EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook – Annex D2 Back-end implementation specification #7 Settlement

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:	02/07/2026

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

12. Settlement service (SE) 10
12.1. Service description 10
12.1.1. Overview of PSPs' roles in settlement 11
12.1.2. Functional description 12
12.1.3. Interface description 13
12.1.3.1. Sequence diagrams 16
12.1.3.1.1. Funding and defunding transactions 17
12.1.3.1.1.1. Funding transaction 17
12.1.3.1.1.2. Funding transaction with open funding 18
12.1.3.1.1.3. Defunding transaction 20
12.1.3.1.1.4. Defunding transaction with open defunding 22
12.1.3.1.2. Payment transactions 23
12.1.3.1.2.1. Payment transaction with same digital euro PSP for payer and payee 23
12.1.3.1.2.2. Payer-initiated payment transaction 25
12.1.3.1.2.3. Payee-initiated payment transaction 29
12.1.3.1.3. Combined payment transactions 33
12.1.3.1.3.1. Payment transaction and (de)funding with same PSP for payer and payee 33
12.1.3.1.3.2. Payment transaction with open funding and defunding, the same digital euro PSP for payer and payee 34
12.1.3.1.3.3. Payer-initiated payment transaction with different digital euro PSPs and with open funding and defunding 37
12.1.3.1.3.4. Payee-initiated payment transaction with different digital euro PSPs and with open funding and defunding 39
12.1.3.1.4. Refunds 41
12.1.3.1.4.1. Refund for E/M-commerce 41
12.1.3.1.5. Status query 42
12.1.3.1.6. Transaction report 44
12.1.3.1.6.1. Report attributes 44
12.1.3.1.6.2. Transaction report retrieval process 45
12.1.3.2. Overview of API endpoints 46

12.1.3.2.1. DESP API endpoints for PSPs to send requests to DESP 46
12.1.3.2.2. PSP API endpoints for PSPs to receive requests from DESP 48
12.1.3.3. DESP API for PSPs to send requests to DESP 49
12.1.3.3.1. POST /fundings 49
12.1.3.3.1.1. POST /fundings – Request 49
12.1.3.3.1.2. POST /fundings – Response 52
12.1.3.3.2. POST /defundings 53
12.1.3.3.2.1. POST /defundings – Request 53
12.1.3.3.2.2. POST /defundings – Response 56
12.1.3.3.3. POST /payment-instructions 57
12.1.3.3.3.1. POST /payment-instructions – Request 57
12.1.3.3.3.2. POST /payment-instructions – Response 62
12.1.3.3.4. POST /payments 64
12.1.3.3.4.1. POST /payments – Request 64
12.1.3.3.4.2. POST /payments – Response 68
12.1.3.3.5. POST /payments/{payment-id}/status 69
12.1.3.3.5.1. POST /payments/{payment-id}/status – Request 69
12.1.3.3.5.2. POST / payments/{payment-id}/status – Response 71
12.1.3.3.6. GET /payment-instructions/{payment-instruction-id}/status 71
12.1.3.3.6.1. GET /payment-instructions/{payment-instruction-id}/status – Request 71
12.1.3.3.6.2. GET /payment-instructions/{payment-instruction-id}/status – Response 72
12.1.3.3.7. GET /fundings/{funding-id}/status 74
12.1.3.3.7.1. GET /fundings/{funding-id}/status – Request 74
12.1.3.3.7.2. GET /fundings/{funding-id}/status – Response 74
12.1.3.3.8. GET /defundings/{defunding-id}/status 76
12.1.3.3.8.1. GET /defundings/{defunding-id}/status – Request 76
12.1.3.3.8.2. GET /defundings/{defunding-id}/status – Response 76
12.1.3.3.9. POST /payments/{payment-id}/status-inquiries 77
12.1.3.3.9.1. POST /payments/{payment-id}/status-inquiries – Request 78
12.1.3.3.9.2. POST /payments/{payment-id}/status-inquiries – Response 78
12.1.3.3.10. POST /refunds 79

12.1.3.3.10.1. POST /refunds – Request ... 80
12.1.3.3.10.2. POST /refunds – Response ... 83
12.1.3.3.11. GET /refunds/{refund-id}/status ... 85
12.1.3.3.11.1. GET /refunds/{refund-id}/status – Request ... 85
12.1.3.3.11.2. GET /refunds/{refund-id}/status – Response ... 85
12.1.3.3.12. GET /queries/enduser-entries ... 87
12.1.3.3.12.1. GET /queries/end-user-entries – Request ... 87
12.1.3.3.12.2. GET /queries/end-user-entries – Response ... 88
12.1.3.3.13. GET /reports/transactions ... 88
12.1.3.3.13.1. GET /reports/transactions – Request ... 89
12.1.3.3.13.2. GET /reports/transactions – Response ... 89
12.1.3.3.14. GET /available-reports ... 90
12.1.3.3.14.1. GET /available-reports ... 91
12.1.3.3.14.2. GET /available-reports – Response ... 91
12.1.3.4. PSP API for PSPs to receive requests from DESP ... 92
12.1.3.4.1. POST /fundings ... 93
12.1.3.4.1.1. POST /fundings – Request ... 93
12.1.3.4.1.2. POST /fundings – Response ... 94
12.1.3.4.2. POST /fundings/{funding-id}/status ... 95
12.1.3.4.2.1. POST /fundings/{funding-id}/status – Request ... 96
12.1.3.4.2.2. POST /fundings/{funding-id}/status – Response ... 97
12.1.3.4.3. POST /defundings ... 97
12.1.3.4.3.1. POST /defundings – Request ... 98
12.1.3.4.3.2. POST /defundings – Response ... 99
12.1.3.4.4. POST /defundings/{defunding-id}/status ... 100
12.1.3.4.4.1. POST /defundings/{defunding-id}/status – Request ... 101
12.1.3.4.4.2. POST /defundings/{defunding-id}/status – Response ... 102
12.1.3.4.5. POST /payment-instructions ... 102
12.1.3.4.5.1. POST /payment-instructions – Request ... 103
12.1.3.4.5.2. POST /payment-instructions – Response ... 104
12.1.3.4.6. POST /payment-instructions/{payment-instruction-id}/status ... 106

12.1.3.4.6.1. POST /payment-instructions/{payment-instruction-id}/status – Request 106
12.1.3.4.6.2. POST /payment-instructions/{payment-instruction-id}/status – Response..... 109
12.1.3.4.7. POST /payments 109
12.1.3.4.7.1. POST /payments – Request 109
12.1.3.4.7.2. POST /payments – Response 110
12.1.3.4.8. POST / payments/{payment-id}/status 111
12.1.3.4.8.1. POST /payments/{payment-id}/status – Request 111
12.1.3.4.8.2. POST /payments/{payment-id}/status – Response 111
12.1.3.4.9. POST /payments/{payment-id}/status-inquiries..... 112
12.1.3.4.9.1. POST /payments/{payment-id}/status-inquiries – Request..... 112
12.1.3.4.9.2. POST /payments/{payment-id}/status-inquiries – Response 113
12.1.3.4.10. POST /refunds..... 114
12.1.3.4.10.1. POST /refunds – Request..... 114
12.1.3.4.10.2. POST /refunds – Response 116
12.1.3.4.11. POST /refunds/{refund-id}/status 118
12.1.3.4.11.1. POST /refunds/{refund-id}/status – Request 118
12.1.3.4.11.2. POST /refunds/{refund-id}/status - Response 120
12.1.3.4.12. POST /notifications/report-notifications 120
12.1.3.4.12.1. POST /notifications/report-notifications – Request..... 121
12.1.3.4.12.2. POST /notifications//report-notifications – Response 122
Annex A: Reservations v0.90 Carried-over Content for Information Only 124
A.1 Service description..... 124
A.1.1 Distributing PSP requirements 124
A.1.1.1 Functional description 124
A.1.1.2 Interface description..... 125
A.1.1.2.1 Overview of covered scenarios 129
A.1.1.2.1.1 Reservations 130
A.1.1.2.1.1.1 Payee-initiated reservation creation with open funding..... 130
A.1.1.2.1.1.2 Reservation lifecycle management..... 132
A.1.1.2.1.1.3 Settlement – claiming a reservation..... 135
A.1.1.2.2 Overview of API endpoints 135

A.1.1.2.2.1 DESP API endpoints for PSPs to send requests to DESP 135
A.1.1.2.2.2 PSP API endpoints for PSPs to receive requests from DESP 136
A.1.1.2.3 DESP API for PSPs to send requests to DESP 136
A.1.1.2.3.1 POST /reservation-instructions 136
A.1.1.2.3.1.1 POST /reservation-instructions - Request 137
A.1.1.2.3.1.2 POST /reservation-instructions – Response 139
A.1.1.2.3.2 POST /reservation-requests/{id}/confirmation 140
A.1.1.2.3.2.1 POST /reservation-requests/{id}/confirmation – Request 140
A.1.1.2.3.2.2 POST /reservation-requests/{id}/confirmation – Response 142
A.1.1.2.3.3 GET /reservations/{id}/status 144
A.1.1.2.3.3.1 GET /reservations/{id}/status – Request 144
A.1.1.2.3.3.2 GET /reservations/{id}/status – Response 144
A.1.1.2.4 PSP API for PSPs to receive requests from DESP 146
A.1.1.2.4.1 POST /reservation-requests 147
A.1.1.2.4.1.1 POST /reservation-requests – Request 147
A.1.1.2.4.1.2 POST /reservation-requests – Response 149
A.1.1.2.4.2 POST /reservation-instructions/{id}/status 150
A.1.1.2.4.2.1 POST /reservation-instructions/{id}/status – Request 150
A.1.1.2.4.2.2 POST /reservation-instructions/{id}/status – Response 152
A.1.1.2.4.3 POST /reservation-request/{id}/status 153
A.1.1.2.4.3.1 POST /reservation-request/{id}/status – Request 153
A.1.1.2.4.3.2 POST /reservation-request/{id}/status – Response 156
A.1.1.2.4.4 PUT /reservations/{id} 156
A.1.1.2.4.4.1 PUT /reservations/{id} – Request 156
A.1.1.2.4.4.2 PUT /reservations/{id} – Response 158
A.1.1.2.4.5 POST /reservations/{id}/status 159
A.1.1.2.4.5.1 POST /reservations/{id}/status – Request 159
A.1.1.2.4.5.2 POST /reservations/{id}/status – Response 162
A.1.2 Acquiring PSP requirements 162
A.1.2.1 Functional description 162
A.1.2.2 Interface description 162

A.1.2.2.1 Settlement payload structure 162
A.1.2.2.2 Overview of API endpoints 163
A.1.2.2.2.1 DESP API endpoints for PSPs to send requests to DESP 163
A.1.2.2.2.2 PSP API endpoints for PSPs to receive requests from DESP 163
A.1.2.2.3 Overview of covered scenarios 164
A.1.2.2.4 DESP API for PSPs to send requests to DESP 164
A.1.2.2.4.1 POST /reservation-requests 164
A.1.2.2.4.1.1 POST /reservation-requests – Request 164
A.1.2.2.4.1.2 POST /reservation-requests – Response 166
A.1.2.2.4.2 PUT /reservations/{id} 167
A.1.2.2.4.2.1 PUT /reservations/{id} – Request 167
A.1.2.2.4.2.2 PUT /reservations/{id} – Response 170
A.1.2.2.5 PSP API for PSPs to receive requests from DESP 171
A.1.2.2.5.1 POST /reservation-instructions 171
A.1.2.2.5.1.1 POST /reservation-instructions – Request 171
A.1.2.2.5.1.2 POST /reservation-instructions – Response 173

12. Settlement service (SE)

12.1. Service description

The DESP settlement service is responsible for the settlement verification (i.e., checking that a certain amount can be transferred between online digital euro and/or dedicated cash account (DCA) holdings) and settlement recording (i.e., irrevocably and unconditionally transferring a certain amount of digital euro and/or DCA holdings). The settlement service in DESP therefore covers not only payments in digital euro but also the functionalities of funding, defunding and reservation. Based on the information recorded for the settlement of the types of transactions mentioned above, the settlement service provides also settlement reporting (i.e., preparing the necessary settlement confirmation and rejection messages).

The objective of this section is to outline the functionalities that can be invoked by PSPs involved in digital euro transactions, including the encrypted communication between instructing and instructed parties authorising a transaction[2]. The section *Functional description* describes the **types of transactions** processed by the DESP. These include payment, funding, defunding, combined (a payment to be made together with funding and/or defunding), refund and reservation transactions (which reserves an amount of digital euro for subsequent payments)[3]. The outcome of processing a transaction can therefore be either (i) the transfer of funds from the payer, whose entry[4] is debited, to the payee, whose entry is credited; or (ii) the reservation of funds from the payer; or (iii) both.

A transaction may contain payment data[5], settlement data[6], or both. The payment process starts when the first API call[7] with the payment data (and settlement data, if initiated by the digital euro payer PSP), which associates an initial acceptance timestamp to the transaction, reaches the DESP. If the first API call, which contains payment data, is sent by the digital euro payee PSP, then it is a **payee-initiated** payment. If the first API call containing payment data is sent by the digital euro payer PSP, then it is a **payer-initiated** payment, and it also contains settlement data.

The digital euro transactions must be **settled atomically**: either the whole transaction is settled, or nothing is settled. Consequently, a digital euro settlement instruction can only be settled by DESP once it contains data on applicable parts of the foreseen settlement recording (funding, defunding and payment). Since a

[2] Please refer to digital euro glossary:
https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs220420.en.pdf
[3] Reservation transaction is not covered in the current scope of the rulebook and will be included in the later versions.
[4] Entry is either a user entry, which represents the identifier of a digital euro holding in the settlement ledger, or a DCA entry, which represents the identifier of a digital euro dedicated cash account in the settlement ledger.
[5] Payment data is the data exchanged between the PSPs, describing the payment (incl. amount, remittance information), accounts and parties involved, required by the PSPs to process the transaction.
[6] Settlement data is the minimal data set required for DESP to process the transaction. It includes at least entry of both payer and payee, amount, acceptance timestamp and fee calculation related data.
[7] A list of the API calls for initiating a transaction is specified in the *DESP API endpoints* section.

digital euro transaction may involve more than one PSPs, the PSP who initiates the transaction may lack some necessary data to complete it. In such scenario, the digital euro end to end flows foresee a role for DESP to facilitate the build-up of the settlement instruction without back-and-forth of messages among PSPs and no need for one of them to submit the completed instruction for all parties involved. Instead, PSP initiating the transaction sends the API request with **partial settlement data** to the DESP that then takes care of compiling the overall settlement instruction. To do so, the DESP forwards only the necessary information to other PSPs involved in the transaction, in line with the data minimisation principle, and collects the parts of their responses that are necessary for settlement. Throughout the settlement process, other participants in the transaction chain, such as commercial bank money PSPs or digital euro payee PSPs, contribute with additional settlement data. This combined information enables DESP to compile a comprehensive settlement instruction with **complete settlement data** that allows atomic settlement, ensuring all aspects of the transaction, including any (de)funding, are settled simultaneously. This process applies equally to reservations, refunds, and funding or defunding transactions that involve multiple PSPs.

12.1.1. Overview of PSPs' roles in settlement

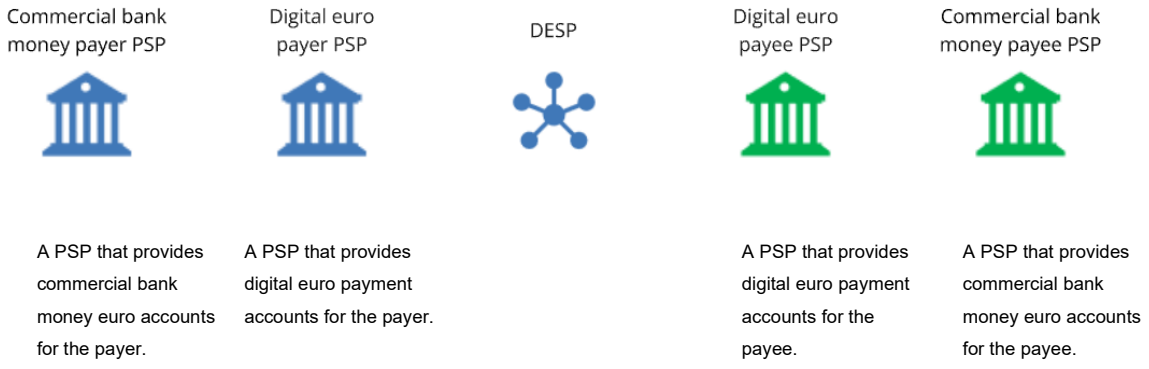
Settlement of a transaction requires PSPs to perform two to four different roles:

(1) digital euro payer's PSP,

(2) digital euro payee's PSP,

(3) commercial bank money payer's PSP,

(4) commercial bank money payee's PSP.



