THE Berlin GROUP

A EUROPEAN STANDARDS INITIATIVE

Joint Initiative on a PSD2 Compliant XS2A Interface

NextGenPSD2 XS2A Framework

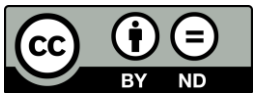
Errata for Version 1.3

14 February 2019

License Notice

This Specification has been prepared by the Participants of the Joint Initiative pan-European PSD2-Interface Interoperability* (hereafter: Joint Initiative). This Specification is published by the Berlin Group under the following license conditions:

- "Creative Commons Attribution-NoDerivatives 4.0 International Public License"

  This means that the Specification can be copied and redistributed in any medium or format for any purpose, even commercially, and when shared, that appropriate credit must be given, a link to the license must be provided, and indicated if changes were made. You may do so in any reasonable manner, but not in any way that suggests the licensor endorses you or your use. In addition, if you remix, transform, or build upon the Specification, you may not distribute the modified Specification.

- Implementation of certain elements of this Specification may require licenses under third party intellectual property rights, including without limitation, patent rights. The Berlin Group or any contributor to the Specification is not, and shall not be held responsible in any manner for identifying or failing to identify any or all such third party intellectual property rights.
- The Specification, including technical data, may be subject to export or import regulations in different countries. Any user of the Specification agrees to comply strictly with all such regulations and acknowledges that it has the responsibility to obtain licenses to export, re-export, or import (parts of) the Specification.

---

* The 'Joint Initiative pan-European PSD2-Interface Interoperability' brings together participants of the Berlin Group with additional European banks (ASPSPs), banking associations, payment associations, payment schemes and interbank processors.

Contents

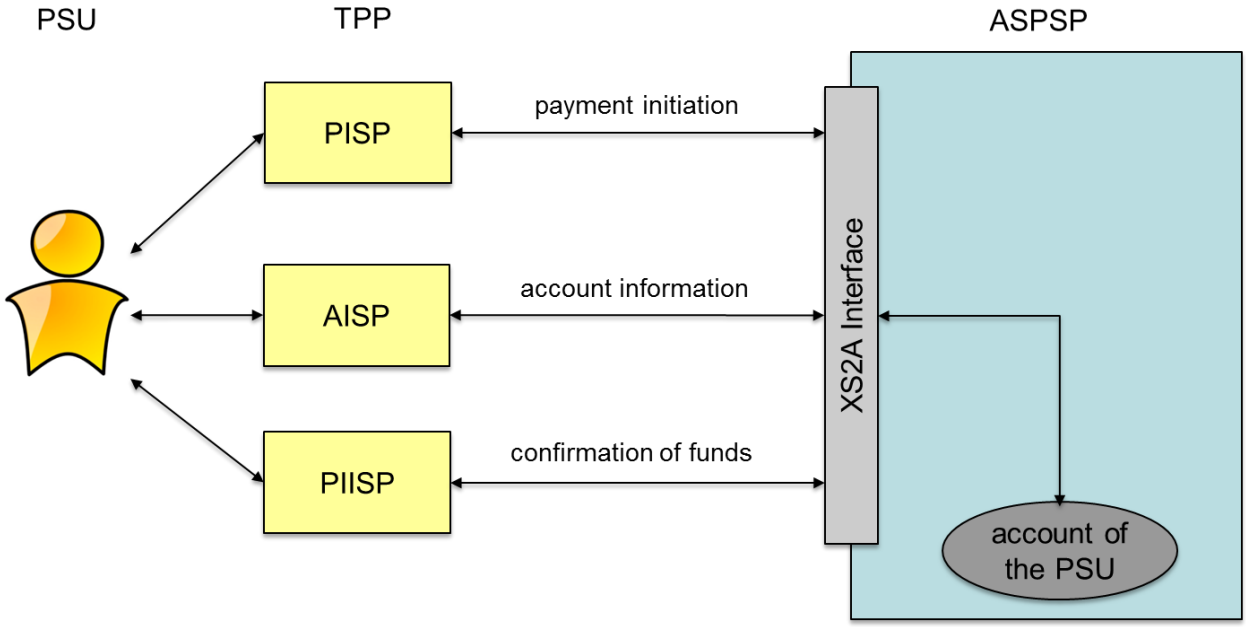
1 Introduction

1.1 Background

The Berlin Group started to publish its XS2A Framework in Version 1.3 on 15 October 2018. This framework consists of the two Documents

- [XS2A OR]: Operational Rules and
- [XS2A IG]: Implementation Guidelines.

The following account access services are covered by this framework:



This document is covering errata in version 1.3 of the Berlin Group XS2A framework. In the change log, an overview on the errata is given. Errata of a more editorial character are not covered in the change log.

