PSD2 – Technical Design TPP

Version: 1.9.3

30/11/2023

Authorisations and version control

Version	Date	Affects	Brief description of the change
1.9.3	November 2023	ALL	Correction of minor errata. - Added the optional psuName attribute of Type Max140Text to the account details data structure to carry the PSU name. In the case of a corporate account, this could be the person acting on behalf of the company. - Added the "Account Owner" data type in the account detail structure to include the name of the account owners. - Added "psuName" and compound data type "account Owner" in request 6.3.6 Obtain payment status.

CONTENTS

1. INTRODUCTION

1.1 Scope

This document provides the Technical Design of the interface with Third-Party Providers (TPPs) and the HUB in order to comply with the PSD2 directive. The functions which Banco de Sabadell (hereinafter, ASPSP) makes available will be published in it.

1.2 Glossary

The acronyms and definitions used throughout the document are set forth in the table below.

Acronym	Definition
ASPSP	Account Servicing Payment Service Provider Provides and maintains customer accounts from which payments can be made.
PISP	Payment Initiation Service Provider It initiates a payment order at the user's request, from a payment account from another provider.
AISP	Account Information Service Provider It provides customer information on accounts from other providers.
TPP	Third-party provider It exercises services defined by PSD2 on behalf of a PSU. If it is necessary to provide the service, it accesses the PSU's account(s) which are managed by an ASPSP using the ASPSP's XS2A Interface. It sends request messages to the ASPSP's XS2A interface and receives the corresponding response messages from that ASPSP.
PIISP	Payment Instrument Issuers Service Provider It provides the user with a payment instrument to initiate and process payment transactions.
PSU	This could be either a natural or legal person according to the PSD2 legislation. This is the person who implicitly or explicitly instructs the TPP to perform any ASPSP service.

2. GENERAL DESCRIPTION OF THE SYSTEM

Below, in the Figure 1: Core Module Diagram, the different Functional Modules that make up the system are displayed, which will be subsequently detailed.

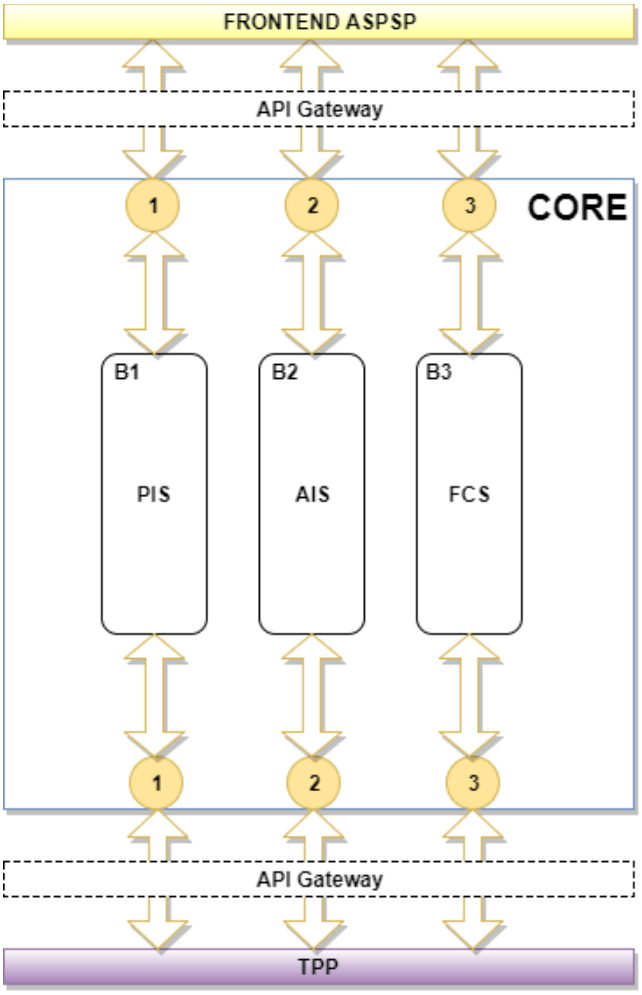


Figure 1: Core Module Diagram

Service		Functionality	Status
CORE	PIS	Start simple payment single signature	Available
		Start recurring payments	Available
		Start future payments	Available
		Check payment status	Available
		Execute payment start	Available
		Retrieve information from the start of the payment	Available
		Payment cancellation (Pending consultation Redsys)	Available
	AIS	Consent of information about payment accounts and / or cards	Available
		Retrieve information on consent	Available
		Check payment status	Available
		Remove consent	Available
		Reading list of accessible accounts with/without balances	Available
		Reading of accounts details with/without balances	Available
		Reading of balances	Available
		Reading of transactions with/without balances	Available
		Reading of transaction details	Not supported
		List of standing orders	Not supported
	FCS	Establish consent	Available
		Retrieve consent information	Available
		Check consent state	Available
		Remove consent	Available
		Confirmation of funds	Available
	SCA	SCA by redirection flow	Available
		SCA by decoupled flow	Not supported
		Embedded SCA	Not supported
	OAUTH	Obtaining the access token	Available
		Renewal of the access token	Available
	Common processes	Initiate explicit authorization	Available
		SCA status query	Available
		Obtain authorisation data	Available
		Update authorisation sub-resources	Available

Table 1: CORE Services

Service		Functionality	Status
SVA	DIR. ASPSPs	List of available ASPSPs	Available
	PIS	Payment initiation with a list of accounts available for the PISP	Available

		Start of recurring payments with list of accounts available for PISP	Available
	AIS	Notice of data available in PUSH mode	Pending

Table 2: Value-Added Services

3. TRANSPORT LAYER

The following information is valid for PRODUCTION environment.

3.1 Communications between TPP - ASPSP

Channel https (TLS 1.2) + TWOWAY-SSL

The communication between the TPP and the ASPSP is always secured by the use of a MATLS 1.2 connection (2WAYSSL) with client authentication.

In summary, the validations to apply:

- TLS 1.2 communication with Mutual Authentication with Client Certificate (MATLS 1.2)
- Based on X509 certificates from recognized CAs (Digicert) and eIDAS certificates from TPPs issued by valid QTSPs PSD2
- Temporary validity of the certificate
- Common Name of the certificate Subject should be the one expected
- Complete certification chain validation
- CRL validation

4. APPLICATION LAYER

4.1 Location of message parameters

The definition of the interface follows the REST services approach. This approach allows message parameters to be transported at different levels:

- Message parameters as part of the HTTP layer (HTTP headers)
- Message parameters defining additional query parameters in the path (information in the path of the URL)
- Message parameters as part of the HTTP body

The parameters contained in the corresponding HTTP body will be encoded in JSON.

The parameters are encoded in:

- spinal-case (lowercase letters) at path level
- Spinal-case (starting with capital letters) at the HTTP header level
- lowerCamelCase for query parameters (query params) and JSON-based parameters.

The following principles apply in the definition of the API:

- Defining the content syntax
- Certificates and signature data required
- PSU identification data (based on access token)
- Protocol level data such as request timestamp or request/transaction identifiers

Message parameters as part of the path level:

- Provider identification
- Service identification
- Payment Type Identification
- Resource ID

Query parameters:

- Additional information needed to process GET requests to filter information

Message parameters as part of the HTTP body:

- Business data
- PSU authentication data
- Information Messages
- Hyperlinks to fully address the TPP-ASPSP process

4.2 Signing messages under BG 1.3.x specifications

All requests will be signed to the ASPSP.

4.2.1 Signing Messages Between Tpp - Aspsp Tpp -

The TPP will always sign all petitions sent to the ASPSP and the ASPSP must validate them.

The signature must be included in the HTTP headers as defined in the Berlin Group - Implementation Guidelines, chapter 4.

The electronic signature of the TPP is based on a certificate for electronic signature. This certificate must be issued by a valid QTSP PSD2.

In summary, the validations to apply:

- Based on eIDAS issued by valid QTSP PSD2
- Temporary validity of the certificate
- Common Name of the certificate Subject should be the one expected
- Complete certification chain validation
- CRL validation
- Signing of the message following the Berlin Group standard - Implementation Guidelines v1.3.x

In general, all requests (except for OAuth2 authorize as a pre-step) will include the following header fields for the message signature:

Field	Description	Type	Mandat.	Format
Digest	It is contained if the Signature field is travelling. See 9.1 Signature for more information. tpp documentation.	String	MA	^.{1,100} $ Ex: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signing of the request by the HUB. See 9.1Signature for more information.	String	MA	See 9.1Signature for more information.
TPP-Signature-Certificate	HUB certificate used to sign the Base64 request. See 9.1Signature for more information.	String	MA	^.{1,5000}$ EX: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

4.3 API interface structure

The interface is resource oriented. Resources can be directed under the API endpoints.

Using additional content parameters {parameters}, where:

- {provider} is the host and path of the API
- v1.1 is the version of this specification
- {service} has the values consents, Payments, bulk-payments, periodic-payments, accounts, card-accounts, or funds-confirmations, and which are extended by adding more information related to the type of product and the scope requested.

- {¿query-parameters} are parameters that provide details about GET access methods
- {parameters} are attributes defined in JSON encoding

The structure of the request / response is described according to the following categories:

- Path: attributes encoded in the Path
- Query parameters: attributes added to the path after the sign '?' as flags to address processes or filter attributes for GET access methods. Boolean type access parameters must always be used with the values true or false.
- Header: attributes encoded in the HTTP header of the request or the response
- Request: attributes of the request
- Response: response attributes in JSON

The HTTP response codes, which can be used in the interface, will be defined later.

4.4 PSU Context Data Requirements (HTTP headers)

The following elements are used to send information about the PSU-TPP interface and are used for the ASPSP risk management procedures. It is highly recommended to send these elements in all requests for Initiate Payment or Establish Consent transaction flows. For example, in flows where a PSU authentication is required (Except in OAuth2 as a pre-step). The following table will not be repeated in the following sections for better readability. The only exception is in certain requests where a condition other than "optional" applies. For example, PSU-IP-Address.

Note: the information about the PSU-TPP interface could be used by the ASPSP as input for fraud detection and risk management systems. You can use this information also to exclude some authentication methods (for example, some ASPSP does not allow to receive an OTP by SMS on the same device that triggers the transaction). In addition, it allows ASPSPs to receive specific information from the partner device in order to be able to support an app-to-app redirection procedure for the TPP. For these reasons, it is highly recommended that TPPs include all of this information in related requests. Failure to provide all the necessary information could lead to a classification of the PSU device as unusable for the authentication method or a classification of the current transaction as "high risk", for example due to session attacks. Due to this, the probability of a rejection of the transaction due to fraud detection and / or risk management could be increased.

Field	Description	Type	Mandat.	Format
PSU-IP-Address	IP address of the HTPP request between the PSU and the TPP.	String	OB	IPv4 and IPv6 Ex: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP port of the HTTP request between the PSU and the TPP if available.	String	OP	^.{1,5}$ Ex: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTTP request between the PSU and the TPP.	String	OP	^.{1,50}$ Ex: PSU-Accept: application / json
PSU-Accept-Charset	Accept charset header of the HTTP request between PSU and the TPP.	String	OP	^.{1,50}$ Ex: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTTP request between PSU and the TPP.	String	OP	^.{1,50}$ Ex: PSU-Accept-Encoding: gzip

PSU-Accept-Language	Accept language header of the HTTP request between PSU and the TPP.	String	OP	^.{1,50}$ Ex: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	Ex: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between PSU and TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	Ex: PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID should not be modified until the application is uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Location corresponding to the HTTP request between the PSU and the TPP	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;,][\\d]*.[\\d]*$ Ex: PSU-Geo-Location: GEO:90.023856;25.345963

4.5 Requirements on TPP URIs to be applied by the ASPSP

The TPP can provide multiple URIs to the ASPSP as parameters for the next steps of the protocol.

For security reasons, it must be ensured that these URIs are secured by the certificate used by the TPP for their identification. Apply as follows:

The URIs provided by the Hub in the TPP-Redirect-URI or TPP-Nok-Redirect-URI fields must comply with the domain secured by the TPP certificate in the CN field or in its SubjectAltName. It is taken into account that for cases like example-hub.com in the TPP-Redirect-URI like:

- www.example-hub.com/xs2a/v1.1/service/asdf o
- redirections.example-hub.com/xs2a/v1.1/service/asdf

They would be valid cases.

Wildcard certificates are taken into account to validate.

Requests that do not meet the requirement will be rejected.

4.6 Addressing process of the API by hyperlinks

The XS2A API requires several requests for the initiation of payment and account information services from the TPP to the ASPSP. In Initiate Payment requests and Establish Consent requests, a resource is generated by the ASPSP. The "location" header of the response will normally contain a link to the created resource.

Additionally, the ASPSP can embed the hyperlink together with a "tag" for the semantics of the same in the response of these first requests and for all the following requests in the services. This hyperlink will be relative to save space, except in cases such as redirections where it will be absolute.

The hyperlink "tag" carries the functionality of the resource directed by the link. For example, "authorise-transaction". This link indicates that the results of the SCA method must be sent to the resource directed by this link to authorize, for example, a payment.

The hyperlinks for addressing are carried in the "_links" element. This can contain one or more hyperlinks.

5. API ACCESS METHODS

The following tables provide an overview of the HTTP access methods supported by API endpoints and API-generated resources.

Conditions in the following tables

Additionally, it is defined when a supported method is mandatory for ASPSP by this specification or when it is an optional feature. It should be noted that the given condition is relative to the parent node of the path. For example, the condition on the GET method /v1.1/consents/{consentId} applies only if the POST endpoint /v1.1/consents is supported.

It should be noted that any of the methods used by the TPP, which are addressing dynamically created resources in this API, can only apply to resources which have been created before by the TPP itself.

5.1 OAuth2 endpoints

Endpoint	Method	Cond.	Description
/authorize	GET	MA	Redirection to the ASPSP login website to obtain the authCode.
/token	POST	MA	Allows to send the authCode to obtain the access token.
/token	POST	MA	Refresh the access token if it has expired.

5.2 Payment Endpoints

Endpoint	Method	Cond.	Description
/payments/{payment-product}	POST	MA	Creates a payment initiation resource accessible under the {paymentId} with all relevant data for the corresponding payment product. This is the first step in the API to initiate the referred payment.

/ payments / {payment-product} / {paymentId}	GET	MA	Gets the details of an initiated payment.
/payments/{payment-product}/{paymentId}/state	GET	MA	Gets the state of the payment transaction.
/periodic-payments/{payment-product}	POST	OP	Creates a standing order resource for periodic/recurring payment accessible under the {paymentId} with all relevant data for the corresponding payment product. This is the first step in the API to initiate the referred periodic/recurring payment.
/ payments / {payment-product} / {paymentId}	GET	MA	Gets the details of an initiated standing order for periodic/recurrent payment.
/periodic-payments/{payment-product}/{paymentId}/state	GET	MA	Gets the state of the standing order transaction for periodic/recurrent payment.
{payment-service}/{payment-product}/{paymentId}/authorisations	POST	MA	Create an authorization sub-resource and start the authorization process. The ASPSP could make the use of this access method unnecessary in case only a single SCA process is needed, as the related authorisation resource could be automatically created by the ASPSP after the payment data is sent with the first POST request to /payments/{payment-product}.
{payment-service}/{payment-product}/{paymentId}/authorisations	GET	MA	Gets the list of authorization sub-resource IDs that have been created.
{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}	GET	MA	Gets the SCA state of the authorization.
{payment-service}/{payment-product}/{paymentId}	DELETE	OP	Cancel the accessible payment under the paymentId resource if applicable for the payment service, payment product and received in the period of time that the cancellation is allowed. The response to this DELETE command will tell the TPP when: • The access method was rejected • The access method was correct

			• The access method is generally applicable but requires an additional authorization process.
{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations	POST	OP	Initiates the authorisation of the cancellation of the payment accessible under the paymentId resource if requested by the ASPSP (e.g. DELETE method is not sufficient) and if applicable for the payment service, and received within the time period that is cancellable.
{payment-service}/{payment-product}/{paymentId}/ cancellation-authorisations	GET	MA	Gets the list of cancellation authorization sub-resources that have been created. **Note**: if the POST command on this endpoint is supported, then this GET method must also be supported.
{payment-service}/{payment-product}/{paymentId}/ cancellation-authorisations/{authorisationId}	GET	MA	Gets the SCA state of the cancellation authorisation. **Note**: if the POST command on this endpoint is supported, then this GET method must also be supported.

5.3 AccountEndpoints

Endpoint	Method	Cond.	Description
/accounts	GET	MA	Reads all account identifiers for which the PSU has granted access on the /consents endpoint. In addition, relevant account information and links to the corresponding account information resources may be provided if the necessary permissions have been provided. **Note**: the endpoint / consents optionally offer to grant access on all **available** PSU payment **accounts** .In this case, this endpoint will release the information of all available payment accounts from the PSU to the ASPSP.

/accounts?withBalance	GET	MA	Obtain the identifiers of the available payment accounts along with balance information, depending on the consent granted.
/accounts/{account-id}	GET	MA	Gets detailed information about the accessed account.
/accounts/{account-id}?withBalance	GET	MA	Gets detailed information on the accessed account along with balance information.
/accounts/{account-id}/balances	GET	MA	Obtains detailed information on the balances of the account accessed.
/ accounts / {account-id} / transactions	GET	MA	Obtains a list of movements (transactions) of the accessed account. For a given account, additional parameters are, for example, date from, date from, and date to.
/accounts/{account-id}/transactions?withBalance	GET	MA	Obtains a list of movements (transactions) of the accessed account together with balances.

Note: the {account-id} parameter can be tokenized by the ASPSP in such a way that the current account numbers, such as IBANs or PANs, are not part of the API path definition for data protection reasons. This tokenization is managed by the ASPSP.

5.4 Account Consent Endpoints

Endpoint	Method	Cond.	Description
/consents	POST	MA	Creates a consent resource, defining access permissions on specific accounts of a PSU. These accounts are explicitly routable on the PATH as parameters.
/consents	POST	MA	Optionally, an ASPSP could accept specific access permissions to access all PSD2 services on all available accounts.

			Another option is that an ASPSP could accept a request where only the access permissions are reported but not the accounts. In this case, the selection of accounts is subsequently managed between the PSU and the ASPSP. As a last option, the ASPSP can accept requests with the following access permissions: • Get a list of available payment accounts • Get a list of available payment accounts with balances
/consents/{consentId}	GET	MA	Gets the exact definition of the consent resource, including the validity state.
/consents/{consentId}	DELETE	MA	Ends the directed consent.
/consents/{consentId}/state	GET	MA	Gets the state of the directed consent.
/consents/{consentId}/authorisations	POST	MA	Create an authorization sub-resource and start the authorization process. The ASPSP could make the use of this access method unnecessary in case only a single SCA process is needed, as the related authorisation resource could be automatically created by the ASPSP after the consents data is sent with the first POST /consents request.
/consents/{consentId}/authorisations	GET	MA	Gets the list of authorization sub-resource IDs that have been created.
/consents/{consentId}/authorisations/{authorisationId}	GET	MA	Gets the SCA state of the authorization.
/consents/{consentId}/authorisations/{authorisationId}	PUT	MA	Updates data in the authorization resource, if necessary.

5.5 Fund confirmation Consent endpoints

Endpoint	Method	Cond.	Description
/consents/confirmation-of-funds	POST	MA	Create a consent resource for funding confirmation.
/consents/confirmation-of-funds/{consentId}	GET	MA	Gets the exact definition of the consent resource, including the validity state.
/consents/confirmation-of-funds/{consentId}	DELETE	MA	Ends the directed consent.
/consents/confirmation-of-funds/{consentId}/state	GET	MA	Gets the state of the directed consent.
/consents/confirmation-of-funds/{consentId}/authorisations	POST	MA	Create an authorization sub-resource and start the authorization process. The ASPSP could make the use of this access method unnecessary in case only a single SCA process is needed, as the related authorisation resource could be automatically created by the ASPSP after the submission of the consent data with the first POST /consents/confirmation-of-funds request.
/consents/confirmation-of-funds/{consentId}/authorisations	GET	MA	Gets the list of authorization sub-resource IDs that have been created.
/consents/confirmation-of-funds/{consentId}/authorisations/{authorisationId}	GET	MA	Gets the SCA state of the authorization.
/consents/confirmation-of-funds/{consentId}/authorisations/{authorisationId}	PUT	MA	Updates data in the authorization resource, if necessary.

5.6 Fund Confirmation Endpoints

Endpoint	Method	Cond.	Description
/ funds-confirmations	POST	MA	Checks when a specific amount is available at a certain point in time for an account related to a TPP/card or targeted by TPP and IBAN.

5.7 Value Added Services (VAS) Endpoints

Endpoint	Method	Cond.	Description
/sva/payments/{payment-product}	POST	MA	Creates a payment initiation resource accessible under the {paymentId} with all relevant data for the corresponding payment product. This is the first step in the API to initiate the referred payment without having to inform the issuer's account.
/sva/periodic-payments/{payment-product}	POST	MA	Creates a periodic payment initiation resource accessible under the {paymentId} with all relevant data for the corresponding payment product. This is the first step in the API to initiate the referenced periodic payment without the need to inform the issuer's account.

6. DESCRIPTION OF CORE SERVICES

6.1 PIS: Payment Initiation Service

6.1.1 Payment Initiation Flows

The payment initiation flow depends on the SCA approach implemented by the ASPSP.

Note: The flows do not always cover all the variations or complexities of the implementation and are sample flows.

6.1.1.1 SCA flow by redirection: implicit start of authorization process

The image below depicts Figure 2: Start of payment with OAuth2 as pre-step and SCA flow by redirectionthe sequence of requests/responses and redirections that are necessary in the flow where strong authentication (SCA) by redirection is needed (SCA over OAuth2 is not applied).

The characteristics of this flow are:

- TPP-Redirect-Preferred: true (SCA's TPP preference for redirection) or not reported (ASPSP decides for redirection)

- TPP-Explicit-Authorization-Preferred: false - TPP preference to initiate the payment authorization process implicitly
- The PSU has only one SCA method

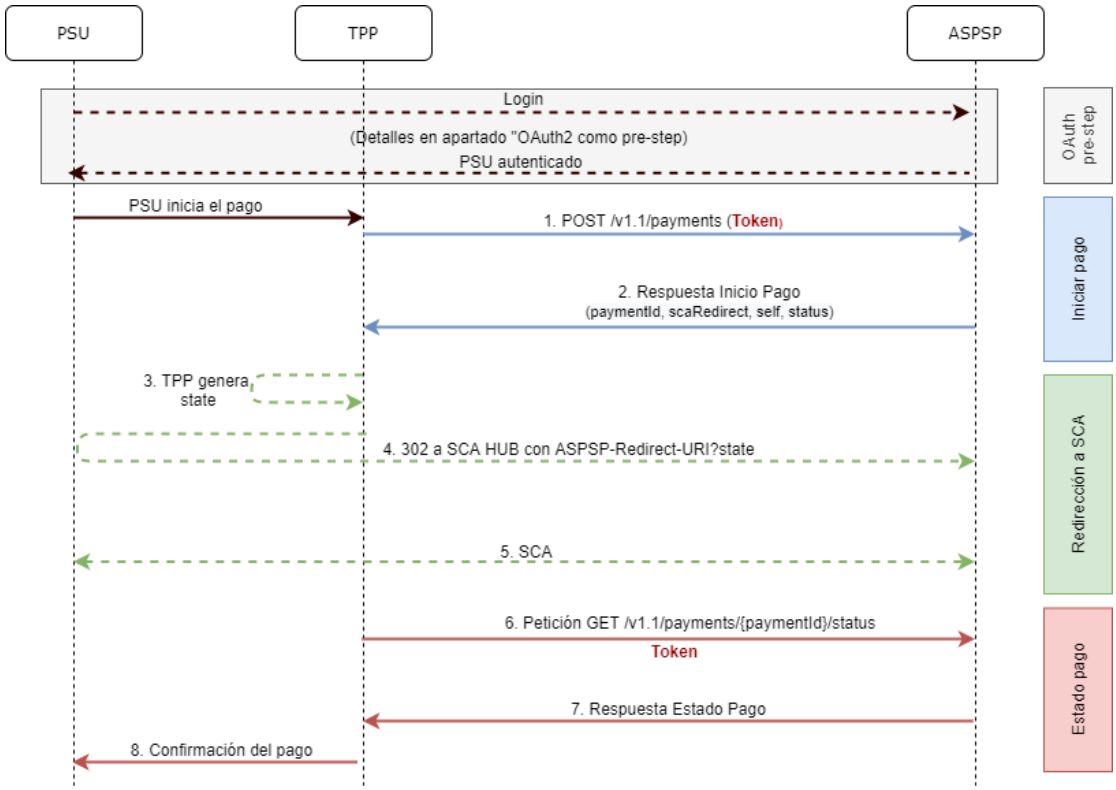


Figure 2: Start of payment with OAuth2 as pre-step and SCA flow by redirection and start of the implicit authorization process

OAuth2 (pre-step)

The main purpose of this flow is to authenticate the PSU to get access to the services displayed by its ASPSP through the use of an access token obtained after the application of this protocol.

In order to simplify, the detail of this flow has been omitted from the Figure 4 Figure 2: Start of payment with OAuth2 as pre-step and SCA flow by redirection and can be found in the section 6.1**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.VERIFY

Note: this step is optional. Only applies if no valid access token is available.

PSU initiates payment

The PSU wants to pay through the TPP.

1. Start Payment Request (TPP → ASPSP)

The TPP sends a POST request to initiate payment with *token* to the ASPSP. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **Payment data:** transfer type, ordering IBAN, beneficiary IBAN, amount, currency, concept ...
- **Data for risk scoring calculation:** IP, port, user-agent, language, location, HTTP headers ...
- **X-Request-ID:** identifier of the operation assigned by the TPP.

- **Access token** from TPP to Hub
- **TPP-Redirect-Preferred:** true (SCA flow preference by redirection) or not reported (ASPSP decides SCA by redirection).
- **TPP-Redirect-URI:** Return URI of the TPP after redirection to SCA.
- **TPP-Explicit-Authorization-Preferred:** false - TPP preference to initiate authorization implicitly

- **Other data**

2. Start Payment Response (ASPSP → TPP)

The ASPSP responds to the TPP indicating that strong authentication (SCA) is required, returning:

- **transactionStatus**: ISO 20022 state of the received payment start.
- **paymentId**: identifier of the generated resource that refers to the current payment initiation operation.

- **_links**

    - **scaRedirect**: links to the Hub endpoint where after receiving the redirect from the TPP it redirects back to the scaRedirect of the ASPSP. This URL can add security parameters to allow session maintenance during redirection.

      https://hub.example.com/auth

    - **self**: link to the payment resource generated by the Hub for the payment initiation request received from the TPP.
    - **state**: link of the Hub to which the TPP can make a request to check the state of the payment.

- **Other data**

3. TPP generates state

The TPP, after receiving the response to initiate payment, generates a value for *state* (XSRF token) that it must link to the PSU browser session.

4. Redirect to scaRedirect Hub (TPP → ASPSP)

The TPP redirects the PSU to the authentication endpoint by adding to it the field*state* as a query-param.

HTTP/1.1 302 Found
Location: https://hub.example.com/auth?state=qwerty

5. SCA between PSU ←→ ASPSP

During this redirection process, the ASPSP will be able to:

- Show commissions to the PSU if required
- Show ASPSP-PSU interface for SCA

8. Payment State Request (TPP → ASPSP)

The TPP will send a request for payment state with *token* to know the state of the payment.

9. Payment State Response (ASPSP → TPP)

The ASPSP updates the state of the operation and responds to the TPP.

10. Payment confirmation

The TPP confirms the states of the payment to the PSU.

6.1.1.2 SCA flow by redirection: implicit start of authorization process.

Below in Figure 5: Initiation of payment with OAuth2 as pre-step and SCA flow by redirection and initiation of explicit authorisation process with/without selection of SCA methodthe sequence of requests/responses and redirections that are necessary in the flow where strong authentication (SCA) by redirection is needed (SCA over OAuth2 is not applied).

