EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook –

Annex D2

Back-end implementation specifications #5

Dispute management

IMPORTANT NOTICE:

This rulebook is an interim draft of the digital euro rulebook developed by RDG

A separate set of pilot documentation has been developed that can be found here.

Although the pilot documentation is based on the draft rulebook, the draft rulebook should not be used for pilot or implementation purposes.

Rulebook version:	0.91
Status:	DRAFT
Date:	02/07/2025

DISCLAIMERS FOR DRAFT RULEBOOK v0.91

Preliminary and non-binding nature of version 0.91

This document represents a preliminary draft version (version 0.91) of the digital euro scheme rulebook and reflects the ECB's continuous effort to develop a draft rulebook in close cooperation with the Rulebook Development Group (RDG)[1], comprising senior representatives from European associations representing both the supply and demand side of the retail payments market. Version 0.91 is non-binding and does not necessarily reflect the final views of the ECB, the Eurosystem, the RDG, or any of its members or their constituencies.

No reliance for implementation

Due to its preliminary nature, the draft rulebook version 0.91 is not intended for use as a basis for implementing any systems, processes, or policies related to the digital euro or to the beta digital euro in a Digital Euro Pilot context. Any such actions, prior to the publication of the officially approved rulebook, are under actors' own responsibility.

[1] For more information on the RDG, refer to:
https://www.ecb.europa.eu/euro/digital_euro/timeline/rulebook/html/index.en.html

PREAMBLE

The draft digital euro scheme rulebook is being developed by the Eurosystem together with the support from the digital euro scheme rulebook development group (RDG). The current draft rulebook (v0.91) has been further developed compared to the last version 0.9 of the draft rulebook, which was commented by the RDG and its constituencies. The current draft has been advanced in both structure and content based on the RDG comments received, further elaborations and discussions, and benefited from the various RDG workstreams.

The current version of the rulebook is based on the European Commission's 2023 proposal for a regulation on the establishment of the digital euro (2023/0212/COD) and the Regulation on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro (2023/0211/COD). Given both proposals are currently progressing through the legislative process, and subject to amendments from the EU co-legislators, the rulebook will require updates once both regulations have been finalised for adoption. Additionally, other areas of the rulebook will be further developed in line with ongoing elaborations on subject matters and decisions by the Governing Council of the ECB or are dependent on the work of service providers.

As a result, all along this draft rulebook, text highlighted in yellow refers to placeholders to be updated at later stage when associated decisions or developments are made. It is worth noting that the draft rulebook assumes a single-account set-up for individual digital euro end-users, which deviates from the possibility of having multiple digital euro payment accounts as implied by the European Commission's 2023 proposal for a regulation on the establishment of the digital euro.

The Eurosystem is also cognisant that political agreement has been achieved on the Payment Services Regulation (PSR) and the Third Payment Services Directive (PSD3). The agreed measures must be formally adopted by the European Parliament and the Council of the European Union before they enter into force. The rulebook will be updated accordingly.

The purpose of the current draft is to update the RDG and its constituencies on the progress made following the market consultation, coordinated by the RDG and concluded on 31 October 2025, and to serve as a basis for the further development of the draft rulebook. This document represents a preliminary draft version which has not yet been subject to a general language and editorial review.

Table of Contents

1.	**Dispute management service**	**5**
1.1.	Service description	5
1.2.	Distributing requirements	5
1.2.1.	*Function description*	*5*
1.2.2.	*Interface description*	*7*
1.3.	Acquiring PSP requirements	38

1. Dispute management service

1.1. Service description

The dispute management process aims at ensuring that digital euro PSPs have the required service to support them in managing disputes.

The dispute management process is divided into two phases: the pre-dispute and the dispute resolution.

Pre-dispute phase

The **pre-dispute phase** facilitates the payer and payee to clarify via their PSPs the underlying case between them. This situation can be triggered for example when the payer does not recognise the transaction due to missing transaction details or there is a duplicate transaction. Provision of additional information from payee to payer via their PSPs might help to resolve and close the case.

Dispute phase

The **dispute phase** is triggered after an unsuccessful pre-dispute phase. The payer – via a PSP – initiates the dispute process for the cases where the payee did not provide any answer or where the resolution proposal was not considered sufficient from the payer's perspective.