1.2 Change Log

Version	Change/Note	Approved
20 Dec 2018	First version of Errata on NextGenPSD2 Framework version 1.3	NextGenPSD2 TF
14 Feb 2019	Second version of Errata on NextGenPSD2 Framework version 1.3 Changes relative to first version of Errata are noted by	NextGenPSD2 TF

	revision marks. Errata cover detailed technical errata as well as the following clarifications and extensions mandated by regulatory or security requirements: - extensions of the provision of TPP-Redirect Header to authorisation resources - restricting the domains of TPP-Redirect headers to domains secured by the TPP eIDAS QWAC certificate. - new TPP header to indicate the TPP preference for a rejection of a payment initiation if not sufficient funds are available - usage of the Consent-ID as a TPP header for the confirmation of funds service, if this service has been consented by the PSU through the new NextGenPSD2 XS2A Extended Service to be published soon. - allowing banks or communities of banks to extend the JSON based bulk payments by an optional field paymentInformationID - allowing banks or communities of banks to mandate certain fields in the JSON crossborder payment formats.	

2 Errata in Operational Rules

No Errata.

3 Errata in Implementation Guidelines

Section	Change	Rationale
New	A new section 4.8 has been added (shifting all later 4.x sections further) about security requirements on TPP-URIs.	Security Requirement
4.8.5	The GET access method on the path signing-baskets/{basketId} is set from Mandatory to Optional due to the fact of different implementations within banks in Online Banking.	Erratum
4.8.5	The GET access method on the path signing-baskets/{basketId}/status has been added.	Erratum
4.9	The usage of HTTP response code 405 was extended to a reject of a cancellation by adding the following paragraph: "DELETE Response code in case of cancellation of a payment initiation, where the payment initiation cannot be cancelled due to legal or other operational reasons."	Erratum
4.9	The HTTP Response code "409 Conflict" was added with the description "The request could not be completed due to a conflict with the current state of the target resource."	Erratum
4.10	The following paragraph is added after the first paragraph: " In cases, where no message code is defined for an HTTP response code in Section 14.11, the additional error information is not used, since the messageCode is a mandatory subfield. In this case, the HTTP code gives sufficient information about the error situation."	Erratum

4.10.1	Example 2 shall be corrected (comma, brackets wrong):
	{ "tppMessages": [{
	"category": "ERROR",
	"code": "PSU_CREDENTIALS_INVALID",
	"text": "additional text information of the ASPSP up to 512 characters"
	}],
	"_links": {
	"updatePsuAuthentication": {"href": "/v1/payments/sepa-credit-transfers/1234-wertiq-983/authorisations/123auth456"}
		Erratum

Section	Change	Rationale
	} }	
5.3.1	In the description of the http header field TPP-Redirect-Preferred, the first paragraph has been changed to "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"." This entry is not mandated in the integrated OAuth case, since the redirect URI is transported during the OAuth protocol.	Erratum
5.3.1	For both headers TPP-Redirect-URI and TPP-Nok-Redirect-URI, a note was added that the requirements of the new section 4.8 apply (see below).	Security Requirement
5.3.1	Add a new optional header TPP-Rejection-NoFunds-Preferred of type Boolean which is described as follows: "If it equals "true" then the TPP prefers a rejection of the payment initiation in case the ASPSP is providing an integrated confirmation of funds request an the result of this is that not sufficient funds are available. If it equals "false" then the TPP prefers that the ASPSP is dealing with the payment initiation like in the ASPSPs online channel, potentially waiting for a certain time period for funds to arrive to initiate the payment. This parameter might be ignored by the ASPSP."	Added Functionality
5.3.4.1	Example has the wrong executionRule constant. NOTE: executionRule value "preceding" was misspelled in earlier Errata. Corrected Example body: { "instructedAmount": {"currency": "EUR", "amount": "123"}, "debtorAccount": {"iban": "DE40100100103307118608"}, "creditorName": "Merchant123",	

Section	Change	Rationale

	<pre>"creditorAccount": {"iban": "DE23100120020123456789"},
	"remittanceInformationUnstructured": "Ref Number Abonnement",
	"startDate": "2018-03-01",
	"executionRule": "preceeding",
	"frequency": "monthly",
	"dayOfExecution": "01"
	}</pre>	

5.3.4.2	executionRule description in the request body table is wrong. Note: executionRule value "preceding" was misspelled in earlier Versions of Errata. Corrected description: "following" or "preceeding" supported as values. This data attribute defines the behavior when recurring payment dates falls on a weekend or bank holiday. The payment is then executed either the "preceeding" or "following" working day. ASPSPs might reject the request due to the communicated value, if rules in Online-Banking are not supporting this execution rule.	