The characteristics of this flow are:

- TPP-Redirect-Preferred: true (SCA's TPP preference for redirection) or not reported (ASPSP decides for redirection)
- TPP-Explicit-Authorization-Preferred: true - TPP's preference to start the payment authorization process explicitly or, if you select implicit and the PSU has more than one SCA method, the ASPSP switches to the explicit authorization process.

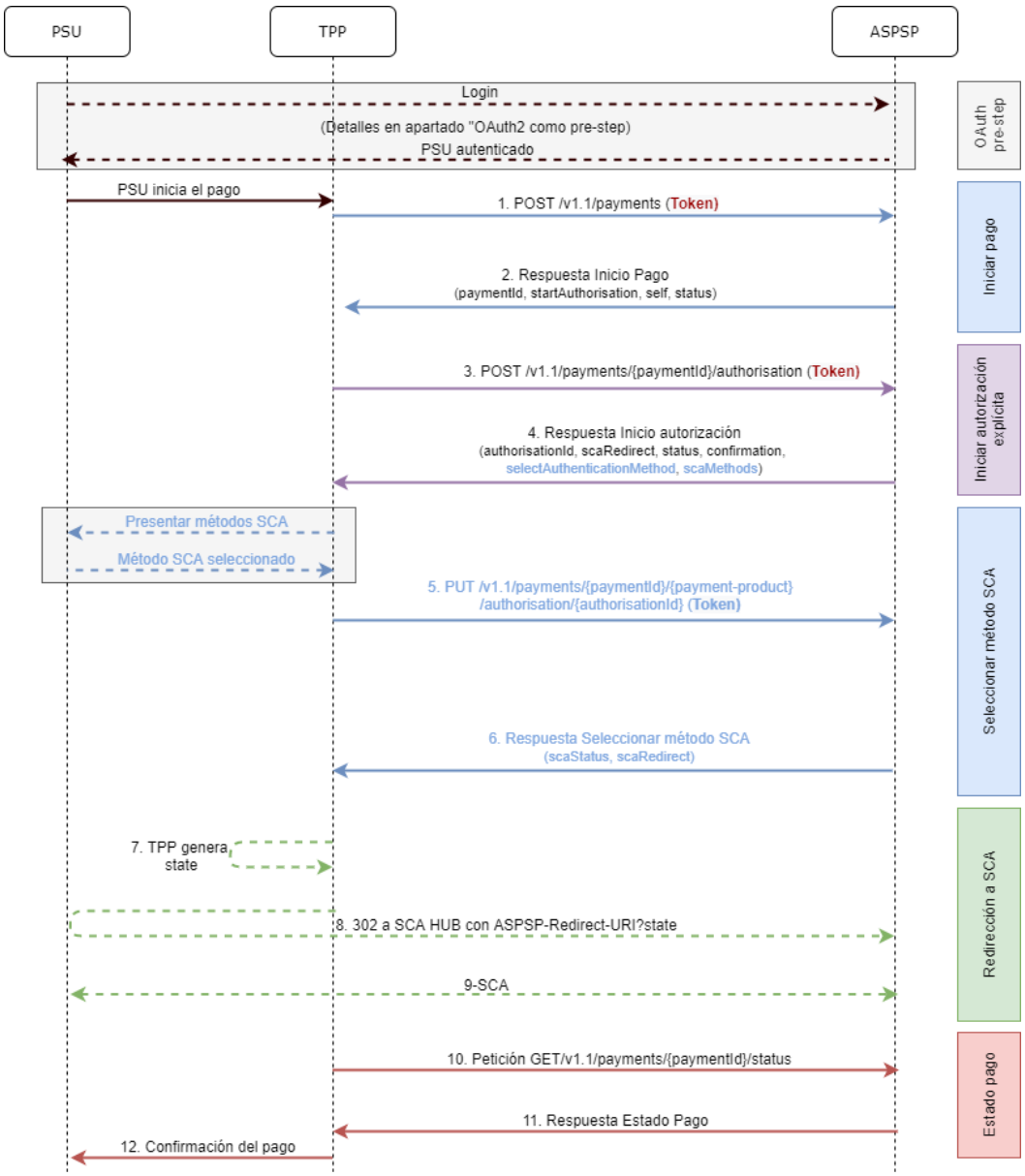


Figure 3: Start of payment with OAuth2 as pre-step and SCA flow by redirection and start of the explicit authorization process with / without selection of the SCA method

OAuth2 (pre-step)

The main purpose of this flow is to authenticate the PSU to get access to the services displayed by its ASPSP through the use of an access token obtained after the application of this protocol.

In order to simplify, the detail of this flow has been omitted from Figure 4: Payment initiation with OAuth2 as pre-step and SCA flow by redirection and can be found in the section 6.1**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.VERIFY

Note: this step is optional. Only applies if no valid access token is available.

PSU initiates payment

The PSU wants to pay through the TPP.

1. Start Payment Request (TPP → ASPSP)

The TPP sends a POST request to initiate payment with *token* to the ASPSP. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **Payment data:** transfer type, ordering IBAN, beneficiary IBAN, amount, currency, concept ...
- **Data for risk scoring calculation:** IP, port, user-agent, language, location, HTTP headers ...
- **X-Request-ID:** identifier of the operation assigned by the TPP.
- Hub access **token**
- **TPP-Redirect-Preferred:** true - SCA flow preference by redirect
- **TPP-Redirect-URI:** Return URI of the TPP after redirection to SCA.
- **TPP-Explicit-Authorization-Preferred:** true - TPP preference to initiate authorization explicitly (current flow)
- **Other data**

2. Initiate Payment Response (ASPSP → TPP)

The Hub, after receiving the response from the ASPSP, responds to the TPP by returning:

- **transactionStatus**: ISO 20022 state with the state of the transaction
- **paymentId**: resource identifier generated by the Hub referring to the current payment initiation transaction.
- **_links**
  - **self**: link to the resource that refers to the payment in the Hub
  - **state**: link of the Hub to which the TPP can make a request to check the state of the payment.
  - **startAuthorisation:** link of the Hub to which the TPP can make a POST request to initiate the authorization of the payment explicitly.
- **Other data**

3. Initiate Authorization Request (TPP → ASPSP)

The TPP sends a POST request to initiate explicit authorization to initiate *token* payment to the ASPSP. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **paymentId:** identifier of the payment to be authorized
- **X-Request-ID:** request identifier assigned by the TPP.
- **Access token** from the TPP

4. Initiate Authorization Response (ASPSP → TPP)

The ASPSP responds to the TPP indicating:

Response 1 - There is only one SCA method available, redirect to SCA is returned:

- **scaStatus**: state in which the SCA is.

- **authorizationId**: identifier of the authorization sub-resource created by the Hub
- **_links**
    - **scaRedirect**: link to the Hub's authentication server to start SCA through a redirect (SCA does not apply over OAuth2). This URL can add security parameters to allow session maintenance during redirection.

      Ex: https://hub.example.com/auth
    - **scaStatus**: link of the Hub to which the TPP can make a request to consult the state of the SCA of the corresponding authorization sub-resource.

      Ex: https://hub.example.com/v1.1/payments/{payment-product}/{paymentId}/authorisations/{authorisationId}
- **Other data**

Response 2 - More than one SCA method available, selection by PSU necessary:

- **scaStatus**: state in which the SCA is.
- **authorizationId**: identifier of the authorization sub-resource created by the Hub
- **scaMethods-** Authentication objects that the PSU has available.
- **_links**
    - **selectAuthenticationMethod**: link of the Hub to which the TPP will be able to refer the SCA method selected by the PSU.

      Ex: https://hub.example.com/v1.1/payments/{payment-product}/{paymentId}/authorisations/{authorisationId}
    - **scaStatus**: link of the Hub to which the TPP can make a request to consult the state of the SCA of the corresponding authorization sub-resource.

      Ex: https://hub.example.com/v1.1/payments/{payment-product}/{paymentId}/authorisations/{authorisationId}
- **Other data**

Present SCA Methods (TPP → PSU) and select method (PSU → TPP)

The TPP, in case of receiving response 2 from the Hub (more than one SCA method), shows the PSU the SCA methods it has available to be selected.

The PSU selects one of the methods available to it.

5. Request Update PSU data (SCA Methods) (TPP → ASPSP)

The TPP sends a PUT request to update the SCA method selected by the PSU with *token* to the Hub. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **authorizationId:** identifier of the authorization sub-resource created by the Hub
- **X-Request-ID:** request identifier assigned by the TPP.

- **Access token** from TPP to Hub
- **methodId:** identifier of the SCA method selected by the PSU

6. Response update PSU data (ASPSP → TPP)

The ASPSP responds to the TPP indicating:

- **scaStatus**: state in which the SCA is.
- **_links**
  - **scaRedirect**: link to the Hub's authentication server to start SCA through a redirect (SCA does not apply over OAuth2). This URL can add security parameters to allow session maintenance during redirection.

    Ex: https://hub.example.com/auth
  - **scaStatus**: link of the Hub to which the TPP can make a request to consult the state of the SCA of the corresponding authorization sub-resource.

    Ex: https://hub.example.com/v1.1/payments/{payment-product}/{paymentId}/authorisations/{authorisationId}
- **Other data**

7. TPP generates state

The TPP, after receiving the response, generates a value for *state* (XSRF token) to be linked to the PSU browser session.

8. Redirection to scaRedirect (TPP → ASPSP)

The TPP, after receiving the response to initiate authorization (or to update the SCA method), redirects the PSU to the authentication endpoint of the Hub and appends the *state* to it as query-param

HTTP/1.1 302 Found
Location: https://hub.example.com/auth?state=qwerty

SCA entre PSU ←→ASPSP

During this redirection process, ASPSP will be able to show ASPSP-PSU interface for SCA

9. Payment State Request (TPP → ASPSP)

The TPP will send a tokenised payment state request to the ASPSP for payment state.

10. Payment State Response (ASPSP → TPP)

The ASPSP updates the state of the operation and responds to the TPP.

6.1.2 Payment initiation

Message sent by the TPP to the ASPSP through the Hub to create a payment initiation.

6.1.2.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/payments/{payment-product}

Path

Field	Description	Type	Mand.	Format
Provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
Aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
payment-product	Payment product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/

Query parameters

Additional parameters for this request are not specified.

Header

Field	Description	Type	Mand.	Format
Content-Type	Value: application/json	String	OB	Content-Type: application/json
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.:

				X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Consent-ID	This field will be ignored by the ASPSP. The session support is specified by the access token.	String	OP	^.{1,36}$ Ex: Consent-ID: 7890-asdf-4321
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. If it is not available, the TPP must use the IP address used by the TPP when it sends this request.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^.{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.:

				PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
TPP-Redirect-Preferred	If it is “true”, the TPP has informed the HUB that it prefers the SCA redirection.	Boolean	OP	E.g.: TPP-Redirect-Preferred: true

	If it is “false”, the TPP has informed the HUB that it prefers not to be redirected to the SCA and the procedure will be carried out by a decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply, depending on the SCA method chosen by the TPP/PSU. **EMBEDDED AND DECOUPLED ARE NOT SUPPORTED IN THIS VERSION**			
TPP-Redirect-URI	The TPP’s URI, where the transaction flow should be redirected to after some of the SCA phases. It is recommended to use this header field at all times. In the future, this field could become mandatory.	String	COND	^.{1,250}$ E.g.: TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting that the transaction flow is redirected in this direction instead of to the TPP-Redirect-URI in the event of a negative result from the SCA redirection method.	String	OP	^.{1,250}$ E.g.: TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"
TPP-Explicit-Authorisation-Preferred	If it is “true”, the TPP prefers to start the authorisation process separately, E.g.: given the need for the authorisation of a set of simultaneous transactions. If it is “false” or the parameter is not used, the TPP has no preference. The TPP accepts a direct authorisation of the transaction in the next step. **Note**: NOT SUPPORTED	Boolean	OP	E.g.: TPP-Explicit-Authorisation-Preferred: false
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes

TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……Ko ZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

The content of the Body is defined in 8.17 SinglePayment following the conditions of the following table.

The fields marked as mandatory (OB) and optional (OP) are supported by the ASPSP with this type of condition.

The fields marked as COND depend on each ASPSP.

Campo	SCT	SCT INST	Target 2	Cross Border CT
endToEndIdentification*	OP	OP	NA	NA
instructionIdentification	NA	NA	NA	NA
debtorName	OP	OP	OP	OP
debtorAccount	OB	OB	OB	OB
debtorId	NA	NA	NA	NA
ultimateDebtor	NA	NA	NA	NA
instructedAmount	OB	OB	OB	OB
currencyOfTransfer	COND	COND	COND	COND
exchangeRateInformation	NA	NA	NA	NA
creditorAccount	OB	OB	OB	OB
creditorAgent	OP	OP	OP	OB/OP
creditorAgentName	NA	NA	NA	NA
creditorName	OB	OB	OB	OB
creditorId	NA	NA	NA	NA
creditorAddress	OP	OP	OP	OB/OP
creditorNameAndAddress	COND	COND	COND	COND
ultimateCreditor	NA	NA	NA	NA
purposeCode	NA	NA	NA	NA
chargeBearer	COND	COND	COND	COND
serviceLevel	NA	NA	NA	NA
remittanceInformationUnstructured	OP	OP	OP	OP

remittanceInformationUnstructuredArray	NA	NA	NA	NA
remittanceInformationStructured	NA	NA	NA	NA
remittanceInformationStructuredArray	NA	NA	NA	NA
requestedExecutionDate	OP	NA	NA	NA
requestedExecutionTime	NA	NA	NA	NA

***NOTE: This field will be used by the ASPSP, optionally to be sent by you, to inform the TPP of the value of the endToEndIdentification that the ASPSP itself includes in this identifier in the transfer itself.**

6.1.2.2 Response

Header

Field	Description	Type	Mand.	Format
Location	It contains the generated link to the resource.	String	OB	^.{1,512}$ E.g.: Location: /v1.1/payments/{payment-product}/{payment-id}
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Returned value if the SCA method has been set. Possible values: • REDIRECT The SCA based on OAuth will be taken as a REDIRECT.	String	COND	E.g.: ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Mand.	Format
transactionStatus	Status of the transaction. Values defined in Annexes in 9.4 Transaction status	String	OB	**ISO 20022** E.g.: "transactionStatus": "RCVD"
paymentId	Resource identifier referred to the payment initiation.	String	OB	^.{1,36}$

				E.g.: "paymentId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
_links	List of hyperlinks to be recognised by the TPP. Types supported in this response: • scaRedirect: in the event of the SCA redirect. Link where the PSU's browser must be redirected by the TPP. • self: link to the resource created by this request. • status: link to retrieve the transaction status.	Links	OB	E.g.: "_links": {…}
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.1.2.3 Examples

Example of an SCA redirection request

POST https://www.hub.com/aspsp-name/v1.1/payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://www.tpp.com/cb

TPP-Nok-Redirect-URI: https://www.tpp.com/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

{
"instructedAmount": {
"currency": "EUR",
"amount": "153.50"
},
"debtorAccount": {
"iban": "ES1111111111111111111111"
},
"creditorAccount": {
"iban": "ES2222222222222222222222"
},
"creditorName": "Name123",
"remittanceInformationUnstructured": "Additional information"
}

Example of a response in the event that the SCA redirection with an implicitly created authorisation sub-resource

HTTP/1.1 201 Created

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 26 Sep 2017 15:02:43 GMT

Location: /v1.1/payments/sepa-credit-transfers/123-qwe-456

Content-Type: application/json

{
"transactionStatus": "RCVD",
"paymentId": "123-qwe-456",
"_links": {
"scaRedirect": {
"href": "https://hub.example.es/authorize"
},
"self": {
"href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456",
"status": {
"href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/status"
},
"scaStatus": {
"href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/authorisations/123auth456"

```
                }
        }
}
```

Example of a request for the SCA decoupled (NOT CURRENTLY DEVELOPED)

POST https://hub.example.es/asp-name/v1.1/payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: false

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
        "instructedAmount": {
                "currency": "EUR",
                "amount": "153.50"
        },
        "debtorAccount": {
                "iban": "ES1111111111111111111111"
        },
        "creditorAccount": {
                "iban": "ES2222222222222222222222"
        },
        "creditorName": "Name123",
        "remittanceInformationUnstructured": "Additional information"
```

}

6.1.3 Future payment initiation

Message sent by the TPP to the ASPSP through the Hub to create a future payment initiation.

This functionality is similar to the Payment Initiation. The only difference that exists is in the messaging of the Start of payment request that supports an optional extra parameter "requestedExecutionDate" to indicate the future date on which the payment would be executed.

In this type of payment, after the execution of SCA, the payment is not executed, but the ASPSP leaves it scheduled to execute on the specified date.

6.1.3.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/payments/{payment-product}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: hub.example.es
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
payment-product	Payment product to use. List of supported products: • sepa-credit-transfers	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/

Query parameters

Additional parameters for this request are not specified.

Header

Field	Description	Type	Mand.	Format
Content-Type	Value: application/json	String	OB	Content-Type: application/json
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.:

				X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. If it is not available, the TPP must use the IP address used by the TPP when it sends this request.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^.{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device.	String	OP	**UUID**

	The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.			^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
TPP-Redirect-Preferred	If it is "true", the TPP has informed the HUB that it prefers the SCA redirection. If it is "false", the TPP has informed the HUB that it prefers not to be redirected to the SCA and the procedure will be carried out by a decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply, depending on the SCA method chosen by the TPP/PSU. **EMBEDDED AND DECOUPLED ARE NOT SUPPORTED IN THIS VERSION**	Boolean	OP	E.g.: TPP-Redirect-Preferred: true
TPP-Redirect-URI	The TPP's URI, where the transaction flow should be redirected to after some of the SCA phases. It is recommended to use this header field at all times. In the future, this field could become mandatory.	String	COND	^.{1,250}$ E.g.: TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting that the transaction flow is redirected in this direction instead of to the TPP-Redirect-URI in the event of a negative result from the SCA redirection method.	String	OP	^.{1,250}$ E.g.: TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"

TPP-Explicit-Authorisation-Preferred	If it is “true”, the TPP prefers to start the authorisation process separately, E.g.: given the need for the authorisation of a set of simultaneous transactions. If it is “false” or the parameter is not used, the TPP has no preference. The TPP accepts a direct authorisation of the transaction in the next step. **Note**: NOT SUPPORTED.	Boolean	OP	E.g.: TPP-Explicit-Authorisation-Preferred: false
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

The Body’s content is defined in 8.17 SinglePayment and the following parameter must also be reported:

Field	Description	Type	Mand.	Format
requestedExecutionDate	The payment will be executed on the reported date. **Note**: this field must be reported.	String	OP	**ISODate** E.g.: "requestedExecutionDate":"2019-01-12"

The fields marked as mandatory (MA) and optional (OP) are supported by the ASPSP with this type of condition.

The fields marked as COND depend on each ASPSP.

Field	SCT	SCT INST	Target 2	Cross Border CT
endToEndIdentification*	NA	NA	NA	NA
instructionIdentification	COND	COND	COND	COND
debtorName	COND	COND	COND	COND
debtorAccount	MA	MA	MA	MA
debtorId	COND	COND	COND	COND
ultimateDebtor	COND	COND	COND	COND
instructedAmount	MA	MA	MA	MA
currencyOfTransfer	COND	COND	COND	COND
exchangeRateInformation	COND	COND	COND	COND
creditorAccount	MA	MA	MA	MA
creditorAgent	OP	OP	OP	OB/OP
creditorAgentName	COND	COND	COND	COND
CreditorName	MA	MA	MA	MA
creditorId	COND	COND	COND	COND
creditorAddress	OP	OP	OP	OP
creditorNameAndAddress	COND	COND	COND	COND
ultimateCreditor	COND	COND	COND	COND
purposeCode	COND	COND	COND	COND
chargeBearer	COND	COND	COND	COND
serviceLevel	COND	COND	COND	COND
remittanceInformationUnstructured	OP	OP	OP	OP
remittanceInformationUnstructuredArray	COND	COND	COND	COND
remittanceInformationStructured	COND	COND	COND	COND
remittanceInformationStructuredArray	COND	COND	COND	COND
requestedExecutionDate	MA	MA	MA	MA
requestedExecutionTime	n.a.	n.a.	n.a.	n.a.

***NOTE: This field will be used by the ASPSP, optionally to be sent by you, to inform the TPP of the value of the endToEndIdentification that the ASPSP itself includes in this identifier in the transfer itself.**

6.1.3.2 Response

HTTP Code

201 if the resource has been created

Header

Field	Description	Type	Mand.	Format
Location	It contains the generated link to the resource.	String	OB	**Max512Text** E.g.: Location: /v1.1/payments/{payment-product}/{payment-id}
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Returned value if the SCA method has been set. Possible values: • REDIRECT The SCA based on OAuth will be taken as a REDIRECT.	String	COND	E.g.: ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Mand.	Format
transactionStatus	Status of the transaction. Values defined in Annexes in 9.4 Transaction status	String	OB	**ISO 20022** E.g.: "transactionStatus": "RCVD"
paymentId	Resource identifier referred to the payment initiation.	String	OB	^.{1,36}$ E.g.: "paymentId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
_links	List of hyperlinks to be recognised by the HUB. Types supported in this response: • scaRedirect: in the event of the SCA redirect. Link where the PSU's browser must be redirected by the HUB. • self: link to the resource created by this request. • status: link to retrieve the transaction status.	Links	OB	E.g.: "_links": {…}
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,512}$

				E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP sent though the HUB.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.1.3.3 Examples

Example of an SCA redirection request

POST https://hub.example.es/aspsp-name/v1.1/payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://tpp.example.es/cb

TPP-Nok-Redirect-URI: https://tpp.example.es/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
        "instructedAmount": {
                "currency": "EUR",
                "amount": "153.50"
        },
        "debtorAccount": {
                "iban": "ES1111111111111111111111"
        },
        "creditorAccount": {
                "iban": "ES2222222222222222222222"
        },
        "creditorName": "Name123",
        "remittanceInformationUnstructured": "Additional information",
```

"requestedExecutionDate": "2019-01-12"

}

6.1.4 Initiation of standing orders for recurring / periodic payments

Message sent by the TPP to the ASPSP through the Hub to create a recurring / periodic payment initiation.

The initiation of recurring payments functionality is specifically covered by the Berlin Group as the initiation of a specific standing order.

A TPP can send an initiation of a recurring payment in which the start date, frequency and the end date must all be provided.

Once authorised by the PSU, the payment will be executed by the ASPSP, if possible, following the "standing order" as it was sent by the TPP. No further action is needed by the TPP.

In this context, this payment is considered a periodic payment to differentiate it from other types of recurring payments where third parties initiate the same amount of money.

Note: to initiate standing order payments, the ASPSP will always request the SCA with Dynamic linking. No exemptions are allowed.

Rules for the dayOfExecution field

- **Daily payments**: the “dayOfExecution” field is not necessary. The first payment is on the “startDate”, and from then on, the payment is made every day.
- **Weekly payments**: if the “dayOfExecution” is required, the possible values are 01=Monday to 07=Sunday. If the “dayOfExecution” is not required, the “startDate” will be the day of the week on which the payment is made. (If the “startDate” is Thursday, the payment will be made every Thursday).
- **Fortnightly payments**: the same rule applies as for weekly payments.
- **Monthly payments or longer payment periods**: the possible values range from 01 to 31. Using the 31st is used as the last day of the month (only for monthly payments). For longer periods an error will be returned.

6.1.4.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/periodic-payments/{payment-product}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: hub.example.es
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

payment-product	Payment product to use. List of supported products: sepa-credit-transfers	String	OB	E.g.: {provider}/{aspsp-name)/v1.1/periodic-payments/sepa-credit-transfers/

Query parameters

Additional parameters for this request are not specified.

Header

Field	Description	Type	Mand.	Format
Content-Type	Value: application/json	String	OB	Content-Type: application/json
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. If it is not available, the TPP must use the IP address used by the TPP when it sends this request.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^.{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$

				E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
TPP-Redirect-Preferred	If it is “true”, the TPP has informed the HUB that it prefers the SCA redirection. If it is “false”, the TPP has informed the HUB that it prefers not to be redirected to the SCA and the procedure will be carried out by a decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply, depending on the SCA method chosen by the TPP/PSU. **EMBEDDED AND DECOUPLED ARE NOT SUPPORTED IN THIS VERSION**	Boolean	OP	E.g.: TPP-Redirect-Preferred: true

TPP-Redirect-URI	The TPP's URI, where the transaction flow should be redirected to after some of the SCA phases. It is recommended to use this header field at all times. In the future, this field could become mandatory.	String	COND	^.{1,250}$ E.g.: TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting that the transaction flow is redirected in this direction instead of to the TPP-Redirect-URI in the event of a negative result from the SCA redirection method.	String	OP	^.{1,250}$ E.g.: TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

The Body's content is defined in 8.17 SinglePayment along with as the definitions listed below:

Field	Description	Type	Mand.	Format
startDate	The first applicable execution day from this date is the first payment.	String	OB	**ISODate** E.g.: "startDate":"2018-12-20"
endDate	The last applicable execution day. If there is nothing entered it is a standing order with no end.	String	OP	**ISODate** E.g.: "endDate":"2019-01-20"

frequency	The frequency of the recurring payment resulting from this standing order. Allowed values: • Daily • Weekly • EveryTwoWeeks • Monthly • EveryTwoMonths • Quarterly • SemiAnnual • Annual	String	OB	**EventFrequency7Code de ISO 20022** E.g.: "frequency":"monthly"
dayOfExecution	"31" is last. Only if the frequency is monthly The regular expression \d{1,2} follows. The date refers to the ASPSP's time zone.	String	COND	\d{1,2} E.g.: "dayOfExecution":"01"

The fields marked as mandatory (MA) and optional (OP) are supported by the ASPSP with this type of condition.

The fields marked as COND depend on each ASPSP.

Field	SCT	SCT INST	Target 2	Cross Border CT
endToEndIdentification*	NA	NA	NA	NA
instructionIdentification	COND	COND	COND	COND
debtorName	COND	COND	COND	COND
debtorAccount	MA	MA	MA	MA
debtorId	COND	COND	COND	COND
ultimateDebtor	COND	COND	COND	COND
instructedAmount	MA	MA	MA	MA
currencyOfTransfer	COND	COND	COND	COND
exchangeRateInformation	COND	COND	COND	COND
creditorAccount	MA	MA	MA	MA
creditorAgent	OP	OP	OP	MA/OP
creditorAgentName	COND	COND	COND	COND
CreditorName	MA	MA	MA	MA
creditorId	COND	COND	COND	COND
creditorAddress	OP	OP	OP	OP
creditorNameAndAddress	COND	COND	COND	COND
ultimateCreditor	COND	COND	COND	COND

purposeCode	COND	COND	COND	COND
chargeBearer	COND	COND	COND	COND
serviceLevel	COND	COND	COND	COND
remittanceInformationUnstructured	OP	OP	OP	OP
remittanceInformationUnstructuredArray	COND	COND	COND	COND
remittanceInformationStructured	COND	COND	COND	COND
remittanceInformationStructuredArray	COND	COND	COND	COND
requestedExecutionDate	n.a.	n.a.	n.a.	n.a.
requestedExecutionTime	n.a.	n.a.	n.a.	n.a.

