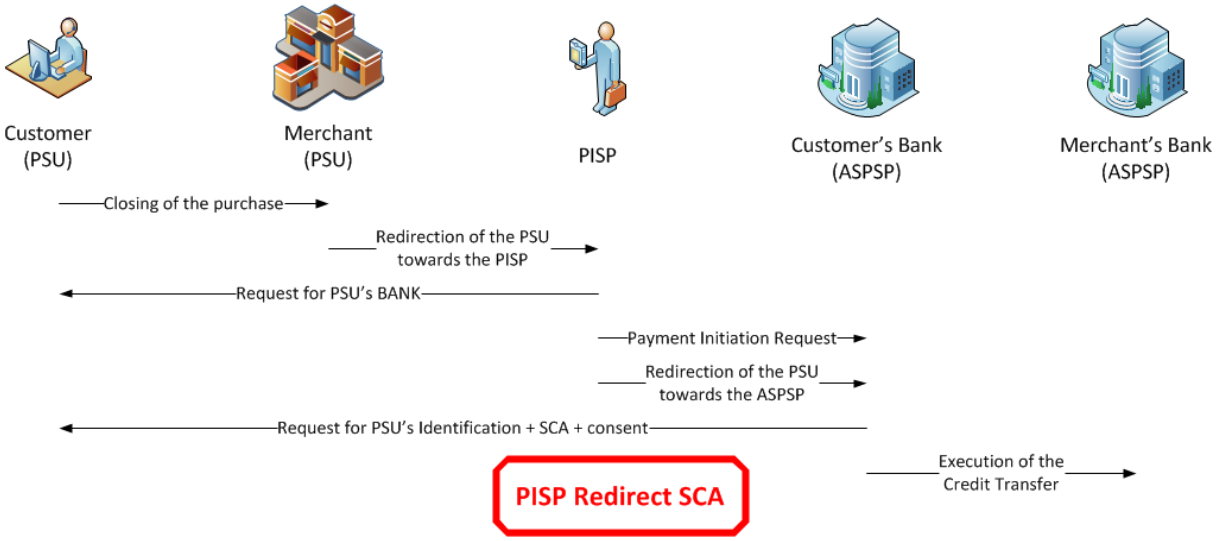
The PSU buys some goods or services on an e-commerce website held by a merchant. Among other payment method, the merchant suggests the use of a PISP service. As there is obviously a contract between the merchant and the PISP, there is no need of such a contract between the PSU and this PISP to initiate the process.

Case of the PSU that chooses to use the PISP service:

- The merchant forwards the requested payment characteristics to the PISP and redirects the PSU to the PISP portal.
- The PISP requests from the PSU which ASPSP will be used.
- The PISP prepares the Payment Request and sends this request to the ASPSP. This request includes:
    - The specification of the SCA approaches that are supported by the PISP (any combination of “REDIRECT”, “EMBEDDED” and “DECOUPLED” values).
    - In case of possible REDIRECT or DECOUPLED SCA approach, one or two call-back URLs to be used by the ASPSP at the finalisation of the authentication and consent process :
        - The first call-back URL will be called by the ASPSP if the Payment Request is processed without any error or rejection by the PSU
        - The second call-back URL is to be used by the ASPSP in case of processing error or rejection by the PSU. Since this second URL is optional, the PISP might not provide it. In this case, the ASPSP will use the same URL for any processing result.
        - Both call-back URLS must be used in a TLS-secured request, including mutual authentication based on each party’s TLS certificate.
    - In case of possible “EMBEDDED” or “DECOUPLED” approaches, a PSU identifier that can be processed by the ASPSP for PSU recognition.
- The ASPSP saves the Payment Request and answers to the PISP. The answer embeds

- A location link of the saved Payment Request that will be further used to retrieve the Payment Request and its status information.
- The specification of the chosen SCA approach taking into account both the PISP and the PSU capabilities.
- In case of chosen REDIRECT SCA approach, the URL to be used by the PISP for redirecting the PSU in order to perform a SCA.

4.5.2.2. Redirect SCA approach

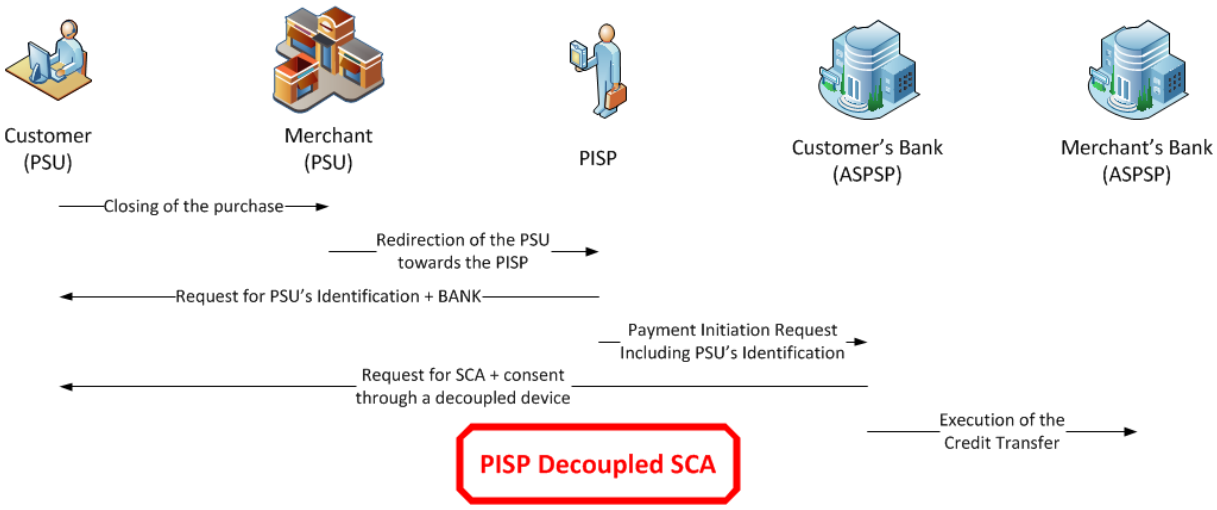


When the chosen SCA approach within the ASPSP answers is set to "REDIRECT":

- The PISP redirects the PSU to the ASPSP which authenticates the PSU
- The ASPSP asks the PSU to give (or deny) his/her consent to the Payment Request
- The PSU chooses or confirms which of his/her accounts shall be used by the ASPSP for the future Credit Transfer.
- The ASPSP is then able to initiate the subsequent Credit Transfer
- The ASPSP redirects the PSU to the PISP using one of the call-back URLs provided within the posted Payment Request

If the PSU neither gives nor denies his/her consent, the Payment Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.5.2.3. Decoupled SCA approach

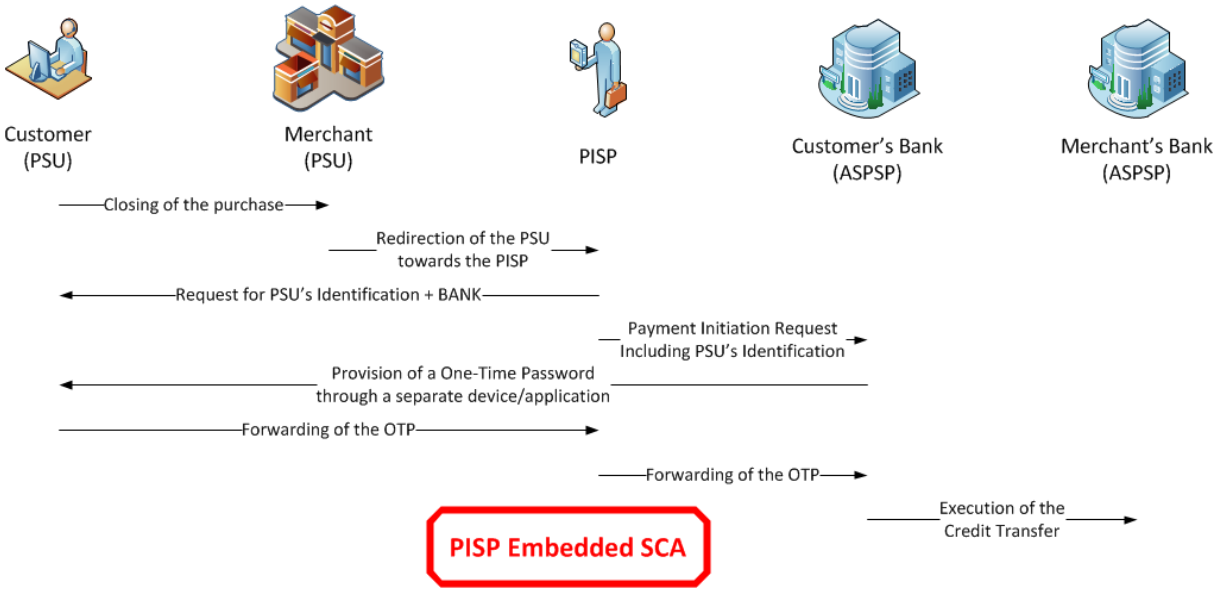


When the chosen SCA approach is "DECOUPLED":

- Based on the PSU identifier provided within the Payment Request by the PISP, the ASPSP gives the PSU with the Payment Request details and challenges the PSU for a Strong Customer Authentication on a decoupled device or application.
- The PSU chooses or confirms which of his/her accounts shall be used by the ASPSP for the future Credit Transfer.
- The ASPSP is then able to initiate the subsequent Credit Transfer
- The ASPSP notifies the PISP about the finalisation of the authentication and consent process by using one of the call-back URLs provided within the posted Payment Request

If the PSU neither gives nor denies his/her consent, the Payment Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.5.2.4. Embedded SCA approach



When the chosen SCA approach within the ASPSP answers is set to "EMBEDDED":

- The TPP informs the PSU that a challenge is needed for completing the Payment Request processing. This challenge will be one of the following:
  - A One-Time-Password sent by the ASPSP to the PSU on a separate device or application.
  - A response computed by a specific device on base of a challenge sent by the ASPSP to the PSU on a separate device or application.
- The PSU unlock the device or application through a "knowledge factor" and/or an "inherence factor" (biometric), retrieves the Payment Request details and processes the data sent by the ASPSP;
- The PSU might choose or confirm which of his/her accounts shall be used by the ASPSP for the future Credit Transfer when the device or application allows it.
- When agreeing the Payment Request, the PSU enters the resulting authentication factor through the PISP interface which will forward it to the ASPSP through a confirmation request (cf. § 4.7)

Case of the PSU neither gives nor denies his/her consent, the Payment Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.5.3. Request content

Whatever the SCA approach, the API entry point is POST /payment-requests

The TPP provides through its request:

- The "OAUTH2 Client Credential" token

- The Payment Request itself through an ISO20022 “pain.013” message-based structure (CreditorPaymentActivationRequest).

This structure embeds only one payment instruction.

FIELD	MULT.	DESC.
paymentRequest	[1..1]	ISO20022: The PaymentRequestResource message is sent by the Creditor sending party to the Debtor receiving party, directly or through agents. It is used by a Creditor to request movement of funds from the debtor account to a creditor.
resourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
paymentInformationId	[1..1]	ISO20022 : Reference assigned by a sending party to unambiguously identify the payment information block within the message.
creationDateTime	[1..1]	ISO20022: Date and time at which a (group of) payment instruction(s) was created by the instructing party.
numberOfTransactions	[1..1]	ISO20022: Number of individual transactions contained in the message.
initiatingParty	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
paymentTypeInformation	[1..1]	ISO20022: Set of elements used to further specify the type of transaction.
instructionPriority	[0..1]	ISO20022: Indicator of the urgency or order of importance that the instructing party would like the instructed party to apply to the processing of the instruction.
serviceLevel	[1..1]	ISO20022: Agreement under which or rules under which the transaction should be processed. Specifies a pre-agreed service or level of service between the parties, as published in an external service level code list. API: Only "SEPA" (SEPA Credit Transfer) or "NURG" (Other Credit Transfer) values are allowed
localInstrument	[0..1]	ISO20022: User community specific instrument. Usage: This element is used to specify a local instrument, local clearing option and/or further qualify the service or service level. API: Only "INST" value is allowed in order to ask for an SEPA instant Payment. Can only be used if ServiceLevel is equal to "SEPA"
categoryPurpose	[0..1]	ISO20022: Specifies the high level purpose of the instruction based on a set of pre-defined categories. This is used by the initiating party to provide information concerning the processing of the payment. It is likely to trigger special processing by any of the agents involved in the payment chain. API: The following values are allowed: - CASH (CashManagementTransfer): Transaction is a general cash management instruction. - DVPM (DeliverAgainstPayment): Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction.
debtor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAccount	[0..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAgent	[0..1]	ISO20022: Unique and unambiguous identification of a financial institution, as assigned under an internationally recognised or proprietary identification scheme. API: Only <Bicfi> element is allowed
bicFi	[1..1]	ISO20022: Code allocated to a financial institution by the ISO 9362 Registration Authority as described in ISO 9362 "Banking - Banking telecommunication messages - Business identification code (BIC)".
creditorAgent	[0..1]	ISO20022: Unique and unambiguous identification of a financial institution, as assigned under an internationally recognised or proprietary identification scheme. API: Only <Bicfi> element is allowed
bicFi	[1..1]	ISO20022: Code allocated to a financial institution by the ISO 9362 Registration Authority as described in ISO 9362 "Banking - Banking telecommunication messages - Business identification code (BIC)".
creditor	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
creditorAccount	[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
ultimateCreditor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
purpose	[0..1]	ISO20022: Underlying reason for the payment transaction, as published in an external purpose code list. API: The following values are allowed for Payment Request - ACCT (Funds moved between 2 accounts of same account holder at the same bank) - CASH (general cash management instruction) may be used for Transfer Initiation - COMC Transaction is related to a payment of commercial credit or debit. - CPKC General Carpark Charges Transaction is related to carpark charges. - TRPT Transport RoadPricing Transaction is for the payment to top-up pre-paid card and electronic road pricing for the purpose of transportation
chargeBearer	[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. API: The following values are allowed for Payment Request - SLEV: Charges are to be applied following the rules agreed in the service level and/or scheme.
paymentInformationStatus	[0..1]	ISO20022: Specifies the status of the payment information. API: Mandatory. The following values are allowed to provide the status of the Payment Request - ACCP (AcceptedCustomerProfile): Preceding check of technical validation was successful. Customer profile check was also successful. - ACSC (AcceptedSettlementCompleted): Settlement on the debtor's account has been completed. - ACSP (AcceptedSettlementInProcess): All preceding checks such as technical validation and customer profile were successful. Dynamic risk assessment is now also successful and therefore the Payment Request has been accepted for execution. - ACTC (AcceptedTechnicalValidation): Authentication and syntactical and semantical validation are successful. - ACWC (AcceptedWithChange): Instruction is accepted but a change will be made, such as date or remittance not sent. - ACWP (AcceptedWithoutPosting): Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account. - RCVD (Received): Payment initiation has been received by the receiving agent. - PDNG (Pending): Payment request or individual transaction included in the Payment Request is pending. Further checks and status update will be performed. - RJCT (Rejected): Payment request has been rejected.