5.4.3.2	The related example needs to be corrected due to wrong executionRule constant. The correct second part of the multipart message is
	
	<pre>--AaaBbbCcc
	Content-Disposition: form-data;
	name="json_standingordermanagement"
	Content-Type: application/json
	{"startDate": "2018-03-01",
	"frequency": "monthly",
	"executionRule": "preceeding",
	"dayOfExecution": "01"
	}
	--AaaBbbCcc--</pre>
		Erratum

5.4.	Payment path was too short. Corrected path is <pre>GET /v1/{payment-service}/{payment-</pre>	Erratum

Section	Change	Rationale
	product}/{paymentId}/status The element payment-product is then also added in the following definition table.	
5.5	Payment path was too short. Corrected path is GET /v1/{payment-service}/{payment-product}/{paymentId} The element payment-product is then also added in the following definition table.	Erratum
5.6	The HTTP code for a successful DELETE of a payment initiation, where no further authentication is needed was changed from 200 to 204.	Erratum
5.6	The TPP headers TPP-Redirect-Preferred, TPP-Redirect-URI, TPP-Nok-Redirect-URI and TPP-Explicit-Authorisation-Preferred have been added to the Payment Cancellation Request, with the same conditions and descriptions like for the Payment Initiation Request.	Erratum
5.6	The definition of the response body is preceded by the following explanation: "In case of HTTP code 204, no response body is used. In case of HTTP code 202, the following body is used:"	Erratum
5.6	In the definition of the response body, the reference to the authorisation endpoint in the entry for "startAuthorisationWithPsuAuthentication" is changed to "cancellation-authorisation" endpoint.	Erratum
5.6	In the same response body definition table, an additional hyperlink was added: "startAuthorisationWithAuthentication MethodSelection": The link to the authorisation end-point, where the cancellation-authorisation sub-resource has to be generated while selecting the authentication method. This link is contained under exactly the same conditions as the data element "scaMethods"	Erratum

Section	Change	Rationale

5.6	In the example for the successful deletion without further authentication, the HTTP code has been adapted and the response body has been deleted (no response body):
	
	Response
	
	`HTTP/1.x 204`
	
	`X-Request-ID: 99391c7e-ad88-49ec-a2ad-99ddcb1f7769`
	`Date: Sun, 13 Aug 2017 17:05:38 GMT`
		Erratum

5.7	Payment path was too short. Corrected path is `GET /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations` The element payment-product is then also added in the following definition table.	Erratum
6.3	A clarifying sentence needs to be added: **Multicurrency Accounts in Reading Balances** The consequence for this function is that an array of balances of all sub-accounts are returned, if a multicurrency account is addressed on aggregation level. The currency of the respective sub-account is implicitly provided as the currency of the balanceAmount element within the balance.	Clarification
6.4.1.1	In the paragraph about side effects, a reference to corporate identification needs to be added as well as a clarification on the fact that one off consents have no side effects. **Side Effects** When this Consent Request is a request where the "recurringIndicator" equals true, and if it exists already a former consent for recurring access on account information for the addressed PSU and potentially addressed corporate identification submitted by this TPP, then the former consent automatically expires as soon as the new consent request is authorised by the PSU. There are no expiration side effects foreseen for Consent Requests	Clarification

Section	Change	Rationale
	where the "recurringIndicator" equals false.	
6.4.1.1	For both headers TPP-Redirect-URI and TPP-Nok-Redirect-URI, a note was added that the requirements of the new section 4.8 apply (see below).	Security Requirement
6.4.1.1	In the validUntil parameter in the body of the Establish Account Information Request, the description is changed to the following, to allow future dates, and future dates adaptions: "This parameter is requesting a valid until date for the requested consent. The content is the local ASPSP date in ISODate Format, e.g. 2017-10-30. Future dates might get adjusted by ASPSP. If a maximal available date is requested, a date in far future is to be used: "9999-12-31". In both cases, the consent object to be retrieved by the GET Consent Request will contain the adjusted date."	Erratum
6.4.1.1	In the description of the frequencyPerDay parameter was extended ~~t~~ to clarify that the frequency is addressing only the Read Account Data Requests without PSU involvement:~~.o~~ "This field indicates the requested maximum frequency for an access without PSU involvement per day. For a one-off access, this attribute is set to "1"." The frequency needs to be greater equal to one. If not otherwise agreed bilaterally between TPP and ASPSP, the frequency is less equal to 4. **Remark for Future**: Additional conditions might be added later to deal with the situation where the PSU is consenting towards the TPP for account access only where the PSU is actively asking.	Clarficiation
6.6.1, 6.6.2, 6.6.3, 6.6.4	For all GET Account Data Requests, the PSU-IP-Address has been added to the request header definitions with the Condition "Conditional" and the following description to identify PSU involvement:	Erratum