***NOTE: If you want to send the endToEndId field, you must report it in the body remittanceInformationUnstructured field. The best practices guide provides how to send the endToEndId field within that field.**

6.1.4.2 Response

Header

Field	Description	Type	Mand.	Format
Location	It contains the generated link to the resource.	String	OB	^.{1,512}$ E.g.: Location: /v1.1/periodic-payments/{payment-product}/{payment-id}
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Returned value if the SCA method has been set. Possible values: • REDIRECT The SCA based on OAuth will be taken as a REDIRECT.	String	COND	E.g.: ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Mand.	Format
transactionStatus	Status of the transaction. Values defined in Annexes in 9.4 Transaction status	String	OB	**ISO 20022** E.g.: "transactionStatus": "RCVD"

paymentId	Resource identifier which references the periodic payment.	String	OB	^.{1,36}$ E.g.: "paymentId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
_links	List of hyperlinks to be recognised by the TPP. Types supported in this response: • scaRedirect: in the event of the SCA redirect. Link where the PSU's browser must be redirected by the TPP. • self: link to the resource created by this request. • status: link to retrieve the transaction status.	Links	OB	E.g.: "_links": {…}
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP sent though the HUB.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.1.4.3 Examples

Example of an SCA redirection request

POST https://hub.example.es/{aspsp-name}/v1.1/periodic-payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://tpp.example.es/cb

TPP-Nok-Redirect-URI: https://tpp.example.es/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
        "instructedAmount": {
        "currency": "EUR",
                "amount": "153.50"
        },
        "creditorAccount": {
```

```
            "iban": "ES2222222222222222222222"
        },
        "creditorName": "Name123","remittanceInformationUnstructured":"Additional Information",
        "startDate": "2018-03-01",
        "frequency": "monthly",
        "dayOfExecution": "01"
}
```


6.1.5 Obtain payment status

This message is sent by the TPP to the HUB to request information on the status of the payment initiation requested by the TPP.

6.1.5.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/status

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
payment-service	Possible values are: • payments • periodic-payments	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments
payment-product	Payment product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/
paymentId	Resource identifier referred to the payment initiation. Sent previously as a response to a payment initiation from the TPP to the HUB.	String	OB	^.{1,36}$ E.g.: 1234-qwer-5678

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Accept	Format supported of the response. Supported values: • application/json	String	OP	^.{1,50}$ E.g.: Accept: application/json
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.:

				PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No additional data is specified.

6.1.5.2 Response

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
transactionStatus	Status of the payment transaction. Values defined in 9.4 Transaction status	String	OB	**ISO20022** E.g.: "transactionStatus":"ACCP"
psuName	Name of the connected PSU. In case of corporate accounts, this could be the person acting on behalf of the company.	String	OP	^.{1,140}$ Ej: “psuName”: “Heike Mustermann”
ownerNames	List of account owner names.	List<AccountOwner>	OP	Ej: “ownerNames”:[…]
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages":[…]

6.1.5.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/v1.1/payments/sepa-credit-transfer/123asdf456/status

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response

HTTP/1.1 200 OK
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json

{

"transactionStatus": " ACCP”

}

6.1.6 Retrieve information from the start of the payment

This message is sent by the TPP through the HUB to the ASPSP to obtain information on the payment initiation.

6.1.6.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
payment-service	Possible values are: • payments • periodic-payments	String	OB	E.g.: {provider}/{aspsp}/ v1.1/payments

payment-product	Payment product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/
paymentId	Resource identifier referred to the payment initiation. Sent previously as a response to a payment initiation from the TPP to the HUB.	String	OB	^.{1,36}$ E.g.: 1234-qwer-5678

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8

PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP.	String	OB	See annexes

	See 9.1 Signature for more information.			
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……..KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No additional data is specified.

6.1.6.2 Response

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

The fields to be returned are those of the original payment initiation request:

- 6.1 Payment initiaition
- 6.1.3 Future payment initiation
- 6.1.4 Initiation of standing orders for recurring / periodic payments

In addition to the following:

Field	Description	Type	Mand.	Format
transactionStatus	Status of the transaction. Values defined in annexes. Short code.	String	OB	**ISO 20022** E.g.: "transactionStatus": "ACCP"
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP sent though the HUB.	List<TppMessage>	OP	E.g.: "tppMessage": […]

6.1.6.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/v1.1/payments/sepa-credit-transfers/123-asdf-456

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response

HTTP/1.1 200 OK

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "instructedAmount": {
                "currency": "EUR",
                "amount": "153.50"
        },
        "debtorAccount": {
                "iban": "ES1111111111111111111111"
        },
        "creditorAccount": {
                "iban": "ES2222222222222222222222"
        },
        "creditorName": "Name123",
        "remittanceInformationUnstructured": "Additional information",
        "transactionStatus": "ACCP"
}
```

6.1.7 Cancelling a payment initiation

This request is sent by the TPP to the ASPSP through the Hub and allows the payment initiation to be cancelled. Depending on the payment service, the payment product and ASPSP's implementation, this request may be sufficient to cancel the payment or an authorisation may be required.

6.1.7.1 Request

Endpoint

DELETE {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}

Path

Field	Description	Type	Mand.	Format
provider	URL of the ASPSP where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
payment-service	Possible values are: • payments • periodic-payments	String	OB	E.g.: {provider}/v1.1/payments
payment-product	Payment product to use. List of supported products: • sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	OB	E.g.: {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/
paymentId	Resource identifier referred to the payment initiation. Sent previously as a response to a payment initiation from the HUB to the ASPSP.	String	OB	^.{1,36}$ E.g.: 123-qwe-456

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format

X-Request-ID	Unique identifier assigned by the TPP for the request and sent through the HUB to the ASPSP	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: DELETE

PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……..KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No additional data is specified.

6.1.7.2 Response

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction and sent through the HUB to the ASPSP.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
transactionStatus	Status of the transaction. Values defined in Annexes in 9.4 Transaction status	String	OB	**ISO 20022** E.g.: "transactionStatus": "CANC"
_links	List of hyperlinks to be recognised by the TPP. These depend on the decision made by the ASPSP to evaluate the translation. Types supported in this response.	Links	COND	E.g.: "_links": {…}
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP sent though the HUB.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.1.7.1 Examples

Example of a request

DELETE https://www.hub.com/aspsp-name/v1.1/payments/sepa-credit-transfers/123-qwe-456

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Content-Type: application/json

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of response when authorisation of the cancellation by the PSU is required

HTTP/1.1 200 OK

X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT

```
{
        "transactionStatus": "ACTC",
        "_links": {
                "startAuthorisation": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations"
                }
        }
}
```


Example response where an authorization of the cancellation by the PSU is not necessary

HTTP / 1.1 204 No content

X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT

Example answer where if an implicit authorization of the cancellation by the PSU is necessary

HTTP / 1.1 202 Ok

X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT


```
{
        "transactionStatus": "ACTC",
        "_links": {
        "scaRedirect": {
                        "href": "https://api.hub.com/authorize"
                },
                "self": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456"
                },
                "state": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/state"
                },
                "scaStatus": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations/qwer-234/state"
                }
        }
}
```


Example answer where if an implicit authorization of the cancellation by the PSU is necessary

HTTP / 1.1 202 Ok

X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT


```
{
        "transactionStatus": "ACTC",
        "_links": {
                "self": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456"
                },
                "state": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/state"
                },
                "startAuthorisation": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations"
                }
        }
}
```


6.2 AIS: Service to establish consent to account information

6.2.1 Characteristics of the different types of consents

6.2.1.1 Consent model

Model	Description
Detailed consent	**Request for consent about the accounts specified** Creates a consent which must be stored by the ASPSP, requesting access to the specified accounts and the requested access. If there was already consent in place, it will expire and the new one will enter into force once it has been authorised by the PSU. The accounts for which consent is requested to access “balances” and/or “transactions” will automatically also have access to “accounts”.
Global consent	**Request consent to gain access to all the access to all accounts for the AIS services of the PSD2** Requests access to all the PSU’s available accounts of PSU for all the AIS services of the PSD2. The accounts are not specified by the TPP. In the request the access accounts that you want to have access to, are not specified. “All PSD2 accounts” is specified in the request, using “allPsd2” in the “allAccounts” value.

Through the HUB, the TPP can retrieve the said information handled by the ASPSP and the PSU with a request to retrieve information on the consent.

After successfully registering an allPsd2 consent, to access the account endpoints, the first endpoint to be invoked is the account listing endpoint.

Bank offered consent

Request consent without specifying the accounts
Request consent to access “accounts”, “balances”, and/or “transactions” without specifying the accounts. In other words, the attributes “accounts”, “balances” and “transactions” will go in a blank array.

To select the accounts to be provided, access must be obtained bilaterally between the ASPSP and the PSU through the ASPSP interface in the redirect flow from OAuth.

In the redirection process the ASPSP will show the PSU their accounts on which it wants to give consent to the TPP.

Through the HUB, the TPP can retrieve the said information handled by the ASPSP and the PSU with a request to retrieve information on the consent.

After successfully registering a consent without specifying the accounts, to access the account endpoints, the first endpoint that must be invoked is the endpoint to obtain details of a consent and then the list of accounts.

6.2.1.2 Recurring access

Recurrent consents

If there is a prior consent for recurring access (recurringIndicator:true) in place and a new request for recurring access is made, as soon as the new consent is accepted by the PSU, the old one will expire and the new requested consent will be the valid one.

A consent with recurring access can have one or more accounts with different types of access (“accounts”, “balances”, “transactions”).

Note: giving access to “balances” and/or “transactions” automatically gives access to these “accounts”.

Non-recurrent consents

A request for consent for a non-recurring access (for one access only with the recurringIndicator:false) will be treated as a new consent (new consentId) without affecting the previously given existing consents.

6.2.1.3 Return of the account holder's name

This specification is based on one of the consent models described in NextGenPSD2 XS2A Framework v1.3.8. In particular, the following model is used for this specification:

- The ASPSP will release the name of the account holder, in this case, the name of the connected PSU, without adopting the extension of the consent model defined in the standard.
- In either case, the final decision to return the PSU name through the API will depend on whether you are currently returning through the ASPSP's online channels.

6.2.1.4 List of standing orders

Obtain the list of standing orders for a specific account. Information is returned as transactions using the "bookingStatus" entry state with the value "information".

6.2.1.5 Consent state information

The state of the consent resource changes during the process of establishing consent. The attribute defined for the consent state is defined as "consentStatus".

The only states supported in the initial phase for consentStatus are "received", "rejected" and "valid".

After successful authorization by a PSU, the consent resource could change its state during its life cycle. The following codes are supported during the consent lifecycle phase:

- "expired": consent has expired (for example, after 90 days)
- "revokedByPsu": consent has been revoked by the PSU
- "terminatedByTpp": the TPP has terminated consent

The TPP can retrieve this state on the GET request to retrieve consent state.

Note: the "expired" state also applies to single-use consent, once they have been used or have expired.

Note: the "terminatedByTpp" state also applies when a recurring consent has been terminated by the TPP by establishing a new recurring consent.

Additionally, the TPP can retrieve the SCA state for consent establishment with the corresponding SCA state GET request.

6.2.2 Account information consent flows

6.2.2.1 SCA flow by redirection: implicit start of authorization process

The image below depicts Figure 4: SCA flow by redirection: implicit start of the authorisation processthe sequence of requests/responses and redirections that are necessary in the flow where strong authentication (SCA) by redirection is needed (SCA over OAuth2 is not applied).

The characteristics of this flow are:

- TPP-Redirect-Preferred: true - SCA TPP preference for redirection
- TPP-Explicit-Authorisation-Preferred: false - TPP preference to initiate the authorisation process associated with consent implicitly
- The PSU has only one SCA method

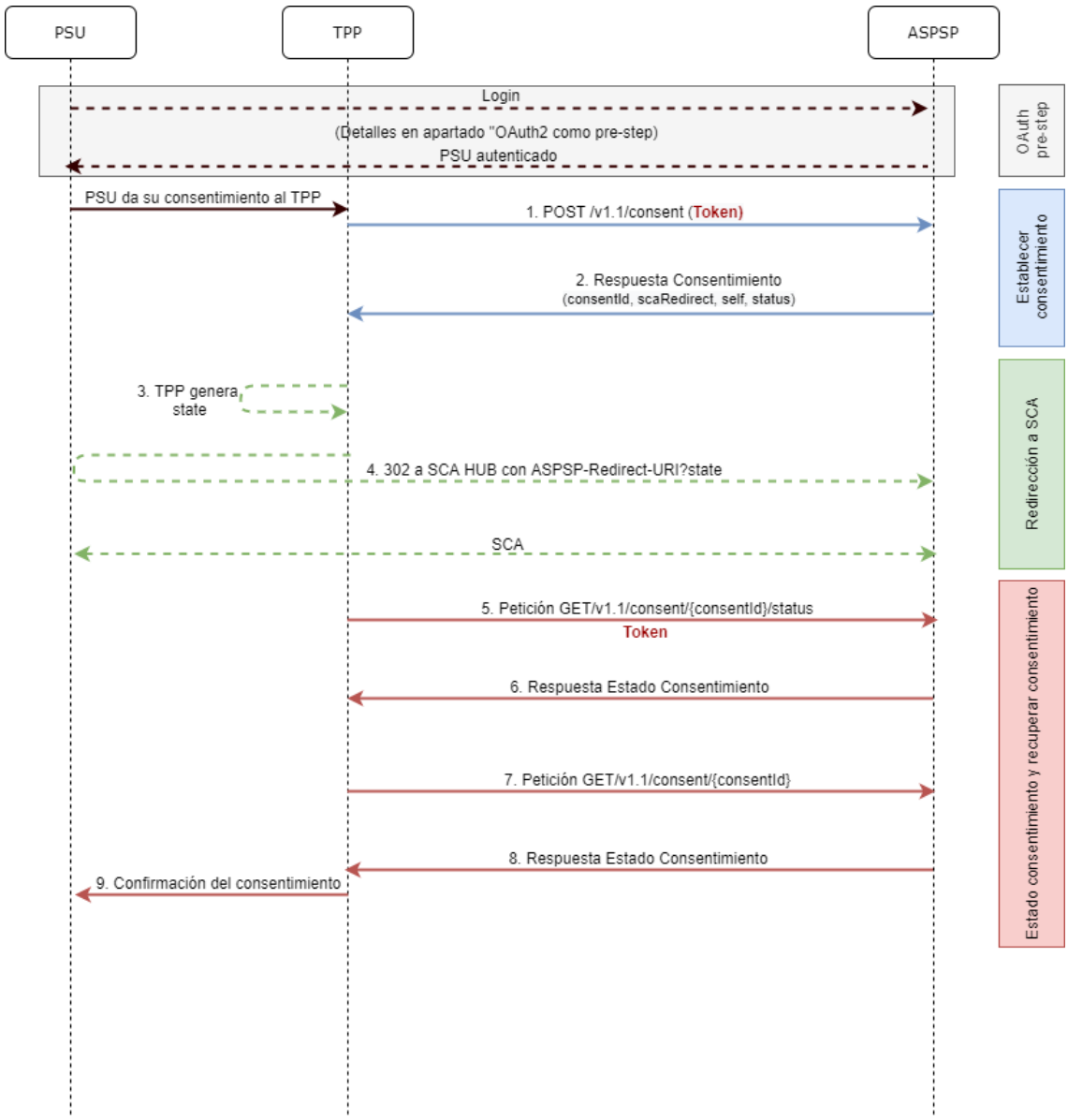


Figure 4: SCA flow by redirection: implicit start of the authorisation process

OAuth2 (pre-step)

The main purpose of this flow is to authenticate the PSU to get access to the services displayed by its ASPSP through the use of an access token obtained after the application of this protocol.

In order to simplify, the detail of this flow has been omitted from the Figure 4 Figure 4: SCA flow by redirection: implicit start of the authorisation process and can be found in the section 6.1**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.VERIFY

Note: this step is optional. Only applies if no valid access token is available.

PSU gives its consent to the TPP

The PSU gives its consent to the TPP to access its accounts

1. Consent Request (TPP → ASPSP)

The TPP sends a POST request for consent of tokenised account information to the ASPSP. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **Consent data:** list of IBANs and/or PANs and types of access to which the PSU has given its consent, recurrence, validity, frequency of daily access...
- **X-Request-ID:** identifier of the operation assigned by the TPP.
- **Access token** from the TPP
- **TPP-Redirect-Preferred:** true - SCA flow preference by redirect
- **TPP-Redirect-URI:** Return URI of the TPP after redirection to SCA.
- **TPP-Explicit-Authorisation-Preferred:** false - TPP preference to initiate authorisation implicitly (current flow)

- **Other data**

2. Response of Consent (ASPSP → TPP)

The ASPSP responds to the TPP indicating that Strong Authentication (SCA) is required by redirecting to the Hub's authentication endpoint, returning:

- **consentStatus-** State of the consent resource.
- **consentId**: identifier generated by the Hub that refers to the consent resource.

- **_links**

    - **scaRedirect**: links to the Hub endpoint where after receiving the redirect from the TPP it redirects back to the scaRedirect of the ASPSP. This URL can add security parameters to allow session maintenance during redirection.

      Ex: https://hub.example.com/auth

    - **self**: link to the resource generated by the Hub for the request for consent received from the TPP.
    - **state**: link of the Hub to which the TPP will be able to make a consent state query request.

- **Other data**

3. TPP generates state

The TPP, after receiving the response, generates a value for *state* (XSRF token) to be linked to the PSU browser session.

4. Redirect to scaRedirect (TPP → ASPSP)

The TPP redirects the PSU to the authentication endpoint by adding to it the field*state* as a query-param.

HTTP/1.1 302 Found
Location: https://hub.example.com/auth?state=qwerty

SCA entre PSU ←→ASPSP

During this redirection process, the ASPSP will be able to:

- Show ASPSP-PSU interface for SCA

Note: if the consent request does not indicate the accounts for which consent is to be sought, the PSU will be shown its accounts during the SCA process to select which accounts and types of access, it wants to grant to the TPP.

5. State Consent Request (TPP → ASPSP)

The TPP will send a payment state request with *token* to the ASPSP to know the payment state.

6. Response State Consent (ASPSP → TPP)

The ASPSP updates the consent state and responds to the TPP.

7. Request to Retrieve Consent (TPP → ASPSP)

In case the consent request has travelled without indicating the accounts to be given access and the selection of these accounts has been made by the PSU in the ASPSP interface displayed during the redirect of the SCA flow, the TPP will make a request to retrieve information from the consent requested in order to know which accounts have been authorised by the PSU.

The TPP will send a request to the Hub to retrieve consent with the consent identifier provided by the Hub in the consent request response and with a valid access token.

The HUB will make a request to retrieve consent with the consent identifier provided by the ASPSP in the consent request response and with the access token to the ASPSP and, after obtaining a response from the ASPSP, it will send the consent to the TPP.

8. Response Retrieve Consent (ASPSP → TPP)

The ASPSP sends the consent it requested to the TPP along with the accounts and types of access granted to it.

6.2.2.2 SCA flow by redirection: implicit start of authorization process.

Similar to 6.1.1.2 SCA flow by redirection: implicit start of authorization

6.2.2.3 Access Counter

The access counter is independent for each endpoint / account and its maximum value is determined by the value of the "frequencyPerDay" of the consent.

If a consent establishes a maximum of 4 accesses for the IBAN 1 account and the access types accounts, balances, transactions, then the following will be allowed:

- 4 accesses to the account listing endpoint
- 4 accesses to the account detail endpoint
- 4 accesses to the account balance endpoint
- 4 accesses to the account transaction endpoint

The counter is increased with requests that do not have the PSU-IP-Address informed. If this field is informed with an IP address, it means, according to the standard, that it is a request made with a PSU present, and that request should not be taken into account to increase the counter.

6.2.3 Consent to information on payment accounts

With this service, through the HUB, a TPP can request a consent to access the accounts of the PSU. This request may be for specific accounts but this is not a requirement.

Therefore, the request for consent has the following variations:

- Set up consent to account information for specified accounts.
- Set up consent to account information without specifying which accounts.
- Set up consent to account information for all the AIS access types of the PSD2: “accounts”, “balances” and/or “transactions”.

Note: each consent to information will generate a new resource, i.e. a new consentId.

6.2.3.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/consents

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7

PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
TPP-Redirect-Preferred	If it is "true", the TPP has informed the HUB that it prefers the SCA redirection. If it is "false", the TPP has informed the HUB that it prefers not to be redirected to the SCA and the procedure will be carried out by a decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply, depending on the SCA method chosen by the TPP/PSU. **EMBEDDED IS NOT SUPPORTED IN THIS VERSION** **DECOUPLED CURRENTLY NOT SUPPORTED**	Boolean	OP	E.g.: TPP-Redirect-Preferred: true
TPP-Redirect-URI	The TPP's URI, where the transaction flow should be redirected to after some of the SCA phases. It is recommended to use this header field at all times. In the future, this field could become mandatory.	String	COND	^.{1,250}$ E.g.: TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting that the transaction flow is redirected in this direction instead of to the TPP-Redirect-URI in the event of a negative result from the SCA redirection method.	String	OP	^.{12,50}$ E.g.: TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"
TPP-Explicit-Authorisation-Preferred	If it is "true", the TPP prefers to start the authorisation process separately, e.g.: given the need for the authorisation of a set of simultaneous transactions.	Boolean	OP	E.g.: TPP-Explicit-Authorisation-Preferred: false

	If it is “false” or the parameter is not used, the TPP has no preference. The TPP accepts a direct authorisation of the transaction in the next step. **Note**: IT ONLY ALLOWS THE FALSE OPTION			
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

Field	Description	Type	Mand.	Format
access	Access requested to the services. Only sub-attributes with the tags: "accounts", "balances" and "transactions" are accepted. Additionally, the ASPSP can support the sub-attributes:"allPsd2" with the value "allAccounts".	AccountAccess	OB	E.g.: "access":{…}
recurringIndicator	Possible values: • true: recurring access to the account. • false: one access only.	Boolean	OB	E.g.: "recurringIndicator":true
validUntil	Date to which the consent requests access. To create the maximum possible access period, the value to be used is: 9999-12-31	String	OB	**ISODate** E.g.: "validUntil":"2018-05-17"

	When the consent is retrieved, the maximum possible date will be returned having been adjusted.			
frequencyPerDay	Indicates the frequency of accessing the account per day. 1 if it is one single use.	Integer	OB	E.g.: "frequencyPerDay":4
combinedServiceIndicator	Indicator that a payment will be made in the same session.	Boolean	OB	E.g.: "combinedServiceIndicator": false

6.2.3.2 Response

HTTP Code

201 if the resource has been created

Header

Field	Description	Type	Mand.	Format
Location	It contains the generated hyperlink to the resource	String	OB	**Max512Text** E.g.: Location: /v1.1/consents/{consentId}
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Returned value if the SCA method has been set. Possible values: • REDIRECT The SCA based on OAuth will be taken as a REDIRECT.	String	COND	E.g.: ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Mand.	Format

consentStatus	Authentication status of the consent. See the defined values in 9.5 Consent status	String	OB	E.g.: "consentStatus": "received"
consentId	Resource identifier which references the consent. It must be content if it generated a consent.	String	OB	^.{1,36}$ E.g.: "consentId":"123-QWE-456"
_links	List of hyperlinks to be recognised by the TPP. Types supported in this response: • scaRedirect: in the event of the SCA redirect. Link where the PSU's browser must be redirected by the TPP. • self: link to the resource created by this request. • status: link to retrieve the transaction status. •	Links	OB	E.g.: "_links": {…}
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.2.3.3 Examples

Example of a request for consent on specified accounts with SCA redirection

POST https://www.hub.com/aspsp-name/v1.1/consents

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://www.tpp.com/cb

TPP-Nok-Redirect-URI: https://www.tpp.com/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT


```
{
        "access": {
                "balances": [
                {
                        "iban": "ES1111111111111111111111"
                },
                {
                        "iban": "ES2222222222222222222222",

                },
                {
                        "iban": "ES3333333333333333333333"
                }
                ],
                "transactions": [
                {
                        "iban": "ES1111111111111111111111"
                }
                ]
        },
        "recurringIndicator": true,
        "validUntil": "17/05/2018",
        "frequencyPerDay": 4
}
```


Example of a request for consent of a list of available accounts with SCA redirection

POST https://www.hub.com/aspsp-name/v1.1/consents

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://www.tpp.com/cb

TPP-Nok-Redirect-URI: https://www.tpp.com/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT


```
{
        "access": {
                "availableAccounts": "allAccounts"
        },
        "recurringIndicator": false,
        "validUntil": "17/05/2018",
        "frequencyPerDay": 1
}
```


Example of a response in the event that the SCA redirection with an implicitly generated authorisation sub-resource

HTTP/1.1 201 Created

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 26 Sep 2017 15:02:43 GMT

Location: /v1.1/consents/123-asdf-456

Content-Type: application/json


```
{
        "consentStatus": "received",
        "consentId": "123-asdf-456",
        "_links": {
                "scaRedirect": {
                        "href": "https://hub.example.es/authorize"
                },
                "self": {
                        "href": "/v1.1/consents/123-asdf-456",
                },
                "status": {
                        "href": "/v1.1/consents/123-asdf-456/status"
                },
        }
}
```

6.2.4 Get consent status

This service allows the TPP to find out the status of a request for consent initiated beforehand.

6.2.4.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/consents/{consent-id}/status

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
consentId	Resource identifier which references the consent. Sent previously as a response to a request for consent message from the TPP to the HUB.	String	OB	^.{1,36}$ E.g.:123-qwe-456

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.:

				Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7

PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

There is no additional data sent.

6.2.4.2 Response

HTTP Code

200 if the request has been successful.

This message is returned to the TPP by the HUB as a response to the consent status request message.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
consentStatus	Authentication status of the consent. See the defined values in 9.5 Consent status	String	OB	E.g.: "consentStatus":"valid"
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages":[…]

6.2.4.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/v1.1/consents/123asdf456/status

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response

HTTP/1.1 200 OK
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json

{

"consentStatus": "valid"

}

6.2.5 Retrieve information on the consent

6.2.5.1 Request

This message is sent by the TPP to the HUB as a request to retrieve information from a consent which had been previously created.

Endpoint

GET {provider}/{aspsp}/v1.1/consents/{consentId}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
consentId	Resource identifier which references the consent. Sent previously as a response to a request for consent message from the TPP to the HUB.	String	OB	^.{1,36}$ E.g.: 7890-asdf-4321

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5

PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963

Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……..KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

There is no additional data sent.

6.2.5.2 Response

HTTP Code

200 if the request has been successful.