FIELD	MULT.	DESC.
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Payment Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Payment Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
creditTransferTransaction	[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor.
	[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor.
paymentId	[1..1]	ISO20022: Set of elements used to reference a payment instruction.
ResourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
instructionId	[1..1]	ISO20022: Unique identification as assigned by an instructing party for an instructed party to unambiguously identify the instruction. API: Unique identification shared between the PISP and the ASPSP
endToEndId	[1..1]	ISO20022: Unique identification assigned by the initiating party to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. API: Unique identification shared between the merchant and the PSU
requestedExecutionDate	[1..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
regulatoryReportingCode	[0..1]	Information needed due to regulatory and statutory requirements. Economical codes to be used are provided by the National Competent Authority
remittanceInformation	[1..1]	ISO20022: Information supplied to enable the matching of an entry with the items that the transfer is intended to settle, such as commercial invoices in an accounts' receivable system. API: Only one occurrence is allowed
	[0..1]	Relevant information to the transaction

FIELD	MULT.	DESC.
transactionStatus	[0..1]	ISO20022: Specifies the status of the payment information group. API: Only the following values are allowed to provide the status of the subsequent CREDIT TRANSFER to the Payment Request - RJCT: Payment request or individual transaction included in the Payment Request has been rejected. - PDNG: (Pending): Payment request or individual transaction included in the Payment Request is pending. Further checks and status update will be performed. - ACSP: All preceding checks such as technical validation and customer profile were successful and therefore the Payment Request has been accepted for execution. - ACSC: Settlement on the debtor's account has been completed
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Payment Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Payment Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
supplementaryData	[1..1]	ISO20022: Additional information that cannot be captured in the structured elements and/or any other specific block. API: This structure is used to embed the relevant URLs for returning the status report to the PISP and to specify which SCA approaches are accepted by the PISP and which has been chosen by the ASPSP
acceptedScaApproach	[0..1]	can only be set by the PISP SCA approaches that are supported by the PISP. The PISP can provide several choices separated by commas. REDIRECT: the PSU is redirected by the TPP to the ASPSP which processes identification and authentication DECOUPLED: the TPP identifies the PSU and forwards the identification to the ASPSP which processes the authentication through a decoupled device EMBEDDED: the TPP identifies the PSU and forwards the identification to the ASPSP which starts the authentication. The TPP forwards one authentication factor of the PSU (e.g. OTP or response to a challenge)
	[0..*]	combination of possible values for SCA models
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the SCA and consent process in REDIRECT and DECOUPLED approach
unsuccessfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the failure of the SCA and consent process in REDIRECT and DECOUPLED approach If this URL is not provided by the PISP, the ASPSP will use the "successfulReportUrl" even in case of failure of the Payment Request processing

4.5.4. Response content (if no error)

The ASPSP answers with a “location” link of the saved Payment Request. This link refers to the resource Id of the saved payment to be used afterwards in order to get Payment request and its status.

The following data are also provided.

FIELD	MULT.	DESC.
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
_links	[0..1]	links that can be used for further navigation, especially in REDIRECT approach
consentApproval	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.6. Retrieval of a Payment Request and its status (PISP)

4.6.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PISP role
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP has previously posted a Payment Request which has been saved by the ASPSP (cf. § 4.5.3)
    - The ASPSP has answered with a location link to the saved Payment Request (cf. § 4.5.4)
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.6.2. Business flow

The PISP asks to retrieve the Payment Request that has been saved by the ASPSP. The PISP uses the location link provided by the ASPSP in response of the posting of this request.

The ASPSP returns the previously posted Payment Request which is enriched with:

- The resource identifiers given by the ASPSP
- The status information of the Payment Request and of the subsequent credit transfer

The status information must be available during at least 30 calendar days after the posting of the Payment Request. However, the ASPSP may increase this availability duration, based on its own rules.

4.6.3. Request content

The API entry point is GET /payment-requests/{paymentRequestId}

The PISP provides through its request:

- The “OAUTH2 Client Credential” token
- The resource Id of the saved Payment Request

4.6.4. Response content (if no error)

The response given by the ASPSP includes the previously posted Payment Request which has been enriched

- With the resource Id of the Payment Request that has been created by the ASPSP

- With the status of the Payment Request and the payment instructions

The resource Id of the Payment Request is the one to be used when asking for a given resource through the API.

FIELD	MULT.	DESC.
paymentRequest	[1..1]	ISO20022: The PaymentRequestResource message is sent by the Creditor sending party to the Debtor receiving party, directly or through agents. It is used by a Creditor to request movement of funds from the debtor account to a creditor.
resourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
paymentInformationId	[1..1]	ISO20022 : Reference assigned by a sending party to unambiguously identify the payment information block within the message.
creationDateTime	[1..1]	ISO20022: Date and time at which a (group of) payment instruction(s) was created by the instructing party.
numberOfTransactions	[1..1]	ISO20022: Number of individual transactions contained in the message.
initiatingParty	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
paymentTypeInformation	[1..1]	ISO20022: Set of elements used to further specify the type of transaction.
instructionPriority	[0..1]	ISO20022: Indicator of the urgency or order of importance that the instructing party would like the instructed party to apply to the processing of the instruction.
serviceLevel	[1..1]	ISO20022: Agreement under which or rules under which the transaction should be processed. Specifies a pre-agreed service or level of service between the parties, as published in an external service level code list. API: Only "SEPA" (SEPA Credit Transfer) or "NURG" (Other Credit Transfer) values are allowed
localInstrument	[0..1]	ISO20022: User community specific instrument. Usage: This element is used to specify a local instrument, local clearing option and/or further qualify the service or service level. API: Only "INST" value is allowed in order to ask for an SEPA instant Payment. Can only be used if ServiceLevel is equal to "SEPA"
categoryPurpose	[0..1]	ISO20022: Specifies the high level purpose of the instruction based on a set of pre-defined categories. This is used by the initiating party to provide information concerning the processing of the payment. It is likely to trigger special processing by any of the agents involved in the payment chain. API: The following values are allowed: - CASH (CashManagementTransfer): Transaction is a general cash management instruction. - DVPM (DeliverAgainstPayment): Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction.
debtor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAccount	[0..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAgent	[0..1]	ISO20022: Unique and unambiguous identification of a financial institution, as assigned under an internationally recognised or proprietary identification scheme. API: Only <Bicfi> element is allowed
bicFi	[1..1]	ISO20022: Code allocated to a financial institution by the ISO 9362 Registration Authority as described in ISO 9362 "Banking - Banking telecommunication messages - Business identification code (BIC)".
creditorAgent	[0..1]	ISO20022: Unique and unambiguous identification of a financial institution, as assigned under an internationally recognised or proprietary identification scheme. API: Only <Bicfi> element is allowed
bicFi	[1..1]	ISO20022: Code allocated to a financial institution by the ISO 9362 Registration Authority as described in ISO 9362 "Banking - Banking telecommunication messages - Business identification code (BIC)".
creditor	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
creditorAccount	[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
ultimateCreditor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
purpose	[0..1]	ISO20022: Underlying reason for the payment transaction, as published in an external purpose code list. API: The following values are allowed for Payment Request - ACCT (Funds moved between 2 accounts of same account holder at the same bank) - CASH (general cash management instruction) may be used for Transfer Initiation (R-PISP) - COMC Transaction is related to a payment of commercial credit or debit. - CPKC General Carpark Charges Transaction is related to carpark charges. - TRPT Transport RoadPricing Transaction is for the payment to top-up pre-paid card and electronic road pricing for the purpose of transportation
chargeBearer	[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. API: The following values are allowed for Payment Request - SLEV: Charges are to be applied following the rules agreed in the service level and/or scheme.
paymentInformationStatus	[0..1]	ISO20022: Specifies the status of the payment information. API: Mandatory. The following values are allowed to provide the status of the Payment Request - ACCP (AcceptedCustomerProfile): Preceding check of technical validation was successful. Customer profile check was also successful. - ACSC (AcceptedSettlementCompleted): Settlement on the debtor's account has been completed. - ACSP (AcceptedSettlementInProcess): All preceding checks such as technical validation and customer profile were successful. Dynamic risk assessment is now also successful and therefore the Payment Request has been accepted for execution. - ACTC (AcceptedTechnicalValidation): Authentication and syntactical and semantical validation are successful. - ACWC (AcceptedWithChange): Instruction is accepted but a change will be made, such as date or remittance not sent. - ACWP (AcceptedWithoutPosting): Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account. - RCVD (Received): Payment initiation has been received by the receiving agent. - PDNG (Pending): Payment request or individual transaction included in the Payment Request is pending. Further checks and status update will be performed. - RJCT (Rejected): Payment request has been rejected.

FIELD	MULT.	DESC.
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Payment Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Payment Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
creditTransferTransaction	[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor.
	[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor.
paymentId	[1..1]	ISO20022: Set of elements used to reference a payment instruction.
ResourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
instructionId	[1..1]	ISO20022: Unique identification as assigned by an instructing party for an instructed party to unambiguously identify the instruction. API: Unique identification shared between the PISP and the ASPSP
endToEndId	[1..1]	ISO20022: Unique identification assigned by the initiating party to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. API: Unique identification shared between the merchant and the PSU
requestedExecutionDate	[1..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
regulatoryReportingCode	[0..1]	Information needed due to regulatory and statutory requirements. Economical codes to be used are provided by the National Competent Authority
remittanceInformation	[1..1]	ISO20022: Information supplied to enable the matching of an entry with the items that the transfer is intended to settle, such as commercial invoices in an accounts' receivable system. API: Only one occurrence is allowed
	[0..1]	Relevant information to the transaction

FIELD	MULT.	DESC.
transactionStatus	[0..1]	ISO20022: Specifies the status of the payment information group. API: Only the following values are allowed to provide the status of the subsequent CREDIT TRANSFER to the Payment Request - RJCT: Payment request or individual transaction included in the Payment Request has been rejected. - PDNG: (Pending): Payment request or individual transaction included in the Payment Request is pending. Further checks and status update will be performed. - ACSP: All preceding checks such as technical validation and customer profile were successful and therefore the Payment Request has been accepted for execution. - ACSC: Settlement on the debtor's account has been completed
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Payment Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Payment Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
supplementaryData	[1..1]	ISO20022: Additional information that cannot be captured in the structured elements and/or any other specific block. API: This structure is used to embed the relevant URLs for returning the status report to the PISP and to specify which SCA approaches are accepted by the PISP and which has been chosen by the ASPSP
acceptedScaApproach	[0..1]	can only be set by the PISP SCA approaches that are supported by the PISP. The PISP can provide several choices separated by commas. REDIRECT: the PSU is redirected by the TPP to the ASPSP which processes identification and authentication DECOUPLED: the TPP identifies the PSU and forwards the identification to the ASPSP which processes the authentication through a decoupled device EMBEDDED: the TPP identifies the PSU and forwards the identification to the ASPSP which starts the authentication. The TPP forwards one authentication factor of the PSU (e.g. OTP or response to a challenge)
	[0..*]	combination of possible values for SCA models
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the SCA and consent process in REDIRECT and DECOUPLED approach
unsuccessfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the failure of the SCA and consent process in REDIRECT and DECOUPLED approach If this URL is not provided by the PISP, the ASPSP will use the "successfulReportUrl" even in case of failure of the Payment Request processing
_links	[1..1]	links that can be used for further navigation when having post a Payment Request in order to get the relevant status report.
self	[0..1]	hypertext reference

FIELD	MULT.	DESC.
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
confirmation	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.6.5. Business reason codes in case of rejection

The following table lists all the reason codes to use in case of rejection of the Payment Request or the payment instruction.