Section	Change	Rationale
	"The forwarded IP Address header field consists of the corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."	
6.6.1	In Example 1, Example 2 and Example the value of the cashAccountType is corrected in several occurrences: "cashAccountType": "CACC" ,	Erratum
6.6.2	In the example, the value of the cashAccountType is corrected in several occurrences: "cashAccountType": "CACC" ,	Erratum
6.6.4	In the description of the query parameter dateFrom and dateTo, the following paragraph has been added to clarify the impact of this parameter: "For booked transactions, the relevant date is the booking date. For pending transactions, the relevant date is the entry date, which may not be transparent neither in this API nor other channels of the ASPSP."	Clarification
6.6.4	The following note related to compressing response data is added: "**Note:** The ASPSP might use standard compression methods on application level for the response message as indicated in the content encoding header."	Clarification
6.6.4	In the description of the field transactions, the following sentence has been added: "This account report contains transactions resulting from the query parameters."	Clarification
6.6.4	In the JSON based response, the type of the attribute "balances" has been corrected to "Array of Balance".	Erratum
6.7.1, 6.7.2, 6.7.3, 6.7.4	For all GET Card Account Data Requests, the PSU-IP-Address has been added to the request header definitions with the Condition "Conditional" and the following description to identify PSU involvement: "The forwarded IP Address header field consists of the	Erratum

Section	Change	Rationale
	corresponding HTTP request IP Address field between PSU and TPP. It shall be contained if and only if this request was actively initiated by the PSU."	
6.7.1, 6.7.2, 6.7.3, 6.7.4	In all examples of these sections, some amount entries are without hyphenation. This is changed to amounts with hyphenation.	Erratum
6.7.1	There is a balanceType "nonBilled" in the example. This is corrected to "nonInvoiced".	Erratum
6.7.2	There is a balanceType "nonBilled" in the example. This is corrected to "nonInvoiced".	Erratum
6.7.3	There is a balanceType "nonBilled" in the example. This is corrected to "nonInvoiced".	Erratum
6.7.3	An attribute tag has been corrected from account to cardAccount in the response body of the Read Card Account Balance Request.	Erratum

6.7.4	An attribute tag has been corrected from transaction to cardTransaction with the corresponding Card Account Type in the response body of the Read Card Account Transaction List Request.
	
	The in the following example, the corresponding line was corrected to
	
	`"cardTransactions": {`
	`"booked": [`
	`{`
		Erratum

6.7.4	The type of the attribute "balances" has been corrected to "Array of Balance".	Erratum
6.7.4	The following note related to compressing response data is added: "**Note:** The ASPSP might use standard compression methods on application level for the response message as indicated in the content encoding header."	Clarification
7.1	The TPP headers TPP-Redirect-Preferred, TPP-Redirect-URI and the TPP-Nok-Redirect-URI have been added to the Payment	Erratum

Section	Change	Rationale
	Cancellation Request, with the same conditions and descriptions like for the Payment Initiation Request. For both headers TPP-Redirect-URI and TPP-Nok-Redirect-URI, a note was added that the requirements of the new section 4.8 apply (see below).	

7.2.1	The payment-product was not correctly set in the Path. It is now corrected to
	
	`PUT /v1/{payment-service}/{payment-product}/{paymentId}/authorisations/{authorisationId}`
	
	`And`
	
	`PUT /v1/{payment-service}/{payment-product}/{paymentId}/cancellation-authorisations/{cancelltation~~authorisationId~~}`
		Erratum

7.4	The attribute authorisationId was deleted from the table of path parameters, since not applicable here.	Erratum
7.5	The condition on the attribute scaStatus in the response message is changed to mandatory.	Erratum
8.1	The condition to both attributes paymentIds and consentIds is set to optional. In the description of both attributes it is added that the arrays may **not** be empty.	Erratum
8.1	For both headers TPP-Redirect-URI and TPP-Nok-Redirect-URI, a note was added that the requirements of the new section 4.8 apply (see below).	Security Requirement
8.2	The following sentence was added in the description of the transactionStatus field: For a list of all transactionStatus codes permitted for signing baskets, cp. Section 8.3.	Clarification
8.3	The following sentence was added in the description of the transactionStatus field: For a list of all transactionStatus codes permitted for signing baskets, cp. Section 8.3.	Clarification
8.3	A new section about the message GET Signing Basket Status Request was added.	Erratum
8.3	It was explicitly added that only the values RCVD, ACTC, PATC, CANC or RJCT are supported as codes for transactionStatus for	Clarification