This message is returned to the TPP by the HUB as a response to the message to retrieve information on the consent.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format

access	Access requested to the services. Only sub-attributes with the tags: "accounts", "balances" and "transactions" are accepted. Additionally, the ASPSP can support the sub-attributes "allPsd2" with the value "allAccounts".	Account Access	OB	E.g.: "access": {…}
recurringIndicator	Possible values: • true: recurring access to the account. • false: one access only.	Boolean	OB	E.g.: "recurringIndicator": true
validUntil	Date to which the consent requests access. To create the maximum possible access period, the value to be used is: 9999-12-31 When the consent is retrieved, the maximum possible date will be returned having been adjusted.	String	OB	**ISODate** E.g.: "validUntil": "17/05/2018"
frequencyPerDay	Indicates the frequency of accessing the account per day. 1 if it is one access only.	Integer	OB	E.g.: "frequencyPerDay":4
lastActionDate	Date on which the last modification was made on the consent.	String	OB	**ISODate** E.g.: "lastActionDate":"2018-01-01"
consentStatus	Authentication status of the consent. Values defined in annexes.	String	OB	E.g.: "consentStatus":"valid"
psuMessage	Text to be displayed to the PSU	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages":[…]

6.2.5.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/v1.1/consents/7890-asdf-4321/

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response on the consent of the specified accounts

HTTP/1.1 200 Ok

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "access": {
                "balances": [
                {
                        "iban": "ES1111111111111111111111"
                },
                {
                        "iban": "ES2222222222222222222222",

                },
                {
                        "iban": "ES3333333333333333333333"
                }
                ],
                "transactions": [
                {
                        "iban": "ES1111111111111111111111"
                }
                ]
        },
        "recurringIndicator": true,
        "validUntil": "17/05/2018",
        "frequencyPerDay": 4,
        "lastActionDate": "17/01/2018",
        "consentStatus": "valid"
```

}

Example response on global consent availableAccounts

HTTP/1.1 200 Ok

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json

{
"access": {
"availableAccounts": "allAccounts"
},
"recurringIndicator": true,
"validUntil": "2018-05-17",
"frequencyPerDay": 4,
"lastActionDate": "2018-01-17",
"consentStatus": "valid"
}

6.2.6 Remove consent

6.2.6.1 Request

This request may be sent by a TPP to the HUB to request that a previously created consent be removed.

Endpoint

DELETE {provider}/{aspsp}/v1.1/consents/{consentId}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
consentId	Resource identifier which references the consent. Sent previously as a response to a request for consent message from the TPP to the HUB.	String	OB	^.{1,36}$ E.g.: 7890-asdf-4321

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP.	String	OB	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)

PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: DELETE
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ.....KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

There is no additional data sent.

6.2.6.2 Response

HTTP Code

204 if the request has been successful.

This message is sent by the HUB to the TPP as a response to the consent removal request.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the request.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

No additional fields are specified.

6.2.6.3 Examples

Example of a request

DELETE https://www.hub.com/aspsp-name/v1.1/consents/7890-asdf-4321

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: DELETE

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response

HTTP/1.1 204 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

6.3 AIS: Account information service

6.3.1 Reading of the account list

This service allows to obtain a list of PSU accounts, including account balances if requested and consent is available.

This request is used both for the list of available accounts and for the list of account details. Depending on the consent used in the request.

As a prerequisite, it is assumed that the PSU has given its consent to this access and has been stored by the ASPSP.

Operation of the service according to the type of access specified in the consent:

Access type	Description
account	If the consent associated with the request has this type of access, the account balances included in the consent with "account" access can be listed.
balances	If the consent associated with the request has this type of access, the accounts included in the consent with the "balances" access can be listed and their balances can be obtained if the ASPSP supports this function.
transactions	If the consent has accounts with this type of access, the said accounts can be listed with the "account" access. This type of access does not entail access to "balances".
allPsd2	If the consent associated with the request has this type of access, the accounts included in the consent can be listed and their balances can be obtained. Note: allPsd2 provides all three types of access.

6.3.1.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/accounts{query-parameters}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID**

				^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Consent-ID	Consent identifier obtained in the transaction to request consent.	String	OB	^.{1,36}$ E.g.: Consent-ID: 7890-asdf-4321
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. It must be included if, and only if this request was actively initiated by the PSU.	String	COND	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.:

				PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856; 25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==

Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ…….KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No data goes in the body of this request.

6.3.1.2 Response

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
accounts	List of available accounts.	List<AccountDetails>	OB	E.g.: "accounts": []
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.3.1.3 Examples

Example of a request to a obtain list of available accounts from the PSU

GET https://www.hub.com/aspsp-name/v1.1/accounts

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response to obtain list of the PSU's accessible accounts

Response in which the consent has been given for two distinct IBANs.

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "accounts": [
    {
                "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
                "iban": "ES1111111111111111111111",
                "currency": "EUR",
                "product": "Girokonto",
                "name": "Main Account",
                "_links": {
                        "balances": {
                                "href": "/v1.1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/balances"
                        },
                        "transactions": {
                                "href": "/v1.1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f/transactions"
```

```
                    }
                }
    },
    {
                "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e81g",
                "iban": "ES2222222222222222222222",
                "currency": "USD",
                "name": "US Dollar Account",
                "_links": {
                    "balances": {
                        "href": "/v1.1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/balances"
                    }
                }
        }
        ]
}
```


6.3.2 Reading of the account details

This service allows an account's details to be read.

As a requirement, it is assumed that the PSU has consented to this access and it has been stored by the ASPSP.

Operation of the service according to the type of access specified in the consent:

Access type	Description
account	If the consent associated with the request has this type of access to the account, it can be queried.
balances	If the consent associated with the request has this type of access to the account, it can be queried and its balances can be obtained, provided that the ASPSP supports this function.
transactions	If the consent has accounts with this type of access, the said account can be queried with the "account" access type. This type of access does not entail access to "balances".
allPsd2	If the consent associated with the request has this type of access to the account, it can be queried and its balances can be obtained. Note: allPsd2 provides all three types of access.

6.3.2.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/accounts/{account-id}

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
account-id	Unique identifier assigned by the ASPSP for the account.	String	OB	^.{1,100}$ E.g.: account-id=a1q5w

Query parameters:

Field	Description	Type	Mandat.	Format
withBalance	If included, this function includes balances. This request will be rejected if the access to balances is not covered by the consent or the ASPSP does not support this parameter.	Boolean	OP	Ex: true

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Consent-ID	Consent identifier obtained in the transaction to request consent.	String	OB	^.{1,36}$ E.g.: Consent-ID: 7890-asdf-4321
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. It must be included if, and only if this request was actively initiated by the PSU.	String	COND	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443

PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$

				E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No data goes in the body of this request.

6.3.2.2 Response

HTTP Code

200 if the request has been successful.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
account	Detailed information of the account	AccountDetails	OB	E.g.: "account": {…}
psuMessage	Text to be displayed to the PSU	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.3.2.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/v1.1/accounts/3dc3d5b3-7023-4848-9853-f5400a64e80f

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response for an account with just one currency

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "resourceId": "3dc3d5b3-7023-4848-9853-f5400a64e80f",
                "iban": "ES1111111111111111111111",
                "currency": "EUR",
                "product": "Girokonto",

                "name": "Main Account",
                "_links": {
                        "balances": {
                                "href": "/v1.1/accounts/3dc3d5b3-7023-4848-9853-
                        f5400a64e80f/balances"
                        },
```

```
                    "transactions": {
                        "href": "/v1.1/accounts/3dc3d5b3-7023-4848-9853--5400a64e80f/transactions"
                    }
                }
            }
        }
```


6.3.3 Reading of balances

This service allows the balances of a particular account to be obtained by its identifier.

As a requirement, it is assumed that the PSU has consented to this access and it has been stored by the ASPSP.

Operation of the service according to the type of access specified in the consent:

Access type	Description
account	This service cannot be used with this type of access.
balances	If the consent associated with the request has this type of access to the account balances, they can be queried.
transactions	This service cannot be used with this type of access.
allPsd2	If the consent associated with the request has this type of access to the account balances, they can be queried. Note: allPsd2 provides all three types of access.

6.3.3.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/accounts/{account-id}/balances

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

account-id	Account identifier to be used to read the data. Previously obtained in the reading of the list of accounts. It must be valid at least for the duration of the consent. This ID can be tokenised.	String	OB	^.{1,100}$ E.g.: account-id=a1q5w

Query parameters

No additional fields are specified.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
Consent-ID	Consent identifier obtained in the transaction to request consent.	String	OB	^.{1,36}$ E.g.: Consent-ID: 7890-asdf-4321
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. It must be included if, and only if this request was actively initiated by the PSU.	String	COND	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip

PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device. The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.	String	OP	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$

E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No data goes in the body of this request.

6.3.3.2 Response

HTTP Code

200 if the request has been successful.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
account	Identifier of the account being queried. Note: recommended to be used as it could become a mandatory parameter in future versions.	AccountReference	OP	E.g.: "account": {…}
balances	A list of balances of a certain account.	List<Balance>	OB	E.g.: "balances": {…}
psuMessage	Text to be displayed to the PSU.	String	OP	^.{1,512}$ E.g.: “psuMessage":"Information for the PSU"

tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages":[…]

6.3.3.3 Examples

Example of a request

GET https://www.hub.com/aspsp-name/accounts/3dc3d5b3-7023-4848-9853-f5400a64e81g/balances

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a response

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "balances": [
        {
                "balanceType": "closingBooked",
                "balanceAmount": {
                        "currency": "EUR",
                        "amount": "500.00"
                }
```

```
        },
        {
                "balanceType": "expected",
                "balanceAmount": {
                        "currency": "EUR",
                        "amount": "900.00"
                }
        }
        ]
}
```


6.3.4 Reading of the transactions

This service allows for transactions of a particular account to be obtained via its identifier.

As a requirement, it is assumed that the PSU has consented to this access and it has been stored by the ASPSP.

Operation of the service according to the type of access specified in the consent:

Access type	Description
account	This service cannot be used with this type of access.
balances	If the consent associated with the request has this type of access it will allow the balances to be requested, provided that the ASPSP supports this.
transactions	If the consent associated with the request has this type of access to the account movements, they can be queried.
allPsd2	If the consent associated with the request has this type of access to the account balances, they can be queried. Note: allPsd2 provides all three types of access.

6.3.4.1 Request

Endpoint

GET {provider}/{aspsp}/v1.1/accounts/{account-id}/transactions{query-parameters }

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

account-id	Account identifier to be used to read the data. Previously obtained in the reading of the list of accounts. It must be valid at least for the duration of the consent. This ID can be tokenised.	String	OB	^.{1,100}$ E.g.: account-id=a1q5w

Query parameters

Field	Description	Type	Mand.	Format
dateFrom	Query start date. It is included if the “deltaList” is not included.	String	COND	**ISODate** E.g.: dateFrom=2017-10-25
dateTo	Query end date. The default value is the current date if nothing is entered.	String	OP	**ISODate** E.g.: dateTo=2017-11-05
entryReferenceFrom	If specified, it will give us the results from the call with the preceding entryReferenceFrom given. If it is content, the dateFrom and dateTo attributes are ignored.	String	OP	E.g.: entryReferenceFrom=1234-asdf-567
bookingStatus	Permitted codes are "booked", "pending", "both" and “information”. Currently the booking status “information” only covers standing orders.	String	OB	E.g.: bookingStatus=booked
withBalance	If included, this function includes balances.			withBalance

Note: in case bookingStatus is equal to "information", the query param dateFrom, dateTo, withBalance, deltaList and entryReferenceFrom will be ignored and have no effect on the result.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a pre-authentication on OAuth2.	String	OB	E.g.: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID	Consent identifier obtained in the transaction to request consent.	String	OB	^.{1,36}$ E.g.: Consent-ID: 7890-asdf-4321
Accept	Formats supported by the ASPSP. The TPP can specify the order and type. Supported values: application/json	String	OP	^.{1,50}$ E.g.: Accept: application/json
PSU-IP-Address	IP Address of the HTPP request between the PSU and the TPP. It must be included if, and only if this request was actively initiated by the PSU.	String	COND	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g.: PSU-IP-Address: 192.168.16.5
PSU-IP-Port	IP Port of the HTPP request between the PSU and the TPP, if available.	String	OP	^\\d{1,5}$ E.g.: PSU-IP-Port: 443
PSU-Accept	Accept header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept: application/json
PSU-Accept-Charset	Accept charset header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	Accept encoding header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Encoding: gzip
PSU-Accept-Language	Accept language header of the HTPP request between the PSU and the TPP.	String	OP	^.{1,50}$ E.g.: PSU-Accept-Language: es-ES
PSU-User-Agent	Browser or operating system of the HTTP request between the PSU and the TPP.	String	OP	E.g.: PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used in the interface between the PSU and the TPP. Allowed values: • POST • GET • PUT • PATCH • DELETE	String	OP	E.g.: PSU-Http-Method: GET
PSU-Device-ID	UUID (Universally Unique Identifier) for a device.	String	OP	**UUID**

	The UUID identifies the device or an installation of an application on a device. This ID must not be modified until the application has been uninstalled from the device.			^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-Geo-Location	Corresponding location of the HTPP request between the PSU and the TPP.	String	OP	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g.: PSU-Geo-Location: GEO:90.023856;25.345963
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,5000}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No data goes in the body of this request.

6.3.4.2 Response

HTTP Code

200 if the request has been successful.

Header

Field	Description	Type	Mand.	Format
Content-Type	Possible values: application/json	String	OB	E.g.: Content-Type: application/json

X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
account	Identifier of the account being queried. Note: recommended to be used as it could become a mandatory parameter in future versions.	AccountReference	OP	E.g.: "account": {...}
transactions	The data is returned in JSON format, when the returned data is small in size.	AccountReport	OP	E.g.: "transactions": {...}
_links	List of hyperlinks to be recognised by the TPP. Types supported in this response:	Links	OP	E.g.: "_links": {...}
psuMessage	Text to be displayed to the PSU	String	OP	^.{1,512}$ E.g.: "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": [...]

6.3.4.3 Examples

Example of search request sending search criteria including dateTo and dateFrom

GET

https://www.hub.com/aspsp-name/v1.1/accounts/qwer3456tzui7890/transactions?dateFrom=2017-10-25&dateTo=2017-11-05&bookingStatus=booked

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a search request with the search entryReferenceFrom criterion

GET https://www.hub.com/aspsp-name/v1.1/accounts/qwer3456tzui7890/transactions?entryReferenceFrom=1234-asd-4564700&bookingStatus=booked

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of response with pagination

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
```

```
"transactions": {
    "booked": [
    {
        "entryReference": "1234567",
        },
        "transactionAmount": {
            "currency": "EUR",
            "amount": "256.67"
        },
        "bookingDate": "25/10/2017",
        "valueDate": "26/10/2017",
        "remittanceInformationUnstructured": "Example for Remittance Information"
    },
    {
        "entryReference": "1234568",
        },
        "transactionAmount": {
            "currency": "EUR",
            "content": "343.01"
        },
        "bookingDate": "25/10/2017",
        "valueDate": "26/10/2017",
        "remittanceInformationUnstructured": "Another example for Remittance Information"
    }
    ],
    "_links": {
        "account": {
            "href": "/v1.1/accounts/qwer3456tzui7890"
        },
        "first": {
            "href": "/v1.1/accounts/ qwer3456tzui7890/transactions?
        },
        "next": {
            "href": "/v1.1/accounts/ qwer3456tzui7890/transactions? "
        },
    }
}
}
```

Example of **a response with page numbering**

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "transactions": {
                "booked": [
                {
                        "transactionId": "1234567",
                        "creditorName": "John Miles",
                        "creditorAccount": {
                                "iban": "ES1111111111111111111111"
                        },
                        "transactionAmount": {
                                "currency": "EUR",
                                "amount": "256.67"
                        },
                        "bookingDate": "2017-10-25",
                        "valueDate": "2017-10-26",
                        "remittanceInformationUnstructured": "Example for Remittance Information"
                },
                {
                        "transactionId": "1234568",
                        Ex: "debtorName": "Paul Simpson"
                        "debtorAccount": {
                                "iban": "NL354543123456900"
                        },
                        "transactionAmount": {
                                "currency": "EUR",
                                "content": "343.01"
                        },
                        "bookingDate": "2017-10-25",
                        "valueDate": "2017-10-26",
                        "remittanceInformationUnstructured": "Another example for Remittance Information"
```

```
        }
        ],
        "pending": [
        {
                "transactionId": "123456789",
                "creditorName": "Claude Renault",
                "creditorAccount": {
                        "iban": "NL354543123456900"
                },
                "transactionAmount": {
                        "currency": "EUR",
                        "amount": "-100.03"
                },
                "valueDate": "2017-10-26",
                "remittanceInformationUnstructured": "Another example for Remittance Information"
        }
        ],
        "_links": {
                "account": {
                        "href": "/v1.1/accounts/qwer3456tzui7890"
                },
                "first": {
                        "href": "/v1.1/accounts/qwer3456tzui7890/transactions?page[number]=1&page[size]=15
                },
                "previous": {
                        "href": "/v1.1/accounts/qwer3456tzui7890/transactions?page[number]=2&page[size]=15"
                },
                "next": {
                        "href": "/v1.1/accounts/qwer3456tzui7890/transactions?page[number]=4&page[size]=15"
                },
                "last": {
                        "href": "/v1.1/accounts/qwer3456tzui7890/transactions?page[number]=2&page[size]=15"
                }
        }
}
```

}

Example request to obtain a list of standing orders

GET https://aspsp.example.es/aspsp-name/v1.1/accounts/qwer3456tzui7890/transactions?bookingStatus=information

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Consent-ID: 7890-asdf-4321

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example of a standing order list response

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "transactions": {
                "information": [
                {
                        "creditorName": "John Miles",
                        "creditorAccount": {
                                "iban": "ES1111111111111111111111"
                        },
                        "transactionAmount": {
                                "currency": "EUR",
                                "amount": "256.67"
```

```
                    },
                    "remittanceInformationUnstructured": "Example for Remittance Information",
                    "bankTransactionCode": "PMNT-ICDT-STDO",
                    "additionInformationStructured":{
                    "standingOrderDetails": {
                    "startDate": "2018-03-01",
                    "endDate": "2020-06-31",
                                "executionRule": "preceding",
                                "frequency": "monthly",
                                "dayOfExecution": "24"
                        }
                    }
                }
                ]
        }
}
```


Example of response with error


```
{
        "tppMessages": [{
                "category": "ERROR",
                "code": "ACCESS_EXCEEDED"
        }
    ]
}
```


6.4 FCS: Establish consent for funds confirmation service

6.4.1 Fund confirmation consent

With this service a TPP can report a funds confirmation consent to the ASPSP on a specified account.

Unlike the request to establish consent for information about accounts, this consent has no secondary effects on existing ones.

Ex: it does not invalidate a prior consent.

6.4.1.1 Request

Endpoint

POST {provider}/{aspsp}/v2.1/consents/confirmation-of-funds

Path

Field	Description	Type	Mandat.	Format
provider	URL of the HUB where the service is released.	String	MA	Ex: www.hub.com
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name

Query parameters:

No additional fields are specified.

Header

Field	Description	Type	Mandat.	Format
X-Request-ID	Unique identifier of the operation assigned by the TPP.	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
PSU-ID	Identifier that the PSU uses to identify itself in its ASPSP. It can be reported even if an OAuth token is being used and, in such a case, the ASPSP could check if the PSU-ID and the token match.	String	OP	Ex: PSU-ID: 12345678W
PSU-ID-Type	Type of the PSU-ID. Necessary in scenarios where the PSU has several PSU-IDs as access possibilities.	String	OP	Ex: PSU-ID-Type: NIF
PSU-Corporate-ID	Identifier of "company" in Online Channels.	String	OP	Ex: PSU-Corporate-ID: user@corporate.com
PSU-Corporate-ID-Type	Type of the PSU-Corporate-ID required by the ASPSP to identify its content.	String	OP	Ex: PSU-Corporate-ID-Type: email
Authorization	Bearer Token. Obtained in a previous authentication on OAuth2.	String	MA	Ex: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

TPP-Redirect-Preferred	If "true", the TPP has communicated to the HUB that it prefers SCA by redirection. If "false", the TPP has informed the HUB that it prefers not to be redirected to SCA and the procedure will be by decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply depending on the SCA method chosen by the TPP / PSU. **EMBEDDED NOT SUPPORTED IN THIS VERSION**	Boolean	OP	Ex: TPP-Redirect-Preferred: true
TPP-Redirect-URI	URI of the TPP where the transaction flow must be redirected after any of the SCA phases. It is recommended to always use this header field. In the future, this field could change to mandatory. The domain of this URI is required to be the same as the content in the TPP web certificate.	String	COND	^.{1,250}$ Ex: TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the SCA method by redirection. The domain of this URI is required to be the same as the content in the TPP web certificate.	String	OP	^.{12,50}$ Ex: TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"
TPP-Explicit-Authorisation-Preferred	If equal to true, the TPP chooses to initiate the authorisation process separately, e.g. due to the need for authorisation of a set of operations simultaneously.	Boolean	OP	Ex: TPP-Explicit-Authorisation-Preferred: false

	If false or the parameter is not used, there is no TPP preference. The TPP takes a direct authorisation of the transaction in the next step. **Note**: ASPSP might not take it into account if it doesn't support it.			
TPP-Brand-Logging-Information	This field could be used by the TPP to inform the ASPSP about the brand used by the TPP for the PSU. This information can be used to improve communication between the ASPSP and the PSU or the ASPSP and the TPP.	String	OP	^.{1,70}$ Ex: TPP-Brand-Logging-Information: TPP Brand
TPP-Rejection-NoFunds-Preferred	**Note:** This field will be ignored if it is reported by the TPP.	String	OP	
TPP-Notification-URI	**Note:** This field will be ignored if it is reported by the TPP.	String	OP	
TPP-Notification-Contained-Preferred	**Note:** This field will be ignored if it is reported by the TPP.	String	OP	

Body

Field	Description	Type	Mandat.	Format
account	Account on which the fund consultation is to be carried out.	AccountReference	MA	Ex: "access": {...}
cardNumber	Card number of the card issued by the PIISP. Must be sent if available.	String	OP	^.{1,35}$
cardExpiryDate	Expiry date of the card issued by PIISP.	String	OP	**ISODate** Ex: "validUntil": "2018-05-17"
cardInformation	Additional explanation of the product.	String	OP	^.{1,140}$
registrationInformation	Additional information about the registration process for the PSU. For example, a reference to the TPP/PSU contract.	String	OP	^.{1,140}$

6.4.1.2 Response

HTTP Code

201 if the resource has been created

Response code

HTPP 201 response code if resource is created successfully.

Header

Field	Description	Type	Mandat.	Format
Location	Contains the hyperlink to the generated resource	String	MA	**Max512Text** Ex: Location: /v2.1/consents/confirmation-of-funds/{consentId}
X-Request-ID	Unique identifier of the operation assigned by the TPP.	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Value returned if the SCA method has been set. Possible values: • EMBEDDED • DECOUPLED • REDIRECT The OAuth based SCA will be taken as REDIRECT.	String	COND	Ex: ASPSP-SCA-Approach: REDIRECT
ASPSP-Notification-Support	Not in use. Resource state notification services not supported	Boolean	NA	
ASPSP-Notification-Content	Not in use. Resource state notification services not supported	String	NA	

Body

Field	Description	Type	Mandat.	Format
consentStatus	Consent State Defined values in 9.5 Consent status	String	MA	Ex: "consentStatus": "received"
consentId	Identifier of the resource that refers to the consent. It must be contained if consent was generated.	String	MA	^.{1,36}$ Ex: "consentId": "123-QWE-456"

scaMethods	This element is contained if SCA is required and if the PSU can choose between different authentication methods. If this data is contained, the link "startAuthorisationWithAuthenticationMethodSelection" will also be reported. These methods must be presented to the PSU. **Note:** Only if ASPSP supports SCA method selection	List<AuthenticationObject>	COND	Ex: "scaMethods": [...]
_links	List of hyperlinks to be recognized by the TPP. Supported types in this response: • scaRedirect: in case of SCA by redirection. Link where the PSU browser must be redirected by the TPP. • startAuthorisation: in case an explicit start of transaction authorization is required (no SCA method selection) • startAuthorisationWithAuthenticationMethodSelection: link to the authorisation end-point where the authorisation sub-resource has to be generated while selecting the SCA method. This link is contained under the same conditions as the "scaMethods" field • self: link to the resource created by this request. • state: link to retrieve the state of the transaction. • scaStatus: link to consult the SCA state corresponding to the authorisation sub-resource. This link is only contained if an authorization sub-	Links	MA	Ex: "_links": {...}

	resource has been created.			
psuMessage	Text to show to the PSU.	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message to the TPP	List<TppMessage>	OP	Ex: "tppMessages": […]

6.4.1.3 Examples

Example of consent request

POST https://www.hub.com/aspsp-name/v2.1/consent/confirmation-of-funds

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://www.tpp.com/cb

TPP-Nok-Redirect-URI: https://www.tpp.com/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "cardNumber": "123456781234",
        "cardExpiryDate": "2020-12-31",
        "cardInformation": "MyMerchant Loyalty Card",
        "registrationInformation": "Your contrat Number 1234 with MyMerchant is completed with the registration with your bank."
}
```

Example response in case of SCA by redirection with implicitly generated authorisation sub-resource

HTTP/1.1 201 Created

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 26 Sep 2017 15:02:43 GMT

Location: /v2.1/consents/confirmation-of-funds/123-asdf-456

Content-Type: application/json


```
{
        "consentStatus": "received",
        "consentId": "123-asdf-456",
        "_links": {
                "scaRedirect": {
                        "href": "https://hub.example.es/authorization "
                },
                "self": {
                        "href": "/v2.1/consents/confirmation-of-funds/123-asdf-456",
                },
                "state": {
                        "href": "/v2.1/consents/confirmation-of-funds/123-asdf-456",
                },
                "scaStatus": {
                        "href": "/v2.1/consents/123-asdf-456/authorisations/confirmation-of-funds/123auth456"
                }
        }
}
```


6.4.1 Obtain consent state

This service allows the TPP to know the state of a previously initiated consent request.

6.4.1.1 Request

Endpoint

GET {provider}/{aspsp}/v2.1/consents/confirmation-of-funds/{consent-id}/state

Path

Field	Description	Type	Mandat.	Format

provider	URL of the HUB where the service is released.	String	MA	Ex: www.hub.com
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
consentId	Identifier of the resource that refers to the consent. Previously sent in response to a consent request message from the TPP.	String	MA	^.{1,36}$ Ex:123-qwerty-456

Query parameters:

No additional fields are specified.

Header

Field	Description	Type	Mandat.	Format
X-Request-ID	Unique identifier of the request assigned by the TPP.	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorization	Bearer Token. Obtained in a previous authentication on OAuth2.	String	MA	Ex: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

Body

No additional data travels.

6.4.1.2 Response

This message is returned to the TPP in response to the consent state request message.

Response code

HTTP Code

200 if the request has been successful.

Header

Field	Description	Type	Mandat.	Format
X-Request-ID	Unique identifier of the request assigned by the TPP.	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mandat.	Format
consentStatus	Consent authentication state. Defined values in 9.5 Consent status	String	MA	Ex: "consentStatus":" valid"
psuMessage	Text to show to the PSU	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message to the TPP	List<TppMessage>	OP	Ex: "tppMessages": […]

6.4.1.3 Examples

Example of request

```
GET https://www.hub.com/aspsp-name/v2.1/consents/confirmation-of-funds/123asdf456/state
Accept: application/json
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc
Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-IP-Address: 192.168.8.16
PSU-IP-Port: 443
PSU-Accept: application/json
PSU-Accept-Charset: utf-8
PSU-Accept-Encoding: gzip
PSU-Accept-Language: es-ES
```

```
PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101
Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT
```

Example response

```
HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json

{

      "consentStatus": "valid"

}
```

6.4.2 Retrieve consent information

6.4.2.1 Request

This message is sent by the TPP as a request to retrieve information from a previously created fund confirmation consent. Especially useful for the TPP in cases where consent was managed directly between the ASPSP and the PSU.

Endpoint

GET {provider}/{aspsp}/v2.1/consents/confirmation-of-funds/{consentId}

Path

Field	Description	Type	Mandat.	Format
provider	URL of the HUB where the service is released.	String	MA	Ex: www.hub.com
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
consentId	Identifier of the resource that refers to the consent. Previously sent in response to a consent request message from the TPP.	String	MA	^.{1,36}$ Ex: 7890-asdf-4321

Query parameters:

No additional fields are specified.

Header

The same as those defined in the section 6.4.1.1

Body

No additional data travels.

6.4.2.2 Response

This message is returned to the TPP in response to the message to retrieve consent information.

HTTP Code

200 if the request has been successful.

Header

The same as those defined in the section 6.4.1.2

Body

Field	Description	Type	Mandat.	Format
account	Account on which the fund consultation is to be carried out.	AccountReference	MA	Ex: "access": {...}
cardNumber	Card number of the card issued by the PIISP. Must be sent if available.	String	OP	^.{1,35}$
cardExpiryDate	Expiry date of the card issued by PIISP.	String	OP	**ISODate** Ex: "validUntil": "2018-05-17"
cardInformation	Additional explanation of the product.	String	OP	^.{1,140}$
registrationInformation	Additional information about the registration process for the PSU. For example, a reference to the TPP/PSU contract.	String	OP	^.{1,140}$
consentStatus	Consent State Values defined in annexes.	String	MA	Ex: "consentStatus":"valid"
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message to the TPP	List<TppMessage>	OP	Ex: "tppMessages": [...]

6.4.2.3 Examples

Example of request

GET https://www.hub.com/aspsp-name/v2.1/consents/confirmation-of-funds/7890-asdf-4321/

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example response

HTTP/1.1 200 Ok

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json


```
{
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "cardNumber": "123456781234",
        "cardExpiryDate": "2020-12-31",
        "cardInformation": "MyMerchant Loyalty Card",
        "registrationInformation": "Your contrat Number 1234 with MyMerchant is completed with the registration with your bank."
        "consentStatus": "valid"
}
```


6.4.3 Revoke consent

6.4.3.1 Request

This service allows you to request the deletion of a consent previously created in the ASPSP.