Arbitration

If the payer does not accept the outcome of the dispute phase, the payer can take the case to arbitration. Arbitration is outside of Eurosystem domain and DESP is not involved in the arbitration process. Upon completion of the arbitration, the payer's PSP shall send a notification on the arbitration result to the DESP.

1.2. Distributing requirements

1.2.1. Function description

Pre-dispute phase steps:

1. **Submit pre-dispute request to DESP**

Payer can submit pre-dispute request to the merchant via their respective PSPs through DESP.

2. **Receive pre-dispute request from DESP**

Payee PSP receives pre-dispute requests from the payer's PSP addressed to its merchant at which the payer made a purchase of goods or services and now has a claim to.

3. **Respond to pre-dispute request to DESP**

Payee PSP has to pass the pre-dispute request to the relevant merchant and collect its feedback in order to be able to respond to the pre-dispute. Merchant has to either:

- Accept the pre-dispute request, i.e. agree with the payer claim and apply the appropriate remediation measures – if necessary with the involvement of its PSP; or
- Provide evidence in its own defence. Once the necessary inputs are collected, the payee PSP submits the response to DESP that then validates it and passes the response to the payer PSP.

Once the data is collected, payee PSP sends the response to DESP.

4. **Receive the pre-dispute response from DESP**

Payer receives the pre-dispute response from the merchant via their respective PSPs through DESP.

5. **Send notification on pre-dispute response acceptance or rejection (i.e. status update) to DESP**

Payer can accept or reject the merchant's pre-dispute response. Payer PSP shall send the status update to DESP, that then passes the information to the payee PSP.

6. **Receive notification on pre-dispute response acceptance or rejection (i.e. status update) from DESP**

Payee PSP will receive the response from the payer PSP through DESP. Payer can accept the pre-dispute response or reject it. In both cases the payee PSP has to be notified via DESP.

7. **Send pre-dispute closure notification to DESP (status update)**

Upon successful pre-dispute resolution (pre-dispute positive) payer PSP sends the pre-dispute closure notification to DESP that then DESP forwards to the payee PSP. Payer can at any point decide to close the pre-dispute request. Payer PSP will have to send a pre-dispute closure notification if instructed by the payer.

8. **Receive pre-dispute closure notification from DESP**

Payee PSP is notified on the pre-dispute closure via DESP.

Dispute phase:

1. **Submit dispute request to DESP**

Payer PSP shall submit the dispute request to DESP in case the pre-dispute outcome is negative. Payer PSP can change the dispute reason code at this stage, if deemed necessary.

2. **Receive dispute request from DESP**

Payee PSP shall receive dispute requests from the payer's PSP addressed to its merchant at which the payer previously made a purchase of goods or services and now has a claim to.

3. Respond to dispute request to DESP

Payee PSP collects evidence to be able to respond to the dispute. Once the necessary inputs are collected, the payee PSP submits the response to DESP that then validates it and passes the response to the payer PSP.

4. Receive the dispute response from DESP

Payer PSP receives the dispute response from payee PSP.

5. Send notification on dispute response acceptance or rejection (i.e. status update) to DESP

Payer PSP can accept or reject the payee PSP's dispute response. Payer PSP shall send the status update to DESP, that then passes the information to the payee PSP.

6. Receive notification on dispute response acceptance or rejection (i.e. status update) from DESP

Payee PSP received the notification on the dispute outcome.

7. Send dispute closure notification to DESP (status update)

Upon successful dispute resolution payer PSP sends the dispute closure notification to DESP that then DESP forwards to the payee PSP. Payer can at any point decide to close the dispute request. Payer PSP will have to send a dispute closure notification if instructed by the payer.

8. Receive dispute closure notification from DESP

Payee PSP is notified on the dispute closure via DESP.

9. Send arbitration positive or negative outcome to DESP (status update)

In the case that the payer's PSP does not accept the response (i.e., negative dispute), it has the option of taking the dispute to arbitration. Upon completion of the arbitration, the payer's PSP shall send a notification of arbitration result to the DESP.

1.2.2. Interface description

This section provides a detailed description of the interface designed to facilimate communication between PSPs and the DESP for the dispute management service. The interface is based on RESTful API principles and the data format utilised is JSON (JavaScript Object Notation).