Section	Change	Rationale
	signing baskets.	
9	The following paragraph has been added: " The usage of the "Consent-ID" in the subsequent Payment Initiation Request will then yield to not again ask for a first authentication factor, so the ASPSP will not again provide the PSU authentication link. In a case of SCA exemption for the corresponding payment, this can yield to a situation where no further PSU authentication is needed – the payment will then be executed without further confirmation."	Clarification
10.1	In the data overview table, the condition of the cardNumber was set to "o" for optional.	Erratum
10.1	A new row was established to support the Consent-ID in the overview.	Extension
10.2.	The conditional field Consent-ID of Type string was added to the HTTP headers with the following description: "Shall be provided if the consent of the PSU has been provided through the consent process as defined in [XS2A-COFC]. Otherwise not used."	Extension
10.2	The last paragraph after the explanation following the response body definition is changed to: "If the card number is not registered for any of the sub-accounts, or if the card number is registered for a different sub-account the card number might be ignored." This enables the ASPSP to also reject this message if a not matching card number is used.	Erratum
10.2	The field Authorization was added as optional field with the description: "This field might be used in case where a consent was agreed between ASPSP and PSU through an OAuth2 based protocol, facilitated by the TPP."	Erratum
11.1	The field exchangeRateInformation of type "Payment Exchange Rate" was added to the data elements for single payments. All	Erratum

Section	Change	Rationale
	entries in the table are "n.a."	
11.1	The condition on the fields creditorAgent and~~,~~ creditorAddress~~,~~ has been changed to "conditional" with a footnote "This field might be mandated by ASPSPs generally or depending of the creditor's address' country."	Erratum
11.1	The condition on the fields chargeBearer has been changed to "conditional" with a footnote "This field might be mandated by ASPSPs if no default setting for chargeBearer is provided."	Erratum
11.1	The field creditorNameAndAddress ot type Max140Text was added to the data elements for single payments. All entries in the table are "n.a."	Erratum
11.3	For JSON based bulk payments, an attribute paymentInformationId has been added on bulk level. This attribute has the condition "n.a." indicating that ASPSPs or ASPSP communities need to open up the use of this field explicitly. The condition of this field in this case is optional. **Remark for Future:** This field might be mandated in a next version of the specification.	Erratum
12	For signatures, normalisation of headers have been made explicit (short letters for signed headers). Date has been taken out of the headers to be signed. This has detailed impact on some places in the signature chapter. So, the whole chapter is displayed below with all errata recognised.	Erratum
12	The following remark was added: **Remark:** In case of a multipart message the same method is used to calculate the digest. I.e. a hash of the (whole) message body is calculated including all parts of the multipart message as well as the separators.	Clarification.
13.3	In the description of the grant type attribute in the request, the reference to authorisation Code was corrected to authorization code.	Erratum
14.6	The link "startAuthorisationWithAuthenticationMethodSelection" was added with the description "This is a link to and endpoint where the authorisation of a	Erratum

Section	Change	Rationale
	transaction or of a transaction cancellation shall be started, where the selected SCA method shall be uploaded with the corresponding call."	
14.6	A double entry of the link startAuthorisationWithTransactionAuthorisaction has been deleted.	Erratum
14.6	The link "cardAccount" has been added with description "A link to the resource providing the details of one card account." The link "cardTransactions" has been added with description "A link to the resource providing the transaction history of a dedicated card account."	Erratum
14.11.1	The following paragraph has been added for FORMAT_ERROR in the description: "This applies to headers and body entries. It also applies in cases where these entries are referring to erroneous or not existing data instances, e.g. a malformed IBAN."	Erratum
14.11.1	The following paragraph has been added for PARAMETER_NOT_CONSISTENT in the description: "This applies only for query parameters."	Erratum
14.11.2	The following entry has been added: Code "CANCELLATION_INVALID" http Code: 405 Description: "The addressed payment is not cancellable e.g. due to cut off time passed or legal constraints."	Erratum
14.11.3	The following paragraph has been replaced for ACCESS_EXCEEDED in the description: "The access on the account has been exceeding the consented multiplicity without PSU involvement per day." This is to clarify that this code is used only in case of account information access without PSU involvement.	Erratum
14.13	The code PART was added with the following description:	Erratum

Section	Change	Rationale
	"A number of transactions have been accepted, whereas another number of transactions have not yet achieved 'accepted' status. Remark: This code may be used only in case of bulk payments. It is only used in a situation where all mandated authorisations have been applied, but some payments have been rejected."	
14.18	The type of the attribute usage was changed from Max140Text to Max4Text	Erratum
14.19	The hyperlink types referred to in the description of the _links attribute in the type definition "Card Account Details" are changed from account to cardAccount and transactions to cardTransactions.	Erratum
14.20	The code interimBooked was added with the description: "Balance calculated in the course of the account servicer's business day, at the time specified, and subject to further changes during the business day. The interim balance is calculated on the basis of booked credit and debit items during the calculation time/period specified."	Erratum
14.22	The condition of the attribute booked was set to conditional with the description added: "Shall be contained if bookingStatus parameter is set to "booked" or "both"."	Erratum
14.22	The following description was added for the attribute pending: "Not contained if the bookingStatus parameter is set to "booked"."	Erratum
14.23	The optional attribute additionalInformation was added of type Max512Text with description: "Might be used by the ASPSP to transport additional transaction related information to the PSU."	Erratum
14.23	The attribute exchangeRate was changed to currencyExchange to achieve full ISO20022 compliance. The type was changed to the new type Array of Report Exchange Rate.	Erratum