Endpoint

DELETE {provider}/{aspsp}/v2.1/consents/confirmation-of-funds/{consentId}

Path

Field	Description	Type	Mandat.	Format
provider	URL of the HUB where the service is released.	String	MA	Ex: www.hub.com
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
consentId	Identifier of the resource that refers to the consent. Previously sent in response to a consent request message from the TPP.	String	MA	^.{1,36}$ Ex: 7890-asdf-4321

Query parameters:

No additional fields are specified.

Header

The same as those defined in the section 6.4.1.1

Body

No additional data travels.

6.4.3.2 Response

This message is sent to the TPP in response to the request to remove consent.

Response code

HTPP 204 response code for successful cancellation.

Header

The same as those defined in the section 6.4.1.2

Body

No additional fields are specified.

6.4.3.3 Examples

Example of request

DELETE https://www.hub.com/aspsp-name/v2.1/consents/confirmation-of-funds/7890-asdf-4321

Accept: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: DELETE

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example response

HTTP / 1.1 204 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

6.5 FCS: Fund confirmation service

6.5.1 Fund query

This type of message is used in the fund query service. The TPP sends the request to the HUB to check for funds for a specified amount on the specified account.

.

The HUB communicates with the ASPSP to ask whether the funds are available, and after checking, it answers the TPP.

6.5.1.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/funds-confirmations

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	^.{1,100}$ E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	^.{1,512}$ E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ…….KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

Field	Description	Type	Mand.	Format
cardNumber	Card number issued by the PIISP. This must be sent if it is available.	String	OP	E.g.: "cardNumber": "1111-1111-1111-1111"
account	PSU account number.	Account Reference	OB	E.g.: "account": {"iban":"ES1111111111111111111"}
payee	Business in which the card is accepted as information for the PSU.	String	OP	^.{1,70}$

				E.g.: "payee":"Commercial name"
instructedAmount	This contains the amount and currency to be queried.	Amount	OB	E.g.: "instructedAmount" : {…}

6.5.1.2 Response

This message is returned to the TPP by the HUB as a response to the message to confirm funds.

HTTP Code

200 if the request has been successful.

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction and sent through the HUB to the ASPSP.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Body

Field	Description	Type	Mand.	Format
fundsAvailable	Takes the “true” value "true" if sufficient funds are available at the time of the request, otherwise it will be “false”.	Boolean	OB	E.g.: "fundsAvailable": true
tppMessages	Message for the TPP.	List<TppMessage>	OP	E.g.: "tppMessages": […]

6.5.1.3 Examples

Example of a request

POST https://www.hub.com/aspsp-name/v1.1/funds-confirmations

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 17 Oct 2017 13:15:17 GMT

{

```
        "cardNumber": "87432569872156",
        "account": {
                "iban": "ES1111111111111111111111"
        },
        "payee": "Name123",
        "instructedAmount": {
                "currency": "EUR",
                "amount": "153.50"
        }
}
```


Example of response with available funds

HTTP/1.1 200 Ok
X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT

Content-Type: application/json


```
{
        "fundsAvailable": true
}
```


6.6 Sessions: combination of AIS and PIS services

Session support allows combining AIS and PIS services in the same session.

The session support is determined by the access token obtained after performing the OAuth2 protocol (pre-step)

For the session to be supported, the access token must have been obtained for the “PIS” and “AIS” scope and, the TPP, have the PISP and AISP roles in its eIDAS certificate.

6.7 Processes common to services

6.7.1 Start the authorization process (explicit)

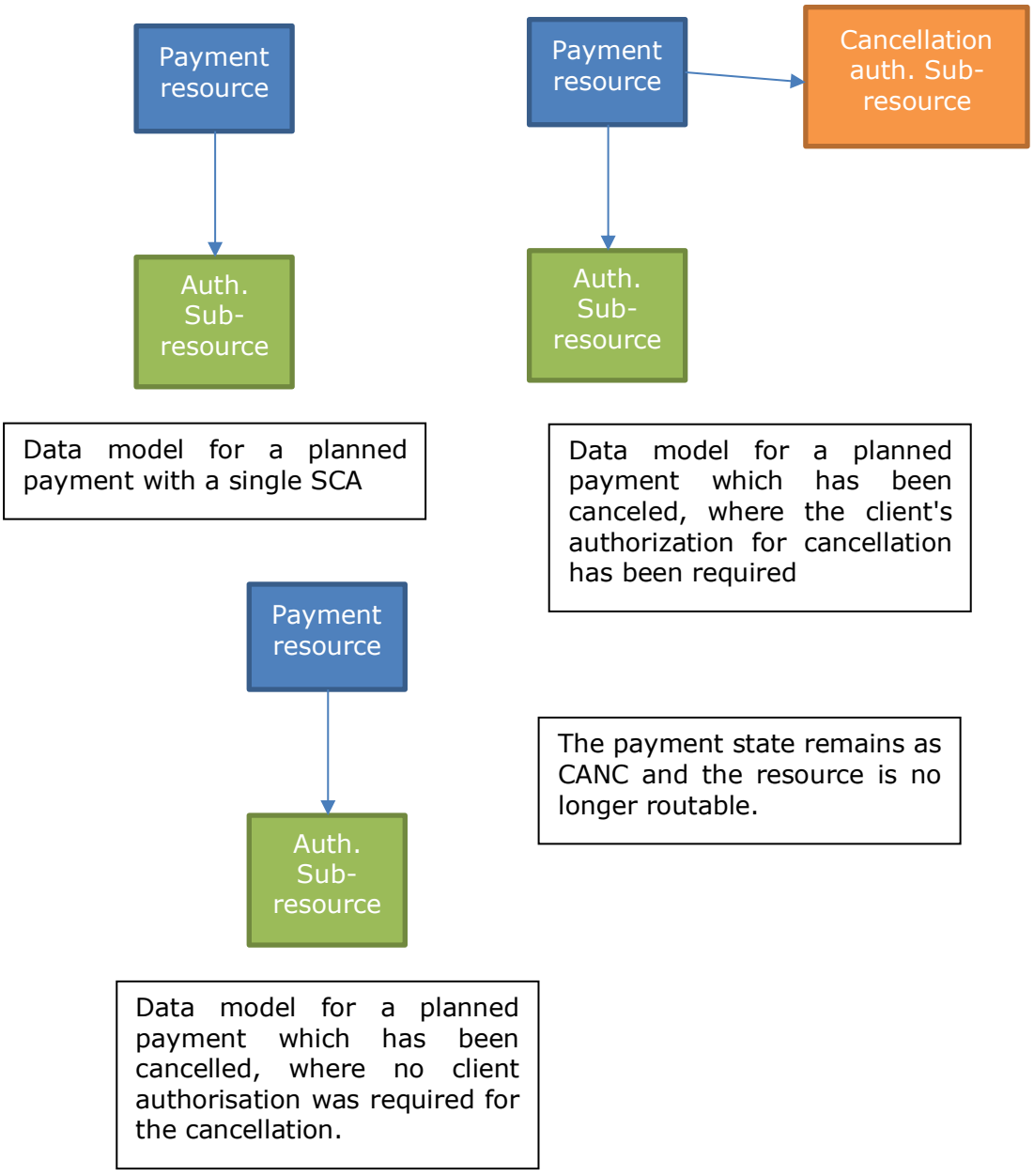
Use

The initiate authorization process is a process required to create a new authorization sub-resource (if not created implicitly). Applies in the following scenarios:

- The ASPSP has indicated with a "startAuthorisation" link in the response to a payment initiation request that an explicit start of the authorisation process is required by the TPP.
- The ASPSP has indicated with a "startAuthorisation" link in response to a request to cancel payment that an explicit start of the authorization process is required by the TPP.
- The ASPSP has indicated with a "startAuthorisation" link in the response to a request for consent to account information that an explicit start of the authorisation process is required by the TPP.

- The ASPSP has indicated with a "startAuthorisation" link in the response to a Confirmation of Funds consent request that an explicit start of the authorisation process is required by the TPP.

Abstract data model



6.7.1.1 Request

Endpoint in case of Fund Confirmation Consent

POST {provider}/{aspsp}/v2.1/consents/confirmation-of-funds/{consentId}/authorisations

Endpoint in case of Start of Payment

POST {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/authorisations

Endpoint in case of Payment Cancellation

POST {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations

Endpoint in case of Account Information Consent

POST {provider}/{aspsp}/v1.1/consents/{consentId}/authorisations

Path

Field	Description	Type	Mandat.	Format
provider	URL of the HUB where the service is released.	String	MA	Ex: hub.example.es
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
payment-service	Possible values are: • payments • bulk-payments • periodic-payments	String	COND	Ex: {provider}/v1.1/payments
payment-product	Paid product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	COND	Ex: {provider}/v1.1/payments/sepa-credit-transfers/
paymentI, consentId	Resource identifier that refers to the initiation of payment.	String	MA	^.{1,36}$ Ex: 123-qwe-456

Query parameters:

No additional parameters are specified for this request.

Header

Field	Description	Type	Mandat.	Format
Content-Type	Value: application / json	String	MA	Content-Type: application/json
X-Request-ID	Unique transaction identifier assigned by the TPP and forwarded via the HUB to the ASPSP	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7

Authorization	Bearer Token. Obtained in a previous authentication on OAuth2.	String	MA	Ex: Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA
PSU-ID	Identifier that the PSU uses to identify itself in its ASPSP. It can be reported even if an OAuth token is being used and, in such a case, the ASPSP could check if the PSU-ID and the token match.	String	OP	Ex: PSU-ID: 12345678W
PSU-ID-Type	Type of the PSU-ID. Necessary in scenarios where the PSU has several PSU-IDs as access possibilities.	String	OP	Ex: PSU-ID-Type: NIF
PSU-Corporate-ID	Identifier of "company" in Online Channels.	String	OP	Ex: PSU-Corporate-ID: user@corporate.com
PSU-Corporate-ID-Type	Type of the PSU-Corporate-ID required by the ASPSP to identify its content. TBD	String	OP	Ex: PSU-Corporate-ID-Type: email
TPP-Redirect-Preferred	If "true", the TPP has communicated to the HUB that it prefers SCA by redirection. If "false", the TPP has informed the HUB that it prefers not to be redirected to SCA and the procedure will be by decoupled flow. If the parameter is not used, the ASPSP will choose the SCA flow to apply depending on the SCA method chosen by the TPP / PSU. **EMBEDDED NOT SUPPORTED IN THIS VERSION**	Boolean	OP	Ex: TPP-Redirect-Preferred: true
TPP-Redirect-URI	HUB URI where the flow of the transaction should be redirected after finishing the SCA by redirect. It is recommended to always use this header field. In the future, this field could change to mandatory.	String	COND	^.{1,250}$ Ex: TPP-Redirect-URI":"https://hub.example.es/cb"

TPP-Nok-Redirect-URI	If this URI is contained, the TPP is requesting to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the SCA method by redirection.	String	OP	^.{1,250}$ Ex: TPP-Nok-Redirect-URI":"https://hub.example.es/cb/nok"

Body

No additional fields are specified.

6.7.1.2 Response

HTTP Code

201 if the resource has been created

Header

Field	Description	Type	Mandat.	Format
Location	Contains the link to the generated resource.	String	MA	Ex: Location: /v1.1/payments/{payment-product}/{paymentId}/authorisations/123qwert/456
X-Request-ID	Unique identifier of the operation assigned by the TPP and sent through the HUB to the ASPSP.	String	MA	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ Ex: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	Value returned if the SCA method has been set. Possible values: • EMBEDDED • DECOUPLED • REDIRECT The SCA based on OAuth2 will be taken as REDIRECT.	String	COND	Ex: ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Mandat.	Format
scaStatus	SCA state	String	MA	Ex: "scaStatus": "received"
authorizationId	Resource identifier that refers to the authorization sub-resource created.	String	MA	^.{1,36}$

				Ex: "authorisationId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
scaMethods	This element is contained if SCA is required and if the PSU can choose between different authentication methods. If this data is contained, the "selectAuthenticationMethod " link will also be reported. These methods must be presented to the PSU. **Note:** Only if ASPSP supports SCA method selection	List<AuthenticationObject>	COND	Ex: "scaMethods": [...]
_links	List of hyperlinks to be recognized by the TPP. Supported types in this response: • scaRedirect: in case of SCA by redirection. Link where the PSU browser must be redirected by the TPP. • selectAuthenticationMethod: link to the authorization or cancellation authorization sub-resource where the selected SCA method will be informed. • scaStatus: link to consult the SCA state corresponding to the authorisation sub-resource.	Links	MA	Ex: "_links": {...}
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,512}$ Ex: "psuMessage": "Información para PSU"
tppMessages	Message for the TPP sent through the HUB.	List<TppMessage>	OP	Ex: "tppMessages": [...]

6.7.1.3 Examples

Example request about a Payment Cancellation

POST https://hub.example.es/aspsp-name/v1.1/payments/sepa-credit-transfers/qwert1234tzui7890/cancellation-authorisations

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:37 GMT

Example response in case of SCA by redirection

HTTP/1.1 201 Created

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 26 Sep 2017 15:02:43 GMT

Location: /v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations/123auth456

Content-Type: application/json


```
{
        "scaStatus": "received",
        "authorisationId": "123auth456",
        "_links": {
                "scaRedirect": {
                        "href": "https://hub.example.es/authorize "
                },
                "scaStatus": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations/123auth456"
                }
        }
}
```


6.7.2 Get authorization sub-resources

It will provide an array of resource identifiers for all generated authorization sub-resources.

6.7.2.1 Request

Endpoint in case of Start of Payment

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/authorisations

Endpoint in case of Payment Cancellation

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations

Endpoint in case of Account Information Consent

GET {provider}/{aspsp}/v1.1/consents/{consentId}/authorisations

Path

Field	Description	Type	Mandat.	Format
provider	URL of the ASPSP where the service is published.	String	MA	Ex: hub.example.es
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
payment-service	Possible values are: • payments • bulk-payments • periodic-payments	String	COND	Ex: {provider}/v1.1/payments
payment-product	Paid product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	COND	Ex: {provider}/v1.1/payments/sepa-credit-transfers/
paymentId, consentId	Resource identifier that refers to the initiation of payment.	String	MA	^.{1,36}$ Ex: 123-qwe-456

Query parameters:

No additional fields are specified.

Header

The same as those defined in the section **¡Error! No se encuentra el origen de la referencia.**

Body

No additional data is specified.

6.7.2.2 Response

HTTP Code

200 if the request has been successful.

Header

The same as those defined in the section **¡Error! No se encuentra el origen de la referencia.**

Body

Field	Description	Type	Mandat.	Format
authorisationIds	Array of authorizationIds. **Note**: required field if it is not a cancellation	Array<String>	COND	^.{1,36}$ Ex: " authorisationIds ": […]
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message for the TPP sent through the HUB.	List<TppMessage>	OP	Ex: "tppMessages": […]

6.7.2.3 Examples

Example of request

GET https://hub.example.es/asp-name/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

Content-Type: application/json

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example response

HTTP/1.1 200 Ok

X-Request-ID: 0ee25bf4-6ff1-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:47 GMT

```
{
        "authorizationIds": ["123auth456"]
}
```

6.7.3 Get SCA state

Message sent by the TPP to the ASPSP through the Hub to request the SCA state of an authorization sub-resource.

6.7.3.1 Request

Endpoint in case of Start of Payment

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}

Endpoint in case of Payment Cancellation

GET {provider}/{aspsp}/v1.1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{authorisationId}

Endpoint in case of Account Information Consent

GET {provider}/{aspsp}/v1.1/consents/{consentId}/authorisations/{authorisationId}

Endpoint in case of Fund Confirmation Consent

GET {provider}/{aspsp}/v2.1/consents/confirmation-of-funds/{consentId}/authorisations/{authorisationId}

Path

Field	Description	Type	Mandat.	Format
provider	URL of the HUB where the service is released.	String	MA	Ex: hub.example.es
aspsp	Name of the ASPSP to which the request is to be made.	String	MA	Ex: aspsp-name
payment-service	Possible values are: • payments • bulk-payments • periodic-payments	String	COND	Ex: {provider}/v1.1/payments
payment-product	Paid product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	COND	Ex: {provider}/v1.1/payments/sepa-credit-transfers/
paymentId, consentId	Resource identifier referring to the initiation of payment or consent	String	MA	^.{1,36}$ Ex: 123-qwe-456
authorizationId	Identifier of the sub-resource associated with the consent.	String	COND	^.{1,36}$

Query parameters:

No additional fields are specified.

Header

The same as those defined in the section **¡Error! No se encuentra el origen de la referencia.**

Body

No additional data is specified.

6.7.3.2 Response

HTTP Code

200 if the request has been successful.

Header

The same as those defined in the section **¡Error! No se encuentra el origen de la referencia.**

Body

Field	Description	Type	Mandat.	Format
scaStatus	SCA state	String	MA	Ex: "scaStatus": "finalised"
trustedBeneficiaryFlag	With this flag the ASPSP could optionally communicate to the TPP that the creditor was part of the list of trusted payees. This attribute is only contained in case of a final state of the scaStatus.	Boolean	OP	Ex: 'trustedBeneficiaryFlag': true
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message for the TPP sent through the HUB.	List<TppMessage>	OP	Ex: "tppMessages": […]

6.7.3.3 Examples

Example of request

GET https://hub.example.es/aspsp-name/v1.1/payments/sepa-credit-transfers/123-qwe-456/cancellation-authorisations/123asd456

X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: GET

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

Date: Sun, 26 Sep 2017 15:02:48 GMT

Example response

HTTP/1.1 200 Ok
X-Request-ID: 96201400-6ff9-11e8-adc0-fa7ae01bbebc

Date: Sun, 26 Sep 2017 15:02:50 GMT

Content-Type: application/json

{

"scaStatus": " finalised"

}

6.8 OAuth2 as a pre-step

6.8.1 Flow

In the scenario shown in the figure, only OAuth2 Figure 5: OAuth2 scenario as a pre-step is represented with its "Authorisation Code Grant" flow and the involvement of the parts.

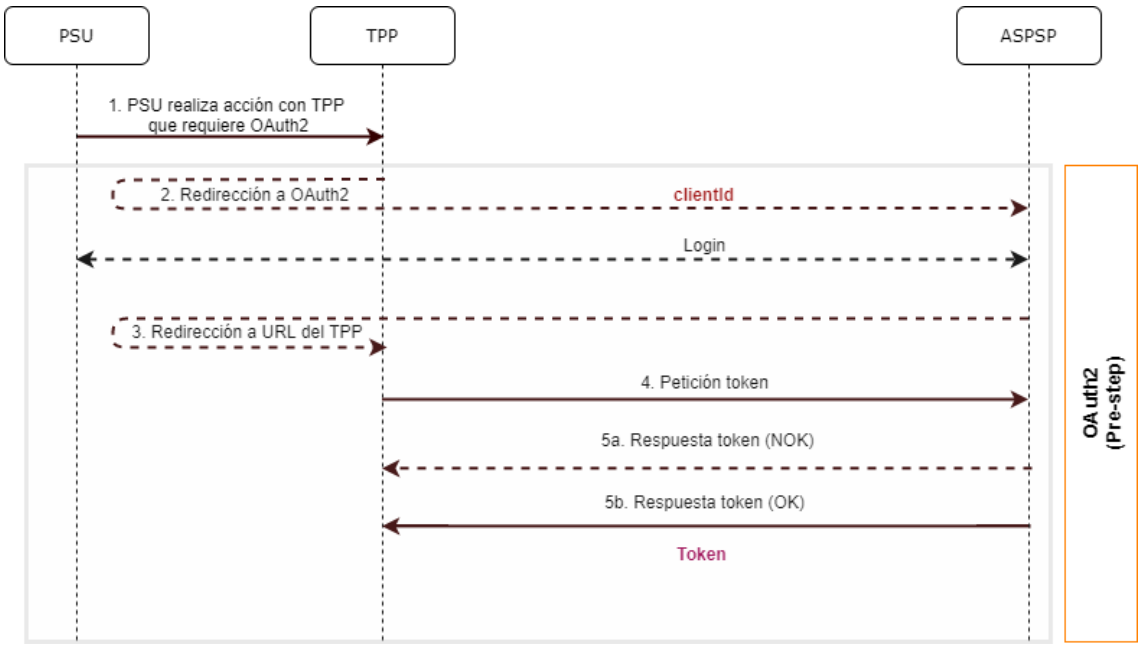


Figure 5: OAuth2 scenario as a pre-step

The points indicated in the flow are described below:

1. PSU performs action with TPP that requires OAuth2

PSU executes action that requires OAuth2.

2. Redirection to OAuth2

The TPP detects that the PSU that is trying to perform the action has not yet logged into the system and, therefore, does not have a valid access token to consume the resources.

In this situation, the TPP routes the PSU browser to perform a redirect to the authorisation URL of the OAuth2 server by informing, among other values, the clientIdTPP and the *redirect_uri* of the TPP to which the *callback* will be performed.

GET / authorize?response_type=code&client_id=PSDES-BDE-3DFD21
&state=asd&redirect_uri=https%3A%2F%2Ftpp%2Eexample%2Ecom%2Fcb&code_challenge=E9Melhoa2O
wvFrEMTJguCHaoeK1t8URWbuGJSstw-cM&code_challenge_method=S256

HTTP/1.1
Host: hub.example.com/aspsp-name

Login

The PSU enters its credentials, *user / pass,* on the *login* page of its ASPSP.

3. Redirection to TPP URL

Once the *login* has been successfully completed, the ASPSP instructs the PSU browser to perform the *callback* to the URL informed of the initial redirection (point 3 of the flow).

In this return redirection, the ASPSP, in case of successful *login*, reports an authorization code, *authCode,* which will be used in a subsequent request to request the access token from the ASPSP.

HTTP/1.1 302 Found
Location: https://hub.example.com/cb?code=SplxlOBeZQQYbYS6WxSbIA&state=xyz

4. Token request (TPP --> ASPSP)

The TPP makes a POST request to the OAuth2 server to obtain the access token that will allow it to consume the displayed API services.

Among the possible values to send, the TPP informs its *clientId* and the *authCode* returned in the redirection (point 3).

5. Token response (ASPSP TPP)

The ASPSP evaluates the data provided in the token request and, if everything was correct, generates an access token (*token)* that will return it in the response.

Note: those ASPSPs that require a payment execution request, may also return an additional token (authToken*)* at this point that will be used later to authorize the payment.

```
HTTP / 1.1 200 OK
Content-Type: application/json; charset=utf-8
Cache-Control: no-store
Pragma: no-cache
{
  "access_token": "1zCsicMWpAA2YotnFZFEjr",
  "token_type": "Bearer",
  "expires_in": 3600,
  "refresh_token": "G5Qx2TlKWIAtGzv3JOkF0X"
}
```

6.8.2 Get authorisation

6.8.2.1 Request

The TPP redirects the PSU so that it carries out the following request to the HUB:

- Web authentication
- Biometric authentication with app-to-app redirection

Endpoint for web authentication

GET
/{aspsp}/authorize?response_type={response_type}&client_id={client_id}&scope={scope}&state={state}&redirect_uri={redirect_uri}&code_challenge={code_challenge}&code_challenge_method={code_challenge_method}

Endpoint for biometric authentication with app-to-app redirection (personal)

GET

/{aspsp}/biometric/app-to-app/personal/authorize?response_type={response_type}&client_id={client_id}&scope={scope}&state={state}&redirect_uri={redirect_uri}&code_challenge={code_challenge}&code_challenge_method={code_challenge_method}

Endpoint for biometric authentication with app-to-app redirection (business)

GET

/{aspsp}/biometric/app-to-app/business/authorize?response_type={response_type}&client_id={client_id}&scope={scope}&state={state}&redirect_uri={redirect_uri}&code_challenge={code_challenge}&code_challenge_method={code_challenge_method}

Either of the two biometric endpoints can be used interchangeably because in both cases it is redirected to the same mobile application.

Once inside, the user must select the desired access type, which may be Private or Corporate access.

If when using the biometric authentication endpoints, the mobile application is not installed on the same device, then the system will load the web login page and the web authentication flow will be followed.

It is recommended to open the biometric authentication endpoint in one of the trusted browsers installed on the device since they have the redirection mechanisms between web and mobile apps implemented. If you choose to use embedded browsers, commonly known as WebViews, it is the responsibility of the Third Party to implement the necessary redirection logic so that the BancSabadell mobile application can be opened.

Sandbox application access for app-to-app redirect testing

There are sandbox applications available for iOS and Android for both BancSabadell and ActivoBank. These applications are intended to test app-to-app redirection in the Sandbox environment. To download, access the compressed files in "zip" from the following links:

Android
https://images.comunicaciones.bancsabadell.com/Web/BANCODESABADELLSA/{56586c33-bb16-436a-b5b4-58b2bb15995b}_PSD2AppSandbox-Android.zip

iOS

https://images.comunicaciones.bancsabadell.com/Web/BANCODESABADELLSA/{190ed11d-1e8f-4f42-bf27-d713da93db21}_PSD2AppSandbox-iOS.zip

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

Query parameters

Field	Description	Type	Mand.	Format
response_type	The value should be set as “code”.	String	OB	E.g.: response_type=code

client_id	"organizationIdentifier" provided in the eIDAS certificate made up of: - PSD - 2 characters of the NCA country code according to the ISO 3166 - Character "-" - 2-8 characters for the NCA identifier (A-Z in upper case) - Character "-" - PSP identifier	String	OB	^.{1,70}$ E.g.: client_id=PSDES-BDE-3DFD246
scope	Possible Scopes: • PIS • AIS • SVA More than one can be specified separating it by a space (%20).	String	OB	^.{1,64}$ E.g.: scope=PIS%20AIS%20SVA
state	Opaque value, generated by the TPP. Used to prevent "cross-site request forgery" (XSRF) attacks.	String	OB	^.{1,64}$ E.g.: state=XYZ
redirect_uri	URL returned to the HUB which will provide the authorisation code that will be subsequently used to obtain the access token.	String	OB	^.{1,250}$ E.g.: redirect_uri=https%3A%2F%2Fwww%2Etpp%2Ecom%2Fcb
code_challenge	PKCE challenge used to prevent code injection attacks. According to RFC 7636.	String	OB	^.{1,128}$ E.g.: code_challenge=E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-cM
code_challenge_method	Method for checking the code which could be "plain" or "S256". Preferred S256 (SHA 256)	String	OP	^.{1,120}$ E.g.: code_challenge_method=S256

Header

No additional fields are specified.

Body

No data goes in the body of this response.

6.8.2.2 OK Response

Response if the request has been processed correctly. This is the result from the redirection initiated by the HUB from the PSU's browser to the return URL provided by the TPP.

Path

No additional fields are specified.

Query Parameters

Field	Description	Type	Mand.	Format
Location	This contains the URI where the redirection to the TPP is performed.	String	OB	E.g.: Location: https://www.tpp.com/cb
code	Authorisation Code for single use generated by the HUB. The recommended duration of the code should not exceed 10 minutes.	String	OB	^.{1,64}$ E.g.: code=SplxlOBeZQQYbYS6WxSbIA
state	Opaque value, generated by the TPP. Used to maintain the state between the request and response. The HUB will include it when PSU's browser is redirected back to the TPP. Used to prevent "cross-site request forgery" attacks.	String	OB	^.{1,64}$ E.g.: state=XYZ

Body

No data goes in the body of this request.

6.8.2.3 Error Response

Response if an error has occurred in the request. This is the result from the redirection initiated by the HUB from the PSU's browser to the return URL provided by the TPP.

Path

No additional fields are specified.

Query Parameters

Field	Description	Type	Mand.	Format

Location	This contains the URI where the redirection to the TPP is performed.	String	OB	E.g.: Location: https://www.tpp.com/cb
error	Code indicating an error has occurred.	String	OB	E.g.: error=invalid_request
state	Value generated by the TPP. Used to maintain the state between the request and response. The HUB will send back the response.	String	OB	E.g.: state=XYZ

Body

No data goes in the body of this request.