ISO20022 CODE AND LABEL	SIGNIFICANCE AND PURPOSE
AC01 (IncorectAccountNumber)	the account number is either invalid or does not exist
AC04 (ClosedAccountNumber)	the account is closed and cannot be used
AC06 (BlockedAccount)	the account is blocked and cannot be used
AG01 (Transaction forbidden)	Transaction forbidden on this type of account
CUST (RequestedByCustomer)	The reject is due to the debtor (refusal or lack of liquidity)
FF01 (InvalidFileFormat)	The reject is due to the original payment activation request which is invalid (syntax, structure or values)
FRAD (FraudulentOriginated)	the Payment Request is considered as fraudulent
MS03 (NotSpecifiedReasonAgentGenerated)	No reason specified by the ASPSP
NOAS (NoAnswerFromCustomer)	The PSU has neither accepted nor rejected the Payment Request and a time-out has occurred
RR01 (MissingDebtorAccountOrIdentification)	The Debtor account and/or Identification are missing or inconsistent
RR03 (MissingCreditorNameOrAddress)	Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing.
RR04 (RegulatoryReason)	Reject from regulatory reason
RR12 (InvalidPartyID)	Invalid or missing identification required within a particular country or payment type.

4.7. Confirmation of a Payment Request (PISP)

4.7.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PISP role
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP has previously posted a Payment Request which has been saved by the ASPSP (cf. § 4.5.3)
    - The ASPSP has answered with a location link to the saved Payment Request (cf. § 4.5.4)
    - The TPP has retrieved the saved Payment request in order to get the relevant resource Ids (cf. § 4.6).
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.7.2. Business flow

Once the Payment Request has been validated and accepted by the PSU, it is the due to the PISP to confirm this Payment Request to the ASPSP in order to complete the process flow.

In REDIRECT and DECOUPLED approach, this confirmation is not a prerequisite to the execution of the Credit Transfer.

4.7.3. Request content

The API entry point is POST /payment-requests/{paymentRequestId}/confirmation

The PISP provides through its request:

- The “OAUTH2 Client Credential” token
- The resource Id of the saved Payment Request
- One authentication factor of the PSU in case of EMBEDDED approach

FIELD		MULT.	DESC.
confirmationRequest		[0..1]	confirmation request resource
	psuAuthenticationFactor	[0..1]	authentication factor forwarded by the TPP to the ASPSP in order to fulfill the strong customer authentication process

4.7.4. Response content (if no error)

The ASPSP answers with an ISO20022 message-based structure in order to give an update of the Payment Request to the PISP in a same way as § 4.6.4.

4.8. Transfer Initiation on behalf of a Payment Account Owner (PISP)

4.8.1. Prerequisites

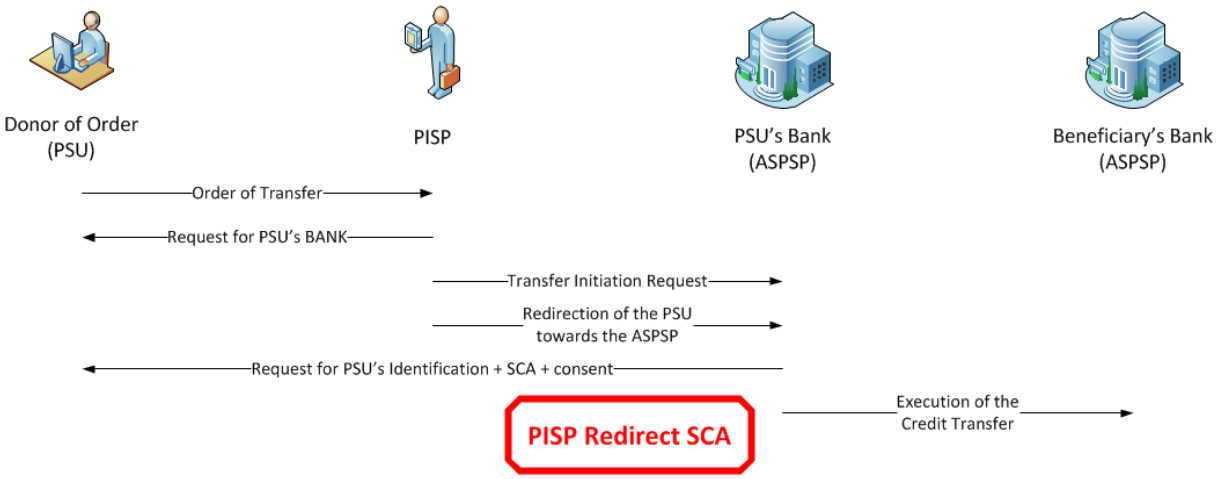
- The TPP has been registered by the Registration Authority for the PISP and AISP roles.
- The TPP and the PSU have a contract for Payment Initiation Services. This contract might also include Aggregation Information Services.
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.8.2. Business flow

4.8.2.1. Common flow

- The PSU provides the PISP with all information needed for the transfer.
- The PISP prepares the Transfer Request and sends this request to the relevant ASPSP that holds the debtor account. This request includes:
    - The specification of the SCA approaches that are supported by the PISP (any combination of “REDIRECT”, “EMBEDDED” and “DECOUPLED” values).
    - In case of possible REDIRECT or DECOUPLED SCA approach, one or two call-back URLs to be used by the ASPSP at the finalisation of the authentication and consent process :
        - The first call-back URL will be called by the ASPSP if the Transfer Request is processed without any error or rejection by the PSU
        - The second call-back URL is to be used by the ASPSP in case of processing error or rejection by the PSU. Since this second URL is optional, the PISP might not provide it. In this case, the ASPSP will use the same URL for any processing result.
        - Both call-back URLS must be used in a TLS-secured request, including mutual authentication based on each party’s TLS certificate.
    - In case of possible “EMBEDDED” or “DECOUPLED” approaches, a PSU identifier that can be processed by the ASPSP for PSU recognition.
- The ASPSP saves the Transfer Request and answers to the PISP. The answer embeds
    - A location link of the saved Transfer Request that will be further used to retrieve the Transfer Request and its status information.
    - The specification of the chosen SCA approach taking into account both the PISP and the PSU capabilities.
    - In case of chosen REDIRECT SCA approach, the URL to be used by the PISP for redirecting the PSU in order to perform a SCA.

4.8.2.2. Redirect SCA approach

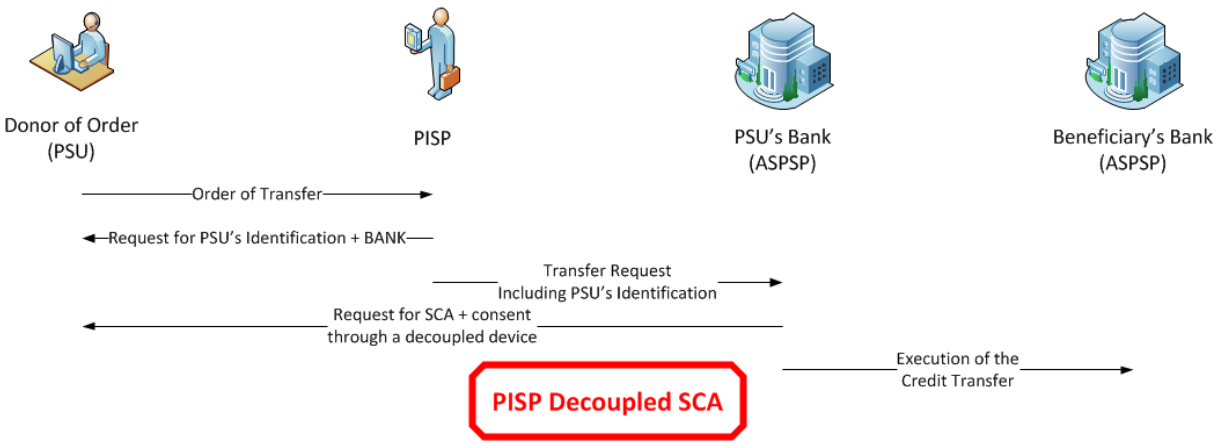


When the chosen SCA approach within the ASPSP answers is set to "REDIRECT":

- The PISP redirects the PSU to the ASPSP which authenticates the PSU
- The ASPSP asks the PSU to give (or deny) his/her consent to the Transfer Request
- The PSU chooses or confirms which of his/her accounts shall be used by the ASPSP for the future Credit Transfer.
- The ASPSP is then able to initiate the subsequent Credit Transfer
- The ASPSP redirects the PSU to the PISP using one of the call-back URLs provided within the posted Transfer Request

If the PSU neither gives nor denies his/her consent, the Transfer Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.8.2.3. Decoupled SCA approach

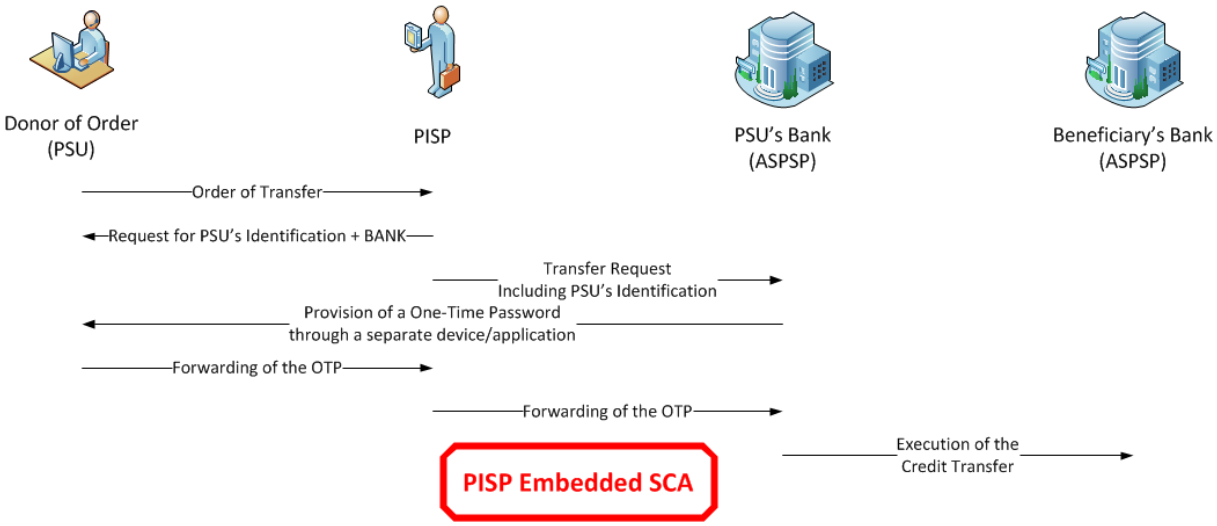


When the chosen SCA approach is "DECOUPLED":

- Based on the PSU identifier provided within the Transfer Request by the PISP, the ASPSP gives the PSU with the Transfer Request details and challenges the PSU for a Strong Customer Authentication on a decoupled device or application.
- The PSU chooses or confirms which of his/her accounts shall be used by the ASPSP for the future Credit Transfer.
- The ASPSP is then able to initiate the subsequent Credit Transfer
- The ASPSP notifies the PISP about the finalisation of the authentication and consent process by using one of the call-back URLs provided within the posted Transfer Request

If the PSU neither gives nor denies his/her consent, the Transfer Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.8.2.4. Embedded SCA approach



When the chosen SCA approach within the ASPSP answers is set to "EMBEDDED":

- The TPP informs the PSU that a challenge is needed for completing the Transfer Request processing. This challenge will be one of the following:
  - A One-Time-Password sent by the ASPSP to the PSU on a separate device or application.
  - A response computed by a specific device on base of a challenge sent by the ASPSP to the PSU on a separate device or application.
- The PSU unlock the device or application through a "knowledge factor" and/or an "inherence factor" (biometric), retrieves the Transfer Request details and processes the data sent by the ASPSP;
- The PSU might choose or confirm which of his/her accounts shall be used by the ASPSP for the future Credit Transfer when the device or application allows it.
- When agreeing the Transfer Request, the PSU enters the resulting authentication factor through the PISP interface which will forward it to the ASPSP through a confirmation request (cf. § 4.10)

If the PSU neither gives nor denies his/her consent, the Transfer Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.8.3. Request content

Whatever the SCA approach, the API entry point is POST /transfer-requests

The TPP provides through its request:

- The “OAUTH2 Client Credential” token
- The Transfer Request itself through an ISO20022 “pain.001” message-based structure (CustomerCreditTransferInitiation).