These different roles can be operated by different PSPs within one digital euro transaction, or a PSP can take a combination of roles. For instance, the same PSP may be a digital euro PSP (either for the payer,

or payee, or both) and at the same time commercial bank money PSP, providing (de)funding services (either for the payer, or payee, or both).

A PSP needs to use different endpoints, each with a different set of data included in the corresponding requests and responses, depending on the role it plays. The introduction to the section *Interface description* outlines the structure of a settlement API request/response payload. The required payload parts, including their objects, depend on the transaction type and on the role of the PSP.

12.1.2. Functional description

The section below shows the different types of transactions that PSPs can support.

Funding transaction

Funding is the process of increasing a digital euro user's holding in their account or device through digital euro issuance, in combination with a reduction of another liquidity source from the digital euro user (e.g., cash or private money)[8]. A scenario in which a digital euro transaction requires debiting a non-digital euro payment account held at another PSP than the user's digital euro PSP is referred to as '**open funding**'.

Defunding transaction

Defunding is the process of reducing a digital euro user's digital euro holdings in their account or device through digital euro redemption, in combination with an increase of digital euro user's private money or an increase in the digital euro user's cash holdings[9]. A scenario in which a digital euro transaction requires crediting a non-digital euro payment account held at another PSP than the user's digital euro PSP is referred to as '**open defunding**'.

Payment transaction

A digital euro payment transaction is initiated by either payer or payee PSP and confirmed by the corresponding PSP. DESP performs settlement once the settlement data and confirmation are received from both payer and payee PSPs. There are different types of payment use cases in digital euro, namely: P2P, e/m-commerce, and point of sale (POS) (see more details in section *Sequence diagrams*) .

Combined payment transaction

A combined transaction is a digital euro transaction involving payment with funding (*reverse waterfall* - if the user does not have sufficient digital euro holdings) or payment with defunding (*waterfall* - if the user's digital euro holding limit is reached). If the digital euro PSP and a commercial bank money PSP are different,

[8] Please refer to digital euro glossary:
https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.dedocs220420.en.pdf
[9] See above.

it is referred to a combined transaction with an *open (de)funding*. DESP performs settlement once the settlement data and confirmation are received from both payer and payee PSPs.

Reservation transaction[10]

A reservation transaction is a digital euro payment transaction subject to pre-authorisation between a payee and a payer. The payer authorises that a certain amount is reserved for a specific purpose (for a specific merchant and services it provides) and the payee can claim the reserved funds at later times. A reservation transaction is created following the same steps as a payment transaction. Instead of recording the settlement of a payment between users beforehand, a reservation is recorded, and funds are moved from the available balance to the reserved balance of the payer. A payment transaction would then need to be submitted every time the reserved funds are claimed by the payee via its PSP. Reverse waterfall might be required if the payer does not have sufficient digital euro holdings to complete the reservation transaction.

Refund transaction[11]

A refund is a reversal (in whole or in part) of an earlier payment initiated by a payee, usually at the payer's request. A refund always requires funding if the original payee's funds are not sufficient to settle the refund and may require defunding on the original payer's side. DESP performs settlement once the settlement data and confirmation are received from both payer and payee PSPs.

12.1.3. Interface description

This section provides a detailed description of the interface designed to facilitate communication between PSPs and the DESP for the settlement service. The interface is based on RESTful API principles and the data format used is JSON (JavaScript Object Notation). The data dictionary, including complex data types, is based on ISO20022 where available.

The structure of the request and response for the settlement service can be summarised as follows:

- **Header** contains metadata about the request. It includes generic data elements that are used in all API endpoints, such as content type, and specific values only used for certain endpoints.
- **Payload:**

[10] Reservation transaction is not covered in the current rulebook version and will be included in the later versions.
[11] The current rulebook version only covers refund transaction for e/m-commerce payment use cases. Refund transaction for POS payment will be included in the later versions.

- **Root** contains top-level data elements of the JSON payload structure, such as UETR, acceptance timestamp and objects.
    - **Objects** contain collections of data elements and are nested within the root.

Payload structure summary for settlement requests

Element	Encryption	Condition to be included in the payload
Root		
UETR	Unencrypted or encrypted[12]	Mandatory for all transactions.
Acceptance date time	Unencrypted or encrypted[13]	Mandatory for all transactions.
Objects:		
Payment Instruction object	Unencrypted	Mandatory in case the message concerns a payment initiated by the payer PSP.
	Encrypted	Included if payer and payee PSPs are different parties, as the content needs to be forwarded to the other PSP.
Payment object	Encrypted	Mandatory in case the message concerns a payment request initiated by the payee PSP.
Refund object	Unencrypted	Mandatory in case the message concerns a refund transaction.
	Encrypted	Included if payer and payee PSPs are different parties and that the content needs to be forwarded to the other PSP.
Funding object	Unencrypted	Only required if payer's digital euro balance is lower than the transaction amount. Mandatory in case the message concerns a funding transaction.
	Encrypted	Included if the digital euro and commercial bank money PSPs are different parties and the content needs to be forwarded to the other PSP.
	Unencrypted	Only required if the transaction results in the payee's digital euro balance exceeding payee's holding limit. Mandatory in case the message concerns a defunding transaction.

[12] UETR is encrypted in endpoints for payee-initiated payments, i.e., POST /payments, POST /payments/{payment-id}/status and GET /payments/{payment-id}/status.
[13] Acceptance timestamp is encrypted in endpoints for payee-initiated payments, i.e., POST /payments, POST /payments/{payment-id}/status.

Defunding object[14]	Encrypted	Included if the digital euro and commercial bank money PSPs are different parties and that the content needs to be forwarded to the other PSP.

Similarly, which data elements are present in settlement notifications and responses received by a PSP depends on the role of the PSP and the context of the transaction.

Additional status elements for settlement notifications and responses

Element	Condition to be included in the payload
Payment instruction ID and status	Mandatory in case the transaction request contains a payment instruction object. Payment instruction ID is present only if the validation result is positive. Only received by the payer's and payee's digital euro PSP.
Refund ID and status	Mandatory in case the transaction request contains a refund object. Refund ID is present only if the validation result is positive. Only received by the payer's and payee's digital euro PSP.
Funding ID and status	Mandatory in case the transaction request contains a funding object. Funding ID is present only if the validation result is positive. Only received by the requester and receiver of the funding request (the payer's digital euro PSP and the payer's commercial bank money PSP).
Defunding ID and status	Mandatory in case the transaction request contains a defunding object. Defunding ID is present only if the validation result is positive. Only received by the requester and receiver of the defunding request (the payee's digital euro PSP and the payee's commercial bank money PSP).

12.1.3.1. Sequence diagrams

This section presents a selection of baseline scenarios that cover the key flows in the digital euro settlement process, taking into account:

- the type of transaction ((de)funding, (combined) payment, refund);
- the party that initiates the process (PSP of payer or payee);

[14] A defunding object could be included in the response (from the PSP to DESP only) to a payment instruction and refunds, if defunding is required

- the role a PSP performs in the process which may vary depending on the user type (e.g., individual or business) and the transaction setup (e.g., single PSP vs multiple PSPs involved);

The description of API calls in sections (*DESP APIs endpoints for PSPs to send requests to DESP* and *PSP APIs endpoints for PSPs to receive requests to DESP*) includes information on whether the steps in the process are conditional (e.g., for funding and defunding).

12.1.3.1.1. Funding and defunding transactions

12.1.3.1.1.1. Funding transaction

The sequence diagram below presents a funding process, in which the digital euro PSP and commercial bank money PSP are the same and all necessary settlement data can be shared with DESP in one API call.

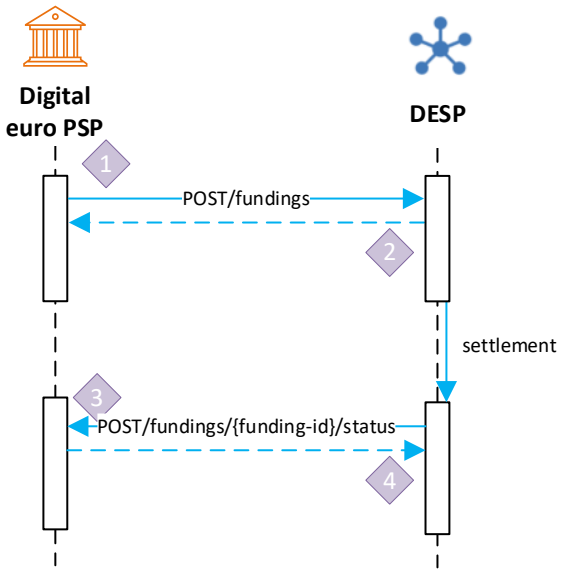


Figure 1: Funding transaction[15]

API call	Description	Covered In section
1	Digital euro PSP sends the request with complete settlement data to DESP.	DESP API POST /fundings - Request

[15] Please see LM-1.1 Online manual funding from non-digital euro payment account - same PSP and LM-1.3 Online scheduled or automated funding from non-digital euro payment account - same PSP

2	Synchronous[16] response from DESP to confirm receipt of the request.	DESP API POST /fundings - Response
3	DESP sends the status of the funding transaction back to digital euro PSP.	PSP API POST /fundings/{funding-id}/status - Request
4	Synchronous response from the digital euro PSP to confirm receipt of the status notification.	PSP API POST /fundings/{funding-id}/status - Response

12.1.3.1.1.2. Funding transaction with open funding

The sequence diagram below presents a funding process in which the digital euro PSP and commercial bank money PSP are different. The commercial bank money PSP needs to provide a validation result.

[16] Synchronous API means that the client sends a request to the server and waits until it receives the response. During this time, the client cannot perform other operations or send additional requests on the same transaction.

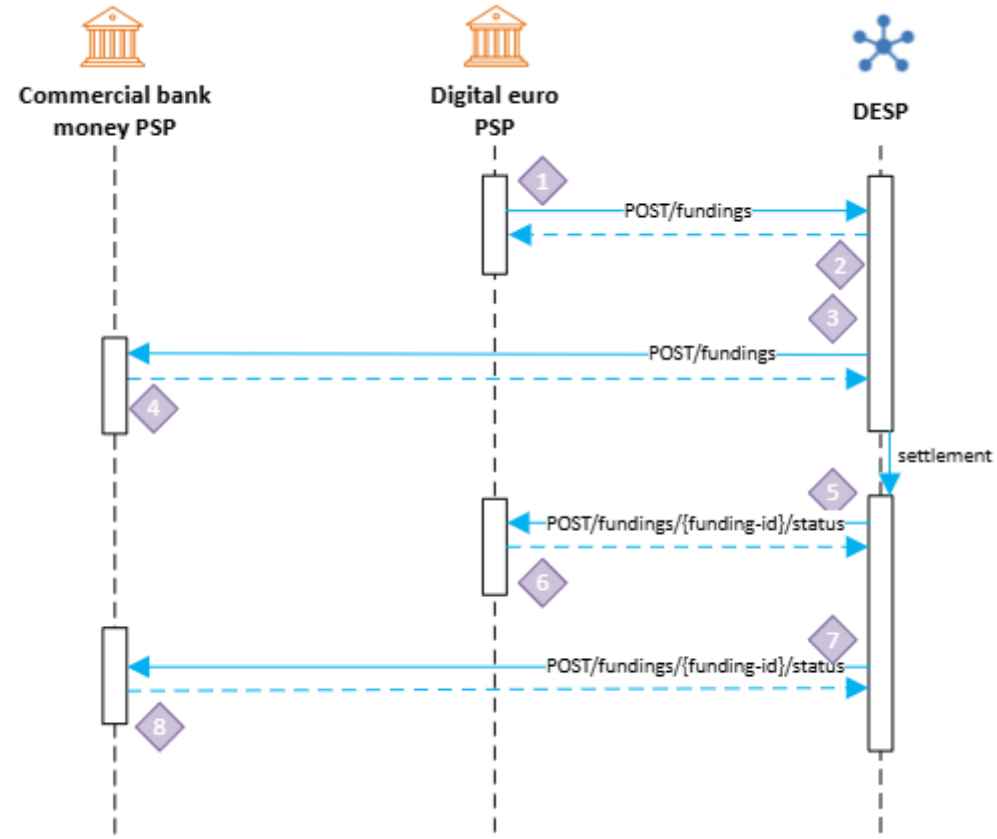


Figure 2: Funding with open funding transaction[17]

API call	Description	Covered In section
1	Digital euro PSP sends the request with partial settlement data to DESP and specifies the commercial bank money PSP identifier.	DESP API POST /fundings - Request
2	Synchronous response from DESP to confirm receipt of the request from API call 1.	DESP API POST /fundings - Response
3	DESP forwards request from API call 1 to commercial bank money PSP.	PSP API POST /fundings - Request

[17] Please see LM-1.2 Online manual funding from non-digital euro payment account - different PSPs and LM-1.4 Online scheduled or automated funding from non-digital euro payment - different PSPs

4	Synchronous response from the commercial bank money PSP that includes validation result and the complement settlement data (if validation result is positive).	PSP API POST /fundings - Response
5	DESP sends status of the funding transaction back to digital euro PSP, simultaneously with API call 7.	PSP API POST /fundings/{funding-id}/status - Request
6	Synchronous response from digital euro PSP to confirm receipt of the status notification.	PSP API POST /fundings/{funding-id}/status - Response
7	DESP sends status of the funding transaction back to commercial bank money PSP, simultaneously with API call 5.	PSP API POST /fundings/{funding-id}/status - Request
8	Synchronous response from commercial bank money PSP to confirm receipt of the status notification.	PSP API POST /fundings/{funding-id}/status - Response

12.1.3.1.1.3. Defunding transaction

The sequence diagram below presents a defunding process, when the digital euro PSP and commercial bank money PSP are the same.

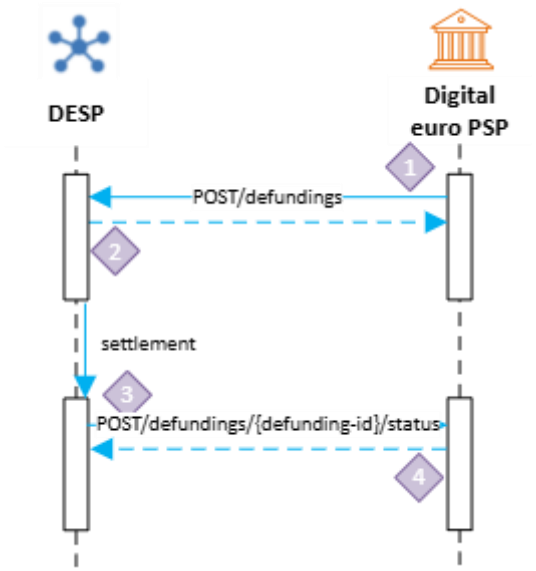


Figure 3: Defunding transaction[18]

API call	Description	Covered In section
1	Digital euro PSP sends the request with complete settlement data to DESP.	DESP API POST /defundings - Request
2	Synchronous response from DESP to confirm receipt of the request.	DESP API POST /defundings - Response
3	DESP sends status of the defunding transaction back to digital euro PSP.	PSP API POST /defundings/{defunding-id}/status - Request
4	Synchronous response from digital euro PSP to confirm receipt of the status notification.	PSP API POST /defundings/{defunding-id}/status - Response

[18] Please see LM-2.1 Online manual defunding to non-digital euro payment account - same PSP and LM-2.3 Online scheduled or automated defunding to non-digital euro payment account - same PSP

12.1.3.1.1.4. Defunding transaction with open defunding

The sequence diagram below presents a defunding process in which the digital euro PSP and commercial bank money PSP are different. The commercial bank money PSP needs to provide a validation result.