Section	Change	Rationale
14.24	The following description has been added to the attribute booked: "Card transaction which have been booked already to the card account."	Erratum
14.24	The link account was changed to cardAccount in the attribute _links	Erratum
14.25	In the description of the markupFeePercentage the phrase "e.g. "0.3" for 0,3%." was added.	Erratum
14.25	The attribute exchangeRate was changed to currencyExchange to achieve full ISO20022 compliance. The type was changed to the new type Array of Report Exchange Rate.	Erratum
14.25	The attribute cardAcceptorCategoryCode was changed to merchantCategoryCode of type Merchant Category Code to achieve full ISO20022 compliance.	Erratum
14.26	The type Exchange Rate was changed to Report Exchange Rate with additional changes to attributes of the type definition, see below. The type of the attribute unitCurrency was changed to Currency Code.	Erratum
14.27	The new type Payment Exchange Rate was added. see below. The type of the attribute unitCurrency was changed to Currency Code.	Erratum
14.28	The separator in the Geo Location was corrected from "," to ";" following [RFC2426]. The " " signs for "GEO:" are used in the Implementation Guidelines only to indicate that GEO: is a constant string. The " " signs will be erased in the next version of the Implementation Guidelines.	Erratum

The following new sections need to be added/rewritten in the Implementation Guidelines

NEW Section: 4.8 Requirements on TPP URIs

The TPP can provide several URIs to the ASPSP as parameters for succeeding protocol steps. For security reasons, it shall be ensured that these URIs are secured by the TPP eIDAS QWAC used for identification of the TPP. The following applies:

URIs which are provided by TPPs in TPP-Redirect-URI or TPP-Nok-Redirect-URI shall comply with the domain secured by the eIDAS QWAC certificate of the TPP in the field CN or SubjectAltName of the certificate. Please note that in case of example-TPP.com as certificate entry TPP-Redirect-URI like

- www.example-TPP.com/xs2a-client/v1/ASPSPidentifcation/mytransaction-id or
- redirections.example-TPP.com/xs2a-client/v1/ASPSPidentifcation/mytransaction-id

would be compliant.

Wildcard definitions shall be taken into account for compliance checks by the ASPSP.

ASPSPs may reject requests, if the provided URIs do not comply.

Remark for Future: For migration reasons, this specification mandates the TPP to keep the TPP-Redirect-URI used within all authorisation processes for a specific transaction during the lifecycle of this transaction constant. This might be removed in the next version of the specification.

Remark for Future: The restrictions on URIs will also apply to TPP-URIs used within future Push Services of the ASPSP.

New Section: 8.3 Get Signing Basket Status Request

Call

```
GET /v1/signing-baskets/{basketId}/status
```

Returns the status of a signing basket object.

Path Parameters

Attribute	Type	Description
basketId	String	ID of the corresponding signing basket object.

Query Parameters

No specific query parameter.

Request Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.
Authorization	String	Conditional	Is contained only, if an OAuth2 based authentication was performed in a pre-step or an OAuth2 based SCA was performed in the current PIS transaction or in a preceding AIS service in the same session, if no such OAuth2 SCA approach was chosen in the current signing basket transaction.

Request Body

No request body.

Response Code

The HTTP response code equals 200.

Response Header

Attribute	Type	Condition	Description
X-Request-ID	UUID	Mandatory	ID of the request, unique to the call, as determined by the initiating party.

Response Body

Attribute	Type	Condition	Description
transactionStatus	Transaction Status	Mandatory	Only the codes RCVD, PATC, ACTC, CANC~~ACWC~~ and RJCT are ~~used~~supported for signing baskets.~~.~~

Example

Request

```
GET https://api.testbank.com/v1/signing-baskets/1234-basket-567/status
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date:                   Sun, 06 Aug 2017 15:05:49 GMT
```

Response

```
HTTP/1.x 200 Ok
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7721
Date:                   Sun, 06 Aug 2017 15:05:51 GMT
Content-Type:           application/json

{
"transactionStatus": "ACTC"
}
```

Rewritten Chapter 12 Signatures

When an ASPSP requires the TPP to send a digital signature as defined in [signHTTP], chapter 4 in his HTTP-Requests, the signature must obey the following requirements according or additional to [signHTTP], chapter 4.