FIELD	MULT.	DESC.
resourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
debtor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAccount	[0..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
creditor	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
creditorAccount	[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD	MULT.	DESC.
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
transferInformationStatus	[0..1]	ISO20022: Specifies the status of the payment information. API: Mandatory. The following values are allowed to provide the status of the Transfer Request - ACCP (AcceptedCustomerProfile): Preceding check of technical validation was successful. Customer profile check was also successful. - ACSC (AcceptedSettlementCompleted): Settlement on the debtor's account has been completed. - ACSP (AcceptedSettlementInProcess): All preceding checks such as technical validation and customer profile were successful. Dynamic risk assessment is now also successful and therefore the Transfer Request has been accepted for execution. - ACTC (AcceptedTechnicalValidation): Authentication and syntactical and semantical validation are successful. - ACWC (AcceptedWithChange): Instruction is accepted but a change will be made, such as date or remittance not sent. - ACWP (AcceptedWithoutPosting): Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account. - RCVD (Received): Payment initiation has been received by the receiving agent. - PDNG (Pending): Payment request or individual transaction included in the Transfer Request is pending. Further checks and status update will be performed. - RJCT (Rejected): Payment request has been rejected.
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Transfer Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Transfer Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Transfer Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used

FIELD	MULT.	DESC.
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
remittanceInformation	[1..1]	ISO20022: Information supplied to enable the matching of an entry with the items that the transfer is intended to settle, such as commercial invoices in an accounts' receivable system. API: Only one occurrence is allowed
	[0..1]	Relevant information to the transaction
supplementaryData	[1..1]	ISO20022: Additional information that cannot be captured in the structured elements and/or any other specific block. API: This structure is used to embed the relevant URLs for returning the status report to the PISP and to specify which SCA approaches are accepted by the PISP and which has been chosen by the ASPSP
acceptedScaApproach	[0..1]	can only be set by the PISP SCA approaches that are supported by the PISP. The PISP can provide several choices separated by commas. REDIRECT: the PSU is redirected by the TPP to the ASPSP which processes identification and authentication DECOUPLED: the TPP identifies the PSU and forwards the identification to the ASPSP which processes the authentication through a decoupled device EMBEDDED: the TPP identifies the PSU and forwards the identification to the ASPSP which starts the authentication. The TPP forwards one authentication factor of the PSU (e.g. OTP or response to a challenge)
	[0..*]	combination of possible values for SCA models
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the SCA and consent process in REDIRECT and DECOUPLED approach
unsuccessfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the failure of the SCA and consent process in REDIRECT and DECOUPLED approach If this URL is not provided by the PISP, the ASPSP will use the "successfulReportUrl" even in case of failure of the Transfer Request processing

4.8.4. Response content (if no error)

The ASPSP answers with a “location” link of the saved Transfer Request. This link refers to the resource Id of the saved payment to be used afterwards in order to get Payment request and its status.

The following data are also provided.

FIELD	MULT.	DESC.
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
_links	[0..1]	links that can be used for further navigation, especially in REDIRECT approach
consentApproval	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.9. Retrieval of a Transfer Request and its status (PISP)

4.9.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PISP role
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP has previously posted a Transfer Request which has been saved by the ASPSP (cf. § 4.8.3)
    - The ASPSP has answered with a location link to the saved Transfer Request (cf. § 4.8.4)
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.9.2. Business flow

The PISP asks to retrieve the Transfer Request that has been saved by the ASPSP. The PISP uses the location link provided by the ASPSP in response of the posting of this request.

The ASPSP returns the previously posted Transfer Request which is enriched with the status information of the Transfer Request.

The status information must be available during at least 30 calendar days after the posting of the Transfer Request. However, the ASPSP may increase this availability duration, based on its own rules.

4.9.3. Request content

The API entry point is GET /transfer-requests/{transferRequestId}

The PISP provides through its request:

- The “OAUTH2 Client Credential” token
- The resource Id of the saved Transfer Request

4.9.4. Response content (if no error)

The response given by the ASPSP includes the previously posted Transfer Request which has been enriched with its status.

FIELD	MULT.	DESC.
transferRequest	[1..1]	Transfert Request structure
resourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
debtor	[0..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
debtorAccount	[0..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.

FIELD	MULT.	DESC.
iban	[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
other	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
creditor	[1..1]	API : Description of a Party which can be either a person or an organization.
name	[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress	[0..1]	ISO20022 : Information that locates and identifies a specific address, as defined by postal services.
country	[1..1]	ISO20022: Country in which a person resides (the place of a person's home). In the case of a company, it is the country from which the affairs of that company are directed.
addressLine	[1..1]	Unstructured address. The two lines must embed zip code and town name
	[0..2]	Address line
organisationId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account
schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
privateId	[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
identification	[1..1]	API: alias of an account

FIELD					MULT.	DESC.
				schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
				issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties
		creditorAccount			[1..1]	Unique and unambiguous identification for the account between the account owner and the account servicer.
			iban		[0..1]	ISO20022: International Bank Account Number (IBAN) - identification used internationally by financial institutions to uniquely identify the account of a customer. Further specifications of the format and content of the IBAN can be found in the standard ISO 13616 "Banking and related financial services - International Bank Account Number (IBAN)" version 1997-10-01, or later revisions.
			other		[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer.
				identification	[1..1]	API: alias of an account
				schemeName	[1..1]	Name of the identification scheme. Possible values for the scheme name, partially based on ISO20022 external code list, are the following: - BANK (BankPartyIdentification): Unique and unambiguous assignment made by a specific bank or similar financial institution to identify a relationship as defined between the bank and its client. - COID (CountryIdentificationCode) : Country authority given organisation identification (e.g., corporate registration number) - SREN (SIREN): The SIREN number is a 9 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation in France. - SRET (SIRET): The SIRET number is a 14 digit code assigned by INSEE, the French National Institute for Statistics and Economic Studies, to identify an organisation unit in France. It consists of the SIREN number, followed by a five digit classification number, to identify the local geographical unit of that entity. - NIDN (NationalIdentityNumber): Number assigned by an authority to identify the national identity number of a person. Other values are also permitted, for instance: - OAUT (OAUTH2): OAUTH2 access token that is owned by the PISP being also an AISP and that can be used in order to identify the PSU - CPAN (CardPan): Card PAN
				issuer	[1..1]	ISO20022: Entity that assigns the identification. this could a country code or any organisation name or identifier that can be recognized by both parties

FIELD	MULT.	DESC.
transferInformationStatus	[0..1]	ISO20022: Specifies the status of the payment information. API: Mandatory. The following values are allowed to provide the status of the Transfer Request - ACCP (AcceptedCustomerProfile): Preceding check of technical validation was successful. Customer profile check was also successful. - ACSC (AcceptedSettlementCompleted): Settlement on the debtor's account has been completed. - ACSP (AcceptedSettlementInProcess): All preceding checks such as technical validation and customer profile were successful. Dynamic risk assessment is now also successful and therefore the Transfer Request has been accepted for execution. - ACTC (AcceptedTechnicalValidation): Authentication and syntactical and semantical validation are successful. - ACWC (AcceptedWithChange): Instruction is accepted but a change will be made, such as date or remittance not sent. - ACWP (AcceptedWithoutPosting): Payment instruction included in the credit transfer is accepted without being posted to the creditor customer's account. - RCVD (Received): Payment initiation has been received by the receiving agent. - PDNG (Pending): Payment request or individual transaction included in the Transfer Request is pending. Further checks and status update will be performed. - RJCT (Rejected): Payment request has been rejected.
statusReasonInformation	[0..1]	ISO20022: Provides detailed information on the status reason. API: Can only be used in status equal to "RJCT". Only the following values are allowed: - AC01 (IncorectAccountNumber): the account number is either invalid or does not exist - AC04 (ClosedAccountNumber): the account is closed and cannot be used - AC06 (BlockedAccount): the account is blocked and cannot be used - AG01 (Transaction forbidden): Transaction forbidden on this type of account - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - FF01 (InvalidFileFormat): The reject is due to the original Transfer Request which is invalid (syntax, structure or values) - FRAD (FraudulentOriginated): the Transfer Request is considered as fraudulent - MS03 (NotSpecifiedReasonAgentGenerated): No reason specified by the ASPSP - NOAS (NoAnswerFromCustomer): The PSU has neither accepted nor rejected the Transfer Request and a time-out has occurred - RR01 (MissingDebtorAccountOrIdentification): The Debtor account and/or Identification are missing or inconsistent - RR03 (MissingCreditorNameOrAddress): Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing. - RR04 (RegulatoryReason): Reject from regulatory reason - RR12 (InvalidPartyID): Invalid or missing identification required within a particular country or payment type.
instructedAmount	[1..1]	ISO20022: structure aiming to carry either an instructed amount or equivalent amount. Both structures embed the amount and the currency to be used. API: only instructed amount can be used
currency	[1..1]	ISO20022: Specifies the currency of the to be transferred amount, which is different from the currency of the debtor's account. A code allocated to a currency by a Maintenance Agency under an international identification scheme, as described in the latest edition of the international standard ISO 4217 "Codes for the representation of currencies and funds".
amount	[1..1]	ISO20022: Amount of money to be moved between the debtor and creditor, before deduction of charges, expressed in the currency as ordered by the initiating party.
remittanceInformation	[1..1]	ISO20022: Information supplied to enable the matching of an entry with the items that the transfer is intended to settle, such as commercial invoices in an accounts' receivable system. API: Only one occurrence is allowed
	[0..1]	Relevant information to the transaction
supplementaryData	[1..1]	ISO20022: Additional information that cannot be captured in the structured elements and/or any other specific block. API: This structure is used to embed the relevant URLs for returning the status report to the PISP and to specify which SCA approaches are accepted by the PISP and which has been chosen by the ASPSP

FIELD	MULT.	DESC.
acceptedScaApproach	[0..1]	can only be set by the PISP SCA approaches that are supported by the PISP. The PISP can provide several choices separated by commas. REDIRECT: the PSU is redirected by the TPP to the ASPSP which processes identification and authentication DECOUPLED: the TPP identifies the PSU and forwards the identification to the ASPSP which processes the authentication through a decoupled device EMBEDDED: the TPP identifies the PSU and forwards the identification to the ASPSP which starts the authentication. The TPP forwards one authentication factor of the PSU (e.g. OTP or response to a challenge)
	[0..*]	combination of possible values for SCA models
appliedScaApproach	[0..1]	The ASPSP, based on the SCA approaches proposed by the PISP, choose the one that it can processed, in respect with the preferences and constraints of the PSU and indicates in this field which approach has been chosen
successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the SCA and consent process in REDIRECT and DECOUPLED approach
unsuccessfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the failure of the SCA and consent process in REDIRECT and DECOUPLED approach If this URL is not provided by the PISP, the ASPSP will use the "successfulReportUrl" even in case of failure of the Transfer Request processing
_links	[1..1]	links that can be used for further navigation when having post a Transfer Request in order to get the relevant status report.
self	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false
confirmation	[0..1]	hypertext reference
href	[1..1]	URI to be used
templated	[0..1]	specifies "true" if href is a URI template, i.e. with parameters. Otherwise, this property is absent or set to false

4.9.5. Business reason codes in case of rejection

The following table lists all the reason codes to use in case of rejection of the Transfer Request.

ISO20022 CODE AND LABEL	SIGNIFICANCE AND PURPOSE
AC01 (IncorectAccountNumber)	the account number is either invalid or does not exist
AC04 (ClosedAccountNumber)	the account is closed and cannot be used
AC06 (BlockedAccount)	the account is blocked and cannot be used
AG01 (Transaction forbidden)	Transaction forbidden on this type of account
CUST (RequestedByCustomer)	The reject is due to the debtor (refusal or lack of liquidity)
FF01 (InvalidFileFormat)	The reject is due to the original payment activation request which is invalid (syntax, structure or values)
FRAD (FraudulentOriginated)	the Transfer Request is considered as fraudulent
MS03 (NotSpecifiedReasonAgentGenerated)	No reason specified by the ASPSP
NOAS (NoAnswerFromCustomer)	The PSU has neither accepted nor rejected the Transfer Request and a time-out has occurred
RR01 (MissingDebtorAccountOrIdentification)	The Debtor account and/or Identification are missing or inconsistent
RR03 (MissingCreditorNameOrAddress)	Specification of the creditor's name and/or address needed for regulatory requirements is insufficient or missing.
RR04 (RegulatoryReason)	Reject from regulatory reason
RR12 (InvalidPartyID)	Invalid or missing identification required within a particular country or payment type.

4.10. Confirmation of a Transfer Request (PISP)

4.10.1. Prerequisites

- The TPP has been registered by the Registration Authority for the PISP role
- The TPP was provided with an OAUTH2 “Client Credential” access token by the ASPSP (cf. § 3.4.3).
- The TPP has previously posted a Transfer Request which has been saved by the ASPSP (cf. § 4.8.3)
    - The ASPSP has answered with a location link to the saved Transfer Request (cf. § 4.8.4)
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its “OAUTH2 Client Credential” access token

4.10.2. Business flow

Once the Transfer Request has been validated and accepted by the PSU, it is the due to the PISP to confirm this Transfer Request to the ASPSP in order to complete the process flow.

In REDIRECT and DECOUPLED approach, this confirmation is not a prerequisite to the execution of the Credit Transfer.

4.10.3. Request content

The API entry point is POST /transfer-requests/{transferRequestId}/confirmation

The PISP provides through its request:

- The “OAUTH2 Client Credential” token
- The resource Id of the saved Transfer Request
- One authentication factor of the PSU in case of EMBEDDED approach

FIELD		MULT.	DESC.
confirmationRequest		[0..1]	confirmation request resource
	psuAuthenticationFactor	[0..1]	authentication factor forwarded by the TPP to the ASPSP in order to fulfill the strong cutomer authentication process

4.10.4. Response content (if no error)

The ASPSP answers with an ISO20022 message-based structure in order to give an update of the Transfer Request to the PISP in a same way as § 4.9.4.