1.2.2.1. Overview of covered scenarios

1.2.2.1.1. Pre-dispute phase

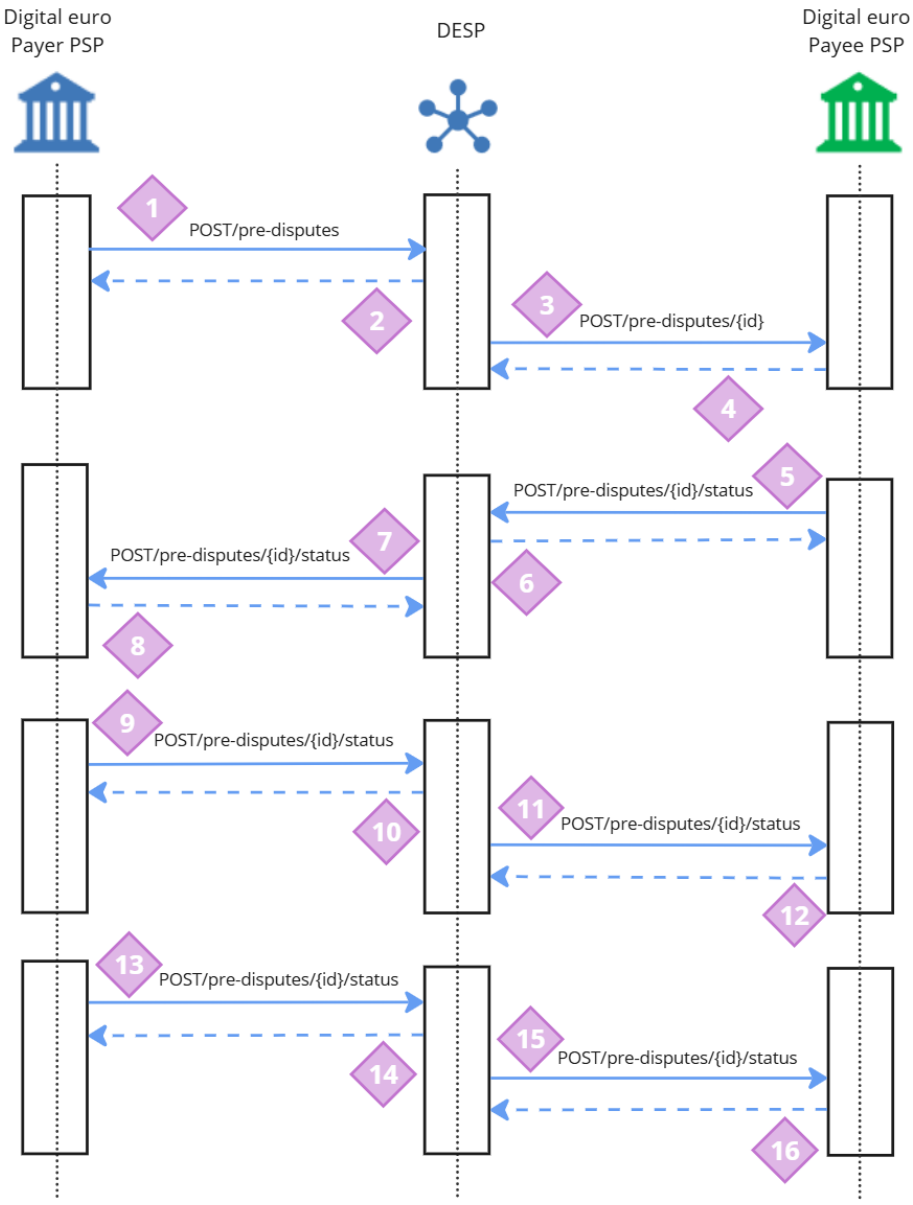

Figure 1 Pre-dispute phase flow

API call	Description	Covered in section

1	Digital euro payer PSP submits pre-dispute request to DESP.	POST/pre-disputes – Request
2	DESP validates the request and sends a validation response including a case ID (if the request is valid).	POST/pre-disputes – Response
3	Digital euro payee PSP receives pre-dispute request from digital euro payer PSP via DESP.	POST/pre-disputes/{id} – Request
4	Digital euro payee PSP confirms the receipt of the request.	POST/pre-disputes/{id} – Response
5	Digital euro payee PSP responds to pre-dispute request.	POST/pre-disputes/{id}/status – Request
6	DESP validates and confirms the pre-dispute request response from digital euro payee PSP.	POST/pre-disputes/{id}/status – Response
7	Digital euro payer PSP receives the pre-dispute response from digital euro payee PSP via DESP.	POST/pre-disputes/{id}/status – Request
8	Digital euro payer PSP confirms the receipt of the pre-dispute response.	POST/pre-disputes/{id} – Response
9	Digital euro payer PSP sends notification on pre-dispute response acceptance or rejection (i.e. status update).	POST/pre-disputes/{id}/status – Request
10	DESP confirms receipt and validates notification on pre-dispute response acceptance or rejection (i.e. status update).	POST/pre-disputes/{id}/status – Response
11	Digital euro payee PSP receives notification on pre-dispute response acceptance or rejection (i.e. status update) from digital euro payer PSP via DESP.	POST/pre-disputes/{id}/status – Request
12	Digital euro payee PSP confirms the receipt of the notification.	POST/pre-disputes/{id}/status – Response
13	Digital euro payer PSP sends pre-dispute closure notification (status update).	POST/pre-disputes/{id}/status – Request
14	Digital euro payer PSP confirms the receipt of the notification.	POST/pre-disputes/{id}/status – Response
15	Digital euro payee PSP receives pre-dispute closure notification from digital euro payer PSP via DESP.	POST/pre-disputes/{id}/status – Request