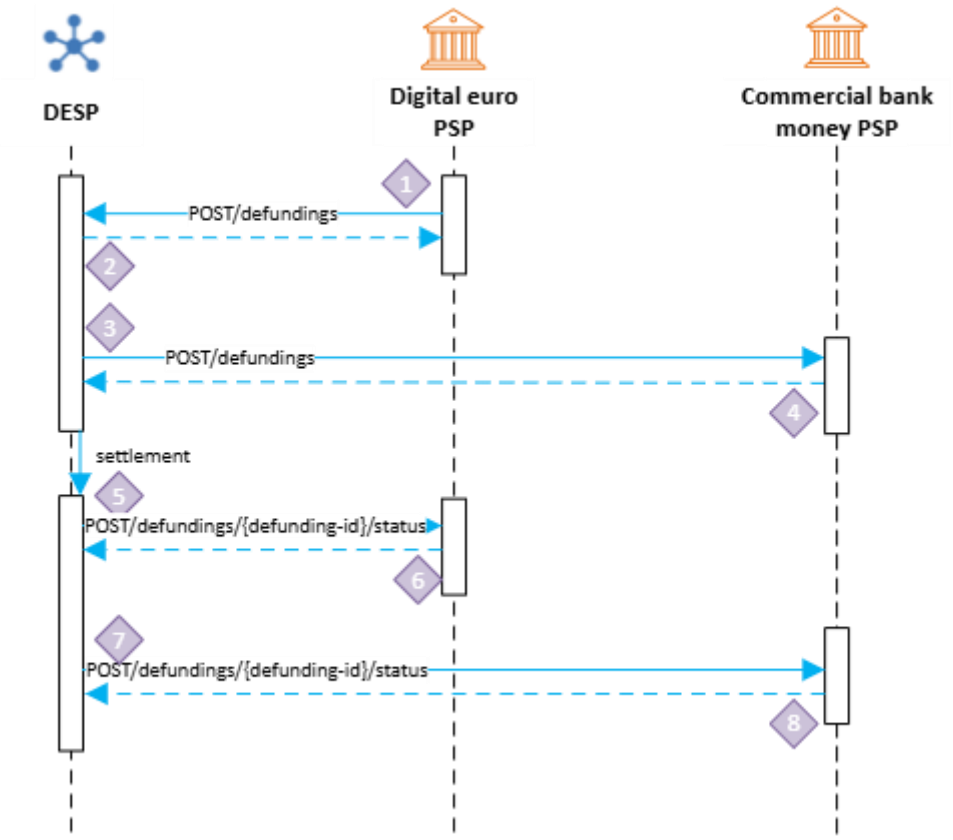


Figure 4: Open defunding transaction[19]

API call	Description	Covered In section
1	Digital euro payer PSP sends the request with partial settlement data to DESP and specifies the commercial bank money PSP identifier.	DESP API POST /defundings - Request

[19] Please see LM-2.2 Online manual defunding to non-digital euro payment account - different PSPs and LM-2.4 Online scheduled or automated defunding to non-digital euro payment account - different PSPs

2	Synchronous response from DESP to confirm receipt of the request from API call number 1.	DESP API POST /defundings - Response
3	DESP forwards request from API call 1 to commercial bank money PSP.	PSP API POST /defundings - Request
4	Synchronous response from commercial bank money PSP that includes validation result and the complement settlement data (if the validation result is positive).	PSP API POST /defundings - Response
5	DESP sends status of the defunding transaction back to digital euro PSP, simultaneously with API call 7.	PSP API POST /defundings/{defunding-id}/status - Request
6	Synchronous response from digital euro PSP to confirm receipt of the status notification.	PSP API POST /defundings/{defunding-id}/status - Response
7	DESP sends status of the defunding transaction back to commercial bank money PSP, simultaneously with API call 5.	PSP API POST /defundings/{defunding-id}/status - Request
8	Synchronous response from commercial bank money PSP to confirm receipt of the status notification.	PSP API POST /defundings/{defunding-id}/status - Response

12.1.3.1.2. Payment transactions

12.1.3.1.2.1. Payment transaction with same digital euro PSP for payer and payee

The sequence diagram below presents a payment process in which the digital euro PSP for a payee and a payer is the same, and no funding/defunding of digital euro is required.

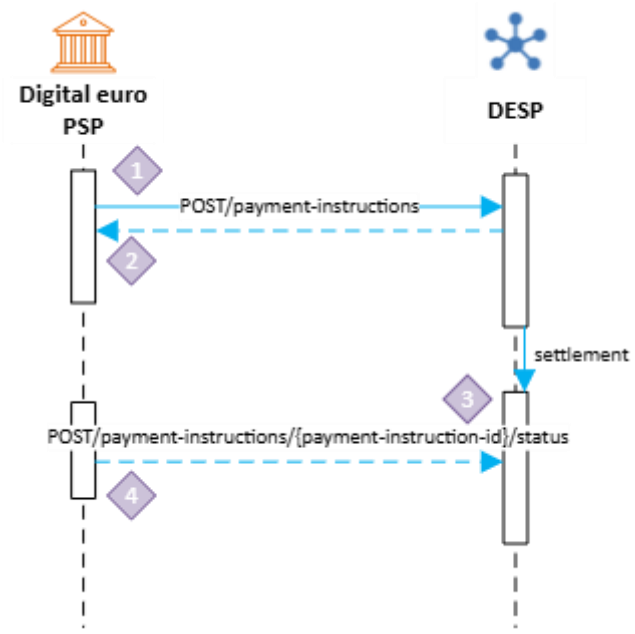


Figure 5: Same payer and payee PSP payment transaction

API call	Description	Covered In section
1	Digital euro PSP sends the request with a payment object with complete settlement data.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to confirm receipt of the request sent in API call 1.	DESP API POST /payment-instructions - Response
3	DESP sends status of the payment transaction back to digital euro PSP.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
4	Synchronous response from digital euro PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response

The sequence diagram below presents a negative scenario when DESP rejects the incoming request. As the request fails at the technical validation step, the status cannot be queried.[20]

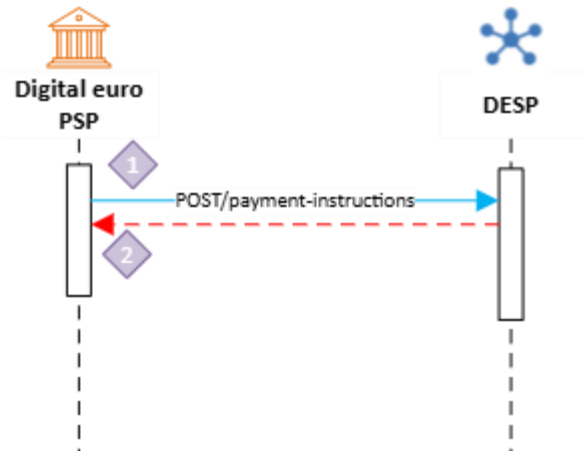


Figure 6: Same payer and payee PSP payment transaction rejected by DESP

API call	Description	Covered In section
1	Digital euro PSP sends the request with a payment object with complete settlement data.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to reject receipt of the request sent in API call 1.	DESP API POST /payment-instructions - Response

12.1.3.1.2.2. Payer-initiated payment transaction

The sequence diagram below presents a payment process initiated by the payer PSP[21], in which the digital euro PSPs for a payee and a payer are different, and no funding/defunding of digital euro is required.

[20] Functional errors that come in a status message can be queried, while any other error (e.g., technical errors with HTTP code 4xx) than status after a 20x message cannot be queried. In case of a technical error, digital euro PSP can submit the same message with a new UETR after the cause is identified.

[21] Examples of the payer-initiated flows: QR code, or payer-initiated alias or DEAN payments. For details, please refer to E2E flows Annex B.

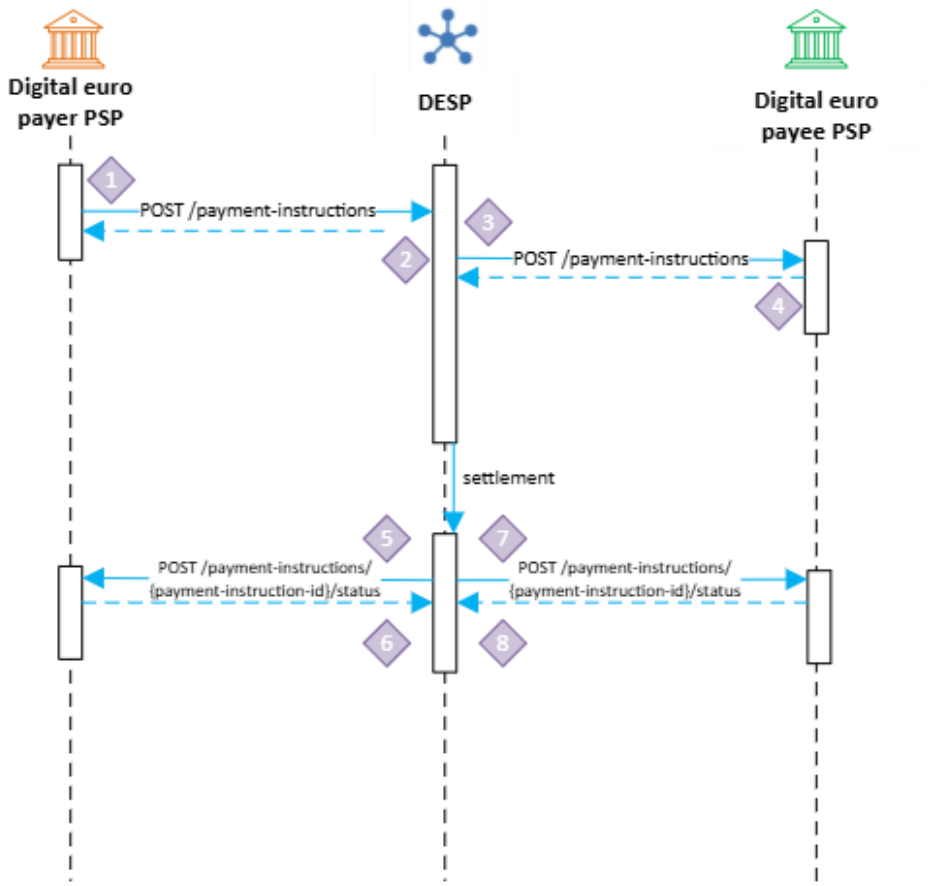


Figure 7: Payer-initiated payment transaction[22]

API call	Description	Covered In section
1	Digital euro payer PSP sends the request with a payment object with partial settlement data.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to confirm receipt of the message sent in API call 1.	DESP API POST /payment-instructions - Response

[22] Please see TM-2.1 E-commerce (including C2G) payment with QR code, XTM-1.1 First alternative for a POS payments with payee-generated QR code, YTM-1.1 Second alternative for a POS payments with payee-generated QR code, TM-2.3 E-commerce (incl. C2G) payment with pay-by-link, TM-2.4 M-commerce payment (in-app), TM-3.1 P2P payment with QR code in-app (payee-initiated), TM-3.10 P2P Account-to-account payment with DEAN (payer initiated) – same PSP, TM-3.5 P2P payment with alias (payer initiated), TM-3.7 P2P payment with payment request by link, TM-4.3 Standing order, TM-3.2 P2P payment with NFC (online), payer initiated and LM-2.8.2 Online purchase with cash back at POS (PwCB) with QR code

3	DESP forwards the request that contains payment object from API call 1 to digital euro payee PSP.	PSP API POST /payment-instructions - Request
4	Synchronous response from digital euro payee PSP to send back the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /payment-instructions - Response
5	DESP sends status of the payment transaction back to digital euro payer PSP, simultaneously with API call 7.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
6	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response
7	DESP sends status of the payment transaction back to digital euro payee PSP, simultaneously with API call 5.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
8	Synchronous response from digital euro payee PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response

The sequence diagram below presents a negative scenario when the payee PSP rejects the incoming request.

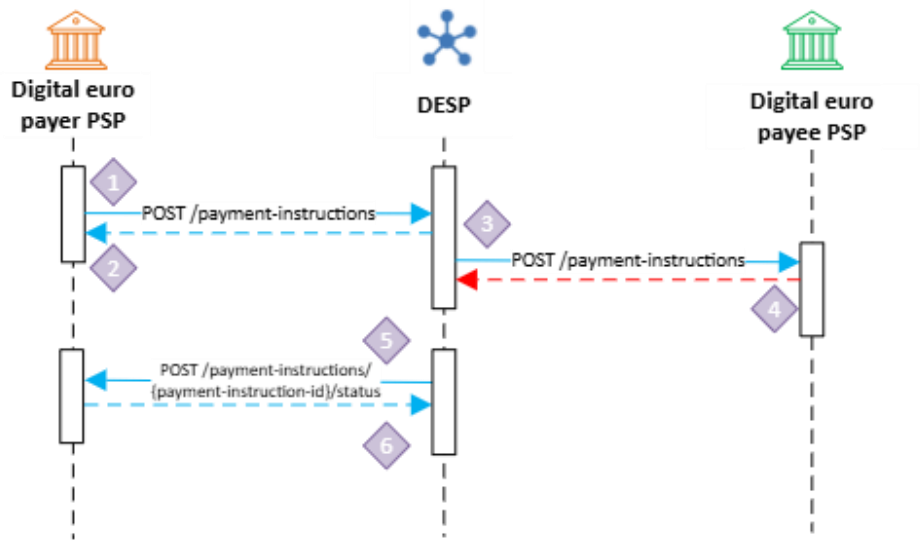


Figure 8: Payer-initiated payment transaction rejected by the payee PSP[23]

API call	Description	Covered In section
1	Digital euro payer PSP sends the request with a payment object with partial settlement data.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to confirm receipt of the message sent in API call 1.	DESP API POST /payment-instructions - Response
3	DESP forwards the request that contains payment object from API call 1 to digital euro payee PSP.	PSP API POST /payment-instructions - Request
4	Synchronous response from digital euro payee PSP to reject the incoming request API call 3.	PSP API POST /payment-instructions - Response
5	DESP sends status of the payment transaction back to the digital euro payer PSP.	PSP API

[23] Please see TM-2.1 E-commerce (including C2G) payment with QR code, XTM-1.1 First alternative for a POS payments with payee-generated QR code, YTM-1.1 Second alternative for a POS payments with payee-generated QR code, TM-2.3 E-commerce (incl. C2G) payment with pay-by-link, TM-2.4 M-commerce payment (in-app), TM-3.1 P2P payment with QR code in-app (payee-initiated), TM-3.10 P2P Account-to-account payment with DEAN (payer initiated) – same PSP, TM-3.5 P2P payment with alias (payer initiated), TM-3.7 P2P payment with payment request by link, TM-4.3 Standing order, TM-3.2 P2P payment with NFC (online), payer initiated and LM-2.8.2 Online purchase with Cash Back at POS (PwCB) with QR code

		POST /payment-instructions/{payment-instruction-id}/status – Request
6	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response

12.1.3.1.2.3. Payee-initiated payment transaction

The sequence diagram below presents a payee-initiated payment transaction, as the first API call containing payment data is submitted by the payee PSP. Examples of the applicable use case are e-commerce payment with alias or DEAN[24], payee-initiated P2P payment with alias or DEAN[25] or NFC/chip-based payment via mobile device, smartcard or wearable at the POS[26].

[24] See E2E flows TM-2.2.
[25] See E2E flows TM-3.6.
[26] See E2E flows TM-1.2, TM-1.3, TM-1.6.

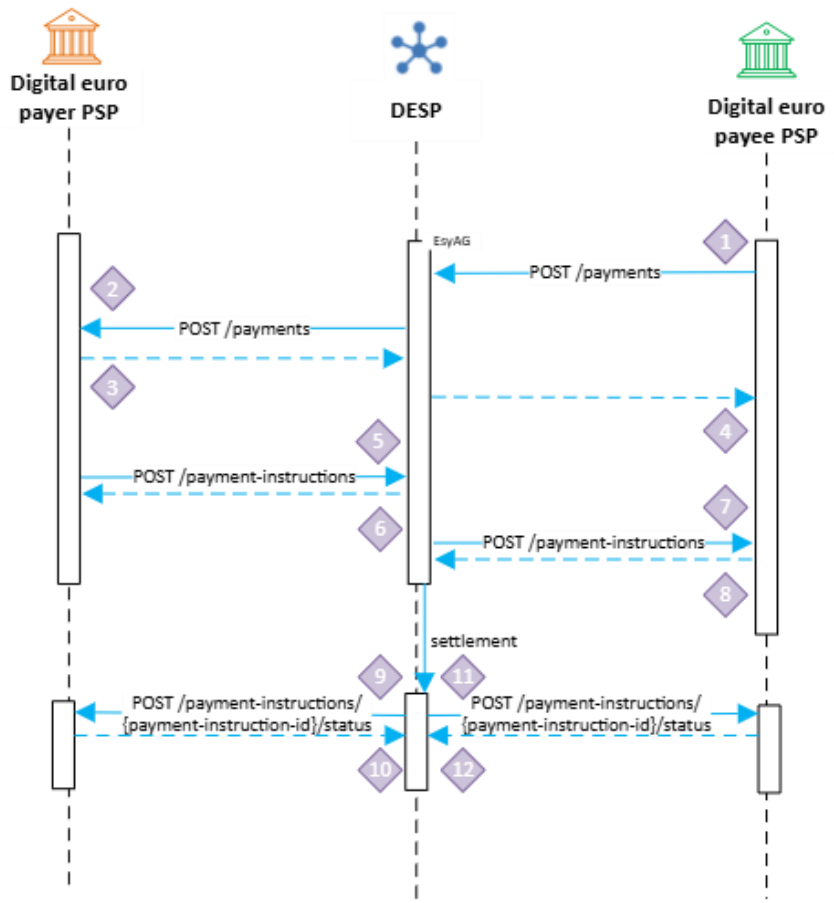


Figure 9: Payer-initiated payment transaction with original request stemming from the payee PSP[27]

API call	Description	Covered In section
1	Payee PSP sends the request for payment API call with encrypted payment data.	DESP API POST /payments - Request
2	DESP forwards the request sent in API call 2.	PSP API POST /payments – Request

[27] Please see TM-2.2 E-commerce (incl. C2G) payment with alias or DEAN, TM-1.6 Online contactless SoftPOS payment with mobile device or wearable - same PSP, TM-1.2 Online contact and contactless POS payment with mobile device, card or wearable - same PSP, TM-3.12 P2P payment with DEAN (payee initiated), TM-3.6 P2P payment with alias (payee initiated) and LM-2.8.1 Online purchase with Cash Back at POS (PwCB) with NFC through card (contact and contactless) or smartphone

3	Payer PSP performs technical validation and responds with acceptance or rejection.[28]	PSP API POST /payments - Response
4	DESP forwards the response sent in API call 3. In the case of a rejection, the flow stops at API call 4.	DESP API POST /payments - Response
5	Payer PSP sends the payment instruction request with a payment object with partial settlement data.	DESP API POST /payment-instructions - Request
6	Synchronous response from DESP to confirm receipt of the message sent in API call 5.	DESP API POST /payment-instructions - Response
7	DESP forwards the request that contains payment object from API call 6 to digital euro payee PSP.	PSP API POST /payment-instructions - Request
8	Synchronous response from digital euro payee PSP to send back the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /payment-instructions - Response
9	DESP sends status of the payment transaction back to digital euro payer PSP, simultaneously with API call 11.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
10	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response
11	DESP sends status of the payment transaction back to digital euro payee PSP, simultaneously with API call 9.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
12	Synchronous response from digital euro payee PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response

[28] Depending on the payment use cases, other API calls can happen between API call 3 and 5. For details please refer to E2E flows. For example, cryptogram check is required for NFC/chip-based payment vis mobile device, smartcard or wearable at the POS; payer authorisation of the payment is required in the app for e-commerce payment with alias or DEAN.