5. AISP Use cases

5.1. PSU Context Retrieval

5.1.1. Request

```
GET http://localhost:8080/v1/accounts
```

5.1.1.1. Headers

```
Date: 2018-04-01T19:48:18.735+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: Bearer 1234567890AZERTYUIOP
PSU-Accept-Charset: en-US
PSU-Accept-Encoding: utf-8
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-Account-Consent-Responsibility: BY-AISP
PSU-HTTP-Method: POST
PSU-Accept-Language: gzip, deflate
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-account-consent-responsibility psu-http-method
psu-accept-language content-type user-agent (request-
target)",signature="luz58sVCjyhL6YlcDN+KBQcouL1s2Q66QY/KIH9U1ya7BDx0eOSbzQLtrlx1
```

+eFd9/+gzuJQPsVrIrADBA29P5cDdhnL8GVY/yeThyUfpQ5RIq9IHQMUs0DLB7Wcb0qH5WQ
UJG/ImF075kAdFGrm+O01XEPV/e22XYDl9qwOn/Q="

5.1.1.2. Body

No body data

5.1.2. Response

Status code: 200

5.1.2.1. Headers

X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT

5.1.2.2. Body


```
{
  "accounts" : [ {
    "resourceId" : "Alias1",
    "bicFi" : "BNKAFRPPXXX",
    "name" : "Compte de Mr et Mme Dupont",
    "usage" : "PRIV",
    "cashAccountType" : "CACC",
    "currency" : "EUR",
    "psuStatus" : "Co-account Holder",
    "_links" : {
      "balances" : {
        "href" : "v1/accounts/Alias1/balances"
      },
      "transactions" : {
        "href" : "v1/accounts/Alias1/transactions"
      }
```

```
      }
   }, {
      "resourceId" : "Alias2",
      "bicFi" : "BNKAFRPPXXX",
      "name" : "Compte de Mme Dupont",
      "usage" : "PRIV",
      "cashAccountType" : "CACC",
      "currency" : "EUR",
      "psuStatus" : "Account Holder",
      "_links" : {
         "balances" : {
            "href" : "v1/accounts/Alias2/balances"
         },
         "transactions" : {
            "href" : "v1/accounts/Alias2/transactions"
         }
      }
   } ],
   "_links" : {
      "self" : {
         "href" : "v1/accounts"
      }
   }
}
```


5.2. Account Balances Retrieval

5.2.1. Request

```
GET http://localhost:8080/v1/accounts/Alias1/balances
```

5.2.1.1. Headers

```
Date: 2018-04-01T19:48:19.910+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
```

```
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: Bearer 1234567890AZERTYUIOP
PSU-Accept-Charset: en-US
PSU-Accept-Encoding: utf-8
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-Account-Consent-Responsibility: BY-AISP
PSU-HTTP-Method: POST
PSU-Accept-Language: gzip, deflate
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-account-consent-responsibility psu-http-method
psu-accept-language content-type user-agent (request-
target)",signature="UdIsOxEvcY7I3c9WjR4bhDtl67wKDH7A1bUglDtc82g0oPzNCuYgNzXb/Co
ptmbjWPvzM1TF1fbT6ceSFhY51+Ml/7PPp6gL7NqfkUGXAogwOOOpzCPk/NcrDRCJqGrVa40
DoH36RMyYsfftxx9ck98BPYuJDdlgWSxxePYey6s="
```

5.2.1.2. Body

No body data

5.2.2. Response

```
Status code: 200
```

5.2.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

5.2.2.2. Body


```
{
  "balances" : [ {
    "name" : "Solde comptable au 12/01/2017",
    "balanceAmount" : {
      "currency" : "EUR",
      "amount" : "123.45"
    },
    "balanceType" : "CLBD",
    "lastCommittedTransaction" : "A452CH"
  }, {
    "name" : "Solde comptable au 12/01/2017",
    "balanceAmount" : {
      "currency" : "EUR",
      "amount" : "105.65"
    },
    "balanceType" : "XPCD",
    "lastCommittedTransaction" : "A452CH"
  } ],
  "_links" : {
    "self" : {
      "href" : "v1/accounts/Alias1/balances"
    },
    "parent-list" : {
      "href" : "v1/accounts"
    },
    "transactions" : {
```

```
        "href" : "v1/accounts/Alias1/transactions"
      }
    }
}
```


5.3. Account Transactions Retrieval

5.3.1. Request

```
GET http://localhost:8080/v1/accounts/Alias1/transactions
```

5.3.1.1. Headers


```
Date: 2018-04-01T19:48:19.965+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: Bearer 1234567890AZERTYUIOP
PSU-Accept-Charset: en-US
PSU-Accept-Encoding: utf-8
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-Account-Consent-Responsibility: BY-AISP
PSU-HTTP-Method: POST
PSU-Accept-Language: gzip, deflate
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
```

```
encoding psu-ip-address psu-user-agent psu-account-consent-responsibility psu-http-method
psu-accept-language content-type user-agent (request-
target)",signature="ltb7LAFxvaO2AUrDAWXReJ53BKxBOk6gvFy0RUrHLkV116FLglvEI+VS6p
YGUJEMqZgDdHyBC294FABuAqRwNLEt6r/SpvXM5Uw0e+yLhiMGXukY8BhGxs3G3nUrofVih
T9jpOtYBIxz/B+JNrgjZvFF6yMLXJmDaZ7mewzW8ZY="
```

5.3.1.2. Body

No body data

5.3.2. Response

```
Status code: 200
```

5.3.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

5.3.2.2. Body

```
{
  "transactions" : [ {
    "entryReference" : "AF5T2",
    "transactionAmount" : {
      "currency" : "EUR",
      "amount" : "12.25"
    },
    "creditDebitIndicator" : "DBIT",
    "status" : "BOOK",
    "bookingDate" : "2017-01-12",
    "remittanceInformation" : [ "Chèque n°XXXXXXX" ]
  }, {
    "entryReference" : "AF5T3",
```

```
      "transactionAmount" : {
         "currency" : "EUR",
         "amount" : "66.38"
      },
      "creditDebitIndicator" : "DBIT",
      "status" : "BOOK",
      "bookingDate" : "2017-01-12",
      "remittanceInformation" : [ "Prélèvement ICS XXXXXXX" ]
   }, {
      "entryReference" : "AF5T4",
      "transactionAmount" : {
         "currency" : "EUR",
         "amount" : "60.00"
      },
      "creditDebitIndicator" : "DBIT",
      "status" : "BOOK",
      "bookingDate" : "2017-01-12",
      "remittanceInformation" : [ "Retrait Carte" ]
   } ],
   "_links" : {
      "self" : {
         "href" : "v1/accounts/Alias1/transactions"
      },
      "parent-list" : {
         "href" : "v1/accounts"
      },
      "balances" : {
         "href" : "v1/accounts/Alias1/balances"
      },
      "last" : {
         "href" : "v1/accounts/Alias1/transactions?page=last"
      },
      "next" : {
         "href" : "v1/accounts/Alias1/transactions?page=next"
      }
```

```
  }
}
```

6. PIISP Use cases

6.1. Account Amount Coverage Check

6.1.1. Request

```
POST http://localhost:8080/v1/funds-confirmations
```

6.1.1.1. Headers

```
Date: 2018-04-01T19:48:20.048+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: Bearer 1234567890AZERTYUIOP
PSU-Accept-Charset: en-US
PSU-Accept-Encoding: utf-8
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: gzip, deflate
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=ig1XyR9g3SRsuzj6XWkgagp2e6S56RUFZ/pNPvcU0gw=
Content-Length: 160
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
```

```
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="wW/li7aU9Usknacl3GQPlojDDBfO0ynJsLMJS8Jt2mTS5JCtpiW4ksgLx0lP2
CqO8MDGo/czdE2zuN3rgjSv4qwkw7PH6cfBbGen+WOlZrQcADpCYS0f6jNwUhJGNTIY2EJP
LDNYEaZAqknLA88+R2UfR70zJMJgwqM3ZqG4Lsg="
```

6.1.1.2. Body

```
{
   "paymentCoverageRequestId" : "MyCoverage123456",
   "instructedAmount" : {
      "currency" : "EUR",
      "amount" : "12345"
   },
   "accountId" : {
      "iban" : "YY13RDHN98392489481620896668799742"
   }
}
```

6.1.2. Response

```
Status code: 200
```

6.1.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

6.1.2.2. Body

```
{
   "request" : {
      "paymentCoverageRequestId" : "MyCoverage123456",
```

```
      "instructedAmount" : {
         "currency" : "EUR",
         "amount" : "12345"
      },
      "accountId" : {
         "iban" : "YY13RDHN983924894816208966687997 42"
      }
   },
   "result" : true,
   "_links" : {
      "self" : {
         "href" : "v1/funds-confirmations"
      }
   }
}
```

7. PISP Use cases (REDIRECT APPROACH)

7.1. Payment Request

7.1.1. Request

```
POST http://localhost:8080/v1/payment-requests
```

7.1.1.1. Headers

```
Date: 2018-04-01T19:48:20.375+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
```

```
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=T7FMsJqT/o8xiHbq/GoeI879JoC0Je77w5fTUlpCyrM=
Content-Length: 1589
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="tCYCZAGxVZLMlo87gHeXyPs2RkoNvOhCdsPvjkGhwkHlU1kT8xRBT3lyb
CT2UcjFrd2WroWaXexC3pYNYHJTwPN9HRV6dVXNRn3Ba2/BOA2n2g/+RELeAX318buwuE
zQqAUOfci9d6d52X00+a5Dpb7h91T0zZuMBsPcxK6n2Sw="
```

7.1.1.2. Body

```
{
   "paymentInformationId" : "MyPmtInfId",
   "creationDateTime" : "2018-04-01T19:48:20.299+02:00",
   "numberOfTransactions" : 1,
   "initiatingParty" : {
      "name" : "MyPreferedPisp",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "12FR5",
         "schemeName" : "COID",
         "issuer" : "ACPR"
```

```
    }
  },
  "paymentTypeInformation" : {
    "serviceLevel" : "SEPA",
    "localInstrument" : "INST",
    "categoryPurpose" : "DVPM"
  },
  "debtor" : {
    "name" : "MyCustomer",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
      "issuer" : "BICXYYTTZZZ"
    }
  },
  "creditor" : {
    "name" : "myMerchant",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "852126789",
      "schemeName" : "SIREN",
      "issuer" : "FR"
    }
  },
  "creditorAccount" : {
    "iban" : "YY64COJH41059545330222956960771321"
  },
  "ultimateCreditor" : {
```

```
      "name" : "myPreferedUltimateMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "85212678900025",
         "schemeName" : "SIRET",
         "issuer" : "FR"
      }
   },
   "purpose" : "COMC",
   "chargeBearer" : "SLEV",
   "creditTransferTransaction" : [ {
      "paymentId" : {
         "instructionId" : "MyInstrId",
         "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-31T00:00:00.000+01:00",
      "instructedAmount" : {
         "currency" : "EUR",
         "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ]
   } ],
   "supplementaryData" : {
      "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
   }
}
```

7.1.2. Response

```
Status code: 201
```

7.1.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/payment-requests/MyPmtInfRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

7.1.2.2. Body

```
{
   "appliedScaApproach" : "REDIRECT",
   "_links" : {
      "consentApproval" : {
         "href" : "https://psd2.aspsp/consent-approval"
      }
   }
}
```

7.2. Payment Request Retrieval

7.2.1. Request

```
GET http://localhost:8080/v1/payment-requests/MyPmtInfRscId
```

7.2.1.1. Headers

```
Date: 2018-04-01T19:48:20.671+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
```

X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O = MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent (request-target)",signature="aqzw11uX5Q/SgOAnIf8W9g1EJENrW34PIptdBQmM5eDohSJCg8UXKJ9JYcWWC28Xxyvr6oHv7pMIUChPPBRhIe33uzJA6PTKmqSRe3dRRMXA/vXayXMstFkicQyENrzgW+h69BFt/1mpk/BxlBWiP17D26SCYARxstBnLYs5LHI="

7.2.1.2. Body

No body data

7.2.2. Response

Status code: 200

7.2.2.1. Headers

X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked

```
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

7.2.2.2. Body

```
{
   "paymentRequest" : {
      "resourceId" : "MyPmtInfRscId",
      "paymentInformationId" : "MyPmtInfId",
      "creationDateTime" : "2018-04-01T17:48:20.299Z",
      "numberOfTransactions" : 1,
      "initiatingParty" : {
         "name" : "MyPreferedPisp",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "organisationId" : {
            "identification" : "12FR5",
            "schemeName" : "COID",
            "issuer" : "ACPR"
         }
      },
      "paymentTypeInformation" : {
         "serviceLevel" : "SEPA",
         "localInstrument" : "INST",
         "categoryPurpose" : "DVPM"
      },
      "debtor" : {
         "name" : "MyCustomer",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "privateId" : {
            "identification" : "FD37G",
```