16	Digital euro payee PSP confirms the receipt of the notification.	POST/pre-disputes/{id}/status – Response

1.2.2.1.2. Dispute phase

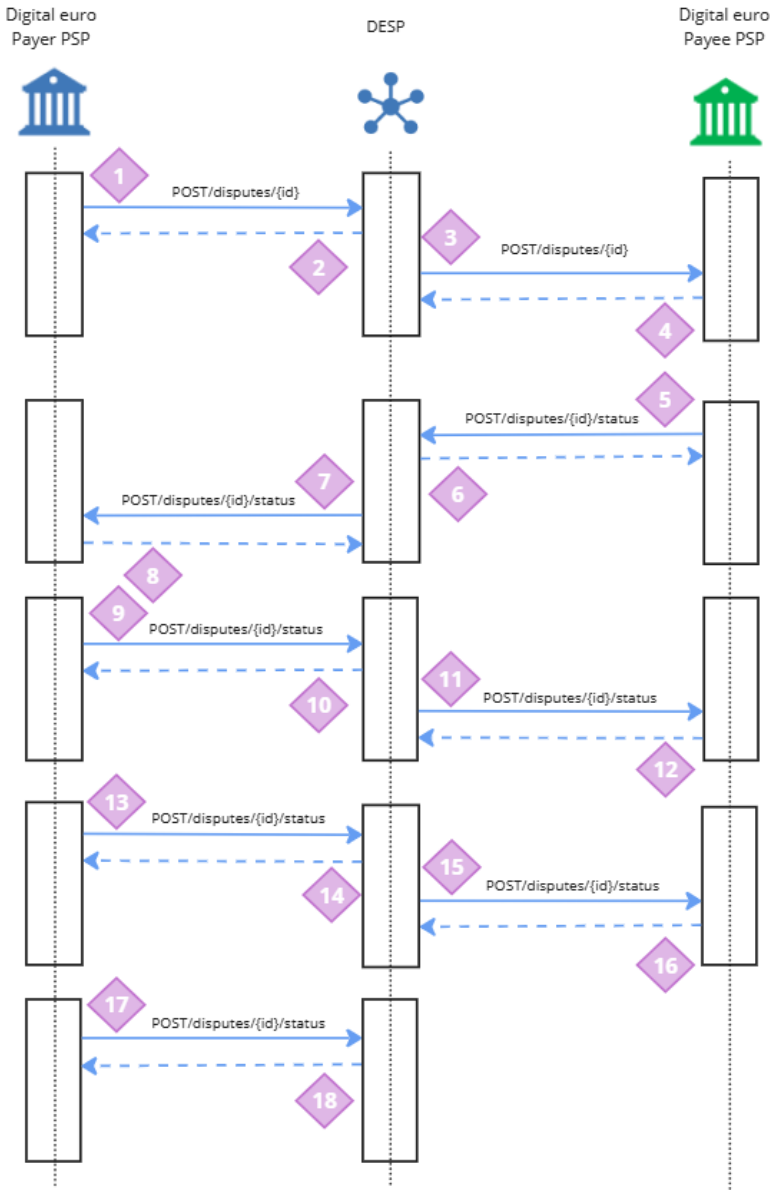

Figure 2 Dispute phase flow

API call	Description	Covered in section
1	Digital euro payer PSP submits dispute request to DESP, including the case ID.	POST/pre-disputes/{id} – Request
2	DESP validates the request. Valid request is forwarded to digital euro payee PSP. If request is not valid, DESP responds to digital euro payer PSP with an appropriate message	POST/disputes/{id} – Response
3	Digital euro payee PSP receives dispute request from digital euro payer PSP via DESP.	POST/disputes/{id} – Request
4	Digital euro payee PSP confirms the receipt of the request.	POST/disputes/{id} – Response
5	Digital euro payee PSP responds to dispute request.	POST/disputes/{id}/status – Request
6	DESP validates and confirms the dispute request response from digital euro payee PSP.	POST/disputes/{id}/status – Response
7	Digital euro payer PSP receives the dispute response from digital euro payee PSP via DESP.	POST/disputes/{id}/status – Request
8	Digital euro payer PSP confirms the receipt of the dispute response.	POST/disputes/{id}/status – Response
9	Digital euro payer PSP sends notification on dispute response acceptance or rejection (i.e. status update).	POST/disputes/{id}/status – Request
10	DESP confirms receipt and validates notification on dispute response acceptance or rejection (i.e. status update).	POST/disputes/{id}/status – Response
11	Digital euro payee PSP receives notification on dispute response acceptance or rejection (i.e. status update) from digital euro payer PSP via DESP.	POST/disputes/{id}/status – Request
12	Digital euro payee PSP confirms the receipt of the notification.	POST/disputes/{id}/status – Response
13	Digital euro payer PSP sends dispute closure notification (status update).	POST/disputes/{id}/status – Request

14	Digital euro payee PSP confirms the receipt of the notification.	POST/disputes/{id}/status – Response
15	Digital euro payee PSP receives dispute closure notification from digital euro payer PSP via DESP.	POST/disputes/{id}/status – Request