The sequence diagram below presents a negative scenario where the request for payment is rejected asynchronously by the digital euro payer PSP (i.e., the rejection is not sent directly to payment request in step 3, but just after some time in step 5).[29]

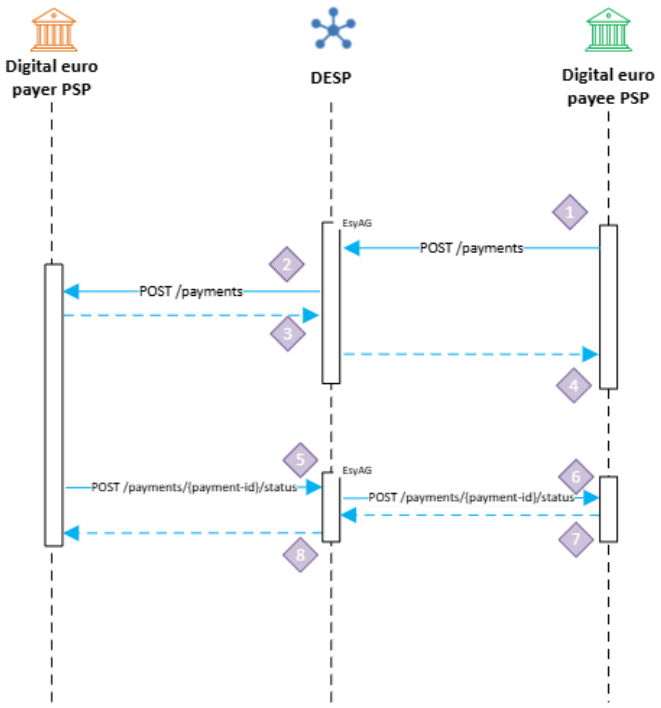


Figure 10: Request for payments asynchronously rejected by the payer PSP[30]

Step 1 to step 4 is the same as in Figure 9.

API call	Description	Covered In section
5	In case of a functional rejection, the payer PSP sends the status of the request for payment.	DESP API POST /payments/{payment-id}/status - Request
6	DESP forwards the request in API call 5 to the payee PSP.	PSP API POST /payments/{payment-id}/status - Request

[29] For example, the payer rejects or does not respond in time to the incoming request in the app in e-commerce payment with alias or DEAN or in payee initiated P2P payment with alias or DEAN.

[30] Please see TM-2.2 E-commerce (incl. C2G) payment with alias or DEAN, TM-1.6 Online contactless SoftPOS payment with mobile device or wearable - same PSP, TM-1.2 Online contact and contactless POS payment with mobile device, card or wearable - same PSP, TM-3.12 P2P payment with DEAN (payee initiated), TM-3.6 P2P payment with alias (payee initiated) and LM-2.8.1 Online purchase with Cash Back at POS (PwCB) with NFC through card (contact and contactless) or smartphone.

7	Synchronous response from the payee PSP to confirm receipt of the status notification.	PSP API POST /payments/{payment-id}/status - Response
8	DESP forwards the response in API call 7 to the payer PSP.	DESP API POST /payments/{payment-id}/status - Response

12.1.3.1.3. Combined payment transactions

12.1.3.1.3.1. Payment transaction and (de)funding with same PSP for payer and payee

The sequence diagram below presents the payment process in which the digital euro PSP for a payee and a payer is the same, as well as for funding/defunding.

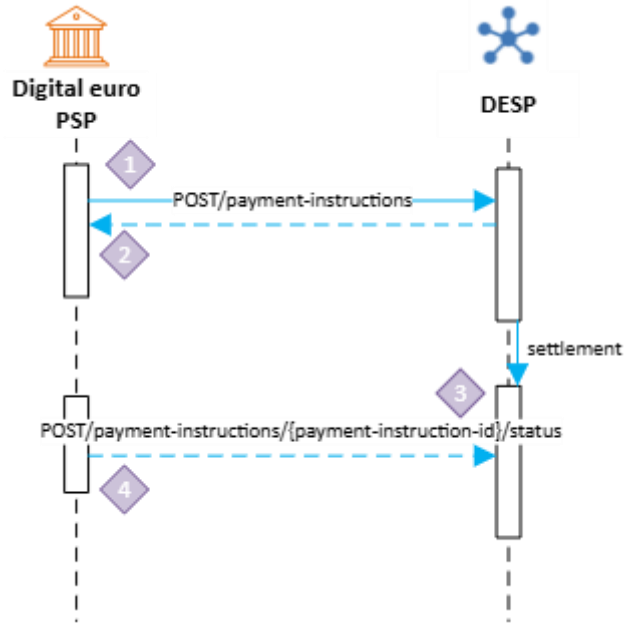


Figure 11: Same payer, payee and (de)funding PSP

API call	Description	Covered In section
1	Digital euro PSP sends the request with (1) payment object with complete settlement data and (2) with funding and/or defunding object(s) with complete settlement data.	DESP API POST /payment-instructions - Request

2	Synchronous response from DESP to confirm the receipt of the message sent in API call 1.	DESP API POST /payment-instructions - Response
3	DESP sends status of the payment transaction back to digital euro PSP.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
4	Synchronous response from digital euro PSP to confirm the receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status - Response

12.1.3.1.3.2. Payment transaction with open funding and defunding, the same digital euro PSP for payer and payee

The sequence diagram below presents a payment process, in which the digital euro PSP for the payee and the payer is the same. Additionally, to complete the instruction, funding and/or defunding, involving a commercial bank money PSP is required.

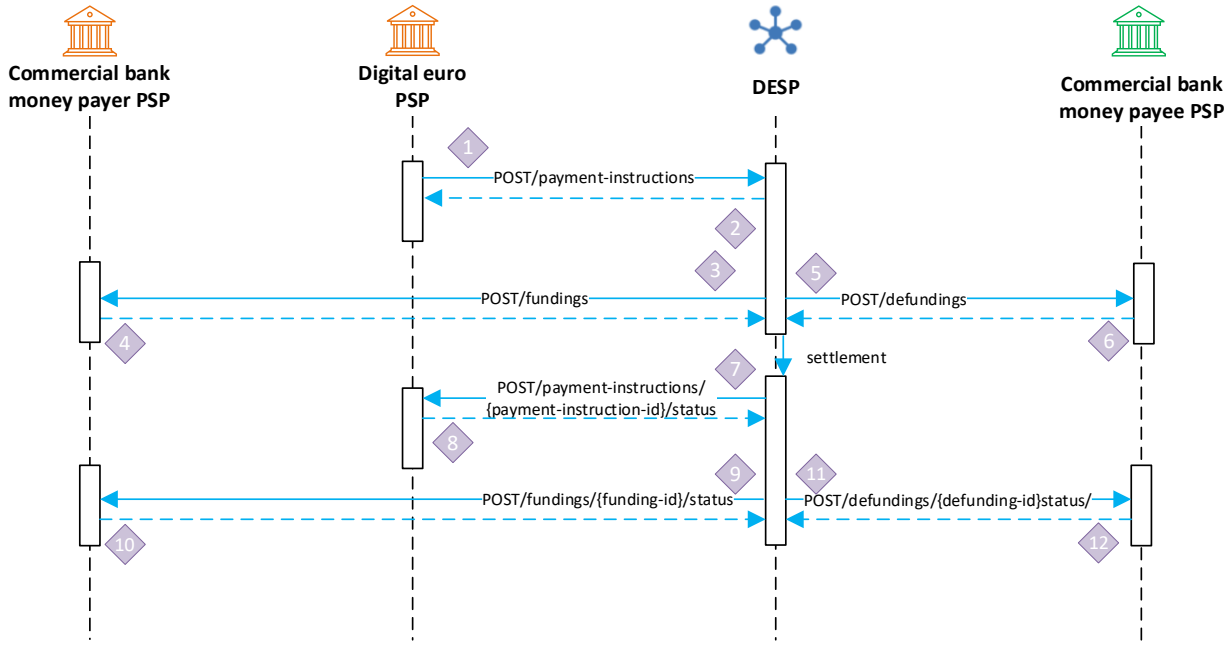


Figure 12: Same payer and payee PSP payment transaction with open funding and defunding

API call	Description	Covered In section
1	Digital euro PSP sends the request with (i) payment object with complete settlement data for the payment part, (ii) and funding object with partial settlement data, and (iii) defunding object with partial settlement data to DESP.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to confirm receipt of the request sent in API call 1.	DESP API POST /payment-instructions - Response
3	DESP forwards funding request from API call 1 to commercial bank money payer PSP, simultaneously with API call 5.	PSP API POST /fundings - Request
4	Synchronous response from commercial bank money payer PSP that includes the validation	PSP API POST /fundings - Response

	result and the complement settlement data (if the validation result is positive).	
5	DESP forwards the defunding request from API call 1 to commercial bank money payee PSP, simultaneously with API call 3.	PSP API POST /defundings - Request
6	Synchronous response from commercial bank money payee PSP that includes the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /defundings - Response
7	DESP sends status of the payment transaction back to digital euro PSP, simultaneously with API call 9 and 11.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
8	Synchronous response from digital euro PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status - Response
9	DESP sends status of the funding back to commercial bank money payer PSP, simultaneously with API call 7 and 11.	PSP API POST /fundings/{funding-id}/status - Request
10	Synchronous response from the commercial bank money payer PSP to confirm receipt of the status notification.	PSP API POST /fundings/{funding-id}/status - Response
11	DESP sends status of the defunding back to commercial bank money payee PSP, simultaneously with API call 7 and 9.	PSP API POST /defundings/{defunding-id}/status - Request
12	Synchronous response from commercial bank money payee PSP to confirm receipt of the status notification.	PSP API POST /defundings/{defunding-id}/status - Response

12.1.3.1.3.3. Payer-initiated payment transaction with different digital euro PSPs and with open funding and defunding

The sequence diagram below presents a payment process initiated by the payer PSP in which the digital euro PSPs for the payee and the payer are different. Additionally, to complete the instruction, funding and/or defunding, involving commercial bank money PSPs is required.

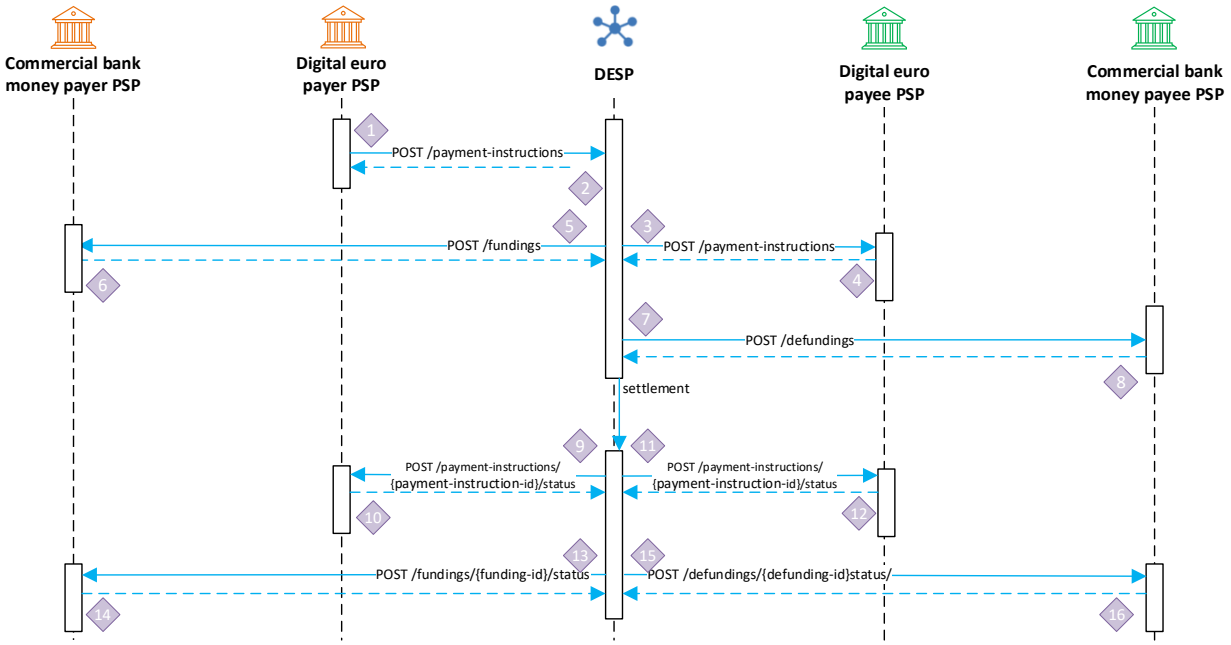


Figure 13: Payer initiated payment transaction with open funding and defunding[31]

API call	Description	Covered In section
1	Digital euro payer PSP sends the request with (i) payment object with partial settlement data and (ii) funding object with partial settlement data to DESP.	DESP API POST /payment-instructions - Request
2	Synchronous response from DESP to confirm receipt of the request sent in API call 1.	DESP API POST /payment-instructions - Response

[31] Please see TM-3.11 P2P account-to-account payment with DEAN (payer initiated) - different PSPs

3	DESP forwards the request that contains payment object from API call 1 to digital euro payee PSP, simultaneously with API call 5.	PSP API POST /payment-instructions - Request
4	Synchronous response from digital euro payee PSP to send back the validation result and (if the validation result is positive) the remaining settlement data for payment object and partial settlement data in the defunding object.	PSP API POST /payment-instructions - Response
5	DESP forwards funding request from API call 1 to commercial bank money payer PSP, simultaneously with API call 3.	PSP API POST /fundings - Request
6	Synchronous response from commercial money payer PSP that includes the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /fundings - Response
7	DESP forwards the request from API call 4 that contains partial defunding data to commercial bank money payee PSP.	PSP API POST /defundings - Request
8	Synchronous response from commercial bank money payee PSP that includes the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /defundings - Response
9	DESP sends status of the payment transaction back to digital euro payer PSP, simultaneously with API call 11, 13 and 15.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request
10	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response
11	DESP sends status of the payment transaction back to digital euro payee PSP, simultaneously with API call 9, 13 and 15.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Request

12	Synchronous response from digital euro payee PSP to confirm receipt of the status notification.	PSP API POST /payment-instructions/{payment-instruction-id}/status – Response
13	DESP sends status of the funding back to commercial bank money payer PSP simultaneously with API call 9, 11 and 15.	PSP API POST /fundings/{funding-id}/status Request
14	Synchronous response from commercial bank money payer PSP to confirm receipt of the status notification.	PSP API POST /fundings/{funding-id}/status Response
15	DESP sends status of the defunding back to commercial bank money payee PSP simultaneously with API call 9, 11 and 13.	PSP API POST /defundings/{defunding-id}/status - Request
16	Synchronous response from commercial bank money payee PSP to confirm receipt of the status notification.	PSP API POST /defundings/{defunding-id}/status - Response

12.1.3.1.3.4. Payee-initiated payment transaction with different digital euro PSPs and with open funding and defunding

The sequence diagram below presents a payment process initiated by the payee PSP in which the digital euro PSPs for the payee and the payer are different. Additionally, to complete the instruction, funding and/or defunding, involving a commercial bank money PSP, is required. The settlement process which is reflected in API call 5 to API call 20 is the same process as described in section 12.1.3.1.2.3 payer-initiated payment transaction with open funding and defunding.