6.8.2.4 Examples

Example of a request

GET https://www.hub.com/aspsp-name/authorize?response_type=code&client_id=PSDES-BDE-3DFD246&scope=PIS%20AIS%20SVA&state=xyz&redirect_uri=https%3A%2F%2Fwww%2Ehub%2Ecom%2Fcb&code_challenge=E9Melhoa2OwvFrEMTJguCHaoeK1t8URWbuGJSstw-cM&code_challenge_method=S256

Example OK response

HTTP/1.1 302 Found

Location: https://www.tpp.com/cb?code=SplxlOBeZQQYbYS6WxSbIA&state=xyz

Example NOK response

HTTP/1.1 302 Found

Location: https://www.tpp.com/cb?error=access_denied&state=xyz

6.8.3 Obtaining the access token

This message is sent by the HUB to ASPSP to exchange the authorization code obtained in the previous step and get the access and refresh tokens.

6.8.3.1 Request

Endpoint

POST {provider}/{aspsp}/token

Path

Field	Description	Type	Mand.	Format

provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name

Request Parameters

Field	Description	Type	Mand.	Format
grant_type	It must have the value of "authorization_code"	String	OB	E.g.: grant_type=authorization_code
client_id	"organizationIdentifier" provided in the eIDAS certificate made up of: - PSD - 2 characters of the NCA country code according to the ISO 3166 - Character "-" - 2-8 characters for the NCA identifier (A-Z in upper case) - Character "-" - PSP identifier	String	OB	^.{1,70}$ E.g.: client_id=PSDES-BDE-3DFD246
code	Authorisation code returned by the ASPSP in the previous authorisation code returned.	String	OB	^.{1,64}$ E.g.: code=SplxlOBeZQQY bYS6WxSbIA
redirect_uri	The URL returned to the TPP where the authorisation code is reported. It must be the same as that reported in the request for the authorisation code.	String	OB	^.{1,250}$ E.g.: redirect_uri=https%3A%2F%2Fwww%2Etpp%2Ecom%2Fcb
code_verifier	The proof key code, PKCE, used to prevent code injection attacks. Based on RFC 7636.	String	OB	E.g.: code_verifier=dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk

Header

No additional fields are specified.

Body

Fields do not go in the Body.

6.8.3.2 OK Response

Response if the request has been processed correctly. This result is given to the request to obtain an access token sent by the HUB to the PSU.

Body

Field	Description	Type	Mand.	Format
access_token	Access token issued by the HUB and attached to the scope asked for in the requested and confirmed by the PSU.	String	OB	^.{1,64}$ E.g.: "access_token":"2YotnFZFEjr1zCsicMWpAA"
token_type	Type of token issued. It will take the value of "Bearer".	String	OB	E.g.: "token_type":"Bearer"
expires_in	Duration of the access token in seconds.	Integer	OP	E.g.: "expires_in":300
refresh_token	Refresh token. It can be used to obtain a new access token if it expires.	String	OP	^.{1,64}$ E.g.: "refresh_token":"tGzv3JOKF0XG5Qx2TlKWIA"

6.8.3.3 Error Response

Response if an error has occurred in the request. This result is given to the request for an access token sent by the TPP to the HUB.

Body

Field	Description	Type	Mand.	Format
error	Code indicating an error has occurred. See more return codes in the annexes.	String	OB	E.g.: "error":"invalid_request"

6.8.3.4 Examples

Example of a request

POST /token HTTP/1.1

Host: https://www.hub.com/aspsp-name

Content-Type: application/x-www-form-urlencoded

grant_type=authorization_code&client_id=PSDES-BDE-3DFD246&code=SplxlOBeZQQYbYS6WxSbIA&redirect_uri=https%3A%2F%2Fwww%2Etpp%2Ecom%2Fcb&code_verifier=dBjftJeZ4CVP-mB92K27uhbUJU1p1r_wW1gFWFOEjXk

Example OK response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Cache-Control: no-store

Pragma: no-cache

{

"access_token": "2YotnFZFEjr1zCsicMWpAA",

"token_type": "Bearer",

"expires_in": 3600,

"refresh_token": "tGzv3JOKF0XG5Qx2TlKWIA"

}

Example NOK response

HTTP/1.1 400 Bad Request

Content-Type: application/json;charset=UTF-8

Cache-Control: no-store

Pragma: no-cache

{

"error": "invalid_request"

}

6.9 Refresh token request

This service is used when the HUB reports that the access_token has expired. We can refresh the access_token by sending the refresh_token associated with the expired access_token through this request.

6.9.1 Request

Endpoint

POST {provider}/{aspsp}/token

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	OB	E.g.: aspsp-name
grant_type	It must have the value of "refresh_token"	String	OB	E.g.: grant_type=refresh_token
client_id	"organizationIdentifier" provided in the eIDAS certificate made up of: - PSD - 2 characters of the NCA country code according to the ISO 3166 - Character "-" - 2-8 characters for the NCA identifier (A-Z in upper case) - Character "-" - PSP identifier	String	OB	^.{1,70}$ E.g.: client_id=PSDES-BDE-3DFD246
refresh_token	Refresh token to obtain a valid access_token.	String	OB	^.{1,64}$ E.g.: refresh_token=tGzv3JOKF0XG5Qx2TlKWIA

Header

No additional data is specified.

Body

No additional data is specified.

6.9.2 Response

Field	Description	Type	Mand.	Format
access_token	Access token issued by the HUB and attached to the scope asked for in the requested and confirmed by the PSU.	String	OB	^.{1,64}$ E.g.: "access_token":"83kdFZFEjr1zCsicMWBB"
token_type	Type of token issued. It will take the value of "Bearer".	String	OB	E.g.: "token_type":"Bearer"

expires_in	Duration of the access token in seconds.	Integer	OP	E.g.: "expires_in":300
refresh_token	Refresh token. It can be used to obtain a new access token if it expires.	String	OP	^.{1,64}$ E.g.: "refresh_token":"28JD3JOKF0NM5Qx2TlCCC"

6.9.3 Examples

POST /token HTTP/1.1

Host: https://www.hub.com

Content-Type: application/x-www-form-urlencoded

grant_type=refresh_token&client_id=PSDES-BDE-3DFD246&refresh_token=tGzv3JOKF0XG5Qx2TlKWIA

Example OK response

HTTP/1.1 200 OK

Content-Type: application/json;charset=UTF-8

Cache-Control: no-store

Pragma: no-cache

{

"access_token": "83kdFZFEjr1zCsicMWBB",

"token_type": "Bearer",

"expires_in": 300,

"access_token": "28JD3JOKF0NM5Qx2TlCCC"

}

7. DESCRIPTION OF VALUE-ADDED SERVICES

7.1 ASPSP services available

This message is sent by the TPP to the HUB to receive information about the ASPSPs which are available in the system.

7.1.1 Version 1

7.1.1.1 Request

Endpoint
GET {provider}/v1.1/sva/aspsps

Path

Field	Description	Type	Mand.	Format
provider	URL of the HUB where the service is published.	String	OB	E.g.: www.hub.com

Header

Field	Description	Type	Mand.	Format
X-Request-ID	Unique identifier assigned by the TPP for the transaction.	String	OB	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.: X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Digest	It is content if it goes in the Signature field. See 9.1 Signature for more information.	String	OB	E.g.: Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Signature of the request for the TPP. See 9.1 Signature for more information.	String	OB	See annexes
TPP-Signature-Certificate	TPP certificate used to sign the request in base64.	String	OB	**eIDAS** E.g.: TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No additional fields are specified.

7.1.1.2 Response

Field	Description	Type	Mand.	Format
aspsps	List of ASPSPs available on the system. The list returned shall be made up of relevant information of the ASPSP.	List<Aspsp>	OB	E.g.: "aspsps":[]

tppMessages	Contains the message type and the code associated with it	Tppmessage	OB	E.g.: "tppMessages":{}

7.1.1.3 Examples

Example of a request

GET https://www.hub.com/v1.1/sva/aspsps

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 29391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 27 Oct 2017 13:15:17 GMT

Example of a response

HTTP/1.1 200 OK

```
{
        "aspsps": [
                {
                        "bic": "XXXXESMMXXX",
                        "name": "aspsp1"
                },
                {
                        "bic": "YYYYESMMXXX",
                        "name": "aspsp2"
                }
        ]
}
```

7.1.2 Version 2

This version includes the name of the API for each ASPSP.

7.1.2.1 Request

Endpoint
GET {provider}/v2/sva/aspsps

Path

Field	Description	Type	Man.	Format
provider	URL of the HUB where the service is published.	String	MAN	E.g. www.hub.com

Header

Field	Description	Type	Man.	Format
X-Request-ID	ID of the request, unique to the call, as determined by the initiating party.	String	MAN	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g. X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Digest	Is contained if and only if the "Signature" element is contained in the header of the request. See 9.1 Signature for more information.	String	MAN	E.g. Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	A signature of the request by the TPP on application level. See 9.1 Signature for more information.	String	MAN	See annexes
TPP-Signature-Certificate	The certificate used for signing the request, in base64 encoding.	String	MAN	**eIDAS** E.g. TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ……KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

No additional fields are specified.

7.1.2.2 Response

Field	Description	Type	Man.	Format
aspsps	List of ASPSPs available in the system. The returned list will be	List<Aspsp>	MAN	E.g. "aspsps":[]

	made up of relevant information on the ASPSP.			
tppMessages	Contains the type of message and the code associated with it	Tppmessage	MAN	E.g. "tppMessages":{}

7.1.2.3 Examples

Example of request

GET https://www.hub.com/v2/sva/aspsps

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 29391c7e-ad88-49ec-a2ad-99ddcb1f7721

Date: Sun, 27 Oct 2017 13:15:17 GMT

Example of response

HTTP/1.1 200 Ok


```
{
        "aspsps": [
                {
                        "bic": "XXXXESMMXXX",
                        "name": "Bank name",
                        "apiName": "nombreBanco1"
                },
                {
                        "bic": "YYYYESMMXXX",
                        "name": "Bank 2 name",
                        "apiName": "nombreBanco2"
                }
        ]
}
```


7.2 SVA: payment initiation with list of available accounts for PISP

This service allows the TPP to initiate a payment without entering information on the debtor's account "debtorAccount" and provides the list of accounts during the SCA flow so that the PSU can select one.

This value service complements the payment API payment and uses the CORE services to:

- Obtain payment status
- Recover payment initiation information

- Cancel payment initiation

7.2.1 Payment Initiation Flows

7.2.1.1 SCA flow by redirection with account selection: implicit start of authorization process

The following represents the sequence of requests / responses that are necessary for this service.

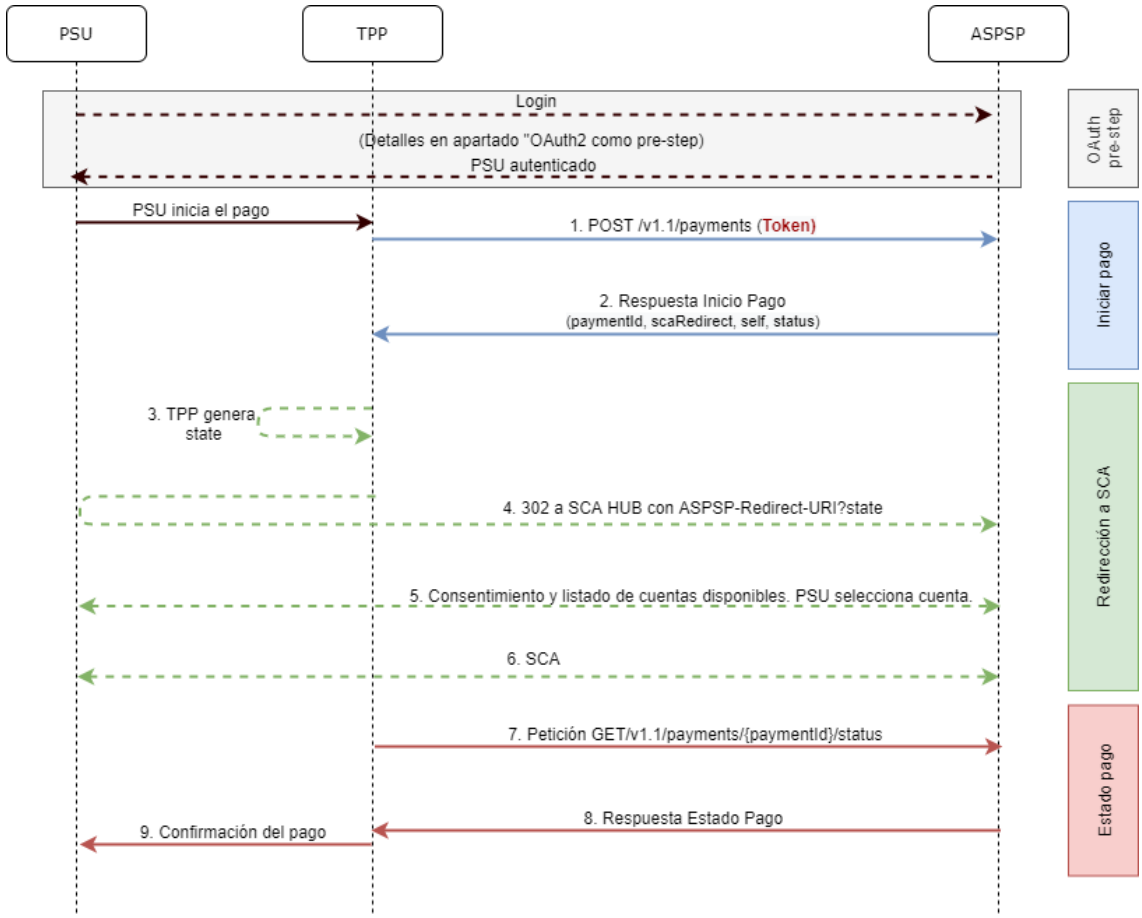


Figure 6: SCA flow by redirection with account selection- implicit start of authorisation process

OAuth2 (pre-step)

The main purpose of this flow is to authenticate the PSU to get access to the services displayed by its ASPSP through the use of an access token obtained after the application of this protocol.

In order to simplify, the detail of this flow has been omitted from the Figure 4 Figure 2: Start of payment with OAuth2 as pre-step and SCA flow by redirection and can be found in the section 6.1**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.VERIFY

Note: this step is optional. Only applies if no valid access token is available.

PSU initiates payment

The PSU wants to pay through the TPP.

1. Start Payment Request (TPP → ASPSP)

The TPP sends a POST request to initiate payment with *token* $_{HUB}$to HUB. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...
- **Payment data:** transfer type, ordering IBAN, beneficiary IBAN, amount, currency, concept ...
- **Data for risk scoring calculation:** IP, port, user-agent, language, location, HTTP headers ...
- **X-Request-ID:** identifier of the operation assigned by the TPP.
- **Access token** from TPP to Hub
- **TPP-Redirect-Preferred:** true (SCA flow preference by redirection) or not reported (ASPSP decides SCA by redirection).
- **TPP-Redirect-URI:** Return URI of the TPP after redirection to SCA.
- **TPP-Explicit-Authorization-Preferred:** false - TPP preference to initiate authorization implicitly
- **Other data**

4. Start Payment Response (ASPSP → TPP)

The Hub, after receiving the response from the ASPSP, responds to the TPP indicating that strong authentication (SCA) is required by redirecting to the authentication endpoint of the Hub, returning:

- **transactionStatus**: ISO 20022 state of the received payment start.
- **paymentId**: resource identifier generated by the Hub referring to the current payment initiation transaction.
- **_links**
    - **scaRedirect**: links to the Hub endpoint where after receiving the redirect from the TPP it redirects back to the scaRedirect of the ASPSP. This URL can add security parameters to allow session maintenance during redirection.

      https://hub.example.com/auth
    - **self**: link to the payment resource generated by the Hub for the payment initiation request received from the TPP.
    - **state**: link of the Hub to which the TPP can make a request to check the state of the payment.
- **Other data**

3. TPP generates state

The TPP, after receiving the response to initiate payment, generates a value for *state* (XSRF token) that it must link to the PSU browser session.

4. Redirect to scaRedirect (TPP → ASPSP)

The TPP redirects the PSU to the authentication endpoint by adding to it the field*state* as a query-param.

HTTP/1.1 302 Found

Location: https://hub.example.com/auth?state=qwerty

SCA entre PSU ←→ASPSP

During this redirection process, the ASPSP will be able to:

- Show consent to the PSU to access the available accounts
- Show available accounts and the PSU selects one of them
- Show commissions to the PSU if required
- Show ASPSP-PSU interface for SCA

6. SCA & Commissions

The ASPSP, after receiving the risk scoring of the operation, decides if SCA is necessary and executes it, showing the commissions.

Note: if the SCA process runs correctly, the payment is started.

11. Payment State Request (TPP → ASPSP)

The TPP will send a request for payment state with *token* to know the state of the payment.

12. Payment State Response (ASPSP → TPP)

The ASPSP updates the state of the operation and responds to the TPP.

7.2.1.2 SCA flow by redirection: implicit start of authorization process

Similar to 6.1.1.2 SCA flow by redirection: implicit start of authorization process.

7.2.2 Payment initiation

This message is sent by the TPP to the HUB to initiate payment without entering information on the debtor's account.

7.2.2.1 Request

Endpoint

POST {provider}/{aspsp}/v1.1/sva/payments/{payment-product}

Path

Field	Description	Type	Man.	Format
provider	URL of the HUB where the service is published.	String	MAN	E.g. www.hub.com
aspsp	Name of the ASPSP to which the request is made.	String	MAN	E.g. aspsp-name

payment-product	Payment product to be used. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	MAN	E.g. {provider}/{aspsp}/v1.1/payments/sepa-credit-transfers/

Header

Field	Description	Type	Man.	Format
Content-Type	Value: application/json	String	MAN	Content-Type: application/json
X-Request-ID	ID of the request, unique to the call, as determined by the initiating party.	String	MAN	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g. X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
Authorisation	Bearer Token. Obtained in a prior authentication on OAuth2.	String	MAN	E.g. Authorisation: Bearer 2YotnFZFEjr1zCsicMWpAA
Consent-ID	This data element may be contained, if the payment initiation transaction is part of a session, i.e. combined AIS/PIS service. This then contains the "consentId" of the related AIS consent, which was performed prior to this payment initiation.	String	OPT	^.{1,36}$ E.g. Consent-ID: 7890-asdf-4321
PSU-IP-Address	The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. If not available, the TPP shall use the IP Address used by the TPP when submitting this request.	String	MAN	^[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}.[0-9]{1,3}$ E.g. PSU-IP-Address: 192.168.16.5

PSU-IP-Port	The forwarded IP Port header field consists of the corresponding HTTP request IP Port field between PSU and TPP, if available.	String	OPT	^\\d{1,5}$ E.g. PSU-IP-Port: 443
PSU-Accept	The forwarded Accept header fields consist of the corresponding HTTP request Accept header fields between PSU and TPP, if available.	String	OPT	^.{1,50}$ E.g. PSU-Accept: application/json
PSU-Accept-Charset	See above	String	OPT	^.{1,50}$ E.g. PSU-Accept-Charset: utf-8
PSU-Accept-Encoding	See above	String	OPT	^.{1,50}$ E.g. PSU-Accept-Encoding: gzip
PSU-Accept-Language	See above	String	OPT	^.{1,50}$ E.g. PSU-Accept-Language: es-ES
PSU-User-Agent	The forwarded Agent header field of the HTTP request between PSU and TPP, if available.	String	OPT	E.g. PSU-User-Agent: Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US; rv:1.9.1.5) Gecko/20091102 Firefox/3.5.5 (.NET CLR 3.5.30729)
PSU-Http-Method	HTTP method used at the PSU – TPP interface, if available. Valid values are: • GET • POST • PUT • PATCH • DELETE	String	OPT	E.g. PSU-Http-Method: POST
PSU-Device-ID	UUID (Universally Unique Identifier) for a device, which is used by the PSU, if available. UUID identifies either a device or a device dependant application installation. In case of an installation identification this ID need to be unaltered until removal from device.	String	OPT	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g. PSU-Device-ID: 5b3ab8e8-0fd5-43d2-946e-d75958b172e7

PSU-Geo-Location	The forwarded Geo Location of the corresponding HTTP request between PSU and TPP if available.	String	OPT	**RFC 2426** ^GEO:[\\d]*.[\\d]*[;][\\d]*.[\\d]*$ E.g. PSU-Geo-Location: GEO:90.023856;25.345963
TPP-Redirect-Preferred	If it equals "true", the TPP prefers a redirect over an embedded SCA approach. If it equals "false", the TPP prefers not to be redirected for SCA. The ASPSP will then choose between the Embedded or the Decoupled SCA approach, depending on the choice of the SCA procedure by the TPP/PSU. If the parameter is not used, the ASPSP will choose the SCA approach to be applied depending on the SCA method chosen by the TPP/PSU. **EMBEDDED AND DECOUPLED ARE NOT SUPPORTED IN THIS VERSION**	Boolean	OPT	E.g. TPP-Redirect-Preferred: true
TPP-Redirect-URI	URI of the TPP, where the transaction flow shall be redirected to after a Redirect. Mandated for the Redirect SCA Approach, specifically when TPP-Redirect-Preferred equals "true". It is recommended to always use this header field. **Remark for Future**: This field might be changed to mandatory in the next version of the specification.	String	COND	^.{1,250}$ E.g. TPP-Redirect-URI":"https://tpp.example.es/cb"
TPP-Nok-Redirect-URI	If this URI is contained, the TPP is asking to redirect the transaction flow to this address instead of the TPP-Redirect-URI in case of a negative result of the redirect SCA method. This might be ignored by the ASPSP.	String	OPT	^.{1,250}$ E.g. TPP-Nok-Redirect-URI":"https://tpp.example.es/cb/nok"

Digest	If it equals "true", the TPP prefers to start the authorisation process separately. This preference might be ignored by the ASPSP, if a signing basket is not supported as functionality. If it equals "false" or if the parameter is not used, there is no preference of the TPP. This especially indicates that the TPP assumes a direct authorisation of the transaction in the next step. **Note**: the ASPSP may not take it into account if it does not support it.	String	MAN	^.{1,100}$ E.g. Digest: SHA-256=NzdmZjA4YjY5M2M2NDYyMmVjOWFmMGNmYTZiNTU3MjVmNDI4NTRlMzJkYzE3ZmNmMDE3ZGFmMjhhNTc5OTU3OQ==
Signature	Is contained if and only if the "Signature" element is contained in the header of the request. See 9.1 Signature for more information.	String	MAN	See annexes
TPP-Signature-Certificate	A signature of the request by the TPP on application level. See 9.1 Signature for more information.	String	MAN	^.{1,5000}$ E.g. TPP-Signature-Certificate: MIIHgzCCBmugAwIBAgIIZzZvBQlt0UcwDQYJ…….KoZIhvcNAQELBQAwSTELMAkGA1UEBhMCVVMxEzARBgNVBA

Body

The content of the Body is defined in 8.17 SinglePayment following the conditions of the following table.

The fields marked as mandatory (OB) and optional (OP) are supported by the ASPSP with this type of condition.

The fields marked as COND depend on each ASPSP.

Field	SCT	SCT INST	Target 2	Cross Border CT
endToEndIdentification*	OP	OP	NA	NA
instructionIdentification	COND	COND	COND	COND
debtorName	COND	COND	COND	COND
debtorAccount	NA	NA	NA	NA
debtorId	COND	COND	COND	COND
ultimateDebtor	COND	COND	COND	COND

instructedAmount	MA	MA	MA	MA
currencyOfTransfer	COND	COND	COND	COND
exchangeRateInformation	COND	COND	COND	COND
creditorAccount	MA	MA	MA	MA
creditorAgent	OP	OP	OP	MA/OP
creditorAgentName	COND	COND	COND	COND
CreditorName	MA	MA	MA	MA
creditorId	COND	COND	COND	COND
creditorAddress	OP	OP	OP	OP
creditorNameAndAddress	COND	COND	COND	COND
ultimateCreditor	COND	COND	COND	COND
purposeCode	COND	COND	COND	COND
chargeBearer	COND	COND	COND	COND
serviceLevel	COND	COND	COND	COND
remittanceInformationUnstructured	OP	OP	OP	OP
remittanceInformationUnstructuredArray	COND	COND	COND	COND
remittanceInformationStructured	COND	COND	COND	COND
remittanceInformationStructuredArray	COND	COND	COND	COND
requestedExecutionDate	n.a.	n.a.	n.a.	n.a.
requestedExecutionTime	n.a.	n.a.	n.a.	n.a.

***NOTE: This field will be used by the ASPSP, optionally to be sent by you, to inform the TPP of the value of the endToEndIdentification that the ASPSP itself includes in this identifier in the transfer itself.**

7.2.2.2 Response

HTTP Code

201 if the resource has been created.

Header

Field	Description	Type	Man.	Format
Location	Location of the created resource (if created)	String	MAN	E.g. Location: /v1.1/payments/{payment-product}/{payment-id}
X-Request-ID	ID of the request, unique to the call, as determined by the initiating party.	String	MAN	**UUID** ^[0-9a-fA-F]{8}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{4}-[0-9a-fA-F]{12}$ E.g.