16	Digital euro payee PSP confirms the receipt of the notification	POST/disputes/{id}/status – Response
17	Digital euro payer PSP sends arbitration positive or negative outcome to DESP (status update).	POST/disputes/{id}/status – Request
18	DESP confirms receipt of the notification.	POST/disputes/{id}/status – Response

1.2.2.2. Overview of API endpoints

DESP API endpoints: For payer PSPs to submit requests to to DESP.

API nr	Description	Sending party	Exposing party	Covered in section
1	Submit pre-dispute request to DESP.	Payer PSP	DESP	POST/pre-disputes
2	Send notification on pre-dispute response acceptance or rejection or pre-dispute closure (i.e. status update) to DESP.	Payer PSP	DESP	POST/pre-disputes/{id}/status
3	Submit dispute request to DESP.	Payer PSP	DESP	POST/disputes/{id}
4	Send notification on dispute response acceptance or rejection, closure or arbitration positive or negative outcome (i.e. status update) to DESP.	Payer PSP	DESP	POST/disputes/{id}/status

PSP API endpoints: For PSPs to receive requests from DESP

API nr	Description	Sending party	Exposing party	Covered in section
5	Receive the pre-dispute request from DESP.	DESP	Payee PSP	POST/pre-disputes/{id}
6	Receive the pre-dispute response from DESP.	DESP	Payee PSP	POST/pre-disputes/{id}/status
7	Receive the dispute request from DESP.	DESP	Payee PSP	POST/disputes/{id}
8	Receive the dispute response from DESP.	DESP	Payee PSP	POST/disputes/{id}/status

1.2.2.3. DESP API for PSPs to send requests to DESP

1.2.2.3.1. POST/pre-disputes

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/pre-disputes	PRE-DISPUTE	PSP submits the pre-dispute request

1.2.2.3.1.1. POST/pre-disputes – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** no applicable.

Request body unencrypted data[2] elements

[2] Unencrypted data elements contain the minimum set of data for DESP to be able to perform the necessary validations. Involved PSPs exchange a larger set of data that is only readable for them and is therefore in the encrypted data elements tables.