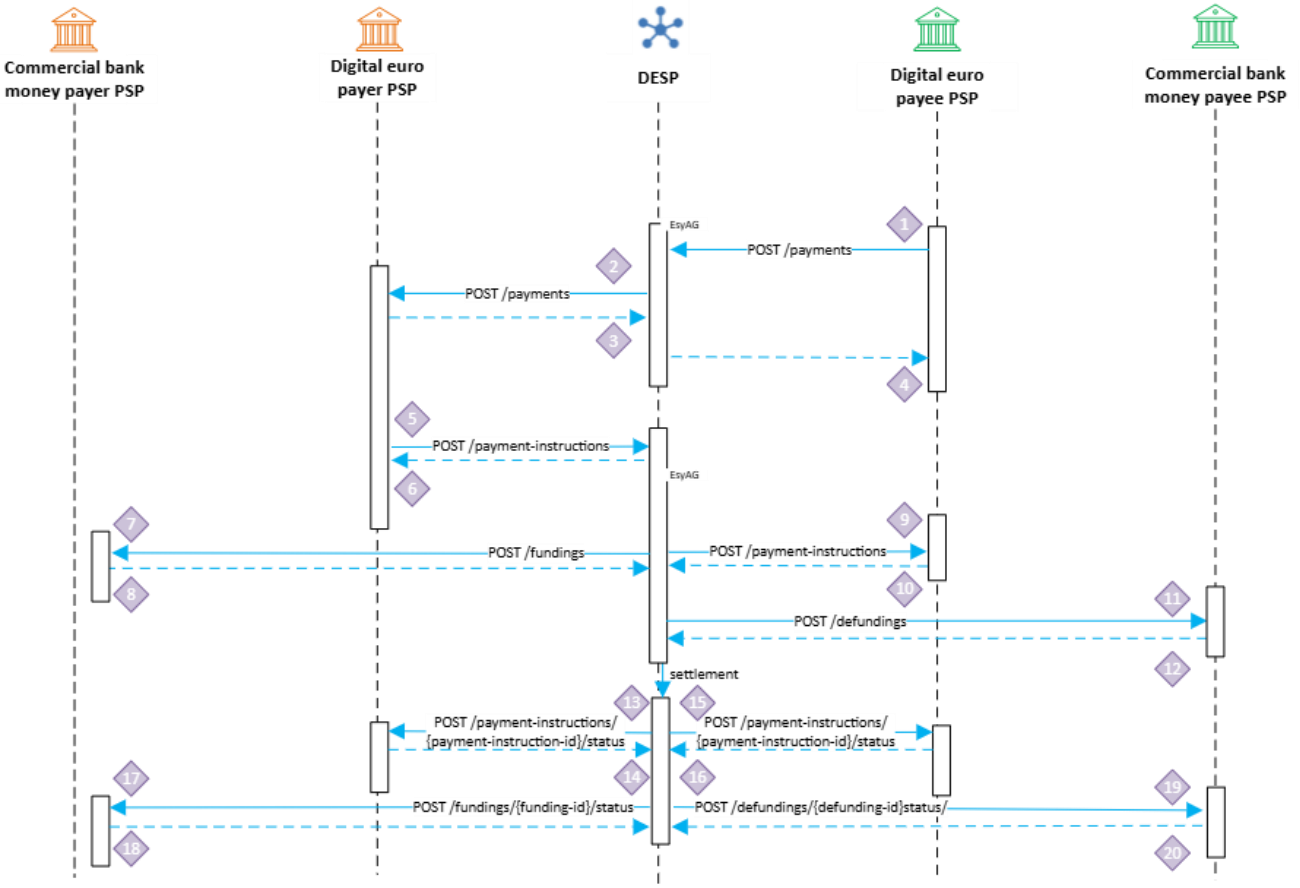


Figure 14: Payee initiated payment transaction with open funding and defunding[32]

API call	Description	Covered In section
1	Payee PSP sends the request for payment API call with encrypted payment data.	DESP API POST /payments - Request
2	DESP forwards the request sent in API call 1.	PSP API POST /payments – Request
3	Payer PSP performs technical validation and responds with acceptance or rejection.[33]	PSP API POST /payments - Response

[32] Please see TM-1.3 Online contact and contactless POS payment with mobile device, card or wearable - different PSPs

[33] Depending on the payment use cases, other API calls can happen between API call 3 and 5. For details please refer to E2E flows. For example, cryptogram check is required for NFC/chip-based payment vis mobile device, smartcard or wearable at the POS; payer authorisation of the payment is required in the app for e-commerce payment with alias or DEAN.

4	DESP forwards the response sent in API call 3. In the case of a rejection, the flow stops at API call 4.	DESP API POST /payments - Response

Step 5- 20 follows the same steps as in Figure 13 (steps 1-16) included under Section 12.2.2.1.3.3 payer-initiated payment transaction with open funding and open defunding.

12.1.3.1.4. Refunds

12.1.3.1.4.1. Refund for E/M-commerce

The sequence diagram below presents an e/m-commerce refund process, in which the digital euro PSPs for a payee and a payer are different, no defunding of digital euro is required, and the commercial bank money PSP of the original payee PSP (e.g., merchant) is the same as the digital euro PSP.

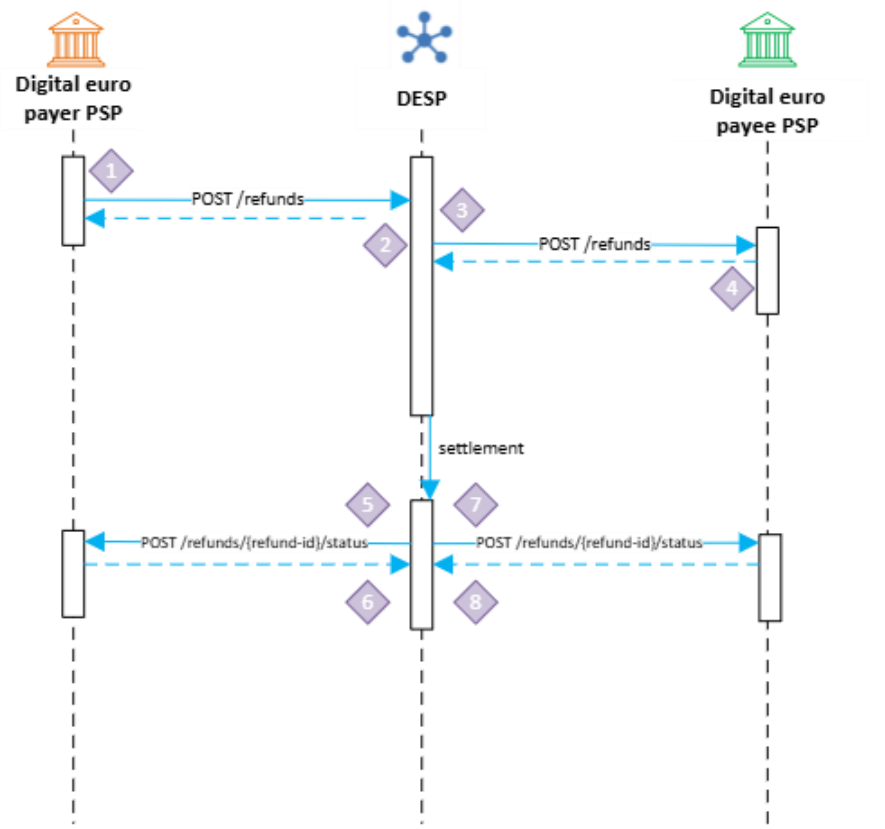


Figure 15: Refund transaction[34]

API call	Description	Covered In section
1	The digital euro payer PSP of the refund (i.e., merchant's PSP, which is the digital euro payee PSP of the original payment) sends a request with refund object and funding object with partial settlement data to DESP.	DESP API POST /refunds – Request
2	Synchronous response from DESP to confirm receipt of the request sent in API call 1.	DESP API POST /refunds – Response
3	DESP forwards the request which contains the refund object from API call 1 to the payee (the original digital euro payer PSP).	PSP API POST /refunds - Request
4	Synchronous response from the payee PSP of the refund to send back the validation result and the complement settlement data (if the validation result is positive).	PSP API POST /refunds – Response
5	DESP sends status of the refund transaction back to the digital euro payer PSP, simultaneously with API call 7.	PSP API POST /refunds/{refund-id}/status - Request
6	Synchronous response from the digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /refunds/{refund-id}/status - Response
7	DESP sends status of the refund transaction back to the digital euro payee PSP, simultaneously with API call 5.	PSP API POST /refunds/{refund-id}/status - Request
8	Synchronous response from the digital euro payee PSP to confirm receipt of the status notification.	PSP API POST /refunds/{refund-id}/status - Response

12.1.3.1.5. Status query

The sequence diagram below presents a query which can be sent by the payee PSP to the payer PSP.

[34] Please see TM-7.2 Refund (e-commerce)

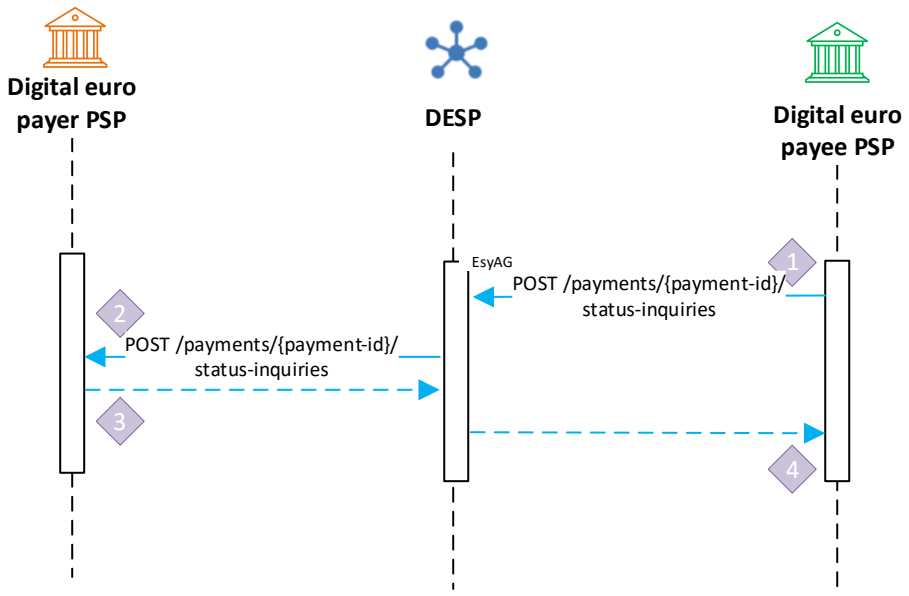


Figure 16: Request for payments query initiated by the Payee PSP

API call	Description	Covered In section
1	The payee PSP sends the query to the payer PSP via DESP	DESP API GET / payments/{payment-id}/status - Request
2	DESP forwards the request in API call 2 to the payer PSP.	PSP API POST /payments/{payment-id}/status-inquiries - Request
3	Synchronous response from the payer PSP to confirm the status of the request.	PSP API POST /payments/{payment-id}/status-inquiries - Response
4	DESP forwards the response in API call 3 to the payer PSP.	DESP API POST /payments/{payment-id}/status-inquiries - Response

12.1.3.1.6. Transaction report

The transactions report enables digital euro PSPs to retrieve detailed information on successfully settled transactions initiated or received by instructing parties serviced by the digital euro PSP. It provides transaction-level data, including identifiers, amounts, timestamps, and originating PSP information.

The report is generated by the DESP based on the PSP request parameters and made available according to the defined reporting frequency. PSPs retrieve the report via dedicated API endpoint once it is available.

The DESP notifies the PSP when the report is ready to be retrieved.

For recovery scenarios, where a report ready notification is not received by the digital euro PSP, or cannot be processed, the PSP may query the DESP for the list of available reports. The DESP in this case returns a list of available reports together with their metadata, allowing the digital euro PSP to identify the relevant transactions report and retrieve it via the dedicated transaction report retrieval endpoint.

12.1.3.1.6.1. Report attributes

Recipient	Mode	View	Frequency
Digital euro PSP	Full or Delta	Detailed	As per subscription

The transactions report shall include the following information:

- the period (e.g., the calendar day) for which the information is retrieved
- currency
- identifier of the digital euro PSP (BIC) originating the transaction
- amount
- transaction reference
- settlement timestamp

12.1.3.1.6.2. Transaction report retrieval process

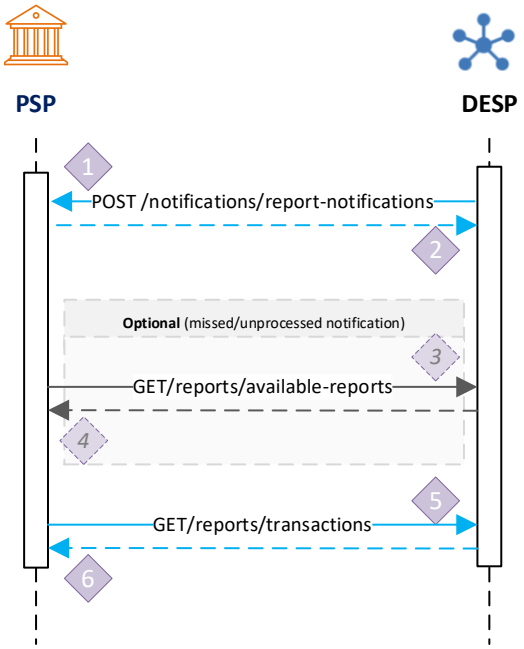


Figure 17: Report retrieval process

API call	Description	Covered In section
1	DESP sends report-ready notification to the digital euro PSP.	POST /notifications/report-notifications - Request
2	Digital euro PSP confirms the receipt of the report-ready notification.	POST /notifications/report-notifications - Response
3(Optional)	Digital euro PSP retrieves the available reports.	GET/reports/available-reports - Request
4(Optional)	DESP provides the list of available reports to the digital euro PSP.	GET/reports/available-reports - Response
5	Digital euro PSP retrieves the transaction report by specifying report parameters.	GET/reports/transactions - Request
6	DESP provides the requested transaction report to the digital euro PSP.	GET/reports/transactions - Response

Steps 3 and 4 are optional and shall be executed in case of missed or unprocessed notifications.

12.1.3.2. Overview of API endpoints

12.1.3.2.1. DESP API endpoints for PSPs to send requests to DESP

API nr	Description	Sending party	Exposing party	Covered in section
1	Digital euro PSP submits a funding request to commercial bank money PSP or submits complete funding settlement data directly to DESP.	Digital euro PSP	Commercial bank money PSP (via DESP) or DESP*	POST /fundings
2	Digital euro PSP submits a defunding request to commercial bank money PSP or submits complete defunding settlement data directly to DESP.	Digital euro PSP	Commercial bank money PSP (via DESP) or DESP*	POST /defundings
3	Digital euro payer PSP submits payment instruction to digital euro payee PSP to start the settlement process. If both payer and payee have the same PSP, the payment instruction is to be submitted directly at this endpoint with complete settlement data to DESP.	Digital euro payer PSP	Digital euro payee PSP (via DESP) or DESP*	POST /payment-instructions
4	Digital euro payee PSP submits payment request to digital euro payer PSP to start the payment process.	Digital euro payee PSP	Digital euro payer PSP (via DESP)	POST /payments
5	Digital euro payer PSP sends status update of a payment request initiated by the digital euro payee PSP.	Digital euro payer PSP	Digital euro payee PSP (via DESP)	POST /payments/{payment-id}/status

6	The digital euro payee PSP of the original payment (payer PSP in refund transaction) sends the refund payment instruction to the digital euro payer PSP of the original payment (payee PSP in refund transaction)	Digital euro payer PSP	Digital euro payee PSP (via DESP)	POST /refunds
7	Digital euro PSP OR commercial bank money PSP queries status of a funding transaction.	Digital euro PSP or commercial bank money PSP	DESP	GET /fundings/{funding-id}/status
8	Digital euro PSP OR commercial bank money PSP queries status of a defunding transaction.	Digital euro PSP or commercial bank money PSP	DESP	GET /defundings/{defunding-id}/status
9	Digital euro payer PSP OR digital euro payee PSP queries status of a payment transaction.	Digital euro payer PSP or Digital euro payee PSP	DESP	GET /payment-instructions/{payment-instruction-id}/status
10	Digital euro payee PSP queries status of a payment request with digital euro payer PSP.	Digital euro payee PSP	Digital euro payer PSP (via DESP)	POST /payments/{payment-id}/status-inquiries
11	Digital euro payer PSP OR digital euro payee PSP queries status of a refund transaction.	Digital euro payer PSP or Digital euro payee PSP	DESP	GET /refunds/{refund-id}/status

12	Digital euro PSP retrieves the transactions report.	PSP	DESP	GET/reports/transactions
13	Digital euro PSP initiates user entry(-ies) query.	PSP	DESP	GET/ queries/enduser-entries
14	Digital euro PSP retrieves the available reports overview.	PSP	DESP	GET /reports/available-reports/?report-type=<report-type>

*When the instructing PSP is the same PSP as the PSP instructed for payment transaction, funding transaction or defunding transaction, and the full settlement data is in the request, then the exposing party will be DESP.

