STET PSD2 API

Documentation Part 2: Functional Model

Author: Robache Hervé

Date: 2019-01-15

Version: 1.4.1.3 (English)

Table of content

4. Functional Model

4.1. Generic Structures

Some structures are generic and common to several request or response data.

4.1.1. AccountIdentification

FIELD	MULT.	DESC.
		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. API: The ASPSP will document which account reference type it will support.
identification	[1..1]	API: Identifier
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 Each implementation of the STET PSD2 API must specify in its own documentation which schemes can actually been used
issuer	[0..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
currency	[0..1]	Specifies the currency of the amount or of the 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".

4.1.2. FinancialInstitutionIdentification

FIELD	MULT.	DESC.
		ISO20022: Unique and unambiguous identification of a financial institution, as assigned under an internationally recognised or proprietary identification scheme.
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)".
clearingSystemMemberId	[0..1]	ISO20022: Information used to identify a member within a clearing system. API: to be used for some specific international credit transfers in order to identify the beneficiary bank
clearingSystemId	[0..1]	ISO20022: Specification of a pre-agreed offering between clearing agents or the channel through which the payment instruction is processed.
memberId	[0..1]	ISO20022: Identification of a member of a clearing system.
name	[0..1]	Name of the financial institution
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. For SEPA payments, only two address lines are allowed.
{arrayItem}	[0..2]	Address line

4.1.3. GenericIdentification

FIELD	MULT.	DESC.
		ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer. API: The ASPSP will document which account reference type it will support.
identification	[1..1]	API: Identifier
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 Each implementation of the STET PSD2 API must specify in its own documentation which schemes can actually been used
issuer	[0..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

4.1.4. GenericLink

FIELD	MULT.	DESC.
		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

4.1.5. PartyIdentification

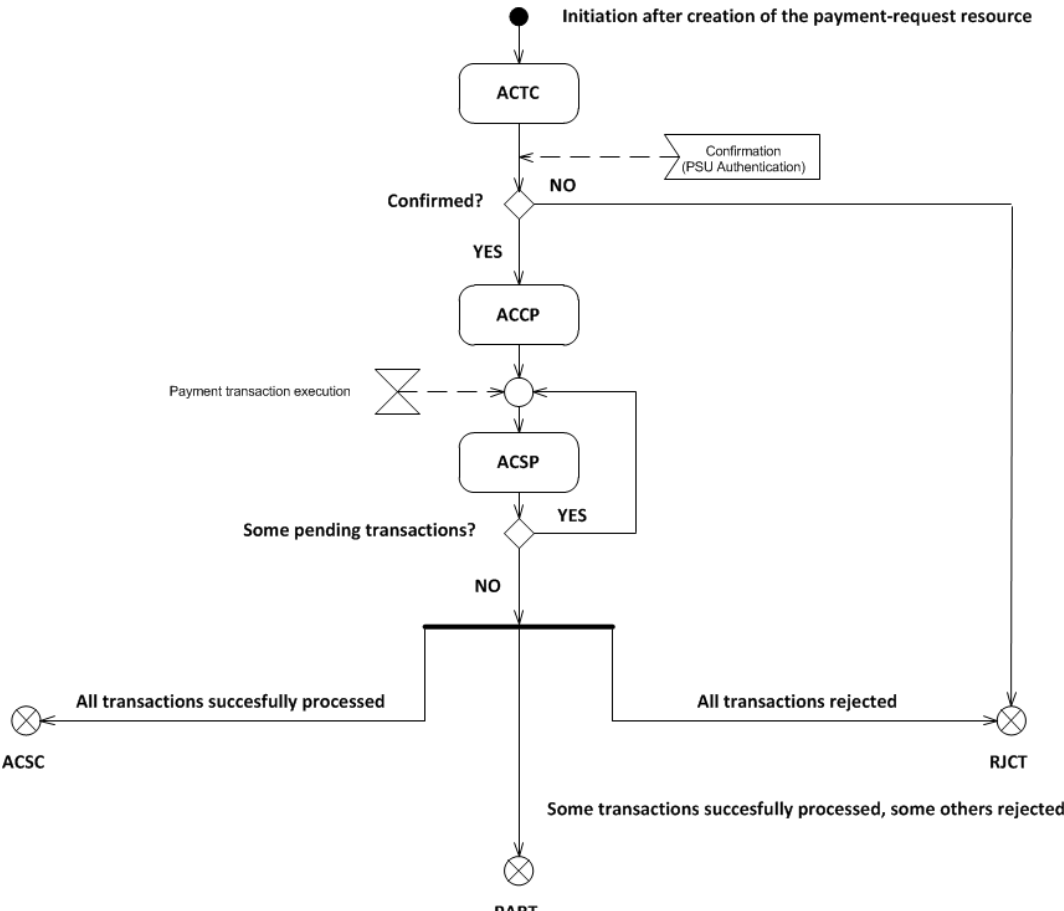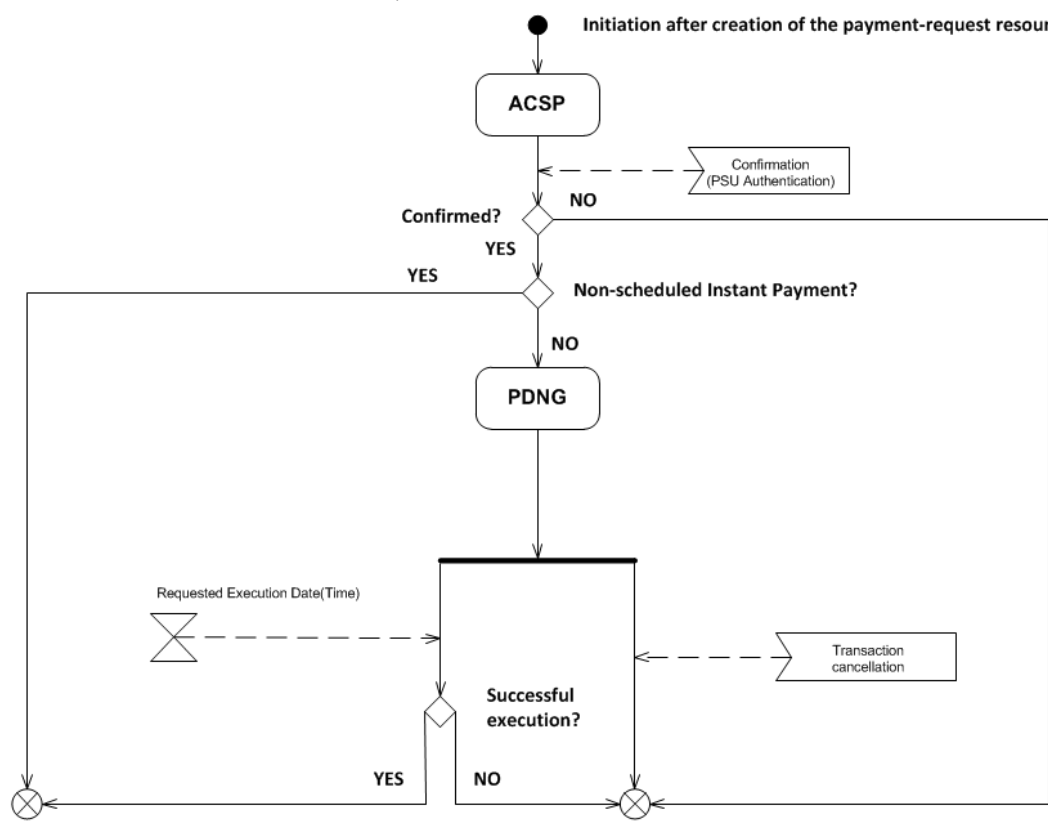| FIELD			MULT.	DESC.
				API : Description of a Party which can be either a person or an organization.
name			[1..1]	ISO20022: Name by which a party is known and which is usually used to identify that party.
postalAddress			[0..1]	ISO20022 : Information that locates and identifies a specific address, 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. For SEPA payments, only two address lines are allowed.
		{arrayItem}	[0..2]	Address line
organisationId			[0..1]	ISO20022: Unique identification of an account, a person or an organisation, as assigned by an issuer. API: The ASPSP will document which account reference type it will support.
	identification		[1..1]	API: Identifier
	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 Each implementation of the STET PSD2 API must specify in its own documentation which schemes can actually been used
	issuer		[0..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. API: The ASPSP will document which account reference type it will support.
	identification		[1..1]	API: Identifier
	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 Each implementation of the STET PSD2 API must specify in its own documentation which schemes can actually been used
	issuer		[0..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

4.1.6. PaymentInformationStatusCode

FIELD	MULT.	DESC.
		ISO20022: Specifies the status of the payment information.