12.1 "Digest" Header mandatory

When a TPP includes a signature as defined in [signHTTP], chapter 4, he also must include a "Digest" header as defined in [RFC3230]. The "Digest" Header contains a Hash of the message body, if the message does not contain a body, the "Digest" header must contain the hash of an empty bytelist. The only hash algorithms that may be used to calculate the Digest within the context of this specification are SHA-256 and SHA-512 as defined in RFC5843].

Remark: In case of a multipart message the same method is used to calculate the digest. I.e. a hash of the (whole) message body is calculated including all parts of the multipart message as well as the separators.

12.2 Requirements on the "Signature" Header

As defined in [signHTTP], chapter 4, a "Signature" header must be present. The structure of a "Signature" header is defined in [signHTTP], chapter 4.1, the following table lists the requirements on the "Signature" header from [signHTTP] and additional requirements specific to the PSD2-Interface.

Elements of the "Signature" Header				
Element	**Type**	**Condition**	**Requirement [signHTTP]**	**Additional Requirement**
keyId	String	Mandatory	The keyId field is a string that the server can use to look up the component they need to validate the signature.	Serial Number of the TPP's certificate included in the "TPP-Signature-Certificate" header of this request. It shall be formatted as follows: keyId="SN=XXX,CA=YYYYYYYYYYYYYYYYY" where “XXX" is the serial number of the certificate in hexadecimal coding given in the TPP-Signature-Certificate-Header and "YYYYYYYYYYYYYYYY" is the full Distinguished Name of the Certification Authority having produced this certificate.
Algorithm	String	Mandatory (Optional in [signHTTP])	The "Algorithm " parameter is used to specify the digital signature algorithm to use when generating the signature. Valid values for this parameter can be found in the Signature Algorithms registry located at http://www.iana.org/assignments/signature-algorithms and MUST NOT be marked "deprecated". It is preferred that the algorithm used by an implementation be derived from the key metadata identified by the 'keyId' rather than from this field. […]The 'algorithm' parameter [..] **will most likely be deprecated in the future**.	Mandatory The algorithm must identify the same algorithm for the signature as presented in the certificate (Element "TPP-Signature-Certificate") of this Request. It must identify SHA-256 or SHA-512 as Hash algorithm.

Elements of the "Signature" Header				
Element	**Type**	**Condition**	**Requirement [signHTTP]**	**Additional Requirement**
Headers	String	Mandatory (Optional in [signHTTP])	The "Headers" parameter is used to specify the list of HTTP headers included when generating the signature for the message. If specified, it should be a lowercased, quoted list of HTTP header fields, separated by a single space character. If not specified, implementations MUST operate as if the field were specified with a single value, the `Date` header, in the list of HTTP headers. Note that the list order is important, and MUST be specified in the order the HTTP header field-value pairs are concatenated together during signing.	Mandatory. Must include • "digest", • "x-request-id", Must conditionally include • "psu-id", if and only if "PSU-ID" is included as a header of the HTTP-Request. • "psu-corporate-id", if and only if "PSU-Corporate-ID" is included as a header of the HTTP-Request. • "tpp-redirect-uri", if and only if "TPP-Redirect-URI" is included as a header of the HTTP-Request. **No other entries may be included.** **Remark:** It is intended to introduce a new http header in a coming version. This new header shall indicate the creation date of a request on the side of the TPP. This new header and will also have to be included in this "Headers" element.

Elements of the "Signature" Header				
Element	**Type**	**Condition**	**Requirement [signHTTP]**	**Additional Requirement**
Signature	String	Mandatory	The "signature" parameter is a base 64 encoded digital signature, as described in RFC 4648 [RFC4648], Section 4. The client uses the `algorithm` and `headers` signature parameters to form a canonicalised `signing string`. This `signing string` is then signed with the key associated with `keyId` and the algorithm corresponding to `algorithm`. The `signature` parameter is then set to the base 64 encoding of the signature.	[No additional Requirements]

Example

Assume a TPP needs to include a signature in the following Request

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Type:           application/json
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address:         192.168.8.78
PSU-ID:                 PSU-1234
PSU-User-Agent:         Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
tpp-redirect-uri: https%3A%2F%2FshortURI_Cchallenge_Mmethod="S256"
Date:                   Sun, 06 Aug 2017 15:02:37 GMT

{
   "instructedAmount": {"currency": "EUR", "amount": "123"},
   "debtorAccount": {"iban": "DE23100100101234567 89"},
   "creditor": {"name": "Merchant123"},
   "creditorAccount": {"iban": "DE23100120020123456789"},
   "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