12.1.3.2.2. PSP API endpoints for PSPs to receive requests from DESP

API nr	Description	Sending party	Exposing party	Covered in section
14	DESP forwards funding request to commercial bank money PSP.	DESP	Commercial bank money PSP	POST /fundings
15	DESP sends status of a funding transaction to commercial bank money PSP or digital euro PSP.	DESP	Commercial bank money PSP or Digital euro PSP	POST /fundings/{funding-id}/status
16	DESP forwards defunding request to commercial bank money PSP.	DESP	Commercial bank money PSP	POST /defundings
17	DESP sends status of a defunding transaction to commercial bank money PSP or digital euro PSP.	DESP	Commercial bank money PSP or Digital euro PSP	POST /defundings/{defunding-id}/status
18	DESP forwards payment instruction to digital euro payee PSP.	DESP	Digital euro payee PSP	POST /payment-instructions
19	DESP sends status of a payment transaction (initiated at POST /payment-	DESP	Digital euro payer and payee PSP	POST /payment-instructions/{payment-instruction-id}/status

	instructions endpoint) to digital euro payer and payee PSP.			
20	DESP forwards payment request from digital euro payee PSP to digital euro payer PSP.	DESP	Digital euro payer PSP	POST /payments
21	DESP forwards status update of a payment request from digital euro payer PSP to digital euro payee PSP.	DESP	Digital euro payee PSP	POST /payments/{payment-id}/status
22	DESP forwards query on status of a payment request from digital euro payee PSP to digital euro payer PSP.	DESP	Digital euro payer PSP	POST /payments/{payment-id}/status-inquiries
23	DESP forwards refund payment instruction to the digital euro payee PSP.	DESP	Digital euro payee PSP	POST /refunds
24	DESP sends status of a refund to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /refunds/{refund-id}/status
25	DESP sends a notification to the PSP when the transaction report is ready to be pulled.	DESP	PSP	POST /notifications/report-notifications

12.1.3.3. DESP API for PSPs to send requests to DESP

In this section, all API endpoints for PSPs to submit requests to DESP (hereafter **DESP API**) are described in detail.

12.1.3.3.1. POST /fundings

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/fundings	Funding	Endpoint for funding transaction initiation

12.1.3.3.1.1. POST /fundings – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp is used for determination of maximum processing time. This is set by the first PSP which starts the settlement process and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	Payment identification2	M
fundingObject	See the next tables.	-	M

Funding object data elements – unencrypted part

Data element	Element description	Type	Presence indicator
instructingAgent	Unique identification of the user's digital euro PSP (BIC).	Financial institution Identification1	M
instructedAgent	Unique identification of the user's commercial bank money PSP (BIC). If the digital euro PSP is the same as the commercial bank money PSP, then the same value as instructing PSP must be filled in.	Financial institution Identification1	M
amount	The amount to be issued in digital euro holding.	Amount	M

userEntry	Identification of the user's digital euro holding in the settlement ledger.	Entry	M
paymentType	Type of the payment.	PaymentType	M
encryptedFundingObject	Encrypted data fields, see next table.		C, mandatory in case of open funding

Funding object data elements – encrypted part

The encrypted part is required for open funding case in which the digital euro PSP is different from the commercial bank money PSP.

Data element	Element description	Type	Presence indicator
digitalEuroAccount	Unique identification of the user's digital euro payment account.	Account reference	M
ownerName	Name of the owner.	Account owner	M
remittanceInformationUnstructured	The field provides additional information about (the purpose of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.	Max140Text	O
remittanceInformationStructured	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	Remittance	O

commercialBankMoneyAccount	Unique identification of the user's non-digital euro payment account.	Account reference	M
accountOwnerName	Name of the owner of the non-digital euro payment account.	Account owner	M
paymentIdentification	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. In case no reference was given by the user, "NOTPROVIDED" must be used.	paymentIdentification1	M

12.1.3.3.1.2. POST /fundings – 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	Description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be	Payment Identification2	M

	located at any time, by any of the parties in the chain. Set by the instructing PSP.		
fundingId	Resource ID generated by DESP to identify the funding transaction.	UUID	M
fundingTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC -ACCP	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'fundingTransactionStatus'

12.1.3.3.2. POST /defundings

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/defundings	Defunding	Endpoint for defunding transaction initiation

12.1.3.3.2.1. POST /defundings – Request

Request header:

- **Technical header:** please refer to section *Technical header (Introduction and exceptions management section)*.

- **API specific header:** not applicable.

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp is used for determination of maximum processing time. This is set by the first PSP which starts the settlement process and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	Payment Identification2	M
defundingObject	See the next table.	Defunding object	M

Defunding object data elements – unencrypted part

Data element	Element description	Type	Presence indicator
instructingAgent	Unique identification of the user's digital euro PSP (BIC).	Financial institution Identification1	M
instructedAgent	Unique identification of the user's commercial bank money PSP (BIC). If digital euro PSP is the same as commercial bank money PSP, then the same value as Instructing PSP must be filled in.	Financial institution Identification1	M
amount	The amount to be redeemed from the digital euro holding.	Amount	M

userEntry	Identification of the user's digital euro holding in the settlement ledger.	Entry	M
paymentType	Type of the payment.	PaymentType	M
encryptedDefundingObject	Encrypted data fields, see next table.		C, mandatory in case of open defunding

Defunding object data elements – encrypted part

Encrypted part is required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Data element	Element description	Type	Presence indicator
digitalEuroAccount	Unique identification of the UETR's digital euro payment account.	Account reference	M
ownerName	Name of the owner.	Account owner	M
remittanceInformationUnstructured	The field provides additional information about (the purpose of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.	Max140Text	O
remittanceInformationStructured	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	Remittance	O

commercialBankMoneyAccount	Unique identification of the user's non-digital euro payment account.	Account reference	M
accountOwnerName	Name of the owner of the non-digital euro payment account.	Account owner	M
paymentIdentification	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. In case no reference was given by the user, "NOTPROVIDED" must be used.	paymentIdentification1	M

12.1.3.3.2.2. POST /defundings – 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	Description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any	Payment Identification2	M

	time, by any of the parties in the chain. Set by the instructing PSP.		
defundingId	Resource ID generated by DESP	UUID	M
defundingTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT - -ACTC -ACCP	TransactionStatus	M
statusReason	Reason for the negative validation result.	statusReason	C, mandatory in case of failure

12.1.3.3.3. POST /payment-instructions

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payment-instructions	Payment instruction	Endpoint for a payer PSP to submit a payment instruction to start the settlement process of a payment transaction.

12.1.3.3.3.1. POST /payment-instructions – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	-Payment Identification2	M
paymentInstructionObject	See the next table.	-	M
fundingObject	See the next table. This object is mandatory to be included if funding is needed.	-	O
defundingObject	See the next table. This object is mandatory to be included if defunding is needed and when payer and payee have the same digital euro PSP.	-	O

Payment instruction object data elements – unencrypted part

Data element	Element description	Type	Presence indicator
debtorAgent	Unique identification of the payer's PSP (BIC).	Financial institution Identification1	M
creditorAgent	Unique identification of the payee's PSP (BIC).	Financial institution Identification1	M
paymentType	Type of the payment.	PaymentType	M

amount	The amount to be transferred from the payer to the payee. This should be the total amount reflected in the encrypted part of the payment object, if additional amount field is used.	Amount	M
debtorEntry	Unique identification of the payer's digital euro holding in the ledger.	Entry	M
creditorEntry	Unique identification of the payee's digital euro holding in the ledger. This field must be included if payer and payee have the same digital euro PSP.	Entry	C, mandatory in case digital euro payer and payee PSPs are the same
encryptedPaymentInstructionObject	Encrypted data fields, see next table.		C, mandatory in case digital euro payer and payee PSPs are different

Payment instruction object data elements – encrypted part

The encrypted part is only required if payer and payee have different digital euro PSPs.

Data element	Element description	Type	Presence indicator
creditorAccount	Unique identification of the payee's digital euro payment account.	Account Reference	M
creditor	Name of the payee.	PartyDescription1	

ultimateCreditor	Payee party details	PartyDescription	O
debtorAccount	Unique identification of the payer's digital euro payment account.	Account Reference	M
debtor	Name of the payer.	PartyDescription1	M
remittanceInformationUnstructured	The field provides additional information about (the purpose of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.	Max140Text	O
remittanceInformationStructured	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	Remittance	O
purposeCode	Predefined code to indicate the purpose of the payment.	Purpose code	O
paymentIdentification	Resource ID generated by the payee PSP to identify a payment request.	PaymentIdentification1	O
transactionAmount	The transaction amount to be transferred from the payer to the payee.	Amount	M
additionalAmount	Amount paid in addition to the transaction amount, e.g., in case of cashback or tip.	Amount	O
totalAmount	Sum of transaction amount and additional amount.	Amount	C, mandatory if 'additionalAmount' field is present.
originalPaymentId	The resource identification of the payment request that is initiated by the payee PSP at POST /payments endpoint.	UUID	C, mandatory if it is a payee-

			initiated payment
originalUetr	The unique end-to-end Transaction Reference of the payment request initiated by the payee PSP at POST /payments endpoint. OriginalUetr refers to the UETR of the original payment.	UUID	C, mandatory if it is a payee-initiated payment

Funding object data elements - unencrypted part

Data element	Element description	Type	Presence indicator
instructedAgent	Unique identification of the payer's commercial bank money PSP (BIC). If digital euro payer PSP is the same as commercial bank money payer PSP, then the same value as digital euro Payer PSP ID must be filled in.	Financial institution Identification1	M
amount	The amount to be issued in digital euro holding.	Amount	M
encryptedFundingObject	Encrypted data fields, see next section.		C, mandatory in case of open funding

Funding object data elements - encrypted part

Encrypted part is only required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part**' in DESP API POST /fundings.

Defunding object data elements - unencrypted part

Defunding object is required only when defunding is required and when payer and payee have the same digital euro PSP.

Data element	Element description	Type	Presence indicator
instructedAgent	Unique identification of the payee's commercial bank money PSP (BIC). If digital euro payee PSP is the same as commercial bank money payee PSP, then the same value as digital euro payee PSP must be filled in.	Financial institution Identification1	M
amount	The amount to be defunded.		M
encryptedDefundingObject	Encrypted data fields, see next section.		C, mandatory in case of open defunding

Defunding object data elements – encrypted part

Encrypted part is required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Defunding object data elements – encrypted part** in DESP API POST /defundings.

12.1.3.3.3.2. POST /payment-instructions – 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	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
paymentInstructionId	Resource ID generated by DESP to identify a payment transaction	UUID	M
paymentTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT - ACTC	TransactionStatus	M
fundingId	Newly created resource ID for the funding part of the payment transaction.	UUID	C, only required if funding object is present in the request and if validation result is positive as indicated in the field 'paymentTransactionStatus'
fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC	TransactionStatus	C, only required if funding object is present in the request
defundingId	Newly created resource ID for the defunding part of the payment transaction.	UUID	C, only required if defunding object is present in the request and if validation result is positive

			as indicated in the field 'paymentTransactionStatus'
defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC	TransactionStatus	C, only required if defunding object is present in the request
statusReason	Reason for the negative validation result.	statusReason	C, mandatory in case of failure as indicated in the field 'paymentTransactionStatus'

12.1.3.3.4. POST /payments

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payments	payment	Endpoint for the payee PSP to send a request for payment.

12.1.3.3.4.1. POST /payments – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp is used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	M
debtorAgent	Unique identification of the payer's PSP (BIC).	FinancialInstutionIdentification1	M
creditorAgent	Unique identification of the payee's PSP (BIC).	FinancialInstutionIdentification1	M
encryptedPaymentObject	See the next table.	-	M

Payment object data elements – encrypted part

Please note that the data elements in this endpoint will be further elaborated.

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
paymentId	Resource ID generated by the payee PSP to identify a payment request.	UUID	M

expiryDateTime	Date and time at which the payment request expires.	ISODateTime	M
transactionAmount	The amount to be transferred from the payer to the payee.	Amount	M
additionalAmount	Amount paid in addition to the transaction amount, e.g., in case of cashback or tip.	Amount	O
totalAmount	Sum of transaction amount and additional amount.	Amount	C, mandatory if 'additionalAmount' field is present.
creditorAccount	Unique identification of the payee's digital euro payment account.	Account Reference	M
creditor	Information of the payee.	PartyDescription	M
ultimateCreditor	Information of the party	partyDescription	O
debtorAccount	Unique identification of the payer's digital euro payment account.	AccountReference	M
debtor	Information of the payer.	PartyDescription	M
remittanceInformationUnstructured	The field provides additional information about (the purpose	Max140Text	O

	of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.		
remittanceInformationStructured	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	Remittance	O
purposeCode	Predefined code to indicate the purpose of the payment.	Purpose Code	O
paymentIdentification1	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain.	PaymentIdentification1	M

	In case no reference was given by the user, "NOTPROVIDED" must be used.		

12.1.3.3.4.2. POST /payments – 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.

Root

The full payload is encrypted. The payload is the same as in PSP API POST /payments.

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a request to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
paymentStatus	Indication of the success or failure of the request. Allowed values: -RJCT	TransactionStatus	M

	-ACTC		
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'payment Status'

12.1.3.3.5. POST /payments/{payment-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payments/{payment-id}/status-inquiries	Payment	Endpoint for the payer PSP to asynchronously confirm status of a payment request.

12.1.3.3.5.1. POST /payments/{payment-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	Presence indicator	Path/header/ query

paymentId	Resource ID generated by the payee PSP to identify a request for payment.	UUID	M	Path

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
debtorAgent	Unique identification of the payer's PSP (BIC).	FinancialInstutionIdentification1	M
creditorAgent	Unique identification of the payee's PSP (BIC).	FinancialInstutionIdentification1	M
encryptedPaymentStatusObject	See the next table.	-	M

Payment status object encrypted part

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a request to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
paymentStatus	Indication of the success or failure of the request. Allowed values: -RJCT	StatusCode	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as

			indicated at the field 'payment Status'

12.1.3.3.5.2. POST / payments/{payment-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 validation**: HTTP Code 204, without response body.

12.1.3.3.6. GET /payment-instructions/{payment-instruction-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/payments/{payment-id}/status-inquiries	Payment	Endpoint for digital euro payer PSP or digital euro payee PSP to query the status of a payment transaction.

12.1.3.3.6.1. GET /payment-instructions/{payment-instruction-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	Presence indicator	Path/header/ query
payment-instruction-Id	Resource identification generated by DESP to identify a payment transaction.	UUID	M	Path

12.1.3.3.6.2. GET /payment-instructions/{payment-instruction-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.

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	Payment Identification2	M
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, mandatory in case of positive request result as indicated at the field 'payment transaction status'
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, mandatory in case of positive validation as indicated at the field 'payment transaction status' and in case funding or/and defunding

			object was/were included in the original request
paymentTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	M
fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if funding object is present in the request
fundingId	Resource ID generated by the DESP for the funding part of the payment transaction.	UUID	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field ‘payment transaction status’
defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if defunding object is present in the request
defundingId	Resource ID generated by the DESP for the defunding part of the payment transaction.	UUID	C, mandatory if defunding object is present in the request and in case of positive validation as indicated at the field ‘payment transaction status’
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field ‘payment transaction status’

12.1.3.3.7. GET /fundings/{funding-id}/status

This endpoint is used for PSPs to query statuses of fundings.

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/fundings/{funding-id}/status	Funding	This endpoint is for commercial bank money payer or payee PSP to query the status of a funding transaction.

12.1.3.3.7.1. GET /fundings/{funding-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	Presence indicator	Path/header/ query
funding-id	Unique identification of the funding transaction for which the status is requested.	UUID	M	path

12.1.3.3.7.2. GET /fundings/{funding-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

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
fundingTransactionStatus	Indication of the success or failure of the request Allowed values: -RJCT -ACSC	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'funding transaction status'
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, in case of a positive validation result as indicated in the field 'funding transaction status'
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, in case of a positive validation result as indicated in the field 'funding transaction status'

12.1.3.3.8. GET /defundings/{defunding-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/defundings/{defunding-id}/status	Defunding	This endpoint for commercial bank money payer or payee PSP to query the status of a defunding transaction.

12.1.3.3.8.1. GET /defundings/{defunding-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	Presence indicator	Path/header/1uery
defunding-id	Unique identification of the defunding transaction for which the status is requested.	UUID	M	path

12.1.3.3.8.2. GET /defundings/{defunding-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.

Data element	Element description	Type	Presence indicator

paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
defundingTransactionStatus	Indication of the success or failure of the request Allowed values: -RJCT -ACSC	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'defunding transaction status'
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, in case of a positive validation result as indicated in the field 'defunding transaction status'
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, in case of a positive validation result as indicated in the field 'defunding transaction status'

12.1.3.3.9. POST /payments/{payment-id}/status-inquiries

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/payments/{payment-id}/status-inquiries	payment	Endpoint for the payee PSP to query status of a payment request with the payer PSP.