				X-Request-ID: 1b3ab8e8-0fd5-43d2-946e-d75958b172e7
ASPSP-SCA-Approach	This data element must be contained, if the SCA Approach is already fixed. Possible values are: • REDIRECT The OAuth SCA approach will be subsumed by REDIRECT.	String	COND	E.g. ASPSP-SCA-Approach: REDIRECT

Body

Field	Description	Type	Man.	Format
transactionStatus	Status of the transaction. Values defined in annexes in 9.4 Transaction status	String	MAN	**ISO 20022** E.g. "transactionStatus": "RCVD"
paymentId	Identifier of the resource that references the payment initiation.	String	MAN	^.{1,36}$ E.g. "paymentId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
transactionFees	Fees associated with the payment.	Amount	OPT	E.g. "transactionFees": {...}
transactionFeeIndicator	If equal to "true", the transaction will involve a fee depending on the ASPSP or what has been agreed between the ASPSP and the PSU. If equal to "false", the transaction will not involve any additional fee for the PSU.	Boolean		E.g. "transactionFeeIndicator": true
_links	List of hyperlinks to be recognised by the TPP. Types supported in this response: • scaRedirect: in case of SCA by redirection. Link where the PSU navigator must be	Links	MAN	E.g. "_links": {...}

	redirected by the TPP. • • self: link to the resource created by this request. • status: link to recover the transaction status.			
psuMessage	Text to show to the PSU.	String	OPT	^.{1,512}$ E.g. "psuMessage": "Information for the PSU"
tppMessages	Message for the TPP	List<TppMessage>	OPT	E.g. "tppMessages": […]

7.2.2.3 Examples

Example of request

POST https://www.hub.com/aspsp-name/v1.1/sva/payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://www.tpp.com/cb

TPP-Nok-Redirect-URI: https://www.tpp.com/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
        "instructedAmount": {
                "currency": "EUR",
```

```
                "amount": "153.50"
        },
        "creditorAccount": {
                "iban": "ES2222222222222222222222"
        },
        "creditorName": "Name123",
        "remittanceInformationUnstructured": "Additional information"
}
```


Example of response


```
HTTP/1.1 201 Created
X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541
ASPSP-SCA-Approach: REDIRECT
Date: Sun, 26 Sep 2017 15:02:43 GMT
Location: /v1.1/payments/sepa-credit-transfers/1234-qwer-5678
{
        "transactionStatus": "RCVD",
        "paymentId": "123-qwe-456",
        "_links": {
                "scaRedirect": {
                        "href": "https://www.hub.com/aspsp-name/authorize"
                },
                "self": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456",
                        "state": {
                        "href": "/v1.1/payments/sepa-credit-transfers/123-qwe-456/state"
                }
        }
}
```


7.3 SVA: Start of standing orders for recurring / periodic payments with list of accounts available for PISP

This service allows the TPP to initiate a payment without entering information on the debtor's account "debtorAccount" and provides the list of accounts during the SCA flow so that the PSU can select one.

This value service complements the payment API payment and uses the CORE services to:

- Obtain payment status
- Recover payment initiation information
- Cancel payment initiation

7.3.1 Periodic Payment Initiation Flows

7.3.1.1 SCA flow by redirection with account selection: implicit start of authorization process

The following represents the sequence of requests / responses that are necessary for this service.

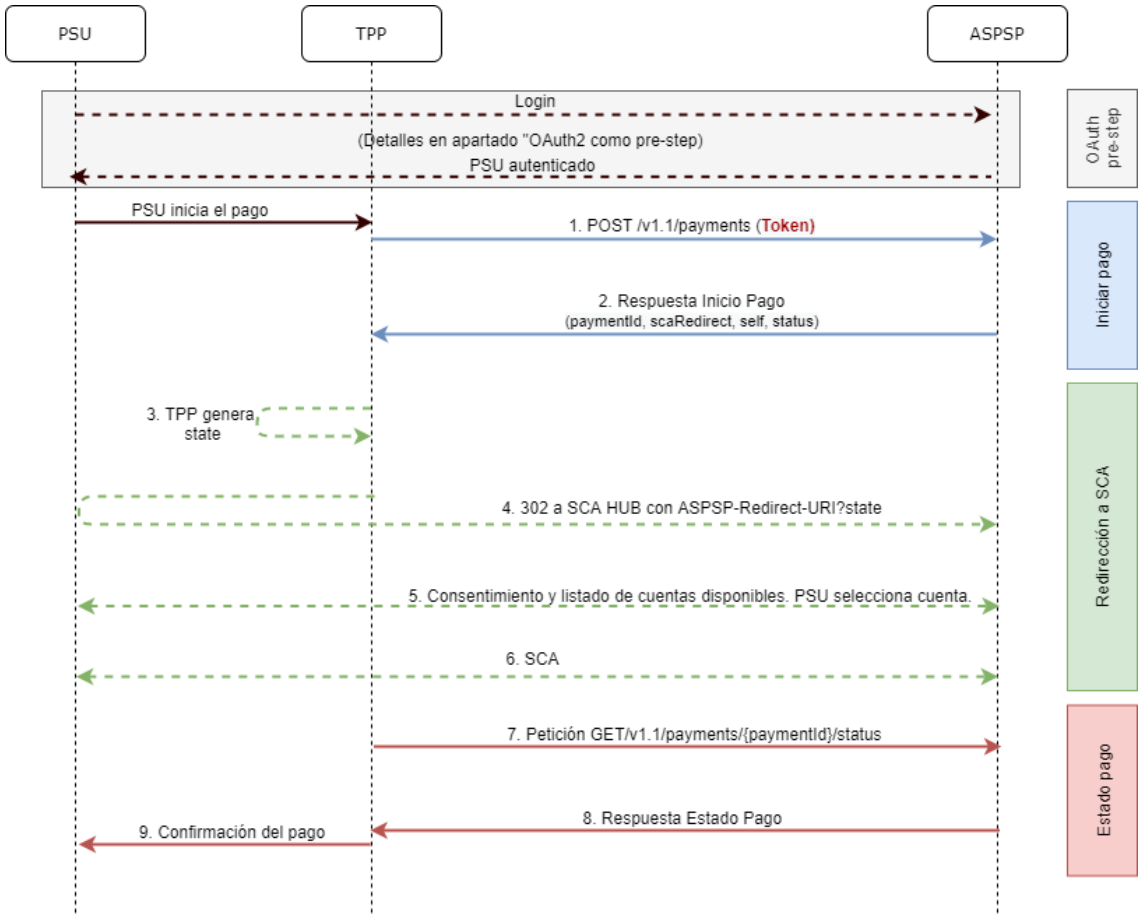


Figure 9: Scenario of starting periodic payment with list of accounts available for PISP

OAuth2 (pre-step)

The main purpose of this flow is to authenticate the PSU to get access to the services displayed by its ASPSP through the use of an access token obtained after the application of this protocol.

For simplicity, the detail of this flow has been omitted and can be found in section 6.1**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**.

Note: this step is optional. Only applies if no valid access token is available.

PSU starts periodic payment

The PSU wants to pay through the TPP.

1. Request Start Periodic Payment (TPP → Hub)

The TPP sends a POST request to initiate periodic payment with *tokenTPP* to the Hub. Among the data reported by the TPP are:

- **TPP data:** identifier, name, roles, NCA, certificate ...

- **Recurring payment details:** type of transfer, IBAN beneficiary, amount, currency, concept...
- **Data for risk scoring calculation:** IP, port, user-agent, language, location, HTTP headers ...
- **X-Request-ID:** identifier of the operation assigned by the TPP.
- **Access token** from the TPP

2. Request for Start Periodic Payment (Hub → ASPSP)

The Hub receives the request from the TPP, stores it and sends a POST request to initiate periodic payment with *tokenHUB to* the ASPSP. Among the data reported by the Hub are:

- **TPP data:** identifier, name, roles, NCA ....
- **Periodic payment data:** transfer type, beneficiary IBAN, amount, currency, concept, periodic payment start date, periodicity, ...
- **X-Request-ID:** identifier of the operation assigned by the TPP.
- **HUB-Transaction-ID:** Hub operation identifier
- **HUB-Request-ID:** Hub request identifier
- **Access token** from the TPP

3. Response Start Periodic Payment (ASPSP → Hub)

The ASPSP returns to the Hub a link to scaRedirect where the accounts available to the PSU will be displayed:

- **transactionStatus**: ISO 20022 state of the start of the periodic payment received.
- **paymentId**: resource identifier generated by the ASPSP that refers to the current recurring payment initiation transaction.
- **_links**
    - **scaRedirect**: link to the ASPSP authentication server where the accounts available to the PSU will be displayed and to initiate SCA via a redirect (SCA over OAuth2 does not apply). This URL can add security parameters to allow session maintenance during redirection.

      https://aspsp.example.com/auth

    - **self**: link to the payment resource generated by the ASPSP for the payment initiation request received from the TPP.
    - **state**: ASPSP link to which the Hub may make a payment state query request.
- Other information regarding the operation.

4. Response Start Periodic Payment (Hub → TPP)

The Hub, after receiving the response from the ASPSP, responds to the indicated TPP the url to which it has to redirect to continue with the process:

- **transactionStatus**: ISO 20022 state of the start of the periodic payment received.
- **paymentId**: resource identifier generated by the Hub referring to the current periodic payment initiation transaction.
- **_links**

- **scaRedirect**: links to the Hub endpoint where after receiving the redirect from the TPP it redirects back to the scaRedirect of the ASPSP. This URL can add security parameters to allow session maintenance during redirection.

  https://hub.example.com/auth

- **self**: link to the payment resource generated by the Hub for the payment initiation request received from the TPP.
- **state**: link of the Hub to which the TPP can make a request to check the state of the payment.

- Other data regarding the operation.

5. Redirection to scaRedirect from the Hub (TPP → Hub)

The TPP, after receiving the response to initiate periodic payment, redirects the PSU to the authentication endpoint of the Hub.

HTTP/1.1 302 Found
Location: https://hub.example.com/auth

6. Redirect to scaRedirect from ASPSP (→ASPSP Hub)

The Hub, upon receiving the redirection from the TPP, will redirect to the ASPSP authentication server where the accounts available to the PSU will be displayed and, if the ASPSP considers it, it will trigger strong authentication (SCA).

HTTP/1.1 302 Found
Location: https://aspsp.example.com/auth

7. SCA entre PSU ←→ASPSP

During this redirection process, the ASPSP will be able to:

- Show consent to the PSU to access the available accounts
- Show available accounts and the PSU selects one of them
- Show commissions to the PSU if required
- Show ASPSP-PSU interface for SCA

8. SCA & Commissions

The ASPSP, after receiving the risk scoring of the operation, decides if SCA is necessary and executes it, showing the commissions.

Note: if the SCA process runs correctly, the payment is started.

9. Redirection to Hub URL (ASPSP → Hub)

After redirection to the SCA in the ASPSP environment, it will return control to the Hub.

HTTP/1.1 302 Found

Location: https://hub.example.com/cb?state=xyz

10. Redirection to TPP URL (→TPP Hub)

The Hub, after receiving the redirection back from the ASPSP at the end of the SCA, redirects to the *callback* URL of the TPP to return control.

HTTP/1.1 302 Found
Location: https://tpp.example.com/cb

11. Request State Periodic Payment (TPP → Hub)

The TPP will send a payment state request with $_{tokenTPP}$ to the Hub for payment state.

12. Periodical Payment State Request (Hub → ASPSP)

The Hub will relay the payment state request with tokenHUB to $_{the}$ ASPSP to know the state of the payment.

Note: the Hub performs an exchange between $_{tokenTPP}$ and $_{tokenHUB.}$

13. Response State Periodic Payment (ASPSP → Hub)

After receiving the periodic payment state request with valid tokenHUB, the ASPSP checks the state of the payment initiation in its systems and returns it to the Hub.

14. State Response Periodic Payment (→TPP Hub)

The Hub after receiving the response from the ASPSP, updates the state of the operation and responds to the TPP.

Confirmation of periodic payment

The TPP confirms the state of the payment to the PSU.

7.3.1.2 SCA flow by redirection: implicit start of authorization process

Similar to 6.1.1.2 SCA flow by redirection: implicit start of authorization process..

7.3.2 Payment initiation completion

Message sent by the TPP to the ASPSP through the Hub to create a recurring / periodic payment start without informing the issuer's account “debtorAccount”.

A TPP can send a recurring payment start where the start date, frequency and, conditionally, end date are provided.

Once authorized by the PSU, the payment will be executed by the ASPSP, if possible, following the “standing order” as it was sent by the TPP. No further action is required from the TPP.

In this context, this payment is considered a periodic payment to differentiate the payment from other types of recurring payments where third parties are initiating the same amount of money.

Reglas campo dayOfExecution

- **Daily payments**: the "dayOfExecution" field is not necessary. The first payment is the "startDate" and, from there, the payment is made every day
- **Weekly payments**: if "dayOfExecution" is required, the possible values are from 01 = Monday to 07 = Sunday. If "dayOfExecution" is not required, "startDate" is taken as the day of the week the payment is made. (If "startDate" is Thursday, the payment would be made every Thursday)
- **Bi-weekly payments**: same rule applies as weekly payments.
- **Monthly payments or higher:** possible values range from 01 to 31. Using 31 as the last day of the month

7.3.2.1 Request

Endpoint

POST {provider}/v1.1/sva/periodic-payments/{payment-product}

Path

Field	Description	Type	Mandat.	Format
provider	URL of the ASPSP where the service is published.	String	MA	Ex: aspsp.example.es
payment-product	Paid product to use. List of supported products: • sepa-credit-transfers • instant-sepa-credit-transfers • target-2-payments • cross-border-credit-transfers	String	MA	Ex: {provider}/v1.1/periodic-payments/sepa-credit-transfers/

Query parameters:

No additional parameters are specified for this request.

Header

The same as those defined in the section **¡Error! No se encuentra el origen de la referencia.**

Body

The content of the Body is defined in Error! Reference source not found**¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.**, following the conditions of these tables, plus those defined below:

Field	Description	Type	Mandat.	Format

startDate	The first applicable day of execution from this date is the first payment	String	MA	**ISODate** xEx: "startDate":"2018-12-20"
executionRule	Supported values: • following • preceding Defines the behavior when recurring payment dates fall on weekends or holidays. Payment is then executed on the preceding or following working day. The ASPSP may reject the request due to the communicated value if the Online Banking rules do not support this execution rule.	String	OP	Ex: "executionRule":"following"
endDate	The last applicable day of execution. If not given, it is an endless standing order.	String	OP	**ISODate** Ex: "endDate":"2019-01-20"
frequency	The frequency of the recurring payment resulting from this standing order. Allowed values: • Daily • Weekly • EveryTwoWeeks • Monthly • EveryTwoMonths • Quarterly • Semi Annual • Annual	String	MA	**EventFrequency7Code de ISO 20022** Ex: "frequency": "Monthly"
dayOfExecution	"31" is last. Follows the regular expression\d{1,2} The date refers to the ASPSP time zone. Only if supported in ASPSP Online Banking.	String	COND	\d{1,2} Ex: "dayOfExecution": "01"

The fields marked as mandatory (MA) and optional (OP) are supported by the ASPSP with this type of condition.

The fields marked as COND depend on each ASPSP.

Field	SCT	SCT INST	Target 2	Cross Border CT
endToEndIdentification*	NA	NA	NA	NA
instructionIdentification	COND	COND	COND	COND
debtorName	COND	COND	COND	COND
debtorAccount	NA	NA	NA	NA
debtorId	COND	COND	COND	COND
ultimateDebtor	COND	COND	COND	COND
instructedAmount	MA	MA	MA	MA
currencyOfTransfer	COND	COND	COND	COND
exchangeRateInformation	COND	COND	COND	COND
creditorAccount	MA	MA	MA	MA
creditorAgent	OP	OP	OP	MA/OP
creditorAgentName	COND	COND	COND	COND
CreditorName	MA	MA	MA	MA
creditorId	COND	COND	COND	COND
creditorAddress	OP	OP	OP	OP
creditorNameAndAddress	COND	COND	COND	COND
ultimateCreditor	COND	COND	COND	COND
purposeCode	COND	COND	COND	COND
chargeBearer	COND	COND	COND	COND
serviceLevel	COND	COND	COND	COND
remittanceInformationUnstructured	OP	OP	OP	OP
remittanceInformationUnstructuredArray	COND	COND	COND	COND
remittanceInformationStructured	COND	COND	COND	COND
remittanceInformationStructuredArray	COND	COND	COND	COND
requestedExecutionDate	n.a.	n.a.	n.a.	n.a.
requestedExecutionTime	n.a.	n.a.	n.a.	n.a.

*** NOTE: If you want to send the endToEndId field, it must be reported within the body remittanceInformationUnstructured field. The best practice guide provides information on how to send the endToEndId field within this field.**

7.3.2.2 Response

HTTP Code

201 if the resource has been created

Header

The same as those defined in the section 6.1.2.2

Body

The same as those defined in the section 6.1.2.2

Body

Field	Description	Type	Mandat.	Format
transactionStatus	Transaction state. Values defined in annexes in 9.4	String	MA	**ISO 20022** Ex: "transactionStatus": "RCVD"
paymentId	Resource identifier that refers to the initiation of payment.	String	MA	^.{1,36}$ Ex: "paymentId": "1b3ab8e8-0fd5-43d2-946e-d75958b172e7"
transactionFees	Commissions associated with payment.	Amount	OP	Ex: "transactionFees": {...}
transactionFeeIndicator	If equal to "true", the transaction will incur a commission according to the ASPSP or as agreed between ASPSP and PSU. If it is equal to "false" or not used, the transaction will not involve any additional fees for the PSU.	Boolean	OP	Ex: "transactionFeeIndicator": true
scaMethods	This element is contained if SCA is required and if the PSU can choose between different authentication methods. If this data is contained, the link "startAuthorisationWithAuthenticationMethodSelection" will also be reported. These methods must be presented to the PSU.	List<AuthenticationObject>	COND	Ex: "scaMethods": [...]
_links	List of hyperlinks to be recognized by the TPP. Supported types in this response: • scaRedirect: in case of SCA by redirection. Link where the PSU browser must be redirected by the Hub. • scaOAuth: in case of SCA and require payment execution. • self: link to the payment initiation resource created by this request.	Links	MA	Ex: "_links": {...}

	• state: link to retrieve the state of the payment initiation transaction.			
psuMessage	Text sent to the TPP through the HUB to be displayed to the PSU.	String	OP	^.{1,500} $ Ex: "psuMessage": "Información para PSU"
tppMessages	Message for the TPP sent through the HUB.	List<TppMessage>	OP	Ex: "tppMessages": […]

7.3.2.3 Examples

Example of request

POST https://aspsp.example.es/v1.1/sva/periodic-payments/sepa-credit-transfers

Content-Encoding: gzip

Content-Type: application/json

HUB-Transaction-ID: 3dc3d5b3-7023-4848-9853-f5400a64e80f

HUB-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

TPP-HUB-ID: PSDES-BDE-3DFD21

TPP-HUB-Name: Nombre del TPP

TPP-HUB-Rol: PSP_PI

TPP-HUB-National-Competent-Authority: BDE

Authorization: Bearer 2YotnFZFEjr1zCsicMWpAA

PSU-IP-Address: 192.168.8.16

PSU-IP-Port: 443

PSU-Accept: application/json

PSU-Accept-Charset: utf-8

PSU-Accept-Encoding: gzip

PSU-Accept-Language: es-ES

PSU-User-Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0) Gecko/20100101 Firefox/54.0

PSU-Http-Method: POST

PSU-Device-ID: f8b3feda-6fe3-11e8-adc0-fa7ae01bbebc

PSU-GEO-Location: GEO:12.526347;54.649862

TPP-Redirect-Preferred: true

TPP-Redirect-URI: https://hub.example.es/cb

TPP-Nok-Redirect-URI: https://hub.example.es/cb/nok

Date: Sun, 26 Sep 2017 15:02:37 GMT

```
{
	"instructedAmount": {
		"currency": "EUR",
		"amount": "153.50"
	},
	"creditorAccount": {
		"iban": "ES2222222222222222222222"
	},
	"creditorName": "Nombre123",
	"remittanceInformationUnstructured": "Información adicional",
	"startDate": "2018-03-01",
	"executionRule": "preceding",
	"frequency": "Monthly",
	"dayOfExecution": "01"
}
```


Example response

HTTP/1.1 201 Created

HUB-Transaction-ID: 3dc3d5b3-7023-4848-9853-f5400a64e80f

HUB-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721

X-Request-ID: 10391c7e-ad88-49ec-a2ad-00aacb1f6541

ASPSP-SCA-Approach: REDIRECT

Date: Sun, 26 Sep 2017 15:02:43 GMT

Location: https://aspsp.example.es/v1.1/periodic-payments/123-qwe-456

Content-Type: application/json


```
{
	"transactionStatus": "RCVD",
	"paymentId": "123-qwe-456",
	"_links": {
		"scaRedirect": {
			"href": "https://aspsp.example.es/authorize"
		},
		"self": {
			"href": "/v1.1/periodic-payments/123-qwe-456",
		"state": {
			"href": "/v1.1/periodic-payments/123-qwe-456/state"
		}
	}
}
```

8. DEFINITION OF COMPOSITE DATA

The various types of composite data used in the requests and responses used in the system are defined below.

8.1 AccountAccess

Field	Description	Type	Mand.	Format
accounts	This specifies the accounts for which detailed information can be requested. If the list is empty, the TPP is requesting all accessible accounts and they will be questioned through a dialogue between the PSU and the ASPSP. Additionally, the list of balances and transactions must also be left blank if they are used.	List<Account Reference>	OP	E.g.: "accounts": […]
balances	Specifies the accounts for which the balances can be requested. If the list is empty, the TPP is requesting all accessible accounts and they will be questioned through a dialogue between the PSU and the ASPSP. Additionally, the list of accounts and transactions must also be left blank if they are used.	List<Account Reference>	OP	E.g.: "balances": […]
transactions	Specifies the accounts for which transactions can be requested. If the list is empty, the TPP is requesting all accessible accounts and they will be questioned through a dialogue between the PSU and the ASPSP. Additionally, the list of balances and accounts must also be left blank if they are used.	List<Account Reference>	OP	E.g.: "transactions": […]

additionalInformation	This attribute will be ignored by the ASPSP	AdditionalInformationAccess	OP	Ej: "additionalInformation": {…}
availableAccounts	Only the value "allAccounts" is admitted.	String	OP	E.g. "availableAccounts": "allAcounts"
availableAccountsWithBalances	Only the value "allAcounts" is admitted	String	OP	E.g. "availableAccountsWithBalances": "allAcounts"
allPsd2	Only the value "allAccounts" is allowed.	String	OP	E.g.: "allPsd2": "allAccounts"

8.2 AccountDetails

Field	Description	Type	Mand.	Format
resourceId	Account identifier to be used in the PATH when data is requested on a dedicated account.	String	COND	^.{1,100}$ E.g.: "resourceId":"3dc3d5b3702348489853f5400a64e80f"
iban	Account IBAN.	String	OP	E.g.: "iban":"ES1111111111111111111"
bban	BBAN of the account, when it doesn't have an IBAN.	String	OP	E.g.: "bban":"20385778983000760236"
currency	Account's currency type.	String	OB	**ISO 4217** E.g.: "currency":"EUR"
ownerNames	List of names of account owners.	List<AccountOwner>	OP	Ej: "ownerNames":[…]
psuName	Name of the connected PSU. In case of corporate accounts, this could be the person acting on behalf of the company.	String	OP	^.{1,140}$ Ej: "psuName": "Heike Mustermann"
name	Name given by the bank or the PSU to the online banking account.	String	OP	^.{1,35}$ E.g.: "name":"Name"
product	Name of the product given by ASPSP to this account.	String	OP	^.{1,35}$ E.g.: "product":"Main Account"
bic	Account BIC.	String	OP	^.{1,12}$ E.g.: "bic":"XSXHXSMMXXX"

_links	Links to the account to retrieve balance and/or transaction information of the account. Links are only supported when the corresponding consent has been given to the account.	Links	OP	E.g.: "links": {…}

8.3 AccountOwner

Field	Description	Type	Mand.	Format
name	Account owner name	String	MA	^.{1,70}$ Ej: “name”: “Heitaki Sun”
role	The following owner codes are used: "owner", "legalRepresentative", "authorizedUser".	String	OP	^.{1,35}$ Ej: “role”:”owner”

8.4 AccountReference

Field	Description	Type	Mand.	Format
iban	Account IBAN	String	COND	E.g.: "iban":"ES1111111111111111111"
bban	BBAN of the account, when it doesn’t have an IBAN.	String	COND	E.g.: "bban":"20385778983000760236"
maskedPan	Masked Primary Account Number of the card.	String	COND	^.{1,35}$ E.g.: "maskedPan":"123456******4567"
msisdn	Alias for access to a payment account through a registered mobile telephone number. **NOT SUPPORTED**	String	COND	^.{1,35}$ E.g.: "msisdn":"…"
currency	Currency type.	String	OP	**ISO 4217** E.g.: "currency":"EUR"

8.5 AccountReport

Field	Description	Type	Mand.	Format
booked	Latest Transactions (annotations) known to the account.	List<Transactions>	COND	E.g.: "booked":[{..}]

	It must be included if the bookingStatus parameter is set as “booked” or “both”.			
pending	Pending account transactions. No content if the bookingStatus parameter is set to “booked”.	List<Transactions>	OP	E.g.: "pending":[{..}]
information	List of standing orders.	List<Transactions>	OP	Ej: "information":[{…}]
_links	The following links are accepted in this object: • account (OB) • first (OP) • next (OP)	Links	OB	E.g.: "_links":[{..}]

8.6 AdditionalInformationAccess

Campo	Descripción	Tipo	Oblig.	Formato
trustedBeneficiaries	This attribute Will be ignored by the ASPSP	List<Account Reference>	OP	trustedBeneficiaries
OwnerName	This attribute Will be ignored by the ASPSP	List<Account Reference>	OP	Ej: "ownerName": {…}

8.7 Address

Field	Description	Type	Mand.	Format
streetName	Street	String	OP	^.{1,70}$ E.g.: "streetName":"Street example"
buildingNumber	Number	String	OP	E.g.: "buildingNumber":"5"
townName	City	String	OP	E.g.: "townName":"Cordoba"
postCode	Postcode	String	OP	E.g.: "postCode":"14100"
country	Country code	String	OB	**ISO 3166** E.g.: "country":"ES"

8.8 Amount

Field	Description	Type	Mand.	Format
currency	Currency of the amount.	String	OB	**ISO 4217** E.g.: "currency":"EUR"
amount	The amount. The decimal point is used as the separator.	String	OB	**ISO 4217** E.g.: "amount":"500.00"

8.9 AuthenticationObject

Field	Description	Type	Mand.	Format
authenticationType	Type of authentication method. Possible values: • SMS_OTP • PUSH_OTP See annex **¡Error! No se encuentra el origen de la referencia. ¡Error! No se encuentra el origen de la referencia.** for more information.	String	MAN	E.g. "authenticationType":"SMS_OTP"
authenticationVersion	Version of the tool associated with the authenticationType.	String	COND	E.g. "authenticationVersion":"1.0"
authenticationMethodId	Id of the authentication method provided by the ASPSP.	String	MAN	^.{1,35}$
name	Name of the authentication method defined by the PSU in the ASPSP online banking. It may also be a description provided by the ASPSP. If the TPP has it available, it must present it to the PSU.	String	MAN	E.g. "name":"SMS OTP to phone 666777888"
explanation	Detailed information about the SCA method for the PSU	String	OPT	

8.10 Aspsp

Field	Description	Type	Mand.	Format
bic	The ASPSP's BIC code.	String	OB	E.g.: "bic":"XXXXXXXXXXX"

name	ASPSP Name	String	OP	E.g.: “name":"Name ASPSP"

8.11 Balance

Field	Description	Type	Mand.	Format
balanceAmount	Amount and currency of the balance.	Amount	OB	E.g.: "balanceAmount": {...}
balanceType	Balance type. Values supported in annex 9.6 Balance types	String	OB	E.g.: "balanceType": "closingBooked"

8.12 ExchangeRate

Field	Description	Type	Mand.	Format
currencyFrom	Source currency.	String	OB	E.g.: "currencyFrom":"USD"
rate	Defines the exchange rate. E.g.: currencyFrom=USD, currencyTo=EUR: 1USD =0.8 EUR with an exchange rate of 0.8.	String	OB	E.g.: "rate":"0.8"
currencyTo	Target currency.	String	OB	E.g.: "currencyTo":"EUR"
rateDate	Rate date.	String	OB	**ISODateTime**
rateContract	Reference to the contract of the rate.	String	OP	

8.13 Href

Field	Description	Type	Mand.	Format
href	Contains a link to a resource.	String	OP	E.g.: "href": "/v1.1/payments/sepa-credit-transfers/asd-1234-jkl"

8.14 Links

Field	Description	Type	Mand.	Format
scaRedirect	The URL used to perform SCA, through a redirect of the PSU's browser.	Href	OP	E.g.: "scaRedirect": {...}

startAuthorisation	Link to endpoint where the authorisation of either the transaction or the cancellation must be initiated.	Href	OP	E.g.: "startAuthorisation":{…}
startAuthorisationWithAuthenticationMethodSelection	Link to endpoint where the authorisation of the either the transaction or the cancellation must be initiated, where the SCA method must be specified in the corresponding call.	Href	OP	E.g.: " startAuthorisationWithAuthenticationMethodSelection ": {…}
self	The link to the resource created for the request. This link can be subsequently used to retrieve the transaction status.	Href	OP	E.g.: "self": {…}
status	The link to retrieve the transaction status. For example, the payment initiation status.	Href	OP	E.g.: "status": {…}
account	Link to the resource that provides the data on an account.	Href	OP	E.g.: "account": {…}
balances	Link to the resource that provides the account balances.	Href	OP	E.g.: "balances": {…}
transactions	Link to the resource that provides the account transactions.	Href	OP	E.g.: "transactions": {…}
first	Browser link for paginated accounts.	Href	OP	E.g.: "first": {…}
next	Browser link for paginated accounts.	Href	OP	E.g.: "next": {…}

8.15 PaymentExchangeRate

Field	Description	Type	Mand.	Format
unitCurrency	Currency in which the exchange rate is expressed in a foreign currency. In the following example EUR1 = xxxCUR, the currency is the EUR.	String	OP	**ISO 4217** E.g.: "unitCurrency": "EUR"

exchangeRate	Factor used to convert an amount from one currency to another. It reflects the price at which one currency was purchased with the other currency.	String	OP	E.g.: "exchangeRate": "1.3"
contractIdentification	Unique identification of the contract to exchange currencies	String	OP	E.g.: "contractIdentification": "1234-qeru-23"
rateType	Specifies the rate used to complete the currency exchange. Allowed values: • SPOT • SALE • AGRD	String	OP	E.g.: "rateType": "SPOT"

8.16 ReportExchangeRate

Field	Description	Type	Mand.	Format
sourceCurrency	Currency from which an amount will be converted in a currency exchange.	String	OB	**ISO 4217** E.g.: "sourceCurrency": "EUR"
exchangeRate	Factor used to convert an amount from one currency to another. It reflects the price at which one currency was purchased with the other currency.	String	OB	E.g.: "exchangeRate": "1.3"
unitCurrency	Currency in which the exchange rate is expressed in a foreign currency. In the following example EUR1 = xxxCUR, the currency is the EUR.	String	OB	**ISO 4217** E.g.: "unitCurrency": "EUR"
targetCurrency	Currency into which the amount will be converted into in a currency exchange.	String	OB	**ISO 4217** E.g.: "targetCurrency": "USD"
quotationDate	Date on which the exchange rate is quoted.	String	OB	**ISODate** E.g.: "quotationDate": "24/01/2019"
contractIdentification	Unique identification of the contract to exchange currencies	String	OP	E.g.: "contractIdentification": "1234-qeru-23"

8.17 SinglePayment

Field	Description	Type	Mand.	Format
endToEndIdentification	Unique identifier of the operation assigned by the initiating party (TPP)	String	OP	^.{1,35}$ Ex: "endToEndIdentification": "12345678901234567890123456789012345"
instructedAmount	Information on the transfer which has been made.	Amount	OB	E.g.: "instructedAmount": {…}
debtorAccount	The originator's account. **Note:** this field can be optional in some services such as bulk payments	AccountReference	OB	E.g.: "debtorAccount": {"iban":"ES1111111111111111111111"}
creditorAccount	Beneficiary's account	AccountReference	OB	E.g.: "creditorAccount": {"iban":"ES1111111111111111111111"}
creditorName	Beneficiary's name	String	OB	^.{1,70}$ E.g.: "creditorName":"Name"
creditorAgent	BIC of the Beneficiary's account.	String	OP	E.g.: "creditorAgent":"XSXHXSMMXXX"
creditorAddress	Beneficiary's address	Address	OP	E.g.: "creditorAddress":{…}
chargeBearer	Only for payment-product: • target-2-payments • cross-border-credit-transfers Allowed values: • DEBT • CRED • SHAR • SLEV	String	OP	**ChargeBearerType1Code de ISO 20022** E.g.: "chargeBearer":"SLEV"
remittanceInformationUnstructured	Additional information. See annex 9.9 Good Practice Guide for recommendations for use.	String	OP	^.{1,140}$ E.g.: "remittanceInformationUnstructured":"Additional information"
requestedExecutionDate	Execution date requested for future payments. **Note**: only if supported by the ASPSP	String	COND	**ISODate**
requestedExecutionTime	Execution time requested. **Note**: only if supported by the ASPSP	String	COND	**ISODateTime**

8.18 StandingOrderDetails

Campo	Descripción	Tipo	Oblig.	Formato
startDate	The first applicable day of execution starting from this date the first payment was/will be executed.	String	OB	**ISODate** Ej: "startDate":"2019-01-20"
endDate	The last applicable day of execution If not given, it is an infinite standing order.		OP	**ISODate** Ej: "endDate":"2019-01-20"
executionRule	NOT SUPPORTED	String	OP	
withinAMonth Flag	Este elemento es solo usado en caso de que la frecuencia sea igual a "monthly". Si este elemento es igual a false, este no tiene efecto. Si es igual a true, entonces la regla de ejecución es anulada si el día de ejecución cae en un mes diferente. Nota: este atributo es usado raramente. used in case of frequency equals "monthly". If this element equals false it has no effect. If this element equals true, then the execution rule is overruled if the day of execution would fall into a different month using the execution rule. Example: executionRule equals "preceding", dayOfExecution equals "02" and the second of a month is a Sunday. In this case, the transaction date would be on the last day of the month before. This would be overruled if withinAMonthFlag equals true and the payment is processed on Monday the third of the Month. Remark: This attribute is rarely supported in the market.	Boolean	OP	Ej: "withinAMonthFlag": true
frequency	The frequency of the recurring payment resulting from this standing order.	Sring	OB	**EventFrequency7Code de ISO 20022** Ej: "frequency

	Allowed values: • Daily • Weekly • EveryTwoWeeks • Monthly • EveryTwoMonths • Quarterly • SemiAnnual • Annual			
monthsOfExecution	The format is following the regular expression \d{1,2}. The array is restricted to 11 entries. The values contained In the array entries shall all be different and the maximum value of one entry is 12. This attribute is contained if and only if the frequency equals "MonthlyVariable". Example: An execution on January, April and October each year is addressed by ["1". "4", "10"].	List<String>	COND	Ej:"monthsOfExecution": ["1", "4", "10"]
multiplicator	This is multiplying the given frequency resulting the exact frequency, e.g. Frequency=weekly and multiplicator=3 means every 3 weeks. **Remark**: This attribute is rarely supported in the market.	Integer	OP	multiplicator
dayOfExecution	"31" is ultimo. The format is following the regular expression \d{1,2}. Example: The first day is addressed by "1". The date is referring to the time zone of the ASPSP.	String	COND	dayOfExecution

limitAmount	Amount limit for fund skimming, e.g. skim all funds above this limit to savings account, i.e. typically a specific periodic payments with fixed remaining amount rather than fixed transaction amount. Amount may be zero as well as below zero, i.e. negative. **Constraints**: transactionAmount needs to be zero and bankTransactionCode needs to specify PMNT-MCOP-OTHR	Amount	COND	limitAmount

8.19 StructuredAdditionalInformation

Campo	Descripción	Tipo	Oblig.	Formato
standingOrderDetails	Details of underlying standing orders.	StandingOrderDetails	OB	Ej: "standingOrderDetails": {...}

8.20 TppMessage

Field	Description	Type	Mand.	Format
category	Category for the type of message received. Possible values: ERROR or WARNING	String	OB	E.g.: "category": "ERROR"
code	Response code. In annex 9.3 Return codes the return codes are listed by service.	String	OB	E.g.: "code":"CONSENT_INVALID"
path	Path to the error field.	String	COND	E.g.: "path":"..."
text	Additional explanatory text.	String	OP	E.g.: "text":"Text example"

8.21 Transactions

Field	Description	Type	Mand.	Format

transactionId	Can be used as access-ID in the API, where more details on an transaction is offered.	String	OP	E.g. "transactionId":"123-asdf-456"
entryReference	Identification of the transaction that can be used, for example, in delta queries.	String	OP	^.{1,35}$ E.g.: "entryReference":"1234-asdf-456"
mandateId	Identification of Mandates, e.g. a SEPA Mandate ID	String	OP	^.{1,35}$ E.g. "mandateId":"…"
checkId	Cheque identifier	String	OP	^.{1,35}$ E.g. "checkId":"…"
bookingDate	Date the transaction was recorded	String	OP	**ISODate** "bookingDate":"2017-10-23"
valueDate	Date on which the settlement becomes available to the account owner in the case of a request for a loan or credit facility.	String	OP	**ISODate** E.g.: "valueDate":"2017-10-23"
transactionAmount	Transaction amount	Amount	OB	E.g.: "transactionAmount": [{..}]
currencyExchange	Currency exchange rate	List<ReportExchangeRate>	OP	E.g.: "currencyExchange": [{…}]
remittanceInformationUnstructured	Field to include additional information on the remittance.	String	OP	^.{1,140}$ E.g.: "remittanceInformationUnstructured":"Additional information"
additionalInformationStructured	Is used if and only if the bookingStatus entry equals "information". Every active standing order related to the dedicated payment account result into one entry.	StructuredAdditionalInformation	OP	Ej: "additionalInformationStructured": {…}
_links	Possible values: • Transaction details	Links	OP	E.g.: "_links": {…}

9. ANNEXES

9.1 Signature

9.1.1 "Digest" header mandatory

The Digest field is mandatory in all requests.

This field contains a hash of the message body. If the message does not contain a body, the "Digest" field must contain a hash of an empty "bytelist". The hash algorithms that may be used to calculate the "Digest" in the context of this specification are SHA-256 and SHA-512.

9.1.2 Signature requirements

The structure of the “Signature” field of the request header must have the following structure:

Item	Type	Mand.	Requirements	Additional requirements
keyId	String	OB	It is a chain that the HUB can use to find the component needed to validate the signature.	Serial number of the TPP certificate included in “TPP-Signature-Certificate”. It must be in the following format: KeyId="SN=XXX,CA= YYYYYYYYYYYYYYYY" In which “XXX” is the certificate serial number encoded in hexadecimal format and “YYYYYYYYYYYYYYYY” is the full “Distinguished Name” of the certifying authority.
Algorithm-ID	String	OB	This is used to specify the algorithm used to generate the signature.	The algorithm must identify the same algorithm for the signature which is presented in the request’s certificate. It should identify SHA-256 or SHA-512.
Headers	String	OP	These are used to specify the list of HTTP headers included when the signature for the message is generated. If specified, it should be a list within quotation marks and in lower case, separated by a blank space. If it is not specified it shall be understood that only one value has been specified. The said specified value is the "Date" attribute from the header of the request. The order of attributes is important and must be the same as the order specified in the list of HTTP headers in this field.	The mandatory fields to be signed are: • digest • x-request-id Optionally, if they can go there and are supported, they can include: • psu-id • psu-corporate-id • tpp-redirect-uri
Signature	String	OB	The “signature” parameter must be in Base64 according to RFC 4648. The TPP uses the header’s algorithm and parameters to form the signature chain to be signed. The chain to sign is signed with the keyId and the corresponding algorithm. The content should go in Base64.	There are no additional requirements.

9.1.3 Example

You want to make a host-to-host request with the following text:


```
{
 "instructedAmount" : {
  "currency" : "EUR",
  "amount" : "16.00"
 },
 "debtorAccount" : {
  "iban" : "ES5140000001050000000001",
  "currency" : "EUR"
 },
 "creditorName" : "Cred. Name",
 "creditorAccount" : {
  "iban" : "ES6621000418401234567891",
  "currency" : "EUR"
 },
 "creditorAddress" : {
  "street" : "Example of street",
  "buildingNumber" : "15",
  "city" : "Cordoba",
  "postalCode" : "14100",
  "country" : "ES"
 },
 "remittanceInformationUnstructured" : "Payment",
 "chargeBearer" : "CRED"
}
```


And you must also add the following headers

- X-Request-ID=a13cbf11-b053-4908-bd06-517dfa3a1861

You must make the following transactions.

9.1.3.1 Generation of the "Digest" header

To do so you must perform the hash of the message body that will be sent. It is vital to do so on the final content once serialised, as the following serialisation processes may introduce changes in the body of the message finally sent, making the signature invalid.

It is possible to use the SHA-256 and SHA-512 algorithms following the RFC 5843. In our example you will use SHA-256 on the body of the message, obtaining the following result:

- Hexadecimal: A5F1CF405B28E44ED29507E0F64495859BA877893D2A714512D16CE3BD8BE562
- Base64: pfHPQFso5E7SlQfg9kSVhZuod4k9KnFFEtFs472L5WI=

Thus the value of the "Digest" header to generate will be:

SHA256=pfHPQFso5E7SlQfg9kSVhZuod4k9KnFFEtFs472L5WI=

The headers you have so far are:

X-Request-ID=a13cbf11-b053-4908-bd06-517dfa3a1861f]
Digest=SHA256=pfHPQFso5E7SlQfg9kSVhZuod4k9KnFFEtFs472L5WI=

9.1.3.2 Generation of the "Signature" header

The "Signature" header is the multi-value type, i.e. it contains within it various pairs of sub-headers of the attribute-value type

Establishment of the "keyId" value

This field is obtained based on a serial number of the certificate in hexadecimal and the DN of the certification authority that generates the certificate.

In our example you obtain the following result:

keyId="SN=-5d803f65,CA=CN=REDSYS-AC-EIDASt-C1,OU=PKI,O=REDSYS,C=ES"

Establishment of the "headers" attribute

You should note that this attribute and some others are shown in the Berlin Group document with the first character in upper case, but in the RFC used by the entity its content is always established in lower case, so we assume that it is an error.

This establishes the fields that will be taken into account signing.

headers="digest x-request-id"

Establishment of the "algorithm" attribute

algorithm="SHA-256"

Construction of the chain to be signed

The chain to be signed according to point 2.2.3 is as follows:

Digest: SHA256=pfHPQFso5E7SlQfg9kSVhZuod4k9KnFFEtFs472L5WI=

X-Request-ID: a13cbf11-b053-4908-bd06-517dfa3a1861f

Generation of the signature

We sign the chain obtained in the above point with the private key of our certificate and pass the result to Base64, obtaining in our specific case the following result:

la8LV3Fny2so4c40OkYFtZvr1mOkOVY1n87iKfIggEkXQjZNcyjp9fFkNtQc+5ZVNESdiqKG8xrawYa5gAm46CvcKCh
NTPaakiEJHcXM5RZPWN0Ns5HjV5mUY2QzD+g5mwqcWvXtBr1vg0bZKN8Zt3+uJMN37NQg9tJNE2yKIJlEPlAYOj
C2PA/yzGSLOdADnXQut9yRvxw8gMCjDtRaKDyWmwG6/crX293hGvBUeff1xvTluWhQzyfx4J6WG0v1ZmpnWdZ
1LF68sToeDGTdu65aVKV2q6qcZzcm5aPV6+mVHX+21Vr6acxiLZdeYUHYJHrzErUN3KJrmt3w2AL7Dw==

9.1.3.3 Generation of the "TPP-Signature-Certificate" header

This header contains the certificate we have used in Base64. For reasons of space only a part is established in the example:

TPP-Signature-Certificate=”MIIEWTCCA0GgAwIBAgI….

9.1.3.4 Definitive headers to send

As seen in the above points the headers that must be sent in the request are:

X-Request-ID=a13cbf11-b053-4908-bd06-517dfa3a1861f

Digest=SHA256=pfHPQFso5E7SlQfg9kSVhZuod4k9KnFFEtFs472L5WI=

Signature=keyId="SN=-5d803f65,CA=CN=REDSYS-AC-EIDASt-C1,OU=PKI,O=REDSYS,C=ES",algorithm="SHA-256",headers="digest x-request-id",signature="la8LV3Fny2so4c40OkYFtZvr1mOkOVY1n87iKfIggEkXQjZNcyjp9fFkNtQc+5ZVNESdiqKG8xrawYa5gAm46CvcKChNTPaakiEJHcXM5RZPWN0Ns5HjV5mUY2QzD+g5mwqcWvXtBr1vg0bZKN8Zt3+uJMN37NQg9tJNE2yKIJlEPlAYOjC2PA/yzGSLOdADnXQut9yRvxw8gMCjDtRaKDyWmwG6/crX293hGvBUeff1xvTluWhQzyfx4J6WG0v1ZmpnWdZ1LF68sToeDGTdu65aVKV2q6qcZzcm5aPV6+mVHX+21Vr6acxiLZdeYUHYJHrzErUN3KJrmt3w2AL7Dw==”

TPP-Signature-Certificate=MIIEWTCCA0GgAwIBAgIEon/…

9.2 HTTP response codes

The HTTP codes followed by this specification and their uses are as follows:

HTTP code	Description
200 OK	• Response Code for PUT and GET requests. • This code is allowed if the request was repeated due to a timeout. The response may be 200 or 201 depending on the implementation of the ASPSP. • The POST request of the FCS also allows a 200 code to be returned as a new resource is not created. • Response code for DELETE requests when the request has been carried out correctly and authorisation is not required.
201 Created	Response code for POST: requests Post where a new resource has been created correctly.
202 Accepted	Response code for DELETE: requests when a payment resource can be cancelled, but authorisation of the cancellation from the PSU is required.
204 No Content	Response code for DELETE: requests where the consent has been deleted successfully. The code indicates that the response was performed, but no content has been returned. It is also used in DELETE requests for a payment initiation in which authentication is not required.

400 Bad Request	A validation error has occurred. This code covers syntax errors in the requests or when there is incorrect data in the payload.
401 Unauthorized	The PSU is not properly authorised to make the request. Try to make the request again with the correct authentication information.
403 Forbidden	Returned if the appeal was referenced in the existing path but cannot be accessed by the TPP or the PSU. This code must only be used for non-sensitive identifiers as it could reveal that the resource exists but that it cannot be accessed.
404 Not found	Returned if the resource or endpoint that was referenced in the path exists but cannot be accessed by the TPP or the PSU. When there are any doubts as to whether a specific ID in the path is sensitive or not, use this code instead of 403.
405 Method Not Allowed	This code is sent only when the method (POST, PUT, GET...) is not supported in a specific endpoint. Response code for DELETE in the event of a payment cancellation, where the payment initiation cannot be cancelled due to legal or other operational reasons.
406 Not Acceptable	The ASPSP cannot generate the content specified by the TPP in the Accept header field.
408 Request Timeout	The server is still working properly, but the request has reached the timeout limit.
409 Conflict	The request could not be completed due to a conflict with the current status of the referenced resource.
415 Unsupported Media Type	The TPP has requested a media type which is not supported by the ASPSP.
429 Too Many Requests	The TPP has exceeded the maximum number of requests allowed by the consent or by the RTS.
500 Internal Server Error	An internal error has occurred in the server.
503 Service Unavailable	The ASPSP server is currently unavailable. This is generally a temporary condition.

9.3 Return codes

Return codes and associated HTTP response codes allowed.

	HTTP code	Code	Description
SIGNATURE CERTIFICATE	401	CERTIFICATE_INVALID	The content of the signature certificate is not valid.
	401	CERTIFICATE_EXPIRED	The signature certificate has expired.
	401	CERTIFICATE_BLOCKED	The signature certificate has been blocked by the ASPSP.
	401	CERTIFICATE_REVOKED	The signature certificate has been revoked by the QTSP.

	401	CERTIFICATE_MISSING	The signature certificate was missing from the request.
SIGNATURE	401	SIGNATURE_INVALID	The signature is not valid.
	401	SIGNATURE_MISSING	The signature, when it is mandatory, is missing from in the message.
GENERAL	400	FORMAT_ERROR	The format of certain fields of the request is incorrect. The fields will be indicated. This applies to fields in the body and the header. It also applies in cases where these entries refer to occasions when there is data that is missing or incorrect.
	400	PARAMETER_NOT_CONSISTENT	The parameters sent by the TPP are not consistent. Only applies to query parameters.
	400	PARAMETER_NOT_SUPPORTED	The parameter is not supported by the ASPSP. It will only be used in those parameters whose support is optional for the ASPSP.
	401	PSU_CREDENTIALS_INVALID	The PSU-ID is not related to the ASPSP or is blocked, or the password or OTP as incorrect.
	400 (payload) 405 (HTTP method)	SERVICE_INVALID	The requested service is not valid for the specified resource or the data sent.
	403	SERVICE_BLOCKED	The service is not available for the PSU due to a block in the ASPSP channel.
	401	CORPORATE_ID_INVALID	The PSU-Corporate-ID could not be associated in the ASPSP systems.
	403 (if resource in path) 400 (if resource in payload)	CONSENT_UNKNOWN	The requested Consent-ID does not coincide for the TPP and the ASPSP.
	401	CONSENT_INVALID	Consent was created by the TPP, but is not valid for the resource / service requested. Or, the definition of the consent is incomplete or is invalid.
	401	CONSENT_EXPIRED	The consent was created by the TPP but has expired and must be refreshed.
	401	TOKEN_UNKNOWN	The token received is unknown to the TPP.

	401	TOKEN_INVALID	The token is associated with the TPP, but it is not valid for the service / resource which are being accessed.
	401	TOKEN_EXPIRED	The token is associated with the TPP, but it has expired and must be refreshed.
	404 (if account-id is in the path) 403 (if another resource is in path) 400 (if it goes in payload)	RESOURCE_UNKNOWN	The resource requested is unknown to the TPP.
	403 (if resource in path) 400 (if resource in payload)	RESOURCE_EXPIRED	The requested resource is associated with the TPP, but it has expired and will no longer be available.
	400	RESOURCE_BLOCKED	The directed resource cannot be directed by the request. It may be blocked, for example by a grouping in the “signing basket”.
	400	TIMESTAMP_INVALID	The timestamp is not in the accepted period of time.
	400	PERIOD_INVALID	The period of time requested is out of range.
	400	SCA_METHOD_UNKNOWN	The SCA method selected in the authentication method selection request is unknown or cannot be associated with the PSU by the ASPSP.
	409	STATUS_INVALID	The directed resource does not allow additional authorisation.
OAuth2	302	invalid_request	The request has not been formed correctly as it has missing parameters, an unsupported value and/or repeated parameters.
	302	unauthorized_client	The authenticated client is not authorised to use this type of authorisation.
	302	access_denied	The resource owner or the authorisation server denies the request.
	302	unsupported_response_type	The authorisation server does not support the method used to obtain the authorisation code.
	302	invalid_scope	The requested scope is invalid, unknown or poorly formed.

	302	server_error	Error 500 that cannot be returned in a redirect, which is returned with this code.
	302	temporarily_unavailable	The authorisation server is unable to process the request at this time due to a temporary overload or due to maintenance being undertaken.
	400	invalid_request	The request has not been formed correctly as it has missing parameters, an unsupported value and/or repeated parameters, includes multiple credentials or uses more than one client authentication mechanism.
	401	invalid_client	Failure to authenticate the client.
	400	invalid_grant	The authorisation provided or the refresh token is invalid, has expired, has been revoked, does not match the URI redirection or was issued to another client.
	400	unauthorized_client	The authenticated client is not authorised to use this type of authorisation.
	400	unsupported_grant_type	The type of authorisation requested is not supported by the authorisation server.
	400	invalid_scope	The requested scope is invalid, unknown, badly formed or exceeds what is allowed.
PIS	403	PRODUCT_INVALID	The payment product requested is not available for the PSU.
	404	PRODUCT_UNKNOWN	The payment product requested is not supported by the ASPSP.
	400	PAYMENT_FAILED	The payment failed. For example, due to risk management reasons.
	400	EXECUTION_DATE_INVALID	The execution date requested is not a valid execution date for the ASPSP.
	405	CANCELLATION_INVALID	The directed payment cannot be cancelled. For example, a long time has passed or due to legal restrictions.
AIS	401	CONSENT_INVALID	Consent was created by the TPP, but is not valid for the resource / service requested. Or, the definition of the consent is incomplete or is invalid.

	400	SESSIONS_NOT_SUPPORTED	The combined service indicator does not support the ASPSP which the request was sent to.
	429	ACCESS_EXCEEDED	The account accesses have exceeded the allowable accesses per day without the PSU being present.
	406	REQUESTED_FORMATS_INVALID	The format requested in the Accept field does not match those offered by the ASPSP.
FCS	400	CARD_INVALID	The card number is unknown to the ASPSP or is not associated with the PSU.
	400	NO_PIIS_ACTIVATION	The PSU has not activated the account to be used for the PIIS associated with the TPP.

9.4 Transaction status

Code	Name	Description
ACCC	AcceptedSettlementCompleted	The settlement of the beneficiary's account has been completed.
ACCP	AcceptedCustomerProfile	The pre-check of the technical validation was correct. The client profile check was also correct.
ACFC	AcceptedFundsChecked	In addition to the client profile, the availability of funds has been checked and confirmed. Note: ISO 20022 approval is needed.
ACSC	AcceptedSettlementCompleted	The settlement of the originator's account has been completed. Use: the use of the first agent (the originator's ASPSP through the HUB) to inform the originator that the transaction has been completed. Important: the reason for this status is to provide the status of the transaction, not for financial information. It can only be used after a bilateral agreement has been entered into.
ACSP	AcceptedSettlementInProcess	The above controls such as technical validations and of the client's profile were correct and therefore, the payment initiation has been accepted to be processed.
ACTC	AcceptedTechnicalValidation	Syntactic and semantic authentication and validation are correct.
ACWC	AcceptedWithChange	The instruction has been accepted, but a modification is required, for example a date or another item of data which has not been sent.

		It is also used to report that a change has been applied, for example, on a payment initiation and that the execution date has been changed.
ACWP	AcceptedWithoutPosting	The payment instruction included in the credit transfer has been accepted without being sent to the beneficiary client.
RCVD	Received	The initiation of payment has been received by the agent (the ASPSP through the HUB).
PATC	PartiallyAcceptedTechnicalCorrect	The payment initiations have been authorised by at least one PSU, but they have not yet been authorised by all the PSUs involved. (Multi-level SCA) Note: ISO 20022 approval is needed.
PDNG	Pending	The payment initiation or the individual transaction included in the payment initiation is pending. Additional checks and status updates will be made.
RJCT	Rejected	The payment initiation or the individual transaction included in the payment initiation has been rejected.
CANC	Cancelled	The payment initiation was cancelled before it was executed. Note: ISO 20022 approval is needed.

9.4.1 Table of payment status transitions in Banco Sabadell's API

Original State	Destination State	Description validation/check
-	RCVD	TPP makes a payment initiation providing the payment details
RCVD	ACWC	The format and ownership of the input data are verified and the commissions are calculated
ACWC	ACSP	TPP presents SCA URL to PSU. Sending OTP to PSU device.
ACSP	PATC	The payment has been signed correctly and the payment is pending to be signed by the rest of the participants
ACSP	ACWP	The payment has been signed correctly and the payment is being processed instant-sepa-credit-transfer
ACWP	ACSC	The payment has been signed correctly and the instant payment has been executed correctly
ACSP	ACSC	The payment has been signed correctly and the payment has been accepted for execution
ACSC	CANC	The payment has been cancelled through the TPP
any	RJCT	During the process, validations of: format, data, ownership, viability, limits, risks, etc. have failed.

9.5 Consent status

Code	Description

received	The consent has been received and is technically correct. The data has not yet been authorised.
rejected	The consent has been rejected.
partiallyAuthorised	Due to a multi-level SCA, some, but not all of the necessary authorisations have been made.
valid	The consent is accepted and valid for requests to read the data and specified in the consent.
revokedByPsu	The consent has been revoked by the PSU to the ASPSP.
expired	The consent has expired.
terminatedByTpp	The corresponding TPP has terminated the consent by using the DELETE request on the created consent resource.

9.6 Balance types

Code	Description
closingBooked	The account balance at the end of the pre-agreed period for the report. The sum of the "openingBooked" balances at the beginning of the period and all entries listed in the account during the pre-agreed period for the report.
expected	Transactions made up of annotated entries and entries pending at the time of the request.
openingBooked	The account balance at the beginning of the pre-agreed period for the report. It is always the same as the "closingBooked" balance of the previous period's report.
interimAvailable	Provisionally available balance. Calculated based on annotations of the credit and debit entries during the specified period of time.
interimBooked	The balance calculated during the working day, at the specified time and subject to change during the day. This balance is calculated including the credit and debit entries made during the specified time/period.
forwardAvailable	Future balance available to the account owner on the specified date.

9.7 Types of sharing commissions

Code	Description
DEBT	All transaction charges are paid by the originator.
CRED	All transaction charges are paid by the beneficiary.
SHAR	Shared charges. The originator and beneficiary pay the charges corresponding to each party.
SLEV	The charges to be applied follow the rules agreed at the service level and/or scheme.

9.8 SCA states

Code	Description
received	The authorization resource has been created successfully.
psuIdentified	The PSU associated with the authorization resource has been identified and authenticated, for example, by a password or by the access token
psuAuthenticated	The PSU related to the authorization or cancellation authorization resource has been identified and authenticated, for example, by password or access token.
scaMethodSelected	The PSU / TPP has selected the SCA flow. If the SCA method is chosen implicitly because there is only one SCA method available, then this state is the first state to report instead of "received"
started	The SCA flow has been started.
unconfirmed	The SCA has been technically successfully terminated by the PSU, but the authorization resource needs the confirmation request from the TPP.
finalised	The SCA flow has been completed successfully.
failed	SCA flow has failed.
exempted	The transaction is exempt from SCA, the associated authorization is correct.

9.9 Good Practice Guide

9.9.1 Lifetime of the scaRedirect link

The validity of the token is 5 minutes for this type of link.