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.

- PART (PartiallyAccepted): A number of transactions have been accepted, whereas another number of transactions have not yet achieved 'accepted' status.

- 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.

4.1.7. TransactionIndividualStatusCode

FIELD	MULT.	DESC.
		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

4.2. Retrieval of the PSU accounts (AISP)

4.2.1. Description

This call returns all payment accounts that are relevant the PSU on behalf of whom the AISP is connected.

Thanks to HYPERMEDIA, each account is returned with the links aiming to ease access to the relevant transactions and balances.

The result may be subject to pagination (i.e. retrieving a partial result in case of having too many results) through a set of pages by the ASPSP. Thereafter, the AISP may ask for the first, next, previous or last page of results.

4.2.2. 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.

4.2.3. Business Flow

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

The ASPSP computes 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 payment account will be provided with its characteristics.

4.2.4. Request

```
get /accounts
```

No Path, Query or Body parameter are specified for this API call.

4.2.5. Response

4.2.5.1. Body (application/hal+json; charset=utf-8)

FIELD					MULT.	DESC.
{responseBody}					[1..1]	HYPERMEDIA structure used for returning the list of the available accounts to the AISP
	accounts				[1..1]	List of PSU account that are made available to the TPP
		{arrayItem}			[0..*]	PSU account that is made available to the TPP
			resourceId		[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
			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)".
			accountId		[0..1]	See generic structure AccountIdentification
			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
			details		[0..1]	Specifications that might be provided by the ASPSP - characteristics of the account - characteristics of the relevant card
			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.
			usage		[0..1]	Specifies the usage of the account - PRIV: private personal account - ORGA: professional account
			cashAccountType		[1..1]	Specifies the type of the account - CACC: Cash account - CARD: List of card based transactions
			product		[0..1]	Product Name of the Bank for this account, proprietary definition
			balances		[0..1]	list of balances provided by the ASPSP
			{arrayItem}		[1..*]	Structure of an account balance
				name	[1..1]	Label of the balance
				balanceAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.
				currency	[1..1]	Specifies the currency of the amount or of the 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]	See generic structure GenericLink
				transactions	[0..1]	See generic structure GenericLink
	_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]	See generic structure GenericLink
		endUserIdentity			[0..1]	See generic structure GenericLink
		beneficiaries			[0..1]	See generic structure GenericLink
		first			[0..1]	See generic structure GenericLink
		last			[0..1]	See generic structure GenericLink
		next			[0..1]	See generic structure GenericLink
		prev			[0..1]	See generic structure GenericLink

4.3. Retrieval of an account balances report (AISP)

4.3.1. Description

This call returns a set of balances for a given PSU account that is specified by the AISP through an account resource Identification

4.3.2. 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.
- The TPP has previously retrieved the list of available accounts for the PSU

4.3.3. Business flow

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

The ASPSP answers by providing a list of balances on this account.

- The ASPSP must provide at least the accounting balance on the account.
- The ASPSP can provide other balance restitutions, e.g. instant balance, as well, if possible.
- Actually, from the PSD2 perspective, any other balances that are provided through the Web-Banking service of the ASPSP must also be provided by this ASPSP through the API.

4.3.4. Request

```
get /accounts/{accountResourceId}/balances
```

4.3.4.1. Path Parameters

FIELD	MULT.	DESC.
accountResourceId	[1..1]	Identification of account resource to fetch

4.3.5. Response

4.3.5.1. Body (application/hal+json; charset=utf-8)

FIELD	MULT.	DESC.
{responseBody}	[1..1]	HYPERMEDIA structure used for returning the list of the relevant balances for a given account to the AISP
balances	[1..1]	List of account balances
{arrayItem}	[1..*]	Structure of an account balance
name	[1..1]	Label of the balance
balanceAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.
currency	[1..1]	Specifies the currency of the amount or of the 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]	See generic structure GenericLink
parent-list	[0..1]	See generic structure GenericLink
transactions	[0..1]	See generic structure GenericLink

4.4. Retrieval of an account transaction set (AISP)

4.4.1. Description

This call returns transactions for an account for a given PSU account that is specified by the AISP through an account resource identification.
The request may use some filter parameter in order to restrict the query

- on a given imputation date range
- past a given incremental technical identification

The result may be subject to pagination (i.e. retrieving a partial result in case of having too many results) through a set of pages by the ASPSP. Thereafter, the AISP may ask for the first, next, previous or last page of results.

4.4.2. 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

- o 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.
- The TPP has previously retrieved the list of available accounts for the PSU

4.4.3. 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.

4.4.4. Request

get /accounts/{accountResourceId}/transactions

4.4.4.1. Path Parameters

FIELD	MULT.	DESC.
accountResourceId	[1..1]	Identification of account resource to fetch

4.4.4.2. Query Parameters

FIELD	MULT.	DESC.
dateFrom	[0..1]	Inclusive minimal imputation date of the transactions. Transactions having an imputation date equal to this parameter are included within the result.
dateTo	[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

4.4.5. Response

4.4.5.1. Body (application/hal+json; charset=utf-8)

FIELD	MULT.	DESC.
{responseBody}	[1..1]	HYPERMEDIA structure used for returning the list of the transactions for a given account to the AISP
transactions	[1..1]	List of transactions
{arrayItem}	[0..*]	structure of a transaction
resourceId	[0..1]	API: Identifier assigned by the ASPSP for further use of the created resource through API calls
entryReference	[0..1]	Technical incremental identification of the transaction.
transactionAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.

			FIELD	MULT.	DESC.
			currency	[1..1]	Specifies the currency of the amount or of the 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 amount - CRDT: Credit type amount - DBIT: Debit type amount
			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 If the transaction is not yet booked. This field must be valued with a scheduled booking date.
			valueDate	[0..1]	Value date of the transaction on the account
			transactionDate	[0..1]	Date used for specific purposes: - for card transaction: date of the transaction - for credit transfer: acquiring date of the transaction - for direct debit: receiving date of the transaction
			remittanceInformation	[0..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
			{arrayItem}	[0..*]	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]	See generic structure GenericLink
		parent-list		[0..1]	See generic structure GenericLink
		balances		[0..1]	See generic structure GenericLink
		first		[0..1]	See generic structure GenericLink
		last		[0..1]	See generic structure GenericLink
		next		[0..1]	See generic structure GenericLink
		prev		[0..1]	See generic structure GenericLink

4.5. Forwarding the PSU consent (AISP)

4.5.1. Description

In the mixed detailed consent on accounts

- the AISP captures the consent of the PSU
- then it forwards this consent to the ASPSP

This consent replaces any prior consent that was previously sent by the AISP.

4.5.2. 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

o 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.

4.5.3. Business Flow

The PSU specifies to the AISP which of his/her accounts will be accessible and which

functionalities should be available.

The AISP forwards these settings to the ASPSP.

The ASPSP answers by HTTP201 return code.

4.5.4. Request

`put /consents`

4.5.4.1. Body (application/json)

FIELD	MULT.	DESC.
{requestBody}	[0..1]	Requested access services.
balances	[1..1]	List of accessible accounts for one given functionality
{arrayItem}	[0..*]	See generic structure AccountIdentification
transactions	[1..1]	List of accessible accounts for one given functionality
{arrayItem}	[0..*]	See generic structure AccountIdentification
trustedBeneficiaries	[1..1]	Indicator that access to the trusted beneficiaries list was granted or not to the AISP by the PSU - true: the access was granted - false: the access was not granted
psuIdentity	[1..1]	Indicator that access to the PSU identity, first name and last name, was granted or not to the AISP by the PSU - true: the access was granted - false: the access was not granted

4.5.5. Response

4.6. Retrieval of the identity of the end-user (AISP)

4.6.1. Description

This call returns the identity of the PSU (end-user).

4.6.2. 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

- o 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.

4.6.3. Business Flow

The AISP asks for the identity of the PSU.

The ASPSP answers with the identity, i.e. first and last names of the end-user.

4.6.4. Request

```
get /end-user-identity
```

No Path, Query or Body parameter are specified for this API call.