12.1.3.3.9.1. POST /payments/{payment-id}/status-inquiries – Request

Request header:

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

Data element	Element description	Type	Presence indicator	Path/header/ query
payment-id	Resource identification generated by the payee PSP to identify a payment request.	UUID	M	path

Request body data elements

Data element	Element description	Type	Presence indicator
debtorAgent	Unique identification of the payer's PSP (BIC).	FinancialInstutionIdentification1	M

12.1.3.3.9.2. POST /payments/{payment-id}/status-inquiries – 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).*[35]
- **In case of positive technical validation**: HTTP Code 200.

Root

The full payload is encrypted.

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a request to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
paymentStatus	Indication of the success or failure of the request. Allowed values: -RJCT - -ACSC	StatusCode	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'payment Status'

12.1.3.3.10. POST /refunds

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/refunds	Refund	Endpoint to initiate a refund transaction.

[35] In case payer PSP sends back a negative technical validation error, it will be forwarded by DESP with problem+json if specified by the payer PSP in the synchronous response of PSP API POST /payments.

12.1.3.3.10.1. POST /refunds – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp is used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
refundObject	See the table below.	-	M
fundingObject	See the table below. This object is mandatory to be included if funding is needed.	-	O
DefundingObject	See the table below. This object is mandatory to be included if defunding is needed.	-	O

Refund object data elements – unencrypted part

Data element	Element description	Type	Presence indicator

debtorAgent	Unique identification of the payer's PSP (the payee PSP of the original payment that is being refunded).	Financial institution Identification1	M
creditorAgent	Unique identification of the payee's PSP (the payer PSP of the original payment that is being refunded).	Financial institution Identification1	M
paymentType	Type of the payment.	PaymentType	M
amount	The amount to be transferred from the payer to the payee (from the original payee to the original payer). This could be the full amount of the original payment or a lower amount.	Amount	M
debtorEntry	Unique identification of the payer's digital euro holding in the ledger.	Entry	M
creditorEntry	Unique identification of the payee's digital euro holding in the ledger. This field must be included if payer and payee have the same digital euro PSP.	Entry	O
encryptedRefundObject	Encrypted data fields, see next table.		C, mandatory in case digital euro payer and payee PSPs are different

Refund object data elements – encrypted part

Data element	Element description	Type	Presence indicator
creditorAccount	Unique identification of the payee's (original payee's) digital euro payment account.	Account Reference	M

creditor	Name of the payee (original payer).	PartyDescription1	M
debtorAccount	Unique identification of the payer's (original payee's) digital euro payment account.	Account Reference	M
debtor	Name of the payer (original payee).	PartyDescription1	M
remittanceInformationUnstructured	The field provides additional information about (the purpose of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.	Max140Text	O
remittanceInformationStructured	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	Remittance	O
purposeCode	Predefined code to indicate the purpose of the payment.	Purpose Code	O
paymentIdentification	Unique identification, as assigned by the initiating user, to unambiguously identify the transaction. This identification is passed on, unchanged, throughout the entire end-to-end chain. In case no reference was given by the user, "NOTPROVIDED" must be used.	PaymentIdentification1	M
originalPaymentInstructionId	The resource identification of the payment transaction that is being refunded.	UUID	M
originalUetr	The unique end-to-end Transaction Reference of the payment transaction that is being refunded. OriginalUetr	PaymentIdentification2	M

	refers to the UETR of the original payment.		

Funding object data elements - non-encrypted part

Same as '**Funding object data elements – non-encrypted part**' in DESP API POST /payment-instructions.

Funding object data elements - encrypted part

The encrypted part is required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part** in DESP API POST /fundings.

12.1.3.3.10.2. POST /refunds – 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	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification1	M

refundId	Resource identification generated by DESP to identify a refund payment transaction.	UUID	M
refundTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC	TransactionStatus	M
fundingId	Newly created resource ID for the funding part of the payment transaction.	UUID	C, only required if funding object is present in the request and if validation result is positive as indicated in the field ‘refund transaction status’
fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC	TransactionStatus	C, only required if funding object is present in the request
defundingId	Newly created resource ID for the defunding part of the payment transaction.	UUID	C, mandatory if defunding object is present in the request and in case of positive validation as indicated at the field ‘refund transaction status’
defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if defunding object is present in the request

statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'refund transaction status'

12.1.3.3.11. GET /refunds/{refund-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/refunds/{refund-id}/status	Refund	Endpoint for digital euro payer PSP or digital euro payee PSP to query the status of a refund transaction.

12.1.3.3.11.1. GET /refunds/{refund-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	Presence indicator	Path/header/ query
refund-id	Resource identification generated by DESP to identify a refund transaction.	UUID	M	path

12.1.3.3.11.2. GET /refunds/{refund-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.

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, mandatory in case of positive request result as indicated at the field 'refundTransactionStatus'
refundTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	M
fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if funding object is present in the request
fundingId	Resource ID generated by the DESP for the funding part of the payment transaction.	UUID	C, mandatory if funding object is present in the request and in case of positive validation as

			indicated at the field 'refundTransactionStatus'
defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if defunding object is present in the request
defundingId	Resource ID generated by the DESP for the defunding part of the payment transaction.	UUID	C, mandatory if defunding object is present in the request and in case of positive validation as indicated at the field 'refundTransactionStatus'
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'refundTransactionStatus'

12.1.3.3.12. GET /queries/enduser-entries

Applicable endpoints and methods:

Method	Endpoint	Resource	Description
GET	/v1/queries/end-user-entries ?entryId=<entryId>	QUERIES	User entry(ies) query

12.1.3.3.12.1. GET /queries/end-user-entries – Request

Request header:

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

Data element	Element description	Type	Presence indicator	Path/header/query

entryId	The identifier that identifies the entry.	Entry	C, either entry identifier or Digital euro PSP identifier to be filled	query

12.1.3.3.12.2. GET /queries/end-user-entries – 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.

Data element	Element description	Type	Presence indicator
dateTime	Timestamp of the generation of the response.	ISODateTime	M
digitalEuroAgent	The BIC of the digital euro PSP that manages the entries.	financialInstitutionIdentification1	M
entryId	The identifier that identifies the entry.	Entry	M
availableAmount	The amount available related to the entry.	Amount	M
reservedAmount	The amount reserved on the entry.	Amount	M
totalAmount	The sum of available and reserved amount related to the entry.	Amount	M

12.1.3.3.13. GET /reports/transactions

Applicable endpoints and methods:

Method	Endpoint	Resource	Description
GET	/v1/reports/transactions/?reportId=<reportId>	REPORTS	Transactions report

12.1.3.3.13.1. GET /reports/transactions – Request

Request header:

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

Data element	Element description	Type	Presence indicator	Path/header/1uery
reportId	The ID of the report as pushed by the notification, or retrieved from the list of available reports	uuid	M	query

12.1.3.3.13.2. GET /reports/transactions – 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.

Data element	Element description	Type	Presence indicator
reportedDate	The date for which the transactions are included.	ISODate	M

currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code.	Currency Code	M
digitalEuroAgent	The BIC of the digital euro PSP for which the report is generated.	financialInstitutionIdentification1	M
reportStartDateTime	Start timestamp for which the account statement is issued.	ISODatetime	M
reportEndDateTime	End timestamp for which the account statement is issued.	ISODatetime	M
The following fields repeat per each transaction			
originatingDigitalEuroAgent	The BIC of the digital euro PSP originating the transaction.	financialInstitutionIdentification1	M
amount	The amount of the transaction.	Amount	M
paymenInstructiontId	Resource ID generated by DESP to identify a payment instruction.	UUID	M
paymentType	Type of the payment.	PaymentType	M
settlementBusinessDay	RTGS business day on which the payment instruction is settled	IsoDate	C, mandatory in case of successful settlement
settlementDateTime	The timestamp when the settlement took place.	ISODateTime	C, mandatory in case of successful settlement

12.1.3.3.14. GET /available-reports

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/ reports/available-reports?report-type=<report-type>	REPORTING	Endpoint for recipient to retrieve the statement of account turnover.

12.1.3.3.14.1. GET /available-reports

Request header:

- **Technical header:** please refer to section 5.3.3.1.
- **API specific header:**

Data element	Element description	Type	Presence indicator	Path/header/ query
reportType	Indicates the type of report. Values: - DEUR: Digital euro report - DETR: Digital euro transactions report - FECR: Fee calculation report - REDR: Repository data report	Report Type	O	Query

12.1.3.3.14.2. GET /available-reports – Response

Response header

- **Technical header:** please refer to section 5.3.3.1
- **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.

The report body consist of an array of the following attributes

Data element	Element description	Type	Presence indicator
reportType	Indicates the type of report. Values: - TRRE; Transactions Report	Report Type	M
The below data elements repeat per available report instance			
reportId	Unique identification of the report that is generated by DESP and allows the PSP to GET the report.	uuid	M
reportMode	Indicates whether the report is requested in full mode or delta mode. Values: - FULL - DELTA	Report Mode	M
reportRtgsDate	The RTGS date for which the report is available.	ISODate	O
reportCalenderDate	The calendar date for which the report is available.	ISODate	O
reportStartDateTime	Start timestamp for which the report is issued.	ISODateTime	C, in case of delta mode only
reportEndDateTime	End timestamp for which the report is issued.	ISODateTime	C, in case of delta mode only

12.1.3.4. PSP API for PSPs to receive requests from DESP

This section describes in detail all API endpoints for PSPs to receive requests from DESP (hereafter **PSP API**).

12.1.3.4.1. POST /fundings

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/fundings	Funding	This endpoint is used for the commercial bank money PSP to receive and validate funding requests.

12.1.3.4.1.1. POST /fundings – Request

Funding requests might result from other endpoints in open funding case, such as DESP API:

- POST /payment-instructions
- POST /refunds

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M

fundingObject	See the next table.	Funding Object	M

Funding object data elements – unencrypted section

The user entry that was specified by the instructing PSP will not be forwarded to Instructed PSP.

Data element	Element description	Type	Presence indicator
fundingId	Resource ID generated by DESP to identify the funding transaction or the funding leg of a payment/reservation transaction.	UUID	M
instructingAgent	Unique identification of the user's digital euro PSP (BIC).	Financial institution Identification1	M
InstructedAgent	Unique identification of the user's commercial bank money PSP (BIC).	Financial institution Identification1	M
amount	The amount to be issued in digital euro holding.	Amount	M
paymentType	Type of the payment.	PaymentType	M
encryptedFundingObject	Encrypted data fields, see next section.		M

Funding object data elements – encrypted section

Same as '**Funding object data elements – encrypted part**' in DESP API POST /fundings.

12.1.3.4.1.2. POST /fundings – 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.

Response Body

Root

Data element	Description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
fundingTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACCP	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'funding transaction status'

12.1.3.4.2. POST /fundings/{funding-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/fundings/{funding-id}/status	Funding	Endpoints for DESP to provide status of a funding transaction

12.1.3.4.2.1. POST /fundings/{funding-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	Presence indicator	Path/header/ query
funding-id	Resource ID generated by DESP to identify the funding.	UUID	M	path

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
fundingTransactionStatus	Indication of the success or failure of the request Allowed values: -RJCT	TransactionStatus	M

	-ACSC		
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'funding transaction status'
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, mandatory in case of successful settlement
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, mandatory in case of successful settlement

12.1.3.4.2.2. POST /fundings/{funding-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 204, without response body.

12.1.3.4.3. POST /defundings

Applicable endpoint and method:

Method	Endpoint	Resource	Description

POST	/v1/defundings	Defunding	This endpoint is for commercial bank money PSP to receive and validate defunding requests.

12.1.3.4.3.1. POST /defundings – Request

Defunding requests might result from other endpoints from open defunding, such as DESP API:

- POST /payment-instructions
- POST /refunds

or response to PSP API:

- POST /payment-instructions
- POST /refunds

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be	paymentIdentification2	M

	located at any time, by any of the parties in the chain. Set by the instructing PSP.		
defundingObject	See the next table.	-	M

Defunding object data elements – unencrypted section

The user entry, that was specified by the instructing PSP will not be forwarded to instructed PSP.

Data element	Element description	Type	Presence indicator
defundingId	Resource ID generated by DESP to identify the defunding transaction or the defunding leg of a payment transaction.	UUID	M
instructingAgent	Unique identification of the user's digital euro PSP (BIC).	Financial institution Identification1	M
InstructedAgent	Unique identification of the user's commercial bank money PSP (BIC).	Financial institution Identification1	M
amount	The amount to be redeemed from the digital euro holding.	Amount	M
paymentType	Type of the payment.	PaymentType	M
encryptedDefundingObject	Encrypted data fields, see next section.		M

Defunding object data elements – encrypted section

Same as '**Defunding object data elements – encrypted part** in DESP API POST /defundings.

12.1.3.4.3.2. POST /defundings – 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.

Response Body

Root

Data element	Description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
defundingTransactionStatus	Indication of the success or failure of the request Allowed values: -RJCT -ACCP	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'funding transaction status'

12.1.3.4.4. POST /defundings/{defunding-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/defundings/{defunding-id}/status	Defunding	Endpoints for DESP to provide status of a defunding transaction

12.1.3.4.4.1. POST /defundings/{defunding-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	Presence indicator	Path/header/1uery
defunding-id	Resource ID generated by DESP to identify the defunding.	UUID	M	path

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	paymentIdentification2	M
defundingTransactionStatus	Indication of the success or failure of the request Allowed values: -RJCT -ACSC	TransactionStatus	M

statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'funding transaction status'
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, mandatory in case of successful settlement
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, mandatory in case of successful settlement

12.1.3.4.4.2. POST /defundings/{defunding-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 204, without response body.

12.1.3.4.5. POST /payment-instructions

Applicable endpoint and method:

Method	Endpoint	Resource	Description

POST	/v1/payment-instructions	Payment instruction	This endpoint is for DESP to forward payment instruction from digital euro payer PSP to payee PSP.

12.1.3.4.5.1. POST /payment-instructions – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
acceptanceDateTime	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	Payment Identification2	M
paymentInstructionObject	See the next table.	-	M

Payment instruction object data elements - unencrypted part

The payer entry that was specified by the payer PSP will not be forwarded to the payee PSP.

Data element	Element description	Type	Presence indicator
paymentInstructionId	Resource ID generated by DESP to identify a payment transaction	UUID	M
debtorAgent	Unique identification of the payer's PSP (BIC).	Financial institution Identification1	M
creditorAgent	Unique identification of the payee's PSP (BIC).	Financial institution Identification1	M
paymentType	Type of the payment.	PaymentType	M
amount	The amount to be transferred from the payer to the payee. This should be the total amount reflected in the encrypted part of the payment object, if additional amount field is used.	Amount	M
encryptedPaymentInstructionObject	Encrypted data fields, see next section.		M

Payment instruction object data elements - encrypted part

Same as '**Payment instruction object data elements – encrypted part**' in DESP API POST /payment-instructions.

12.1.3.4.5.2. POST /payment-instructions – 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.

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
paymentTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACCP	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'payment transaction status'
paymentInstructionObject	See the next table.	-	C, mandatory in case of positive validation as indicated at the field 'payment transaction status'
paymentDefundingObject	See the next table. This object is mandatory to be included if defunding is needed.	-	O

Payment Instruction object data elements – unencrypted part

Data element	Element description	Type	Presence indicator
creditorEntry	Unique identification of the user's digital euro holding in the ledger.	Entry	M

Payment defunding object data elements – unencrypted part

Same as '**Defunding object data elements – unencrypted part**' in DESP API POST /payment-instructions.

Payment defunding object data elements – encrypted part

The encrypted part is required for open defunding case when the digital euro payee PSP is different from the commercial bank money payee PSP.

Same as '**Defunding object data elements – encrypted part** in DESP API POST /defundings.

12.1.3.4.6. POST /payment-instructions/{payment-instruction-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payment-instructions/{payment-instruction-id}/status	Payment	Endpoint for digital euro payer and/or payee PSP to receive the status of a payment instruction from DESP

12.1.3.4.6.1. POST /payment-instructions/{payment-instruction-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	Presence indicator	Path/header/ query
payment-instruction-id	Resource ID generated by DESP to identify a payment transaction.	UUID	M	path

Request body data elements:

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, mandatory in case of positive validation as indicated at the field 'payment transaction status'
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, mandatory in case of successful settlement
paymentTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	M

fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if funding object is present in the request
fundingId	Resource ID generated by the DESP for the funding part of the payment transaction.	UUID	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field ‘payment transaction status’
defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if defunding object is present in the request
defundingId	Resource ID generated by the DESP for the defunding part of the payment transaction.	UUID	C, mandatory if defunding object is present in the request and in case of positive validation as indicated at the field ‘payment transaction status’
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field ‘payment transaction status’

12.1.3.4.6.2. POST /payment-instructions/{payment-instruction-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 204, without response body.