Data element	Element description	Type	Length	Presence indicator
Payment ID	Resource ID for the disputed payment transaction.	STR	TBA	M
UETR	Unique end-to-end transaction reference of the disputed payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Payee PSP ID	BIC of the payee PSP holding the payee's digital euro payment account.	STR	11	M
Transaction settlement date and time	Date and time of the disputed transaction.	ISODateTime	10	M
Total transaction amount	Total amount of the disputed transaction, with 2 decimal positions.	STR	14.3	M
Disputed amount	Amount the payer disputes, with 2 decimal positions.	STR	14.3	M, cannot be higher than the original amount
Transaction Currency	The currency in which the amount is expressed. ISO 4217 three-letter code.	STR	3	M
Pre-dispute reason code	Reason code set by payer PSP. See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted[3] data elements

[3] Involved PSPs exchange a larger set of data that is only readable for them and is therefore in the encrypted data elements tables.

Data element	Element description	Type	Length	Presence indicator
Payer DEAN	Unique identification of the individual user's (payer's) digital euro payment account.	STR	18	C, either payer DEAN and name or token needs to be provided
Payer name	Name of the payer.	STR	70	C, either payer DEAN and name or token needs to be provided
Payer token	NFC token	STR	TBA	C, either payer DEAN and name or NFC token needs to be provided
Payee name	Name of the payee.	STR	70	C, mandatory in case of C2B payments, registered company name of the business user payee.
Payee trade name	Name of the business user payee as it is presented to customers.	STR	25	C, mandatory in case of C2B payments.
Payee DEAN	Unique identification of the payer's digital euro payment account.	STR	18	M
Payee location (town)	Town of the business user payee.	STR	*13*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the

				payee's central registered address.
Payee location (ZIP-Code)	ZIP-code of the business user payee.	NUM	10	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (country)	Country of the business user payee.	STR	*2*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (address)	Address (street name and building number) of the business user payee.	STR	30	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Transaction type	e.g. Purchase, Reservation, Purchase with cashback, cash withdrawal.	STR	*4*	M
Transaction environment	Placeholder – to be specified.	ANS	8	M

Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document	STR	36	C, mandatory in case there is an attachment
The data below is only used for recurring transactions				
Recurring payment frequency	The field specifies the frequency of a recurring payment. Please refer to Annex D 1 Acquiring PSP requirements, section 8.3.1.1.2.1 Incoming message table for the possible values.	SSET	4	M
Confirmation indicator	The field specifies if each recurring payment required authentication and confirmation by the payer.	BOOL	NA	M
End date	The field specifies the date at which the authorisation for the series of recurring payment ends.	ISODateTime	26	M
Recurring payments agreement ID	Agreement ID of the recurring payments.	STR	tbd	M
The data below is only used for reservation transactions				
Reservation ID	Resource ID for the reservation transaction.	STR	tbd	M
Reservation expiry date and time	Specifies the date and time at which the reservation ends and any still reserved amount will be released.	ISODateTime	11	O

1.2.2.3.1.2. POST/pre-disputes – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 201.

Data element	Element description	Type	Length	Presence indicator
Pre-dispute status	See Rulebook section 6.	SSET	11	M
Reason	Pre-dispute message is rejected by DESP if: - Disputed transaction processing date is beyond the allowed timelines - Disputed amount is higher than the original transaction amount - A process is already ongoing for the disputed transaction - Other, technical reason	STR	TBA	C, filled in if the request status is not valid, i.e. rejected by DESP, otherwise empty
Pre-dispute ID	ID of the pre-dispute case.	STR	TBA	C, filled if the request is valid

1.2.2.3.2. POST/pre-disputes/{id}/status

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/pre-disputes/{id}/status	PREDISPUTE	PSP sends pre-dispute status update.

1.2.2.3.2.1. POST/pre-disputes/{id}/status – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Pre-dispute ID	Unique reference identifying the pre-dispute case.	STR	TBA	M

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Pre-dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	C, not used in case of closure notification
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	SSET	Max. 50 Mb	C, not used in case of closure notification
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment

1.2.2.3.2.2. POST/pre-disputes/{id}/status – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.3.3. POST/disputes/{id}

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/disputes/{id}	DISPUTE	PSP submits the dispute request

1.2.2.3.3.1. POST/disputes/{id} – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Dispute ID	ID of the dispute case.	STR	TBA	M, this is inherited from the pre-dispute phase.