```
            "schemeName" : "BANK",
            "issuer" : "BICXYYTTZZZ"
        }
    },
    "debtorAgent" : {
        "bicFi" : "BNKAFRPPXXX"
    },
    "creditor" : {
        "name" : "myMerchant",
        "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
            "identification" : "852126789",
            "schemeName" : "SIREN",
            "issuer" : "FR"
        }
    },
    "creditorAccount" : {
        "iban" : "YY64COJH4105954533022295696077 1321"
    },
    "ultimateCreditor" : {
        "name" : "myPreferedUltimateMerchant",
        "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
            "identification" : "85212678900025",
            "schemeName" : "SIRET",
            "issuer" : "FR"
        }
    },
    "purpose" : "COMC",
```

```
      "chargeBearer" : "SLEV",
      "paymentInformationStatus" : "ACSC",
      "creditTransferTransaction" : [ {
        "paymentId" : {
          "instructionId" : "MyInstrId",
          "endToEndId" : "MyEndToEndId"
        },
        "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
        "instructedAmount" : {
          "currency" : "EUR",
          "amount" : "124.35"
        },
        "remittanceInformation" : [ "MyRemittanceInformation" ],
        "transactionStatus" : "ACSC"
      } ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
        "appliedScaApproach" : "REDIRECT",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
      "self" : {
        "href" : "v1/payment-requests/MyPmtInfRscId"
      },
      "confirmation" : {
        "href" : "v1/payment-requests/MyPmtInfRscId/confirmation"
      }
    }
}
```

7.3. Payment Request Confirmation

7.3.1. Request

```
POST http://localhost:8080/v1/payment-requests/MyPmtInfRscId/confirmation
```

7.3.1.1. Headers

```
Date: 2018-04-01T19:48:20.714+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=RBNvo1WzZ4oRRq0W9+hknpT7T8If536DEMBg9hyq/4o=
Content-Length: 2
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="V00hg0xcS0fLoyOJWcbzPHUfUUzMfJrOf5iKIrtlah7MBGZJF9uhoLO6NZoQ
RfYY9Fr+q/BkMK97ibuVB8w6vZ15MOd0zPLMb5akZ6TKqox/9WuPr3PIx58jHKlJuMcVlE609O
8JIZoSXUnnioVQ6f4gDKcQWRLPozVx69etiy4="
```

7.3.1.2. Body

```
{ }
```

7.3.2. Response

```
Status code: 200
```

7.3.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

7.3.2.2. Body

```
{
   "paymentRequest" : {
      "resourceId" : "MyPmtInfRscId",
      "paymentInformationId" : "MyPmtInfId",
      "creationDateTime" : "2018-04-01T17:48:20.299Z",
      "numberOfTransactions" : 1,
      "initiatingParty" : {
         "name" : "MyPreferedPisp",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "organisationId" : {
            "identification" : "12FR5",
            "schemeName" : "COID",
            "issuer" : "ACPR"
         }
      },
```

```
  "paymentTypeInformation" : {
    "serviceLevel" : "SEPA",
    "localInstrument" : "INST",
    "categoryPurpose" : "DVPM"
  },
  "debtor" : {
    "name" : "MyCustomer",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
      "issuer" : "BICXYYTTZZZ"
    }
  },
  "debtorAgent" : {
    "bicFi" : "BNKAFRPPXXX"
  },
  "creditor" : {
    "name" : "myMerchant",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "852126789",
      "schemeName" : "SIREN",
      "issuer" : "FR"
    }
  },
  "creditorAccount" : {
    "iban" : "YY64COJH41059545330222956960771321"
  },
```

```
    "ultimateCreditor" : {
      "name" : "myPreferedUltimateMerchant",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "85212678900025",
        "schemeName" : "SIRET",
        "issuer" : "FR"
      }
    },
    "purpose" : "COMC",
    "chargeBearer" : "SLEV",
    "paymentInformationStatus" : "ACSC",
    "creditTransferTransaction" : [ {
      "paymentId" : {
        "instructionId" : "MyInstrId",
        "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
      "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "transactionStatus" : "ACSC"
    } ],
    "supplementaryData" : {
      "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
      "appliedScaApproach" : "REDIRECT",
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
    }
  },
```

```
  "_links" : {
    "self" : {
      "href" : "v1/payment-requests/MyPmtInfRscId"
    }
  }
}
```

7.4. Transfer Request

7.4.1. Request

```
POST http://localhost:8080/v1/transfer-requests
```

7.4.1.1. Headers

```
Date: 2018-04-01T19:48:20.753+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=duD7wo3ZbzUjuyHamxoc87oa5NiaJbjXAoiJ0E7vr3U=
Content-Length: 745
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
```

```
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent digest content-length (request-target)",signature="hkKan21UQsw92j63zM4sXJJ9gTnZy3/RC4fqEf/yftZHgaHh2JaSe8UVTX6C+lFy+MBUsU6Ej5N36X5l2KuGBWciVgWZGtuqtWyF2IkLMaOoSpRwWbJlyJJ4OZCjgWnl8wZTRqwdXG/zhS7to6uew9QsjDauC1jSDt1X25HAgfg="
```

7.4.1.2. Body

```
{
   "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
         "identification" : "FD37G",
         "schemeName" : "BANK",
         "issuer" : "BICXYYTTZZZ"
      }
   },
   "creditor" : {
      "name" : "myMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "852126789",
         "schemeName" : "SIREN",
         "issuer" : "FR"
      }
   },
```

```
  "creditorAccount" : {
     "iban" : "YY64COJH41059545330222956960771321"
  },
  "instructedAmount" : {
     "currency" : "EUR",
     "amount" : "124.35"
  },
  "remittanceInformation" : [ "MyRemittanceInformation" ],
  "supplementaryData" : {
     "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
     "successfulReportUrl" : "http://myPisp/PaymentSuccess",
     "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
  }
}
```


7.4.2. Response

```
Status code: 201
```

7.4.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/transfer-requests/MyTransferRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT
```

7.4.2.2. Body


```
{
  "appliedScaApproach" : "REDIRECT",
  "_links" : {
     "consentApproval" : {
        "href" : "https://psd2.aspsp/consent-approval"
     }
```

```
  }
}
```

7.5. Transfer Request Retrieval

7.5.1. Request

```
GET http://localhost:8080/v1/transfer-requests/MyTransferRscId
```

7.5.1.1. Headers

```
Date: 2018-04-01T19:48:20.795+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type
user-agent (request-
target)",signature="r8zJSnsSddprwaNUf9RPMhHRH3aTcKn2uNPq33gkhBxxUZleHRuGP9uVY
```

yXPJVNbPewpqkImvomvqPD+QiNq67OMeRbPaVCGL0AdoVhANHnEiMcFWLwSlywCyr0Zvlf
9LovmSeqruvFsNqRMhUedS96LyRIIJRoaDhnMQGXVBaQ="

7.5.1.2. Body

No body data

7.5.2. Response

Status code: 200

7.5.2.1. Headers

X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:19 GMT

7.5.2.2. Body


```
{
  "transferRequest" : {
    "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
        "identification" : "FD37G",
        "schemeName" : "BANK",
        "issuer" : "BICXYYTTZZZ"
      }
    },
    "creditor" : {
      "name" : "myMerchant",
```

```
        "postalAddress" : {
          "country" : "FR",
          "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
          "identification" : "852126789",
          "schemeName" : "SIREN",
          "issuer" : "FR"
        }
      },
      "creditorAccount" : {
        "iban" : "YY64COJH41059545330222956960771321"
      },
      "transferInformationStatus" : "ACSC",
      "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
        "appliedScaApproach" : "REDIRECT",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
      "self" : {
        "href" : "v1/transfer-requests/MyTransferRscId"
      },
      "confirmation" : {
        "href" : "v1/transfer-requests/MyTransferRscId/confirmation"
      }
    }
```

```
}
```

7.6. Transfer Request Confirmation

7.6.1. Request

```
POST http://localhost:8080/v1/transfer-requests/MyTransferRscId/confirmation
```

7.6.1.1. Headers

```
Date: 2018-04-01T19:48:20.819+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=RBNvo1WzZ4oRRq0W9+hknpT7T8If536DEMBg9hyq/4o=
Content-Length: 2
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="am2S/cEbjN1xvUe2Vp/dB0fieqf6K8RRh9QcYTAkCmYYPboi/T3URalqnFbE
```

```
C/ZW3MCYY/SVBS+ngbZNumOwBhqwrEB+f4vnY1kTCEiNzg+izcmQetxCZV1a7+1E17PHq4
XCSN7GprrkEbcap1Wv1A50tUzD5kWfeAQFNspu8nc="
```

7.6.1.2. Body

```
{ }
```

7.6.2. Response

```
Status code: 200
```

7.6.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

7.6.2.2. Body

```
{
  "transferRequest" : {
    "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
        "identification" : "FD37G",
        "schemeName" : "BANK",
        "issuer" : "BICXYYTTZZZ"
      }
    },
    "creditor" : {
```

```
        "name" : "myMerchant",
        "postalAddress" : {
          "country" : "FR",
          "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
          "identification" : "852126789",
          "schemeName" : "SIREN",
          "issuer" : "FR"
        }
      },
      "creditorAccount" : {
        "iban" : "YY64COJH41059545330222956960771321"
      },
      "transferInformationStatus" : "ACSC",
      "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "REDIRECT", "DECOUPLED" ],
        "appliedScaApproach" : "REDIRECT",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
      "self" : {
        "href" : "v1/transfer-requests/MyTransferRscId"
      }
    }
}
```

8. PISP Use cases (DECOUPLED APPROACH)

8.1. Payment Request

8.1.1. Request

```
POST http://localhost:8080/v1/payment-requests
```

8.1.1.1. Headers

```
Date: 2018-04-01T19:48:20.841+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=pyFa13X3OwBumFHZVkG+/1pLQzkUWD7t+Wty1FXkx7Y=
Content-Length: 1589
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="TiDucjmlHAM4Om/TvMcMyBKysDLFStkcoMt5POgqKoVCxpQm0N7NrVey
```

```
2IfjIGrERyQecc73hW1m3V3r4lqMQtK0Nv2TA8SPhdBcMtRF2YlhqvDOaanKLTuAGasX2fb8B4
dEDoJTgpiftIv97o/Ps/FZdE2pdNgweJGE9tbMX8M="
```

8.1.1.2. Body

```
{
  "paymentInformationId" : "MyPmtInfId",
  "creationDateTime" : "2018-04-01T19:48:20.841+02:00",
  "numberOfTransactions" : 1,
  "initiatingParty" : {
    "name" : "MyPreferedPisp",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "12FR5",
      "schemeName" : "COID",
      "issuer" : "ACPR"
    }
  },
  "paymentTypeInformation" : {
    "serviceLevel" : "SEPA",
    "localInstrument" : "INST",
    "categoryPurpose" : "DVPM"
  },
  "debtor" : {
    "name" : "MyCustomer",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
```

```
        "issuer" : "BICXYYTTZZZ"
    }
},
"creditor" : {
    "name" : "myMerchant",
    "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
        "identification" : "852126789",
        "schemeName" : "SIREN",
        "issuer" : "FR"
    }
},
"creditorAccount" : {
    "iban" : "YY64COJH41059545330222956960771321"
},
"ultimateCreditor" : {
    "name" : "myPreferedUltimateMerchant",
    "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
        "identification" : "85212678900025",
        "schemeName" : "SIRET",
        "issuer" : "FR"
    }
},
"purpose" : "COMC",
"chargeBearer" : "SLEV",
"creditTransferTransaction" : [ {
    "paymentId" : {
        "instructionId" : "MyInstrId",
```

```
        "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-31T00:00:00.000+01:00",
      "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ]
   } ],
   "supplementaryData" : {
      "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
   }
}
```


8.1.2. Response

```
Status code: 201
```

8.1.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/payment-requests/MyPmtInfRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

8.1.2.2. Body


```
{
   "appliedScaApproach" : "DECOUPLED"
}
```

8.2. Payment Request Retrieval

8.2.1. Request

```
GET http://localhost:8080/v1/payment-requests/MyPmtInfRscId
```

8.2.1.1. Headers

```
Date: 2018-04-01T19:48:20.877+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type
user-agent (request-
target)",signature="tR5nYOol7IFbFymy0nQ2JhzfBUZWmNt4NnDgFpiMeXIW0a2RYI51YhcC5a
XIFOyqBzlPQ6179kSZjoKy/cRLyriHda8YiIdjEZmmV3G1yOwzMc10OPdLO0ZuO2vBKIeyQ0Ay
B4iQfemq6X10mjQMd2ttUiaPxc31dnb+yDZZETA="
```