4.6.5. Response

4.6.5.1. Body (application/hal+json; charset=utf-8)

FIELD			MULT.	DESC.
{responseBody}			[1..1]	HYPERMEDIA structure used for returning the identity of the PSU
	connectedPsu		[1..1]	Last name and first name that has granted access to the AISP on the accounts data This information can be retrieved based on the PSU's authentication that occurred during the OAUTH2 access token initialisation.
	_links		[1..1]	links that can be used for further navigation when browsing Account Information at one account level - self: link to the end-user identity - parent-list: link to the list of all available accounts
		self	[1..1]	See generic structure GenericLink
		parent-list	[0..1]	See generic structure GenericLink

4.7. Retrieval of the trusted beneficiaries list (AISP)

4.7.1. Description

This call returns all trusted beneficiaries that have been set by the PSU.

Those beneficiaries can benefit from an SCA exemption during payment initiation.

The result may be subject to pagination (i.e. retrieving a partial result in case of having too many results) through a set of pages by the ASPSP. Thereafter, the AISP may ask for the first, next, previous or last page of results.

4.7.2. 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 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 ASPSP takes into account the access token that establishes the link between the PSU and the AISP.

4.7.3. Business Flow

The AISP asks for the trusted beneficiaries list.

The ASPSP answers with a list of beneficiary details structure.

4.7.4. Request

```
get /trusted-beneficiaries
```

No Path, Query or Body parameter are specified for this API call.

4.7.5. Response

4.7.5.1. Body (application/hal+json; charset=utf-8)

FIELD				MULT.	DESC.
{responseBody}				[1..1]	HYPERMEDIA structure used for returning the list of the whitelisted beneficiaries
	beneficiaries			[1..1]	List of trusted beneficiaries
		{arrayItem}		[0..*]	Specification of a beneficiary
			id	[0..1]	Id of the beneficiary
			isTrusted	[0..1]	The ASPSP having not implemented the trusted beneficiaries list must not set this flag. Otherwise, the ASPSP indicates whether or not the beneficiary has been registered by the PSU within the trusted beneficiaries list. - true: the beneficiary is actually a trusted beneficiary - false: the beneficiary is not a trusted beneficiary
			creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
			creditor	[1..1]	See generic structure PartyIdentification
			creditorAccount	[0..1]	See generic structure AccountIdentification
		_links		[1..1]	links that can be used for further navigation when browsing Account Information at one account level - self: link to the beneficiaries - parent-list: link to the list of all available accounts - first: link to the first page of the beneficiaries result - last: link to the last page of the beneficiaries result - next: link to the next page of the beneficiaries result - prev: link to the previous page of the beneficiaries result
			self	[1..1]	See generic structure GenericLink
			parent-list	[0..1]	See generic structure GenericLink
			first	[0..1]	See generic structure GenericLink

		FIELD	MULT.	DESC.
		last	[0..1]	See generic structure GenericLink
		next	[0..1]	See generic structure GenericLink
		prev	[0..1]	See generic structure GenericLink

4.8. Payment coverage check request (CBPII)

4.8.1. Description

The CBPII can ask an ASPSP to check if a given amount can be covered by the liquidity that is available on a PSU cash account or payment card.

4.8.2. Prerequisites

- The TPP has been registered by the Registration Authority for the CBPII role
- The TPP and the PSU have a contract that has been registered by the ASPSP
  - At this step, the ASPSP has delivered an "Authorization Code", a "Resource Owner Password" or a "Client Credential" OAUTH2 access token to the TPP (cf. § 3.4.2).
  - Each ASPSP has to implement either the "Authorization Code"/"Resource Owner Password" or the "Client Credential" OAUTH2 access token model.
  - Doing this, it will edit the [security] section on this path in order to specify which model it has chosen
- The TPP and the ASPSP have successfully processed a mutual check and authentication
- The TPP has presented its OAUTH2 "Authorization Code", "Resource Owner Password" or "Client Credential" access token which allows the ASPSP to identify the relevant PSU.

4.8.3. Business flow

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

The ASPSP answers with a structure embedding the original request and the result as a Boolean.

4.8.4. Request

post /funds-confirmations

4.8.4.1. Body (application/json)

FIELD			MULT.	DESC.
{requestBody}			[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]	Structure aiming to embed the amount and the currency to be used.
		currency	[1..1]	Specifies the currency of the amount or of the 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]	See generic structure AccountIdentification

4.8.5. Response

4.8.5.1. Body (application/hal+json; charset=utf-8)

FIELD				MULT.	DESC.
{responseBody}				[1..1]	HYPERMEDIA structure used for returning the payment coverage report to the CBPII
	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]	Structure aiming to embed the amount and the currency to be used.
			currency	[1..1]	Specifies the currency of the amount or of the 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]	See generic structure AccountIdentification
	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]	See generic structure GenericLink

4.9. Payment request initiation (PISP)

4.9.1. Description

The following use cases can be applied:

- payment request on behalf of a merchant
- transfer request on behalf of the account's owner
- standing-order request on behalf of the account's owner

4.9.1.1. Data content

A payment request or a transfer request might embed several payment instructions having

- one single execution date or multiple execution dates
  - case of one single execution date, this date must be set at the payment level
  - case of multiple execution dates, those dates must be set at each payment instruction level

- one single beneficiary or multiple beneficiaries
  - case of one single beneficiary, this beneficiary must be set at the payment level
  - case of multiple beneficiaries, those beneficiaries must be set at each payment instruction level

Having at the same time multiple beneficiaries and multiple execution date might not be a relevant business case, although it is technically allowed.

Each implementation will have to specify which business use cases are actually supported.

A standing order request must embed one single payment instruction and must address one single beneficiary.

- The beneficiary must be set at the payment level
- The standing order specific characteristics (start date, periodicity...) must be set at the instruction level

Payment request can rely for execution on different payment instruments:

- SEPA Credit Transfer (SCT)

- Domestic Credit Transfer in a non Euro-currency

- International payment

The following table indicates how to use the different fields, depending on the payment instrument:

STRUCTURE	SEPA PAYMENTS	DOMESTIC PAYMENTS IN NON-EURO CURRENCY	INTERNATIONAL PAYMENTS
PaymentTypeInformation/ InstructionPriority (payment level)	"HIGH" for high-priority SCT "NORM" for other SCT Ignored for SCTInst	"HIGH" for high-priority CT "NORM" or ignored for other CT	"HIGH" for high-priority payments "NORM" or ignored for other payments
PaymentTypeInformation/ ServiceLevel (payment level)	"SEPA" for SCT and SCTInst	ignored	ignored
PaymentTypeInformation/ CategoryPurpose (payment level)	"CASH" for transfer request "DVPM" for payment request on behalf of a merchant		"CORT" for generic international payments "INTC" for transfers between two branches within the same company "TREA" for treasury transfers
PaymentTypeInformation/ LocalInstrument (payment level)	"INST" pour les SCTInst Otherwise ignored	ignored or valued with ISO20022 external code list values	
RequestedExecutionDate (either at payment or transaction level)	Mandatory (indicates the date on debit on the ordering party account)		
InstructedAmount (at each transaction level)	Mandatory		
ChargeBearer (at each transaction level)	"SLEV" for SCT and SCTInst	"SLEV" or "SHAR"	"CRED", "DEBT" or "SHAR"
Purpose (at payment level)	Optional		
RegulatoryReportingCode (at each transaction level)	Not used		Mandatory (possibly multiple values)
RemittanceInformation	Optional Unstructured		
Debtor (at payment level)	Mandatory 2 address lines only	Mandatory 4 address lines only	
DebtorAccount (at payment level)	Optional	Optional Account currency may be specified	
DebtorAgent (at payment level)	Optional		
Creditor (either at payment or transaction level)	Mandatory 2 address lines only		
CreditorAccount (either at payment or transaction level)	Mandatory	Mandatory Account currency may be specified	
CreditorAgent (either at payment or transaction level)	Optional		
UltimateCreditor (either at payment or transaction level)	Optional		
ClearingSystemId et ClearingSystemMemberId (either at payment or transaction level)	Not used		Optional

4.9.1.2. Prerequisites for all use cases

- 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

4.9.1.3. Business flow

Payment Request use case

The PISP forwards a payment request on behalf of a merchant.

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.
- The Request can embed several payment instructions having different requested execution date.
- The beneficiary, as being the merchant, is set at the payment level.

Transfer Request use case

The PISP forwards a transfer request on behalf of the owner of the account.

- 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.
- The Request can embed several payment instructions having different beneficiaries.
- The requested execution date, as being the same for all instructions, is set at the payment level.

Standing Order Request use case

The PISP forwards a Standing Order request on behalf of the owner of the account.