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Payment ID	Resource identifier for the disputed payment transaction.	STR	TBA	M
UETR	Unique end-to-end transaction reference of the disputed payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Payee PSP ID	BIC of the payee PSP holding the payee's digital euro payment account.	STR	11	M
Transaction settlement date and time	Date and time of the disputed transaction.	ISODateTime	10	M
Total transaction amount	Total amount of the disputed transaction, with 2 decimal positions.	STR	14.3	M
Disputed amount	Amount the payer disputes, with 2 decimal positions.	STR	14.3	M, cannot be higher than the original amount
Transaction Currency	The currency in which the amount is expressed. ISO 4217 three-letter code.	STR	3	M
Dispute reason code	Reason code set by payer PSP. See Rulebook section 6.	SSET	11	M, can be changed from the one used in pre-dispute phase
Dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment

1.2.2.3.3.2. POST/disputes/{id} – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 201.

Data element	Element description	Type	Length	Presence indicator
Dispute status	See Rulebook section 6.	SSET	11	M
Reason	Dispute message is rejected by DESP if: Disputed transaction processing date is beyond the allowed timelines Disputed amount is higher than the original transaction amount A process is already ongoing for the disputed transaction Other, technical reason	SSET	TBA	C, filled in if the request status is not valid, i.e. rejected by DESP, otherwise empty
Dispute ID	ID of the dispute case.	STR	TBA	M

1.2.2.3.4. POST/disputes/{id}/status

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/disputes/{id}/status	PREDISPUTE	PSP sends dispute status update

1.2.2.3.4.1. POST/disputes/{id}/status – Request

Request technical header data elements

- Please refer to section Technical header (Introduction and Exceptions management section).

Request API specific header data elements

Data element	Element description	Type	Length	Presence indicator
Dispute ID	Unique reference identifying the dispute case.	STR	TBA	M

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	C, not used in case of closure notification
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case of POS transaction; not used in case of closure notification

1.2.2.3.4.2. POST/disputes/{id}/status – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical header (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.4. PSP API for PSPs to receive requests from DESP

1.2.2.4.1. POST/pre-disputes/{id}

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/pre-disputes/{id}	PREDISPUTE	Payee PSP receives the pre-dispute request

1.2.2.4.1.1. POST/pre-disputes/{id} – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** no applicable.

Request API specific header data elements

Data element	Element description	Type	Length	Presence indicator
Pre-dispute ID	Unique reference identifying the pre-dispute case.	STR	TBA	M

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Payment ID	Resource identifier for the disputed payment transaction.	STR	TBA	M
UETR	Unique end-to-end transaction reference of the disputed payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Payee PSP ID	BIC of the payee PSP holding the payee's digital euro payment account.	STR	11	M
Transaction settlement date and time	Date and time of the disputed transaction.	ISODateTime	10	M
Total transaction amount	Total amount of the disputed transaction, with 2 decimal positions.	STR	14.3	M
Disputed amount	Amount the payer disputes, with 2 decimal positions.	STR	14.3	M, cannot be higher than the original amount
Transaction Currency	The currency in which the amount is expressed. ISO 4217 three-letter code.	STR	3	M
Pre-dispute reason code	Reason code set by payer PSP. See Rulebook section 6.	SSET	11	M
Pre-dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Payer DEAN	Unique identification of the individual user's (payer's) digital euro payment account.	STR	18	C, either payer DEAN and name or token needs to be provided
Payer name	Name of the payer.	STR	70	C, either payer DEAN and name or token needs to be provided
Payer token	NFC token	STR	TBA	C, either payer DEAN and name or NFC token needs to be provided
Payee name	Name of the payee.	STR	70	C, mandatory in case of C2B payments, registered company name of the business user payee.
Payee trade name	Name of the business user payee as it is presented to customers.	STR	25	C, mandatory in case of C2B payments.
Payee DEAN	Unique identification of the payer's digital euro payment account.	STR	18	M
Payee location (town)	Town of the business user payee.	STR	*13*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the

				payee's central registered address.
Payee location (ZIP-Code)	ZIP-code of the business user payee.	NUM	10	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (country)	Country of the business user payee.	STR	*30*	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.
Payee location (address)	Address (street name and building number) of the business user payee.	STR	30	C, mandatory in case of C2B payment, for POS payments the payee's physical location is filled in, for ecommerce payments the payee's central registered address.