8.2.1.2. Body

No body data

8.2.2. Response

Status code: 200

8.2.2.1. Headers

X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT

8.2.2.2. Body


```
{
  "paymentRequest" : {
    "resourceId" : "MyPmtInfRscId",
    "paymentInformationId" : "MyPmtInfId",
    "creationDateTime" : "2018-04-01T17:48:20.841Z",
    "numberOfTransactions" : 1,
    "initiatingParty" : {
      "name" : "MyPreferedPisp",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "12FR5",
        "schemeName" : "COID",
        "issuer" : "ACPR"
      }
    },
    "paymentTypeInformation" : {
```

```
    "serviceLevel" : "SEPA",
    "localInstrument" : "INST",
    "categoryPurpose" : "DVPM"
  },
  "debtor" : {
    "name" : "MyCustomer",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
      "issuer" : "BICXYYTTZZZ"
    }
  },
  "debtorAgent" : {
    "bicFi" : "BNKAFRPPXXX"
  },
  "creditor" : {
    "name" : "myMerchant",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "852126789",
      "schemeName" : "SIREN",
      "issuer" : "FR"
    }
  },
  "creditorAccount" : {
    "iban" : "YY64COJH41059545330222956960771321"
  },
  "ultimateCreditor" : {
```

```
        "name" : "myPreferedUltimateMerchant",
        "postalAddress" : {
          "country" : "FR",
          "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
          "identification" : "85212678900025",
          "schemeName" : "SIRET",
          "issuer" : "FR"
        }
      },
      "purpose" : "COMC",
      "chargeBearer" : "SLEV",
      "paymentInformationStatus" : "ACSC",
      "creditTransferTransaction" : [ {
        "paymentId" : {
          "instructionId" : "MyInstrId",
          "endToEndId" : "MyEndToEndId"
        },
        "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
        "instructedAmount" : {
          "currency" : "EUR",
          "amount" : "124.35"
        },
        "remittanceInformation" : [ "MyRemittanceInformation" ],
        "transactionStatus" : "ACSC"
      } ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
        "appliedScaApproach" : "DECOUPLED",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
```

```
      "self" : {
         "href" : "v1/payment-requests/MyPmtInfRscId"
      },
      "confirmation" : {
         "href" : "v1/payment-requests/MyPmtInfRscId/confirmation"
      }
   }
}
```

8.3. Payment Request Confirmation

8.3.1. Request

```
POST http://localhost:8080/v1/payment-requests/MyPmtInfRscId/confirmation
```

8.3.1.1. Headers

```
Date: 2018-04-01T19:48:20.901+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=RBNvo1WzZ4oRRq0W9+hknpT7T8If536DEMBg9hyq/4o=
```

```
Content-Length: 2
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="fvpH6wG4ueP8BbfdHO4HdiOxNPNLsF1LcWLDSdRR2CFmo0Yaujx3kkXO
fGnm+mTrlZrYMo1uHR1dp1qW1bhEiiL7fkkJDUGTrPLvDKkTIWWRj28WaaFwBYllQGMLu76fe
CcZn4hd89JVG7UNBoS1JQ4IppbZa0+ovoeEEH3i+p8="
```

8.3.1.2. Body

```
{ }
```

8.3.2. Response

```
Status code: 200
```

8.3.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

8.3.2.2. Body

```
{
  "paymentRequest" : {
    "resourceId" : "MyPmtInfRscId",
    "paymentInformationId" : "MyPmtInfId",
    "creationDateTime" : "2018-04-01T17:48:20.841Z",
    "numberOfTransactions" : 1,
    "initiatingParty" : {
      "name" : "MyPreferedPisp",
```

```
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "12FR5",
         "schemeName" : "COID",
         "issuer" : "ACPR"
      }
   },
   "paymentTypeInformation" : {
      "serviceLevel" : "SEPA",
      "localInstrument" : "INST",
      "categoryPurpose" : "DVPM"
   },
   "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
         "identification" : "FD37G",
         "schemeName" : "BANK",
         "issuer" : "BICXYYTTZZZ"
      }
   },
   "debtorAgent" : {
      "bicFi" : "BNKAFRPPXXX"
   },
   "creditor" : {
      "name" : "myMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
```

```
      },
      "organisationId" : {
         "identification" : "852126789",
         "schemeName" : "SIREN",
         "issuer" : "FR"
      }
   },
   "creditorAccount" : {
      "iban" : "YY64COJH41059545330222956960771321"
   },
   "ultimateCreditor" : {
      "name" : "myPreferedUltimateMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "85212678900025",
         "schemeName" : "SIRET",
         "issuer" : "FR"
      }
   },
   "purpose" : "COMC",
   "chargeBearer" : "SLEV",
   "paymentInformationStatus" : "ACSC",
   "creditTransferTransaction" : [ {
      "paymentId" : {
         "instructionId" : "MyInstrId",
         "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
      "instructedAmount" : {
         "currency" : "EUR",
         "amount" : "124.35"
      },
```

```
        "remittanceInformation" : [ "MyRemittanceInformation" ],
        "transactionStatus" : "ACSC"
      } ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
        "appliedScaApproach" : "DECOUPLED",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
      "self" : {
        "href" : "v1/payment-requests/MyPmtInfRscId"
      }
    }
}
```


8.4. Transfer Request

8.4.1. Request

```
POST http://localhost:8080/v1/transfer-requests
```

8.4.1.1. Headers

```
Date: 2018-04-01T19:48:20.933+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
```

```
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=JY9da5HAgRg2ZmJY53JPxe+/XnnpyREegP5SAeEq4QM=
Content-Length: 745
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="G7bwKCQhslJb+a06zOvMx3DJiWYiuvNTNwbnYdsmqcJbTp1xUTlZG4B4H
/TFbPidc/fESXCCXKuAoNd+zAmkEWTLnONwCvDLQy+MGZPbX0h5Rho16o0FCyAn0fcXwYI
Whso9DU/ZvUj+jTL2Vh2eMmP1mHw4sIetJmg/WW1wuao="
```

8.4.1.2. Body

```
{
   "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
         "identification" : "FD37G",
         "schemeName" : "BANK",
         "issuer" : "BICXYYTTZZZ"
      }
   },
   "creditor" : {
      "name" : "myMerchant",
```

```
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "852126789",
         "schemeName" : "SIREN",
         "issuer" : "FR"
      }
   },
   "creditorAccount" : {
      "iban" : "YY64COJH41059545330222956960771321"
   },
   "instructedAmount" : {
      "currency" : "EUR",
      "amount" : "124.35"
   },
   "remittanceInformation" : [ "MyRemittanceInformation" ],
   "supplementaryData" : {
      "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
   }
}
```

8.4.2. Response

```
Status code: 201
```

8.4.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/transfer-requests/MyTransferRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
```

```
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

8.4.2.2. Body

```
{
  "appliedScaApproach" : "DECOUPLED"
}
```

8.5. Transfer Request Retrieval

8.5.1. Request

```
GET http://localhost:8080/v1/transfer-requests/MyTransferRscId
```

8.5.1.1. Headers

```
Date: 2018-04-01T19:48:20.953+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
```

```
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent (request-target)",signature="wQuMjXEQCTrkpTwU4iST/q1Sok/DOCn01uZURoeD/ILIwN9cZ5lp32CkTXE4Yq+lk4/RoZMOawZo/vKCvVPJdtPU1MdD+lQmEWo375pNy0BFyMCOVlmIazYEXnE6K+zul4tklrZhvn+XE3g5++7CsghP1DOYp638b27EDkyHW9Y="
```

8.5.1.2. Body

No body data

8.5.2. Response

```
Status code: 200
```

8.5.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

8.5.2.2. Body

```
{
  "transferRequest" : {
    "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
        "identification" : "FD37G",
        "schemeName" : "BANK",
```

```
            "issuer" : "BICXYYTTZZZ"
         }
      },
      "creditor" : {
         "name" : "myMerchant",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "organisationId" : {
            "identification" : "852126789",
            "schemeName" : "SIREN",
            "issuer" : "FR"
         }
      },
      "creditorAccount" : {
         "iban" : "YY64COJH41059545330222956960771321"
      },
      "transferInformationStatus" : "ACSC",
      "instructedAmount" : {
         "currency" : "EUR",
         "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "supplementaryData" : {
         "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
         "appliedScaApproach" : "DECOUPLED",
         "successfulReportUrl" : "http://myPisp/PaymentSuccess",
         "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
   },
   "_links" : {
      "self" : {
         "href" : "v1/transfer-requests/MyTransferRscId"
      },
```

```
      "confirmation" : {
         "href" : "v1/transfer-requests/MyTransferRscId/confirmation"
      }
   }
}
```

8.6. Transfer Request Confirmation

8.6.1. Request

```
POST http://localhost:8080/v1/transfer-requests/MyTransferRscId/confirmation
```

8.6.1.1. Headers

```
Date: 2018-04-01T19:48:20.974+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=RBNvo1WzZ4oRRq0W9+hknpT7T8If536DEMBg9hyq/4o=
Content-Length: 2
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
```

```
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="MPJS6VlJtXmK8jk/n0OTNfM6cW/k8NgTWS/vg0K5izSeIWO+kgToIELO1bq
WW5Ndh+f6sxxKWwv4GeMpJ/Q/AZ6ZQYYb2OnRDPZQ/zME866T4j9YTMfrs0aoFIUhEnKMn
R1dpcI2rT5wzR49GWkDjncbGO5Kc+2vXd9n93Kdexc="
```

8.6.1.2. Body

```
{ }
```

8.6.2. Response

```
Status code: 200
```

8.6.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

8.6.2.2. Body

```
{
   "transferRequest" : {
      "debtor" : {
         "name" : "MyCustomer",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "privateId" : {
            "identification" : "FD37G",
            "schemeName" : "BANK",
```

```
            "issuer" : "BICXYYTTZZZ"
         }
      },
      "creditor" : {
         "name" : "myMerchant",
         "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
         },
         "organisationId" : {
            "identification" : "852126789",
            "schemeName" : "SIREN",
            "issuer" : "FR"
         }
      },
      "creditorAccount" : {
         "iban" : "YY64COJH41059545330222956960771321"
      },
      "transferInformationStatus" : "ACSC",
      "instructedAmount" : {
         "currency" : "EUR",
         "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "supplementaryData" : {
         "acceptedScaApproach" : [ "DECOUPLED", "EMBEDDED" ],
         "appliedScaApproach" : "DECOUPLED",
         "successfulReportUrl" : "http://myPisp/PaymentSuccess",
         "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
   },
   "_links" : {
      "self" : {
         "href" : "v1/transfer-requests/MyTransferRscId"
      }
```

```
  }
}
```

9. PISP Use cases (EMBEDDED APPROACH)

9.1. Payment Request

9.1.1. Request

```
POST http://localhost:8080/v1/payment-requests
```

9.1.1.1. Headers

```
Date: 2018-04-01T19:48:20.994+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=fC7fOfCY9IWsgWI05GOjxEK2PBnbjdV5M1sF1rX1FvM=
Content-Length: 1588
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
```

```
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="aqiSnkqmL48OTBsdH4Ay2gdw0hqGVZSwM2orH///wNNUsiogeoYtOLeoqH
rHw4Lml3MU//iwKumNwJ2rz0VGJmlWQYGAUTTNXlO2L+9hpVm+9UvC3j9FcJxxU9bng0zUQ
V7pk/F3SCOgwxgEw5RDAZRYxThVmI4ukLDiqKKTRiU="
```

9.1.1.2. Body

```
{
   "paymentInformationId" : "MyPmtInfId",
   "creationDateTime" : "2018-04-01T19:48:20.993+02:00",
   "numberOfTransactions" : 1,
   "initiatingParty" : {
      "name" : "MyPreferedPisp",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "12FR5",
         "schemeName" : "COID",
         "issuer" : "ACPR"
      }
   },
   "paymentTypeInformation" : {
      "serviceLevel" : "SEPA",
      "localInstrument" : "INST",
      "categoryPurpose" : "DVPM"
   },
   "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
```

```
    "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
      "issuer" : "BICXYYTTZZZ"
    }
  },
  "creditor" : {
    "name" : "myMerchant",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "852126789",
      "schemeName" : "SIREN",
      "issuer" : "FR"
    }
  },
  "creditorAccount" : {
    "iban" : "YY64COJH41059545330222956960771321"
  },
  "ultimateCreditor" : {
    "name" : "myPreferedUltimateMerchant",
    "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
    },
    "organisationId" : {
      "identification" : "85212678900025",
      "schemeName" : "SIRET",
      "issuer" : "FR"
    }
  },
  "purpose" : "COMC",
  "chargeBearer" : "SLEV",
```

```
  "creditTransferTransaction" : [ {
    "paymentId" : {
      "instructionId" : "MyInstrId",
      "endToEndId" : "MyEndToEndId"
    },
    "requestedExecutionDate" : "2016-12-31T00:00:00.000+01:00",
    "instructedAmount" : {
      "currency" : "EUR",
      "amount" : "124.35"
    },
    "remittanceInformation" : [ "MyRemittanceInformation" ]
  } ],
  "supplementaryData" : {
    "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
    "successfulReportUrl" : "http://myPisp/PaymentSuccess",
    "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
  }
}
```

9.1.2. Response

```
Status code: 201
```

9.1.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/payment-requests/MyPmtInfRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.1.2.2. Body

```
{
  "appliedScaApproach" : "EMBEDDED"
```

```
}
```

9.2. Payment Request Retrieval

9.2.1. Request

```
GET http://localhost:8080/v1/payment-requests/MyPmtInfRscId
```

9.2.1.1. Headers

```
Date: 2018-04-01T19:48:21.019+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type
user-agent (request-
target)",signature="sAWcYNLjRPkZrhg+vtyA1GKffbp9N2Wn3MyJ4eMTJp8Jcop60GaCV+P4X
ah5cZ+4Rf2ydOWjGsAksivP2xG6LAFQ/7R15+2flVTnj/ZfAYrcYK3/5A57Dtu1qTRVZhDPfDSg
```

```
m7/kRVYIWJaRiTvFFmbChED+QQ0E7cgr/tkfmeY="
```