- The PSU provides the PISP with all information needed for the Standing Order.
- The PISP prepares the Standing Order Request and sends this request to the relevant ASPSP that holds the debtor account.
- The Request embeds one single payment instruction with
  - The requested execution date of the first occurrence
  - The requested execution frequency of the payment in order to compute further execution dates
  - An execution rule to handle cases when the computed execution dates cannot be processed (e.g. bank holydays)
  - An optional end date for closing the standing Order

4.9.1.4. Authentication flows for all use cases

As the request posted by the PISP to the ASPSP needs a PSU authentication before execution, this request will include:

- The specification of the authentication approaches that are supported by the PISP (any combination of "REDIRECT", "EMBEDDED" and "DECOUPLED" values).
- In case of possible REDIRECT or DECOUPLED authentication 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.
- In case of possible "EMBEDDED" or "DECOUPLED" approaches, the PSU identifier that can be processed by the ASPSP for PSU recognition must have been set within the request body [debtor] structure.

The ASPSP saves the request and answers to the PISP. The answer embeds:

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

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

Redirect authentication approach

When the chosen authentication 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
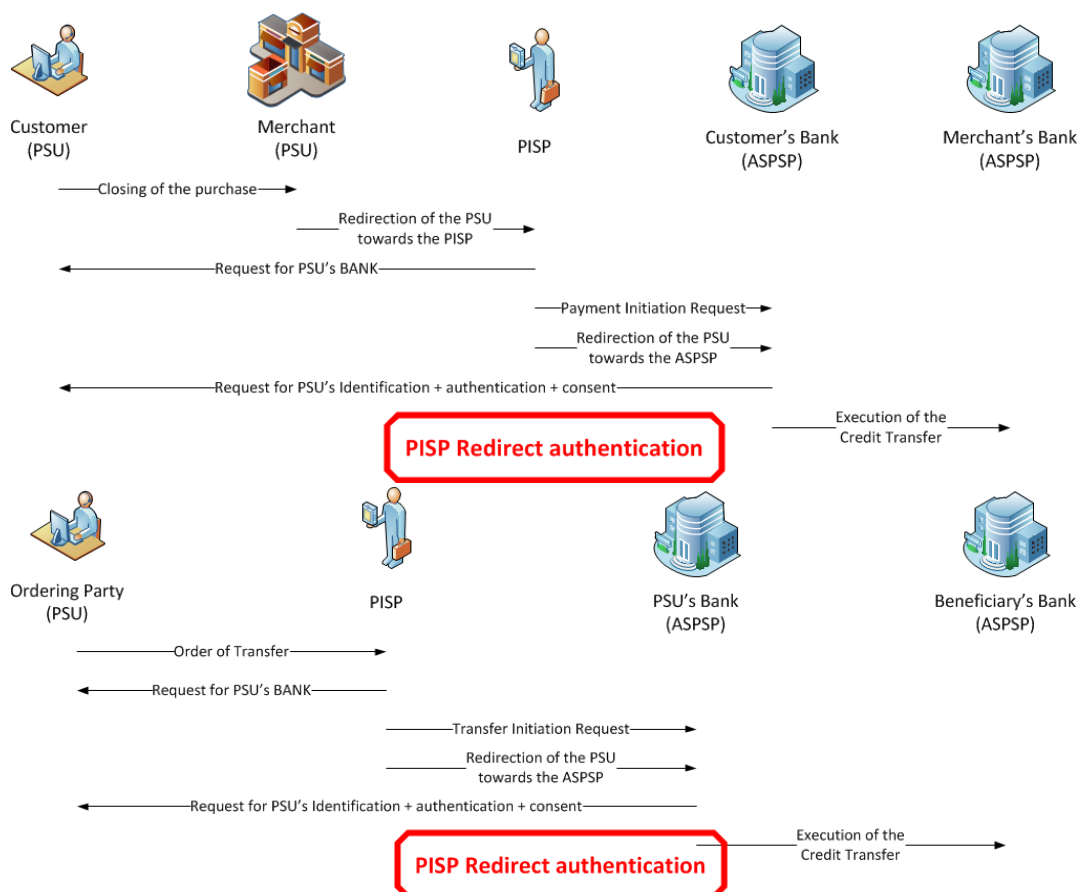
Decoupled authentication approach

When the chosen authentication 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
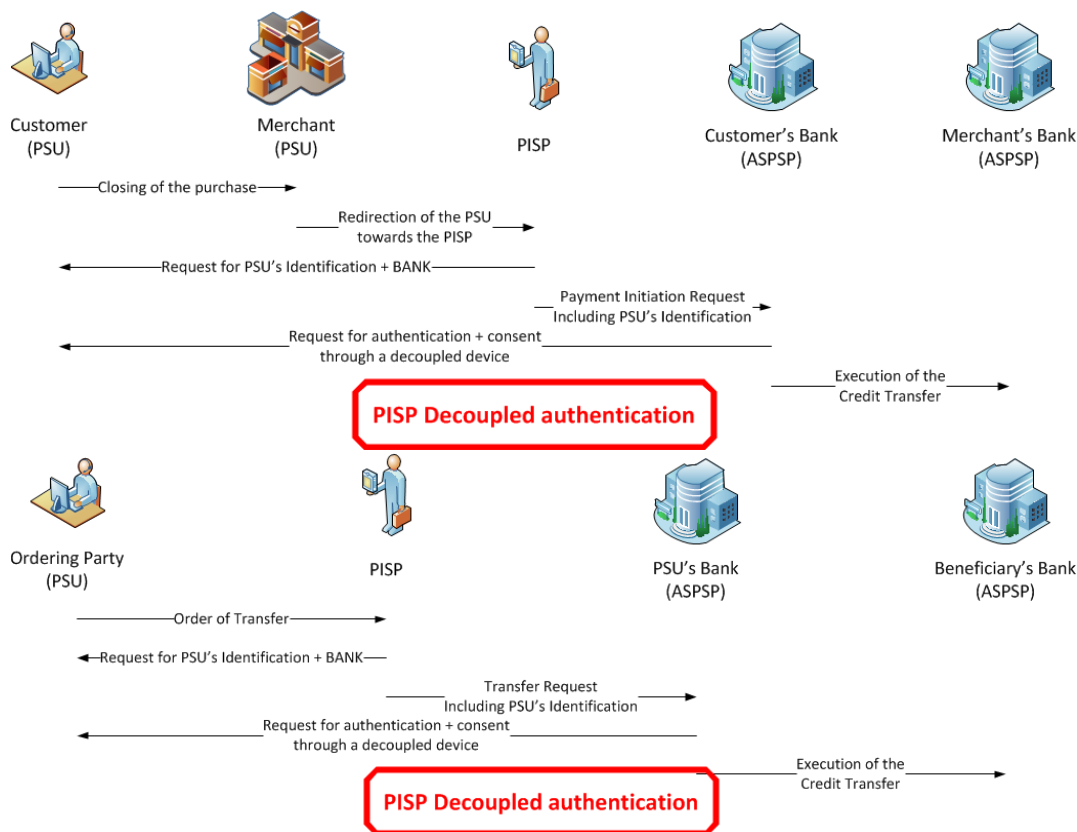
Embedded authentication approach