Transaction type	e.g. Purchase, Reservation, Purchase with cashback, cash withdrawal.	STR	*4*	M
Transaction environment	Placeholder – to be specified.	ANS	8	M
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document	STR	36	C, mandatory in case there is an attachment
The data below is only used for recurring transactions				
Recurring payment frequency	The field specifies the frequency of a recurring payment. Please refer to Annex D 1 Acquiring PSP requirements, section 8.3.1.1.2.1 Incoming message table for the possible values.	SSET	4	M
Confirmation indicator	The field specifies if each recurring payment required authentication and confirmation by the payer.	BOOL	NA	M
End date	The field specifies the date at which the authorisation for the series of recurring payment ends.	ISODateTime	26	M
Recurring payments agreement ID	Agreement ID of the recurring payments.	STR	tbd	M
The data below is only used for reservation transactions				

Reservation ID	Resource ID for the reservation transaction.	STR	tbd	M
Reservation expiry date and time	Specifies the date and time at which the reservation ends and any still reserved amount will be released.	ISODateTime	11	O

1.2.2.4.1.2. POST/pre-disputes/{id} – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.4.2. POST/pre-disputes/{id}/status

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/pre-disputes/{id}/status	PREDISPUTE	PSP receives pre-dispute response

1.2.2.4.2.1. POST/pre-disputes/{id}/status – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Pre-dispute ID	Unique reference identifying the pre-dispute case.	STR	TBA	M

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Pre-dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment

1.2.2.4.2.2. POST/pre-disputes/{id}/status – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.4.3. POST/disputes/{id}

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/disputes/{id}	DISPUTE	Payee PSP receives the dispute request here

1.2.2.4.3.1. POST/disputes/{id} – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Dispute ID	Unique reference identifying the dispute case.	STR	TBA	M, this is inherited from the pre-dispute phase

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Payment ID	Resource identifier for the disputed payment transaction.	STR	TBA	M
UETR	Unique end-to-end transaction reference of the disputed payment transaction.	STR	36	M
Payer PSP ID	BIC of the payer PSP holding the payer's digital euro payment account.	STR	11	M
Payee PSP ID	BIC of the payee PSP holding the payee's digital euro payment account.	STR	11	M
Transaction settlement date and time	Date and time of the disputed transaction.	ISODateTime	10	M
Total transaction amount	Total amount of the disputed transaction, with 2 decimal positions.	STR	14.3	M
Disputed amount	Amount the payer disputes, with 2 decimal positions.	STR	14.3	M, cannot be higher than the original amount
Transaction Currency	The currency in which the amount is expressed. ISO 4217 three-letter code.	STR	3	M
Dispute reason code	Reason code set by payer PSP. See Rulebook section 6.	SSET	11	M, can be changed from the one used in pre-dispute phase
Dispute status	See Rulebook section 6	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment

Attachment hashed value	Hashed value of the encrypted attachments	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment

1.2.2.4.3.2. POST/disputes/{id} – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.2.2.4.4. POST/disputes/{id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/disputes/{id}/status	DISPUTE	PSP receives dispute status updates on this endpoint

1.2.2.4.4.1. POST/disputes/{id}/status – Request

Request header:

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:**

Data element	Element description	Type	Length	Presence indicator
Dispute ID	Unique reference identifying the dispute case.	STR	TBA	M

Request body unencrypted data elements

Data element	Element description	Type	Length	Presence indicator
Dispute status	See Rulebook section 6.	SSET	11	M
The data below is repeated per attached document				
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case there is an attachment
Attachment hashed value	Hashed value of the encrypted attachments.	STR	TBA	C, mandatory in case there is an attachment

Request body encrypted data elements

Data element	Element description	Type	Length	Presence indicator
Business reasoning	Free text entered by the payer's PSP or payer.	STR	1500	M
The data below is repeated per attached document				
Attachment	Base64 encoded attachments to support the case. See Rulebook section 6.	STR	Max. 50 Mb	O
Attached document reference number	Unique identifier of the attached document.	STR	36	C, mandatory in case of POS transaction

1.2.2.4.4.2. POST/disputes/{id}/status – Response

Response header

- **Technical header:** please refer to section Technical header (Introduction and Exceptions management section).
- **API specific header:** not applicable.

Response body data elements

- **In case of negative technical validation error**: please refer to section Technical errors (Introduction and Exceptions management section).
- **In case of positive technical validation**: HTTP Code 200.

1.3. Acquiring PSP requirements

Please see Section 1.2.