9.2.1.2. Body

No body data

9.2.2. Response

```
Status code: 200
```

9.2.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.2.2.2. Body


```
{
  "paymentRequest" : {
    "resourceId" : "MyPmtInfRscId",
    "paymentInformationId" : "MyPmtInfId",
    "creationDateTime" : "2018-04-01T17:48:20.993Z",
    "numberOfTransactions" : 1,
    "initiatingParty" : {
      "name" : "MyPreferedPisp",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "12FR5",
        "schemeName" : "COID",
        "issuer" : "ACPR"
      }
```

```
    },
    "paymentTypeInformation" : {
        "serviceLevel" : "SEPA",
        "localInstrument" : "INST",
        "categoryPurpose" : "DVPM"
    },
    "debtor" : {
        "name" : "MyCustomer",
        "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "privateId" : {
            "identification" : "FD37G",
            "schemeName" : "BANK",
            "issuer" : "BICXYYTTZZZ"
        }
    },
    "debtorAgent" : {
        "bicFi" : "BNKAFRPPXXX"
    },
    "creditor" : {
        "name" : "myMerchant",
        "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
            "identification" : "852126789",
            "schemeName" : "SIREN",
            "issuer" : "FR"
        }
    },
    "creditorAccount" : {
        "iban" : "YY64COJH4105954533022295696077132 1"
```

```
    },
    "ultimateCreditor" : {
      "name" : "myPreferedUltimateMerchant",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "85212678900025",
        "schemeName" : "SIRET",
        "issuer" : "FR"
      }
    },
    "purpose" : "COMC",
    "chargeBearer" : "SLEV",
    "paymentInformationStatus" : "ACSC",
    "creditTransferTransaction" : [ {
      "paymentId" : {
        "instructionId" : "MyInstrId",
        "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
      "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
      },
      "remittanceInformation" : [ "MyRemittanceInformation" ],
      "transactionStatus" : "ACSC"
    } ],
    "supplementaryData" : {
      "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
      "appliedScaApproach" : "EMBEDDED",
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
    }
```

```
  },
  "_links" : {
    "self" : {
      "href" : "v1/payment-requests/MyPmtInfRscId"
    },
    "confirmation" : {
      "href" : "v1/payment-requests/MyPmtInfRscId/confirmation"
    }
  }
}
```

9.3. Payment Request Confirmation

9.3.1. Request

```
POST http://localhost:8080/v1/payment-requests/MyPmtInfRscId/confirmation
```

9.3.1.1. Headers

```
Date: 2018-04-01T19:48:21.037+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
```

```
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=P871WCcozbO2Mk3em1hL6Dw4hTTTZEoi21jII62lHc4=
Content-Length: 46
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="szCNUFiDRn87vLvdF7oqlMykmb2prUgn39wCQmTqc+CFDcbjs+RMANqB
1laP4GcIPt8FBfop4RBkXxxHYEED1LBcsFq5CLx1W78YoxcKua2dKffu57m5jMY8mlk4L/Tc1Q
SIhjG9JYzAyfdDnS7x4KK8KZletE4HLDpNOu7Kdvo="
```

9.3.1.2. Body

```
{
   "psuAuthenticationFactor" : "JJKJKJ788GKJKJBK"
}
```

9.3.2. Response

```
Status code: 200
```

9.3.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.3.2.2. Body

```
{
   "paymentRequest" : {
      "resourceId" : "MyPmtInfRscId",
      "paymentInformationId" : "MyPmtInfId",
```

```
"creationDateTime" : "2018-04-01T17:48:20.993Z",
"numberOfTransactions" : 1,
"initiatingParty" : {
   "name" : "MyPreferedPisp",
   "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
   },
   "organisationId" : {
      "identification" : "12FR5",
      "schemeName" : "COID",
      "issuer" : "ACPR"
   }
},
"paymentTypeInformation" : {
   "serviceLevel" : "SEPA",
   "localInstrument" : "INST",
   "categoryPurpose" : "DVPM"
},
"debtor" : {
   "name" : "MyCustomer",
   "postalAddress" : {
      "country" : "FR",
      "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
   },
   "privateId" : {
      "identification" : "FD37G",
      "schemeName" : "BANK",
      "issuer" : "BICXYYTTZZZ"
   }
},
"debtorAgent" : {
   "bicFi" : "BNKAFRPPXXX"
},
"creditor" : {
```

```
      "name" : "myMerchant",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "852126789",
        "schemeName" : "SIREN",
        "issuer" : "FR"
      }
    },
    "creditorAccount" : {
      "iban" : "YY64COJH4105954533022295696077132l"
    },
    "ultimateCreditor" : {
      "name" : "myPreferedUltimateMerchant",
      "postalAddress" : {
        "country" : "FR",
        "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
        "identification" : "85212678900025",
        "schemeName" : "SIRET",
        "issuer" : "FR"
      }
    },
    "purpose" : "COMC",
    "chargeBearer" : "SLEV",
    "paymentInformationStatus" : "ACSC",
    "creditTransferTransaction" : [ {
      "paymentId" : {
        "instructionId" : "MyInstrId",
        "endToEndId" : "MyEndToEndId"
      },
      "requestedExecutionDate" : "2016-12-30T23:00:00.000Z",
```

```
        "instructedAmount" : {
          "currency" : "EUR",
          "amount" : "124.35"
        },
        "remittanceInformation" : [ "MyRemittanceInformation" ],
        "transactionStatus" : "ACSC"
      } ],
      "supplementaryData" : {
        "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
        "appliedScaApproach" : "EMBEDDED",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
    },
    "_links" : {
      "self" : {
        "href" : "v1/payment-requests/MyPmtInfRscId"
      }
    }
}
```


9.4. Transfer Request

9.4.1. Request

```
POST http://localhost:8080/v1/transfer-requests
```

9.4.1.1. Headers

```
Date: 2018-04-01T19:48:21.053+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
```

```
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=qXkp/DAYItQF8d5aHKaPWHyml0AyzBRSWvgFDfPkXQU=
Content-Length: 744
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="tdq1jLYddEwBPlZbFe7M72i0CjhW7ppwII8lzW72om2J6c4rGWpqrZzZAAxm
ovXIFhsbFPBdDid0wXeyx+NDmOiRbRjJ2OGqUnaG4vaHi7VH+kLFq6/PzhhrANhR/YrZIkfpeY
YqkOrOAEM1HeAuDa+E/uitY7ZstLQ2+ckbBBw="
```

9.4.1.2. Body

```
{
   "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
         "identification" : "FD37G",
         "schemeName" : "BANK",
         "issuer" : "BICXYYTTZZZ"
```

```
      }
   },
   "creditor" : {
      "name" : "myMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "852126789",
         "schemeName" : "SIREN",
         "issuer" : "FR"
      }
   },
   "creditorAccount" : {
      "iban" : "YY64COJH41059545330222956960771321"
   },
   "instructedAmount" : {
      "currency" : "EUR",
      "amount" : "124.35"
   },
   "remittanceInformation" : [ "MyRemittanceInformation" ],
   "supplementaryData" : {
      "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
      "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
   }
}
```


9.4.2. Response

```
Status code: 201
```

9.4.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
location: v1/transfer-requests/MyTransferRscId
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.4.2.2. Body

```
{
   "appliedScaApproach" : "EMBEDDED"
}
```

9.5. Transfer Request Retrieval

9.5.1. Request

```
GET http://localhost:8080/v1/transfer-requests/MyTransferRscId
```

9.5.1.1. Headers

```
Date: 2018-04-01T19:48:21.072+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
Digest:
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
```

```
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
User-Agent: Swagger-Codegen/1.0.0/java
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location digest x-
request-id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-
encoding psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type
user-agent (request-
target)",signature="jTOoMYoeG7dMhsna+kORljgOQOkJk7zhuWxt+l5U7ykfOSIAFpcAkkJ4kyD
SnrRyqIL9H6jiyP80ulrg/2ml0/ggjRBK+QNujuBY2otv5ZFNJmvL7KBjiFqQq0VED57CA5uw6E+8
RDzQn9yfHrf9+GH5qdpPAJaM4V2LN54P60M="
```

9.5.1.2. Body

No body data

9.5.2. Response

```
Status code: 200
```

9.5.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.5.2.2. Body

```
{
  "transferRequest" : {
    "debtor" : {
      "name" : "MyCustomer",
      "postalAddress" : {
        "country" : "FR",
```

```
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "privateId" : {
            "identification" : "FD37G",
            "schemeName" : "BANK",
            "issuer" : "BICXYYTTZZZ"
        }
    },
    "creditor" : {
        "name" : "myMerchant",
        "postalAddress" : {
            "country" : "FR",
            "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
        },
        "organisationId" : {
            "identification" : "852126789",
            "schemeName" : "SIREN",
            "issuer" : "FR"
        }
    },
    "creditorAccount" : {
        "iban" : "YY64COJH41059545330222956960771321"
    },
    "transferInformationStatus" : "ACSC",
    "instructedAmount" : {
        "currency" : "EUR",
        "amount" : "124.35"
    },
    "remittanceInformation" : [ "MyRemittanceInformation" ],
    "supplementaryData" : {
        "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
        "appliedScaApproach" : "EMBEDDED",
        "successfulReportUrl" : "http://myPisp/PaymentSuccess",
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
    }
```

```
  },
  "_links" : {
    "self" : {
      "href" : "v1/transfer-requests/MyTransferRscId"
    },
    "confirmation" : {
      "href" : "v1/transfer-requests/MyTransferRscId/confirmation"
    }
  }
}
```

9.6. Transfer Request Confirmation

9.6.1. Request

```
POST http://localhost:8080/v1/transfer-requests/MyTransferRscId/confirmation
```

9.6.1.1. Headers

```
Date: 2018-04-01T19:48:21.087+02:00
PSU-Date: 2017-06-08T09:33:55.954+02:00
Accept: application/hal+json; charset=utf-8
PSU-GEO-Location: GEO:52.506931,13.144558
X-Request-ID: GGF3YUD3BDJK
PSU-Referer: http://en.wikipedia.org/wiki/Main_Page
PSU-IP-Port: 12345
PSU-Accept: text/plain
Authorization: authorization_example
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip, deflate
PSU-IP-Address: 10.10.10.10
PSU-User-Agent: Mozilla
PSU-HTTP-Method: POST
PSU-Accept-Language: en-US
Content-Type: application/json
```

```
User-Agent: Swagger-Codegen/1.0.0/java
Digest: SHA-256=P871WCcozbO2Mk3em1hL6Dw4hTTTZEoi21jII62lHc4=
Content-Length: 46
Signature: keyId="SN=123,CA=CN = PSD2-CORE ROOT CA, OU = DEMO, O =
MYQTSP",algorithm="rsa-sha256",headers="date psu-date accept psu-geo-location x-request-
id psu-referer psu-ip-port psu-accept authorization psu-accept-charset psu-accept-encoding
psu-ip-address psu-user-agent psu-http-method psu-accept-language content-type user-agent
digest content-length (request-
target)",signature="NSOptpIBmLHhw1MfJ69qt2STW/5UdI3wAxFAfsgkDoIp3EsO1ALULHoA3w
vX66dWvWpcz3Jx6Z9FC/32ugGRGA+WDRTCYH7CA4inrPz2+BsaklwW41iYW1dZIcu34bN0h
uq8qDRDB3Njmsqw3HNfjDv1e3LHm5SoWvEaiF+mt7c="
```

9.6.1.2. Body

```
{
   "psuAuthenticationFactor" : "JJKJKJ788GKJKJBK"
}
```

9.6.2. Response

```
Status code: 200
```

9.6.2.1. Headers

```
X-Request-ID: GGF3YUD3BDJK
Content-Type: application/hal+json;charset=UTF-8
Transfer-Encoding: chunked
Date: Sun, 01 Apr 2018 17:48:20 GMT
```

9.6.2.2. Body

```
{
   "transferRequest" : {
      "debtor" : {
         "name" : "MyCustomer",
```

```
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "privateId" : {
         "identification" : "FD37G",
         "schemeName" : "BANK",
         "issuer" : "BICXYYTTZZZ"
      }
   },
   "creditor" : {
      "name" : "myMerchant",
      "postalAddress" : {
         "country" : "FR",
         "addressLine" : [ "18 rue de la DSP2", "75008 PARIS" ]
      },
      "organisationId" : {
         "identification" : "852126789",
         "schemeName" : "SIREN",
         "issuer" : "FR"
      }
   },
   "creditorAccount" : {
      "iban" : "YY64COJH41059545330222956960771321"
   },
   "transferInformationStatus" : "ACSC",
   "instructedAmount" : {
      "currency" : "EUR",
      "amount" : "124.35"
   },
   "remittanceInformation" : [ "MyRemittanceInformation" ],
   "supplementaryData" : {
      "acceptedScaApproach" : [ "EMBEDDED", "REDIRECT" ],
      "appliedScaApproach" : "EMBEDDED",
      "successfulReportUrl" : "http://myPisp/PaymentSuccess",
```

```
        "unsuccessfulReportUrl" : "http://myPisp/PaymentFailure"
      }
   },
   "_links" : {
      "self" : {
         "href" : "v1/transfer-requests/MyTransferRscId"
      }
   }
}
```