When the chosen authentication 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)
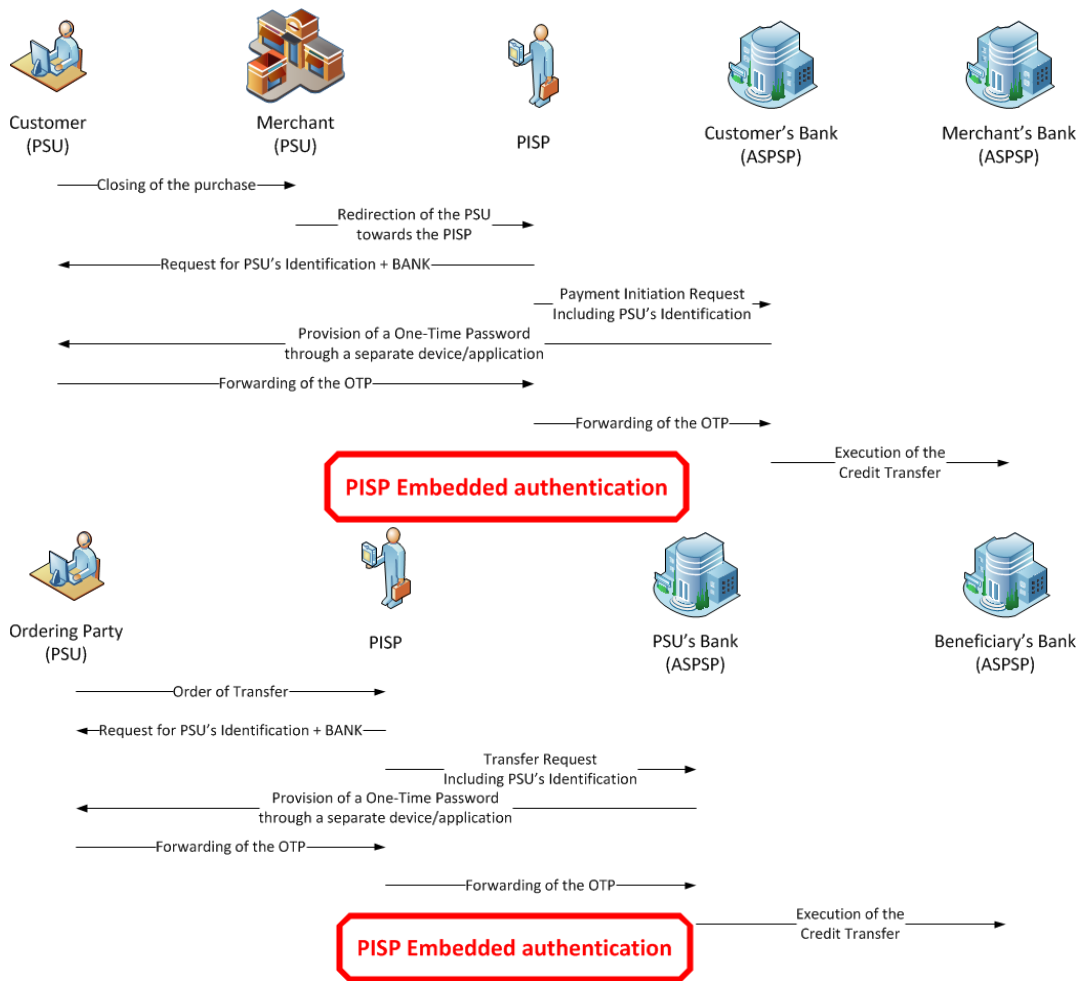
4.9.2. Request

post /payment-requests

4.9.2.1. Body (application/json)

FIELD	MULT.	DESC.
{requestBody}	[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. API: Information about the creditor (Id, account and agent) might be placed either at payment level or at instruction level. Thus multi-beneficiary payments can be handled. The requested execution date can be placed either at payment level when all instructions are requested to be executed at the same date or at instruction level. The latest case includes: - multiple instructions having different requested execution dates - standing orders settings
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. API: Each ASPSP will specify a maximum value for this field taking into accounts its specificities about payment request handling
initiatingParty	[1..1]	See generic structure PartyIdentification

FIELD	MULT.	DESC.
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. API: This field is useless for SCTInst and thus should be ignored.
serviceLevel	[0..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) value is 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: "INST" value is to be used in order to ask for an SEPA instant Payment (SCTInst). For International payments, this field may be valued with one of the ISO20022 external code to specify with payment instrument should be used by the creditor's bank.
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:

CodeName	Name	Definition
CASH	CashManagementTransfer	Transaction is a general cash management instruction.
CORT	TradeSettlementPayment	Transaction is related to settlement of a trade, eg a foreign exchange deal or a securities transaction.
DVPM	DeliverAgainstPayment	Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction.
INTC	IntraCompanyPayment	Transaction is an intra-company payment, ie, a payment between two companies belonging to the same group.
TREA	TreasuryPayment	Transaction is related to treasury operations. E.g. financial contract settlement.

FIELD	MULT.	DESC.
debtor	[0..1]	See generic structure PartyIdentification
debtorAccount	[0..1]	See generic structure AccountIdentification
debtorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
beneficiary	[0..1]	Specification of a beneficiary
id	[0..1]	Id of the beneficiary
creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
creditor	[1..1]	See generic structure PartyIdentification
creditorAccount	[0..1]	See generic structure AccountIdentification
ultimateCreditor	[0..1]	See generic structure PartyIdentification
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

FIELD				MULT.	DESC.
chargeBearer				[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. The following values are allowed:

CodeName	Name	Definition
DEBT	BorneByDebtor	All transaction charges are to be borne by the debtor.
CRED	BorneByCreditor	All transaction charges are to be borne by the creditor.
SHAR	Shared	In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor.
SLEV	FollowingServiceLevel	Charges are to be applied following the rules agreed in the service level and/or scheme.

FIELD				MULT.	DESC.
	requestedExecutionDate			[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
	creditTransferTransaction			[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API: Each ASPSP will specify a maxItems value for this field taking into accounts its specificities about payment request handling
		{arrayItem}		[1..*]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API:
		paymentId		[1..1]	ISO20022: Set of elements used to reference a payment instruction.
			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	[0..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.
			requestedExecutionDate	[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment. API: This field indicates the date at which the debtor account should be debited. In most of the cases, especially for international payments, the date of the credit on the credit account cannot be set. Only SCTInst can guarantee having the same date for this credit. This date can be used in the following cases: - the single requested execution date for a payment having several instructions. In this case, this field must be set at the payment level. - the requested execution date for a given instruction within a payment. In this case, this field must be set at each instruction level. - The first date of execution for a standing order. When the payment cannot be processed at this date, the ASPSP is allowed to shift the applied execution date to the next possible execution date for non-standing orders. For standing orders, the [executionRule] parameter helps to compute the execution date to be applied.
			endDate	[0..1]	The last applicable day of execution for a given standing order. If not given, the standing order is considered as endless.
			executionRule	[0..1]	Execution date shifting rule for standing orders This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceding" or "following" working day. ASPSP might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule. - FWNG: following - PREC: preceding

			FIELD		MULT.	DESC.
			frequency		[0..1]	Frequency rule for standing orders.
						The following codes from the "EventFrequency7Code" of ISO 20022 are supported.
						- DAIL: Daily
						- WEEK: Weekly
						- TOWK: EveryTwoWeeks
						- MNTH: Monthly
						- TOMN: EveryTwoMonths
						- QUTR: Quarterly
						- SEMI: SemiAnnual
						- YEAR: Annual
						However, each ASPSP might restrict these values into a subset if needed.
			instructedAmount		[1..1]	Structure aiming to embed the amount and the currency to be used.
				currency	[1..1]	Specifies the currency of the amount or of the 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.
			beneficiary		[0..1]	Specification of a beneficiary
				id	[0..1]	Id of the beneficiary
				creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
				creditor	[1..1]	See generic structure PartyIdentification
				creditorAccount	[0..1]	See generic structure AccountIdentification
			ultimateCreditor		[0..1]	See generic structure PartyIdentification
			regulatoryReportingCodes		[0..1]	List of needed regulatory reporting codes for international payments
				{arrayItem}	[1..10]	Information needed due to regulatory and statutory requirements.
						Economical codes to be used are provided by the National Competent Authority
			remittanceInformation		[0..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
				{arrayItem}	[0..*]	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 authentication approaches are accepted by the PISP and which has been chosen by the ASPSP
			acceptedAuthenticationApproach		[0..1]	can only be set by the PISP
						authentication 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)
				{arrayItem}	[1..*]	combination of possible values for authentication approaches
			scaHint		[0..1]	can only be set by the PISP
						Hint given by the merchant and/or the PISP about an SCA exemption context
			successfulReportUrl		[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the authentication 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 authentication 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

4.9.3. Response

4.9.3.1. Body (application/hal+json; charset=utf-8)

		FIELD	MULT.	DESC.
{responseBody}			[1..1]	data forwarded by the ASPSP top the PISP after creation of the Payment Request resource creation
	appliedAuthenticationApproach		[0..1]	The ASPSP, based on the authentication 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]	See generic structure GenericLink

4.10. Retrieval of a payment request (PISP)

4.10.1. Description

The following use cases can be applied:

- retrieval of a payment request on behalf of a merchant
- retrieval of a transfer request on behalf of the account's owner
- retrieval of a standing-order request on behalf of the account's owner

The PISP has sent a Request through a POST command.

The ASPSP has registered the Request, updated if necessary the relevant identifiers in order to avoid duplicates and returned the location of the updated Request.

The PISP gets the Request that has been updated with the resource identifiers, and eventually the status of the Payment/Transfer Request and the status of the subsequent credit transfer.

4.10.2. 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 Request which has been saved by the ASPSP (cf. § 4.5.3)
  - The ASPSP has answered with a location link to the saved Payment/Transfer 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

4.10.3. Business flow

The PISP asks to retrieve the Payment/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 Payment/Transfer 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.