So the body would encode to the following String in Base64:

eyAgICANCiAgICJpbnN0cnVjdGVkQW1vdW50IjogeyJjdXJyZW5jeSI6ICJFVVIiLCAiYW1vdW50IjogIjEyMyJ9LA0KICAgImRlYnRvckFjY291bnQiOiB7ImliYW4iOiAiREUyMzEwMDEwMDEwMTIzNDU2Nzg5In0sDQogICAiY3JlZGl0b3IiOiB7Im5hbWUiOiAiTWVyY2hhbnQxMjMifSwNCiAgICJcmVkaXRvckFjY291bnQiOiB7ImliYW4iOiAiREUyMzEwMDEyMDAyMDEyMzQ1Njc4OSJ9LA0KICAgInJlbWl0dGFuY2VJbmZvcm1hdGlvblVuc3RydWN0dXJlZCI6ICJSZWYgTnVtYmVyIE1lcmNoYW50Ig0KfQ==

and SHA-256 of the request body is

F9li3V7yu8S/QKVOhWiiiqJBhGMVId8UGZ4sBRVPkok=in Base64 ('17D962DD5EF2BBC4BF40A54E8568A28AA24184631521DF14199E2C05154F9289' in hexadecimal representation).

So using signature algorithm rsa-sha256 the signed request of the TPP will be

```
POST https://api.testbank.com/v1/payments/sepa-credit-transfers
Content-Type:           application/json
X-Request-ID:           99391c7e-ad88-49ec-a2ad-99ddcb1f7721
PSU-IP-Address:         192.168.8.78
PSU-ID:                 PSU-1234
PSU-User-Agent:          Mozilla/5.0 (Windows NT 10.0; WOW64; rv:54.0)
Gecko/20100101 Firefox/54.0
tpp-redirect-uri: https%3A%2F%2FshortURI_Cchallenge_Mmethod="S256"
Date:                   Sun, 06 Aug 2017 15:02:37 GMT
Digest:                 SHA-
256=ZuYiOtZkVxhjWmwTO5lOpsPevUNMezvk6dfb6fVhebM=
Signature:              keyId="SN=9FA1,CA=CN=D-TRUST%20CA%202-1%202015,O=D-
Trust%20GmbH,C=DE",algorithm="rsa-sha256",
   headers="digest x-request-id psu-id tpp-redirect-uri",
   signature="Base64(RSA-SHA256(signing string))"
TPP-Signature-Certificate: TPP's_eIDAS_Certificate

{
   "instructedAmount": {"currency": "EUR", "amount": "123"},
   "debtorAccount": { "iban": "DE23100100101234567 89"},
   "creditor": { "name": "Merchant123"},
   "creditorAccount": {"iban": "DE23100120020123456789"},
   "remittanceInformationUnstructured": "Ref Number Merchant"
}
```

Where *signing string* is

```
digest: SHA-256=ZuYiOtZkVxhjWmwTO5lOpsPevUNMezvk6dfb6fVhebM=
x-request-id: 99391c7e-ad88-49ec-a2ad-99ddcb1f7721
psu-id: PSU-1234
tpp-redirect-uri: https%3A%2F%2FshortURI_Cchallenge_Mmethod="S256"
```

NOTE: The header fields to be signed are denoted in small letters to clarify that the digest will use small letters for normalisation.

New Subsections in Chapter 14 Complex Data Types

14.26 Report Exchange Rate

Attribute	Type	Condition	Description
sourceCurrency	Currency Code	Mandatory	Currency from which an amount is to be converted in a currency conversion.
exchangeRate	String	Mandatory	Factor used to convert an amount from one currency into another. This reflects the price at which one currency was bought with another currency.
unitCurrency	Currency Code	Mandatory	Currency in which the rate of exchange is expressed in a currency exchange. In the example 1EUR = xxxCUR, the unit currency is EUR.
targetCurrency	Currency Code	Mandatory	Currency into which an amount is to be converted in a currency conversion.
quotationDate	ISODate	Mandatory	Date at which an exchange rate is quoted.
contractIdentification	String	Optional	Unique identification to unambiguously identify the foreign exchange contract.

14.27 Payment Exchange Rate

Attribute	Type	Condition	Description
unitCurrency	Currency Code	Optional	Currency in which the rate of exchange is expressed in a currency exchange. In the example 1EUR = xxxCUR, the unit currency is EUR.
exchangeRate	String	Optional	Factor used to convert an amount from one currency into another. This reflects the price at which one currency was

Attribute	Type	Condition	Description
			bought with another currency.
contractIdentification	String	Optional	Unique identification to unambiguously identify the foreign exchange contract.
rateType	String	Optional	Specifies the type used to complete the currency exchange. Only SPOT, SALE and AGRD is allowed.