4.10.4. Request

```
get /payment-requests/{paymentRequestResourceId}
```

4.10.4.1. Path Parameters

FIELD	MULT.	DESC.
paymentRequestResourceId	[1..1]	Identification of the Payment Request Resource

4.10.5. Response

4.10.5.1. Body (application/hal+json; charset=utf-8)

FIELD				MULT.	DESC.
{responseBody}				[1..1]	HYPERMEDIA structure used for returning the original Payment Request to the PISP
	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. API: Information about the creditor (Id, account and agent) might be placed either at payment level or at instruction level. Thus multi-beneficiary payments can be handled. The requested execution date can be placed either at payment level when all instructions are requested to be executed at the same date or at instruction level. The latest case includes: - multiple instructions having different requested execution dates - standing orders settings
		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. API: Each ASPSP will specify a maximum value for this field taking into accounts its specificities about payment request handling
		initiatingParty		[1..1]	See generic structure PartyIdentification
		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. API: This field is useless for SCTInst and thus should be ignored.
			serviceLevel	[0..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) value is 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: "INST" value is to be used in order to ask for an SEPA instant Payment (SCTInst). For International payments, this field may be valued with one of the ISO20022 external code to specify with payment instrument should be used by the creditor's bank.

FIELD			MULT.	DESC.
		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: **CodeName** / **Name** / **Definition** CASH / CashManagementTransfer / Transaction is a general cash management instruction. CORT / TradeSettlementPayment / Transaction is related to settlement of a trade, eg a foreign exchange deal or a securities transaction. DVPM / DeliverAgainstPayment / Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction. INTC / IntraCompanyPayment / Transaction is an intra-company payment, ie, a payment between two companies belonging to the same group. TREA / TreasuryPayment / Transaction is related to treasury operations. E.g. financial contract settlement.
	debtor		[0..1]	See generic structure PartyIdentification
	debtorAccount		[0..1]	See generic structure AccountIdentification
	debtorAgent		[0..1]	See generic structure FinancialInstitutionIdentification
	beneficiary		[0..1]	Specification of a beneficiary
		id	[0..1]	Id of the beneficiary
		isTrusted	[0..1]	The ASPSP having not implemented the trusted beneficiaries list must not set this flag. Otherwise, the ASPSP indicates whether or not the beneficiary has been registered by the PSU within the trusted beneficiaries list. - true: the beneficiary is actually a trusted beneficiary - false: the beneficiary is not a trusted beneficiary
		creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
		creditor	[1..1]	See generic structure PartyIdentification
		creditorAccount	[0..1]	See generic structure AccountIdentification
	ultimateCreditor		[0..1]	See generic structure PartyIdentification
	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

FIELD				MULT.	DESC.
	chargeBearer			[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. The following values are allowed: **CodeName / Name / Definition table:** **DEBT** — BorneByDebtor: All transaction charges are to be borne by the debtor. **CRED** — BorneByCreditor: All transaction charges are to be borne by the creditor. **SHAR** — Shared: In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor. **SLEV** — FollowingServiceLevel: Charges are to be applied following the rules agreed in the service level and/or scheme.
	paymentInformationStatus			[0..1]	See generic structure PaymentInformationStatusCode
	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 - AM18 (InvalidNumberOfTransactions): the number of transactions exceeds the ASPSP acceptance limit - CH03 (RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture): The requested execution date is too far in the future - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - DS02 (OrderCancelled): An authorized user has cancelled the order - 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.
	fundsAvailability			[0..1]	indicator that the payment can be covered or not by the funds available on the relevant account - true: payment is covered - false: payment is not covered
	booking			[0..1]	indicator that the payment can be immediately booked or not - true: payment is booked - false: payment is not booked
	requestedExecutionDate			[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
	creditTransferTransaction			[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API: Each ASPSP will specify a maxItems value for this field taking into accounts its specificities about payment request handling
		{arrayItem}		[1..*]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API:
		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

				FIELD	MULT.	DESC.
				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	[0..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.
				requestedExecutionDate	[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment. API: This field indicates the date at which the debtor account should be debited. In most of the cases, especially for international payments, the date of the credit on the credit account cannot be set. Only SCTInst can guarantee having the same date for this credit. This date can be used in the following cases: - the single requested execution date for a payment having several instructions. In this case, this field must be set at the payment level. - the requested execution date for a given instruction within a payment. In this case, this field must be set at each instruction level. - The first date of execution for a standing order. When the payment cannot be processed at this date, the ASPSP is allowed to shift the applied execution date to the next possible execution date for non-standing orders. For standing orders, the [executionRule] parameter helps to compute the execution date to be applied.
				endDate	[0..1]	The last applicable day of execution for a given standing order. If not given, the standing order is considered as endless.
				executionRule	[0..1]	Execution date shifting rule for standing orders This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceding" or "following" working day. ASPSP might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule. - FWNG: following - PREC: preceding
				frequency	[0..1]	Frequency rule for standing orders. The following codes from the "EventFrequency7Code" of ISO 20022 are supported. - DAIL: Daily - WEEK: Weekly - TOWK: EveryTwoWeeks - MNTH: Monthly - TOMN: EveryTwoMonths - QUTR: Quarterly - SEMI: SemiAnnual - YEAR: Annual However, each ASPSP might restrict these values into a subset if needed.
				instructedAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.
				currency	[1..1]	Specifies the currency of the amount or of the 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.
				beneficiary	[0..1]	Specification of a beneficiary
				id	[0..1]	Id of the beneficiary
				isTrusted	[0..1]	The ASPSP having not implemented the trusted beneficiaries list must not set this flag. Otherwise, the ASPSP indicates whether or not the beneficiary has been registered by the PSU within the trusted beneficiaries list. - true: the beneficiary is actually a trusted beneficiary - false: the beneficiary is not a trusted beneficiary
				creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
				creditor	[1..1]	See generic structure PartyIdentification
				creditorAccount	[0..1]	See generic structure AccountIdentification
				ultimateCreditor	[0..1]	See generic structure PartyIdentification
				regulatoryReportingCodes	[0..1]	List of needed regulatory reporting codes for international payments
				{arrayItem}	[1..10]	Information needed due to regulatory and statutory requirements. Economical codes to be used are provided by the National Competent Authority
				remittanceInformation	[0..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

			FIELD		MULT.	DESC.
			{arrayItem}		[0..*]	Relevant information to the transaction
			transactionStatus		[0..1]	See generic structure TransactionIndividualStatusCode
			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 - AM18 (InvalidNumberOfTransactions): the number of transactions exceeds the ASPSP acceptance limit - CH03 (RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture): The requested execution date is too far in the future - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - DS02 (OrderCancelled): An authorized user has cancelled the order - 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 authentication approaches are accepted by the PISP and which has been chosen by the ASPSP
			acceptedAuthenticationApproach		[0..1]	can only be set by the PISP authentication 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)
			{arrayItem}		[1..*]	combination of possible values for authentication approaches
			appliedAuthenticationApproach		[0..1]	The ASPSP, based on the authentication 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
			scaHint		[0..1]	can only be set by the PISP Hint given by the merchant and/or the PISP about an SCA exemption context
			successfulReportUrl		[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the authentication 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 authentication 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.
		request			[0..1]	See generic structure GenericLink
		confirmation			[0..1]	See generic structure GenericLink

4.11. Modification of a Payment/Transfer Request (PISP)

4.11.1. Description

The PISP sent a Payment/Transfer Request through a POST command.

The ASPSP registered the Payment/Transfer Request, updated if necessary the relevant

identifiers in order to avoid duplicates and returned the location of the updated Request.

The PISP got the Payment/Transfer Request that has been updated with the resource identifiers, and eventually the status of the Payment/Transfer Request and the status of the subsequent credit transfer.

The PISP request for the payment cancellation (global cancellation) or for some payment instructions cancellation (partial cancellation)

No other modification of the Payment/Transfer Request is allowed.

4.11.2. Prerequisites

- The TPP was 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 previously posted a Payment/Transfer Request which was saved by the ASPSP (cf. § 4.5.3)
  - o The ASPSP answered with a location link to the saved Payment/Transfer Request (cf. § 4.5.4)
  - o The PISP retrieved the saved Payment/Transfer Request (cf. § 4.5.4)
- The TPP and the ASPSP successfully processed a mutual check and authentication
- The TPP presented its "OAUTH2 Client Credential" access token.
- The TPP presented the payment/transfer request.
- The PSU was successfully authenticated.

4.11.3. Business flow

the following cases can be applied:

- Case of a payment with multiple instructions or a standing order, the PISP asks to cancel the whole Payment/Transfer or Standing Order Request including all non-executed payment instructions by setting the [paymentInformationStatus] to "RJCT" and the relevant [statusReasonInformation] to "DS02" at payment level.
- Case of a payment with multiple instructions, the PISP asks to cancel one or several payment instructions by setting the [transactionStatus] to "RJCT" and the relevant [statusReasonInformation] to "DS02" at each relevant instruction level.

Since the modification request needs a PSU authentication before committing, the modification request includes:

- The specification of the authentication approaches that are supported by the PISP (any combination of "REDIRECT", "EMBEDDED" and "DECOUPLED" values).
- In case of possible REDIRECT or DECOUPLED authentication approach, one or two call-back URLs to be used by the ASPSP at the finalisation of the authentication and consent process :
  - o 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

- o 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.
  - o Both call-back URLS must be used in a TLS-secured request.
- 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 updated Payment/Transfer Request and answers to the PISP. The answer embeds

- The specification of the chosen authentication approach taking into account both the PISP and the PSU capabilities.
- In case of chosen REDIRECT authentication approach, the URL to be used by the PISP for redirecting the PSU in order to perform an authentication.

4.11.4. Authentication flows for both use cases

4.11.4.1. Redirect authentication approach

When the chosen authentication 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 global or partial Cancellation
- The ASPSP is then able to initiate the subsequent cancellation
- The ASPSP redirects the PSU to the PISP using one of the call-back URLs provided within the posted Payment Request cancellation

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

4.11.4.2. Decoupled authentication approach

When the chosen authentication approach is "DECOUPLED":

- Based on the PSU identifier provided within the Payment Request by the PISP, the ASPSP provides the PSU with the Cancellation Request details and challenges the PSU for a Strong Customer Authentication on a decoupled device or application.
- The PSU confirms or not the Payment Request global or partial Cancellation
- The ASPSP is then able to initiate the subsequent cancellation
- The ASPSP notifies the PISP about the finalisation of the authentication and cancellation 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 Cancellation Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.11.4.3. Embedded authentication approach

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

- The TPP informs the PSU that a challenge is needed for completing the Payment Request cancellation 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 cancellation details.
- The PSU confirms or not the Payment Request global or partial Cancellation
- When agreeing the Payment Request cancellation, 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 Cancellation Request shall expire and is then rejected to the PISP. The expiration delay is specified by each ASPSP.

4.11.5. Request

`put /payment-requests/{paymentRequestResourceId}`

4.11.5.1. Path Parameters

FIELD	MULT.	DESC.
paymentRequestResourceId	[1..1]	Identification of the Payment Request Resource

4.11.5.2. Body (application/json)

FIELD	MULT.	DESC.
{requestBody}	[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. API: Information about the creditor (Id, account and agent) might be placed either at payment level or at instruction level. Thus multi-beneficiary payments can be handled. The requested execution date can be placed either at payment level when all instructions are requested to be executed at the same date or at instruction level. The latest case includes: - multiple instructions having different requested execution dates - standing orders settings
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. API: Each ASPSP will specify a maximum value for this field taking into accounts its specificities about payment request handling
initiatingParty	[1..1]	See generic structure PartyIdentification
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. API: This field is useless for SCTInst and thus should be ignored.

FIELD		MULT.	DESC.
	serviceLevel	[0..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) value is 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: "INST" value is to be used in order to ask for an SEPA instant Payment (SCTInst). For International payments, this field may be valued with one of the ISO20022 external code to specify with payment instrument should be used by the creditor's bank.
	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:

Table within categoryPurpose:

CodeName	Name	Definition
CASH	CashManagementTransfer	Transaction is a general cash management instruction.
CORT	TradeSettlementPayment	Transaction is related to settlement of a trade, eg a foreign exchange deal or a securities transaction.
DVPM	DeliverAgainstPayment	Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction.
INTC	IntraCompanyPayment	Transaction is an intra-company payment, ie, a payment between two companies belonging to the same group.
TREA	TreasuryPayment	Transaction is related to treasury operations. E.g. financial contract settlement.

FIELD		MULT.	DESC.
debtor		[0..1]	See generic structure PartyIdentification
debtorAccount		[0..1]	See generic structure AccountIdentification
debtorAgent		[0..1]	See generic structure FinancialInstitutionIdentification
beneficiary		[0..1]	Specification of a beneficiary
	id	[0..1]	Id of the beneficiary
	creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
	creditor	[1..1]	See generic structure PartyIdentification
	creditorAccount	[0..1]	See generic structure AccountIdentification
ultimateCreditor		[0..1]	See generic structure PartyIdentification
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

FIELD				MULT.	DESC.

FIELD				MULT.	DESC.
chargeBearer				[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. The following values are allowed: **CodeName / Name / Definition:** DEBT — BorneByDebtor — All transaction charges are to be borne by the debtor. CRED — BorneByCreditor — All transaction charges are to be borne by the creditor. SHAR — Shared — In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor. SLEV — FollowingServiceLevel — Charges are to be applied following the rules agreed in the service level and/or scheme.
paymentInformationStatus				[0..1]	See generic structure PaymentInformationStatusCode
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 - AM18 (InvalidNumberOfTransactions): the number of transactions exceeds the ASPSP acceptance limit - CH03 (RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture): The requested execution date is too far in the future - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - DS02 (OrderCancelled): An authorized user has cancelled the order - 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.
requestedExecutionDate				[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
creditTransferTransaction				[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API: Each ASPSP will specify a maxItems value for this field taking into accounts its specificities about payment request handling
	{arrayItem}			[1..*]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API:
		paymentId		[1..1]	ISO20022: Set of elements used to reference a payment instruction.
			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	[0..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.

			FIELD	MULT.	DESC.
			requestedExecutionDate	[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment. API: This field indicates the date at which the debtor account should be debited. In most of the cases, especially for international payments, the date of the credit on the credit account cannot be set. Only SCTInst can guarantee having the same date for this credit. This date can be used in the following cases: - the single requested execution date for a payment having several instructions. In this case, this field must be set at the payment level. - the requested execution date for a given instruction within a payment. In this case, this field must be set at each instruction level. - The first date of execution for a standing order. When the payment cannot be processed at this date, the ASPSP is allowed to shift the applied execution date to the next possible execution date for non-standing orders. For standing orders, the [executionRule] parameter helps to compute the execution date to be applied.
			endDate	[0..1]	The last applicable day of execution for a given standing order. If not given, the standing order is considered as endless.
			executionRule	[0..1]	Execution date shifting rule for standing orders This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceding" or "following" working day. ASPSP might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule. - FWNG: following - PREC: preceding
			frequency	[0..1]	Frequency rule for standing orders. The following codes from the "EventFrequency7Code" of ISO 20022 are supported. - DAIL: Daily - WEEK: Weekly - TOWK: EveryTwoWeeks - MNTH: Monthly - TOMN: EveryTwoMonths - QUTR: Quarterly - SEMI: SemiAnnual - YEAR: Annual However, each ASPSP might restrict these values into a subset if needed.
			instructedAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.
			currency	[1..1]	Specifies the currency of the amount or of the 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.
			beneficiary	[0..1]	Specification of a beneficiary
			id	[0..1]	Id of the beneficiary
			creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
			creditor	[1..1]	See generic structure PartyIdentification
			creditorAccount	[0..1]	See generic structure AccountIdentification
			ultimateCreditor	[0..1]	See generic structure PartyIdentification
			regulatoryReportingCodes	[0..1]	List of needed regulatory reporting codes for international payments
			{arrayItem}	[1..10]	Information needed due to regulatory and statutory requirements. Economical codes to be used are provided by the National Competent Authority
			remittanceInformation	[0..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
			{arrayItem}	[0..*]	Relevant information to the transaction
			transactionStatus	[0..1]	See generic structure TransactionIndividualStatusCode

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 - AM18 (InvalidNumberOfTransactions): the number of transactions exceeds the ASPSP acceptance limit - CH03 (RequestedExecutionDateOrRequestedCollectionDateTooFarInFuture): The requested execution date is too far in the future - CUST (RequestedByCustomer): The reject is due to the debtor: refusal or lack of liquidity - DS02 (OrderCancelled): An authorized user has cancelled the order - 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 authentication approaches are accepted by the PISP and which has been chosen by the ASPSP
acceptedAuthenticationApproach	[0..1]	can only be set by the PISP authentication 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)
{arrayItem}	[1..*]	combination of possible values for authentication approaches
scaHint	[0..1]	can only be set by the PISP Hint given by the merchant and/or the PISP about an SCA exemption context
successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the authentication 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 authentication 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

4.11.6. Response

4.11.6.1. Body (*/*)

FIELD	MULT.	DESC.
{responseBody}	[1..1]	data forwarded by the ASPSP top the PISP after creation of the Payment Request resource creation
appliedAuthenticationApproach	[0..1]	The ASPSP, based on the authentication 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]	See generic structure GenericLink

4.12. Confirmation of a payment request or a modification request (PISP)

4.12.1. Description

The PISP confirms one of the following requests

- payment request on behalf of a merchant
- transfer request on behalf of the account's owner
- standing-order request on behalf of the account's owner

The ASPSP answers with a status of the relevant request and the subsequent Credit Transfer.

4.12.2. 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 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 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

4.12.3. Business flow

Once the PSU has been authenticated, it is the due to the PISP to confirm the 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.

4.12.4. Request

`post /payment-requests/{paymentRequestResourceId}/confirmation`

4.12.4.1. Path Parameters

FIELD	MULT.	DESC.
paymentRequestResourceId	[1..1]	Identification of the Payment Request Resource

4.12.4.2. Body (application/json)

FIELD	MULT.	DESC.
{requestBody}	[0..1]	Confirmation request resource
psuAuthenticationFactor	[0..1]	authentication factor forwarded by the TPP to the ASPSP in order to fulfil the strong customer authentication process

4.12.5. Response

4.12.5.1. Body (application/hal+json; charset=utf-8)

FIELD			MULT.	DESC.
{responseBody}			[1..1]	HYPERMEDIA structure used for returning the original Payment Request to the PISP
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. API: Information about the creditor (Id, account and agent) might be placed either at payment level or at instruction level. Thus multi-beneficiary payments can be handled. The requested execution date can be placed either at payment level when all instructions are requested to be executed at the same date or at instruction level. The latest case includes: - multiple instructions having different requested execution dates - standing orders settings
	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. API: Each ASPSP will specify a maximum value for this field taking into accounts its specificities about payment request handling
	initiatingParty		[1..1]	See generic structure PartyIdentification
	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. API: This field is useless for SCTInst and thus should be ignored.
		serviceLevel	[0..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) value is 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: "INST" value is to be used in order to ask for an SEPA instant Payment (SCTInst). For International payments, this field may be valued with one of the ISO20022 external code to specify with payment instrument should be used by the creditor's bank.

FIELD	MULT.	DESC.
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:

CodeName	Name	Definition
CASH	CashManagementTransfer	Transaction is a general cash management instruction.
CORT	TradeSettlementPayment	Transaction is related to settlement of a trade, eg a foreign exchange deal or a securities transaction.
DVPM	DeliverAgainstPayment	Code used to pre-advise the account servicer of a forthcoming deliver against payment instruction.
INTC	IntraCompanyPayment	Transaction is an intra-company payment, ie, a payment between two companies belonging to the same group.
TREA	TreasuryPayment	Transaction is related to treasury operations. E.g. financial contract settlement.

FIELD	MULT.	DESC.
debtor	[0..1]	See generic structure PartyIdentification
debtorAccount	[0..1]	See generic structure AccountIdentification
debtorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
beneficiary	[0..1]	Specification of a beneficiary
id	[0..1]	Id of the beneficiary
isTrusted	[0..1]	The ASPSP having not implemented the trusted beneficiaries list must not set this flag. Otherwise, the ASPSP indicates whether or not the beneficiary has been registered by the PSU within the trusted beneficiaries list. - true: the beneficiary is actually a trusted beneficiary - false: the beneficiary is not a trusted beneficiary
creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
creditor	[1..1]	See generic structure PartyIdentification
creditorAccount	[0..1]	See generic structure AccountIdentification
ultimateCreditor	[0..1]	See generic structure PartyIdentification
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

FIELD				MULT.	DESC.
	chargeBearer			[0..1]	ISO20022: Specifies which party/parties will bear the charges associated with the processing of the payment transaction. The following values are allowed: **CodeName** / **Name** / **Definition** DEBT / BorneByDebtor / All transaction charges are to be borne by the debtor. CRED / BorneByCreditor / All transaction charges are to be borne by the creditor. SHAR / Shared / In a credit transfer context, means that transaction charges on the sender side are to be borne by the debtor, transaction charges on the receiver side are to be borne by the creditor. In a direct debit context, means that transaction charges on the sender side are to be borne by the creditor, transaction charges on the receiver side are to be borne by the debtor. SLEV / FollowingServiceLevel / Charges are to be applied following the rules agreed in the service level and/or scheme.
	fundsAvailability			[0..1]	indicator that the payment can be covered or not by the funds available on the relevant account - true: payment is covered - false: payment is not covered
	booking			[0..1]	indicator that the payment can be immediately booked or not - true: payment is booked - false: payment is not booked
	requestedExecutionDate			[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment.
	creditTransferTransaction			[1..1]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API: Each ASPSP will specify a maxItems value for this field taking into accounts its specificities about payment request handling
		{arrayItem}		[1..*]	ISO20022: Payment processes required to transfer cash from the debtor to the creditor. API:
		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	[0..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.
			requestedExecutionDate	[0..1]	ISO20022: Date at which the initiating party requests the clearing agent to process the payment. API: This field indicates the date at which the debtor account should be debited. In most of the cases, especially for international payments, the date of the credit on the credit account cannot be set. Only SCTInst can guarantee having the same date for this credit. This date can be used in the following cases: - the single requested execution date for a payment having several instructions. In this case, this field must be set at the payment level. - the requested execution date for a given instruction within a payment. In this case, this field must be set at each instruction level. - The first date of execution for a standing order. When the payment cannot be processed at this date, the ASPSP is allowed to shift the applied execution date to the next possible execution date for non-standing orders. For standing orders, the [executionRule] parameter helps to compute the execution date to be applied.
			endDate	[0..1]	The last applicable day of execution for a given standing order. If not given, the standing order is considered as endless.

				FIELD	MULT.	DESC.
				executionRule	[0..1]	Execution date shifting rule for standing orders This data attribute defines the behaviour when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceding" or "following" working day. ASPSP might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule. - FWNG: following - PREC: preceding
				frequency	[0..1]	Frequency rule for standing orders. The following codes from the "EventFrequency7Code" of ISO 20022 are supported. - DAIL: Daily - WEEK: Weekly - TOWK: EveryTwoWeeks - MNTH: Monthly - TOMN: EveryTwoMonths - QUTR: Quarterly - SEMI: SemiAnnual - YEAR: Annual However, each ASPSP might restrict these values into a subset if needed.
				instructedAmount	[1..1]	Structure aiming to embed the amount and the currency to be used.
				currency	[1..1]	Specifies the currency of the amount or of the 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.
				beneficiary	[0..1]	Specification of a beneficiary
				id	[0..1]	Id of the beneficiary
				isTrusted	[0..1]	The ASPSP having not implemented the trusted beneficiaries list must not set this flag. Otherwise, the ASPSP indicates whether or not the beneficiary has been registered by the PSU within the trusted beneficiaries list. - true: the beneficiary is actually a trusted beneficiary - false: the beneficiary is not a trusted beneficiary
				creditorAgent	[0..1]	See generic structure FinancialInstitutionIdentification
				creditor	[1..1]	See generic structure PartyIdentification
				creditorAccount	[0..1]	See generic structure AccountIdentification
				ultimateCreditor	[0..1]	See generic structure PartyIdentification
				regulatoryReportingCodes	[0..1]	List of needed regulatory reporting codes for international payments
				{arrayItem}	[1..10]	Information needed due to regulatory and statutory requirements. Economical codes to be used are provided by the National Competent Authority
				remittanceInformation	[0..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
				{arrayItem}	[0..*]	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 authentication approaches are accepted by the PISP and which has been chosen by the ASPSP
				acceptedAuthenticationApproach	[0..1]	can only be set by the PISP authentication 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)
				{arrayItem}	[1..*]	combination of possible values for authentication approaches
				appliedAuthenticationApproach	[0..1]	The ASPSP, based on the authentication 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
				scaHint	[0..1]	can only be set by the PISP Hint given by the merchant and/or the PISP about an SCA exemption context
				successfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the finalisation of the authentication and consent process in REDIRECT and DECOUPLED approach

FIELD			MULT.	DESC.
		unsuccessfulReportUrl	[0..1]	URL to be used by the ASPSP in order to notify the PISP of the failure of the authentication 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.
		request	[0..1]	See generic structure GenericLink
		confirmation	[0..1]	See generic structure GenericLink