12.1.3.4.7. POST /payments

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payments	Payment	Endpoint for the digital euro payer PSP to receive a payment request.

12.1.3.4.7.1. POST /payments – Request

Request header:

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

Request body data elements:

Payload is the same as in 'Request body data elements' in DESP API POST /payments

12.1.3.4.7.2. POST /payments – 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.

The full payload must be encrypted.

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a request to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
paymentStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACTC	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'paymentStatus'

12.1.3.4.8. POST / payments/{payment-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/payments/{payment-id}/status-inquiries	Payment	Endpoint for the digital euro payee PSP to receive status confirmation of a payment request from the digital euro payer PSP.

12.1.3.4.8.1. POST /payments/{payment-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	Presence indicator	Path/header/ query
payment-id	Resource ID generated by the payee PSP to identify a payment request.	PaymentIdentification	M	path

Request body data elements:

Payload is the same as in 'Request body data elements' in DESP API POST /payments/{payment-id}/status

12.1.3.4.8.2. POST /payments/{payment-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 204, without response body.

12.1.3.4.9. POST /payments/{payment-id}/status-inquiries

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/payments/{payment-id}/status-inquiries	payment	Endpoint for the digital euro payer PSP to receive query from the digital euro payee PSP for the status of a payment request.

12.1.3.4.9.1. POST /payments/{payment-id}/status-inquiries – Request

Request header:

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

Data element	Element description	Type	Presence indicator	Path/header/ query
payment-id	Resource identification generated by the payee PSP to identify a payment request.	UUID	M	path

Request body data elements

Data element	Element description	Type	Presence indicator

debtorAgent	Unique identification of the payer's PSP (BIC).	FinancialInstutionIdentification1	M

12.1.3.4.9.2. POST /payments/{payment-id}/status-inquiries – 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).[36]
- **In case of positive technical validation**: HTTP Code 200.

Root

The full payload is encrypted.

Data element	Element description	Type	Presence indicator
paymentIdentification	Includes UETR: unique end-to-end transaction reference, a unique, unalterable reference which allows a request to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
paymentStatus	Indication of the success or failure of the request. Allowed values: -RJCT -RCVD	StatusCode	M

[36] In case payer PSP sends back a negative technical validation error, it will be forwarded by DESP with problem+json if specified by the payer PSP in the synchronous response of PSP API POST /payments.

	-ACCP -ACSC		
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'payment Status'

12.1.3.4.10. POST /refunds

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/refunds	Refund	Endpoint for DESP to forward refund instruction from the digital euro payer (original payee) PSP to digital euro payee (original payer) PSP.

12.1.3.4.10.1. POST /refunds – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Presence indicator

acceptanceDateTime	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process and should not be altered by other PSPs.	ISODateTime	M
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the	PaymentIdentification2	M
refundObject	See the table below.	-	M

Refund object data elements – unencrypted part

The payer entry that was specified by the payer PSP (the payee PSP of the original payment that is being refunded) will not be forwarded to the payee PSP (the payer PSP of the original payment that is being refunded).

Data element	Element description	Type	Presence indicator
refundId	Resource identification generated by DESP to identify a refund payment transaction.	UUID	M
debtorAgent	Unique identification of the payer's PSP (the payee PSP of the original payment that is being refunded).	Financial institution Identification1	M
creditorAgent	Unique identification of the payee's PSP (the payer PSP of the original payment that is being refunded).	Financial institution Identification1	M
paymentType	Type of the payment.	PaymentType	M
amount	The amount to be transferred from the payer to the payee (from the original payee to the original payer).	Amount	M

	This could be the full amount of the original payment or a lower amount.		
EncryptedRefundObject	Encrypted data fields, see next section.		M

Refund object data elements – encrypted part

Same as the content '**Refund object data elements – encrypted part**' included in the request DESP API POST /refunds.

12.1.3.4.10.2. POST /refunds – 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.

Root

Data element	Element description	Type	Presence indicator
paymentIdentification	Unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of	PaymentIdentification2	M

	the parties in the chain. Set by the instructing PSP.		
refundTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACCP	TransactionStatus	M
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'refundTransactionStatus'
refundObject	See the table below.	-	M
defundingObject	See the next table. This object is mandatory to be included if defunding is needed.	-	O

Refund object data elements – unencrypted part

Data element	Element description	Type	Presence indicator
creditorEntry	Unique identification of the payee's digital euro holding in the ledger. This field must be included if payer and payee have the same digital euro PSP.	Entry	O

Defunding object data elements – unencrypted part

Same as '**Defunding object data elements – encrypted part**' in DESP API POST /payment-instructions.

Defunding object data elements – encrypted part

The encrypted part is required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Defunding object data elements – encrypted part** in DESP API at section POST /payment-instructions.

12.1.3.4.11. POST /refunds/{refund-id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/refunds/{refund-id}/status	Refund	The endpoint is for the digital euro payee and/or payer PSP to receive the status of a refund transaction from DESP.

12.1.3.4.11.1. POST /refunds/{refund-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	Presence indicator	Path/header/1uery
refund-id	Resource identification generated by DESP to identify a refund transaction.	UUID	M	path

Request body data elements:

Root

Data element	Element description	Type	Presence indicator

paymentIdentification	Includes UETR: unique end-to-end transaction reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	PaymentIdentification2	M
settlementDateTime	Time and date of the moment the settlement was recorded in DESP.	ISODateTime	C, in case of a positive validation result as indicated in the field ‘payment transaction status’
settlementBusinessDay	Business day of the settlement which was recorded in dedicated cash account (DCA) in DESP.	ISODate	C, mandatory in case of successful settlement
refundTransactionStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	M
fundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	M
fundingId	Resource ID generated by the DESP for the funding part of the payment transaction.	UUID	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field ‘refundTransactionStatus’

defundingStatus	Indication of the success or failure of the request. Allowed values: -RJCT -ACSC	TransactionStatus	C, mandatory if defunding object is present in the request
defundingId	Resource ID generated by the DESP for the defunding part of the payment transaction.	UUID	C, mandatory if defunding object is present in the request and in case of positive validation as indicated at the field 'refundTransactionStatus'
statusReason	Reason for the negative business validation result.	statusReason	C, mandatory in case of negative validation as indicated at the field 'refundTransactionStatus'

12.1.3.4.11.2. POST /refunds/{refund-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 204, without response body.

12.1.3.4.12. POST /notifications/report-notifications

Applicable endpoint and method

Method	Endpoint	Resource	Description
POST	/v1/notifications/report-notifications	NOTIFICATION	Report ready notification to PSP.

12.1.3.4.12.1. POST /notifications/report-notifications – Request

Request header:

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

Request body data elements

Data element	Element description	Type	Presence indicator
Agent	The BIC of the digital euro PSP for which the report will be generated.	finacialInstitutionIdentification1	M
reportType	Please see the relevant reference data table.	Report Type	M
reportId	Unique Identification of the generated report	uuid	M
reportMode	Indicates whether the report is requested in full mode or delta mode. Values: - FULL - DELTA	Report Mode	M
reportRtgsDate	The RTGS date for which the report is available.	ISODate	O
reportCalenderDate	The calendar date for which the report is available.	ISODate	O
reportStartDateTime	Start timestamp for which the report is issued.	ISODateTime	C, in case of delta mode only
reportEndDateTime	End timestamp for which the report is issued.	ISODateTime	C, in case of delta mode only

12.1.3.4.12.2. POST /notifications//report-notifications – 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 204.

Annex A: Reservations v0.90 carried-over content for information only

Disclaimer

This annex is included for completeness and contains content carried over from v0.90. The content has not been further updated or reviewed as part of v0.91. It is therefore provided for information only and is not subject to additional review in this release.

The content will be reviewed, updated and incorporated into the main specification body in a future release.

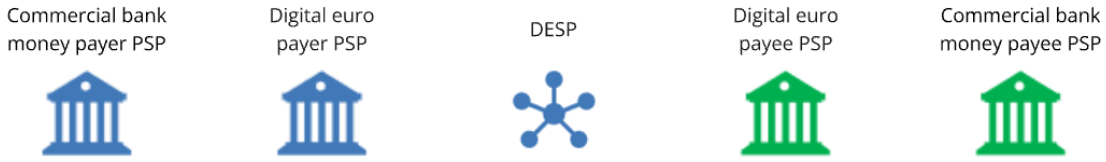
A.1 Service description

A.1.1 Distributing PSP requirements

A.1.1.1 Functional description

The section below shows the different types of transactions that distributing PSPs shall be able to support.

Funding transaction



Funding is the process by which a digital euro user acquires digital euros in exchange for either cash or commercial bank money, thereby creating a direct liability of the Eurosystem[37] to that digital euro user. It can be either manual or automated/scheduled, following pre-defined schedules or rules. The difference between a manual and an automated/scheduled funding lies on the PSP's side – PSPs store the schedules/rulesets and trigger the funding payment request once the conditions are met. From DESP perspective, the request content is identical in both cases. A scenario in which a digital euro transaction requires debiting a non-digital euro payment account held at another PSP than the user's digital euro PSP is referred to as '**open funding**'.

[37] The Eurosystem comprises the European Central Bank and the national central banks of the Member States whose currency is the euro.

Defunding transaction

Defunding is the process whereby a digital euro user exchanges digital euro with cash or commercial bank money. It can be manual or automated/scheduled, with pre-defined schedules or rules. A scenario in which a digital euro transaction requires crediting a non-digital euro payment account held at another PSP than the user's digital euro PSP is referred to as '**open defunding**'.

Payment transaction

A digital euro payment transaction is initiated by either payer or payee PSP and confirmed by the corresponding PSP. DESP performs settlement once the settlement data and confirmation are received from both the payer and payee PSPs. There are different types of payment use cases in digital euro, namely: P2P, e/m-Commerce, and Point of Sale (POS).

Combined payment transaction

A combined transaction is a digital euro transaction involving payment with funding (*reverse waterfall* - if the user does not have sufficient digital euro holdings) or payment with defunding (*waterfall* - if the user's digital euro holding limit is reached). If the digital euro PSP and a commercial bank money PSP are different, it is referred to a combined transaction with an *open (de)funding*.

Reservation transaction

A reservation transaction is a digital euro payment transaction subject to pre-authorisation between a business user and an individual user. The user authorises that a certain amount is reserved for a specific purpose (for specific merchant and services) and the merchant can claim the reserved funds at a later time. A reservation transaction is created following the same steps as a payment transaction. Instead of settlement of a payment, a reservation is recorded, and funds are moved from the available balance to the reserved balance.

Refund transaction

A refund is a reversal (in whole or in part) of an earlier payment initiated by a merchant, usually at the payer's request. A refund always requires funding (as business users have a zero holding limit) and may require defunding on the payer's side.

A.1.1.2 Interface description

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

Introduction of the settlement payload structure is required since it differs from the APIs utilised by other services. The structure of the payload can be summarised as follows:

- **Header** contains metadata about the request. It includes generic data elements that are used in all API endpoints, such as content-type, and specific values only used for certain endpoints.
- **Payload**
    - **Root** contains top-level data elements of the JSON payload structure, such as UETR, acceptance timestamp and objects.
    - **Object** contains collections of data elements and is nested within the root.

Settlement payload structure summary

Element	Encryption	Condition to be included in the payload
UETR	Unencrypted	Mandatory for all transactions.
Acceptance timestamp	Unencrypted	Mandatory for all transactions.
Payment object	Unencrypted	Mandatory in case the message concerns a payment transaction.
	Encrypted	Included if payer and payee PSPs are different parties, as the content needs to be forwarded to the other PSP.
Reservation (payment) object	Unencrypted	Mandatory in case the message concerns a reservation transaction, or in case the message concerns settlement of a reservation transaction, otherwise not present.
	Encrypted	Included if payer and payee PSPs are different parties and that the content needs to be forwarded to the other PSP.
Refund object	Unencrypted	Mandatory in case the message concerns a refund transaction.
	Encrypted	Included if payer and payee PSPs are different parties and that the content needs to be forwarded to the other PSP.
Funding object[38]	Unencrypted	Only required if payer's digital euro balance is lower than the transaction amount. Mandatory in case the message concerns a funding transaction.
	Encrypted	Included if the digital euro and commercial bank money PSPs are different parties and the content needs to be forwarded to the other PSP.
Defunding object[39]	Unencrypted	Only required if the transaction results in the payee's digital euro balance exceeding payee's holding limit. Mandatory in case the message concerns a defunding transaction.
	Encrypted	Included if the digital euro and commercial bank money PSPs are different parties and that the content needs to be forwarded to the other PSP.

[38] A funding object could be included in the response (from the PSP to DESP only) to a payment request, reservation request and reservation modification, if funding is required.
[39] A defunding object could be included in the response (from the PSP to DESP only) to a payment instruction and refunds, if defunding is required

Similarly, which data elements are present in settlement notifications and responses received by a PSP depends on the role of the PSP and the context of the transaction.

Settlement status structure summary

Element	Condition to be included in the payload
Payment ID and status	Mandatory in case the transaction request contains a payment object or refund object. Payment ID is present only if the validation result is positive. Only received by the payer's and payee's digital euro PSP.
Reservation ID and status	Mandatory in case the transaction request contains a reservation object. Reservation ID is present only if the validation result is positive. Only received by the payer's and payee's digital euro PSP.
Funding ID and status	Mandatory in case the transaction request contains a funding object. Funding ID is present only if the validation result is positive. Only received by the requester and receiver of the funding request (the payer's digital euro PSP and the payer's commercial bank money PSP).
Defunding ID and status	Mandatory in case the transaction request contains a defunding object. Defunding ID is present only if the validation result is positive. Only received by the requester and receiver of the defunding request (the payee's digital euro PSP and the payee's commercial bank money PSP).

Payload example: initiate a funding transaction (DESP API POST /fundings)


```
{
  "acceptanceTimestamp": "2025-01-01T13:00:00.999Z",
  "uetr": "3fc3d0e9-1efb-4eef-ace6-d9d59b62fec5",
  "fundingObject": {
    "instructingPSP": {
      "bicfi": "PARTYAMMXXX"
    },
    "instructedPSP": {
      "bicfi": "PARTYBMMXXX"
    },
    "amount": {
      "currency": "EUR",
      "amount": "250.00"
    },
    "endUserEntry": "string",
    "paymentType": "P2P",
    "fundingData": {
      "encryptionKey": "#@!~W^@FVVJH!@#Y*@^TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)
JD)(J@)#DJ@)D)(#QKG&*#%E%!$122610)",
```

```
      "encryptedFundingData": "U2FsdGVkX19lqQIW3Hec8fzP4a3LIal/VZFi942bB7f97Jy+HtZNoS7kkIJXozOnnGH2ORhqurP
JB9lqETiirfMTg06wYXGihU/Ded3Y+/J/K5auoo9Pc5IbVM//CMxd1sBT06vpEznDMLHAquovBOrPeday1gCwELVm"
    }
  }
}
```


Payload example: initiate a payment transaction with open funding (reverse waterfall) (DESP API POST /payment-instructions)


```
{
  "acceptanceTimestamp": "2025-01-01T13:00:00.999Z",
  "uetr": "3fc3d0e9-1efb-4eef-ace6-d9d59b62fec5",
  "paymentObject": {
    "payerPSPId": {
      "bicfi": "PARTYAMMXXX"
    },
    "payeePSPId": {
      "bicfi": "PARTYBMMXXX"
    },
    "paymentType": "P2P",
    "amount": {
      "currency": "EUR",
      "amount": "299.99"
    },
    "payerEntry": "string",
    "paymentInstructionData": {
      "encryptionKey": "#@!~W^@FVVJH!@#Y*@^TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)
JD)(J@)#DJ@)D)(#QKG&*#%E%!$122610)",
      "encryptedpaymentInstructionData": "#@!~W^@FVVJH!@#Y*@^TD@#IEHD@(#*DO#(E@#_E)()(@#)JD)(J@)#DJ@)D)(#Q
KG&*#%E%!$122610)#@!~W^@FVVJH!@#Y*@^TD@#IEHD@(#*DO#(E@#_E)()(@#)JD)(J@)#DJ@)D)(#QKG&*#%E%!$122610)"
    }
  },
  "fundingObject": {
    "instructedPSPId": {
      "bicfi": "PARTYCMMXXX"
    },
    "amount": {
      "currency": "EUR",
      "amount": "100.00"
    },
    "fundingData": {
      "encryptionKey": "#@!~W^@FVVJH!@#Y*@^TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)JD)TD@#I#(E@#_E)()(@#)
JD)(J@)#DJ@)D)(#QKG&*#%E%!$122610)",
      "encryptedFundingData": U2FsdGVkX19lqQIW3Hec8fzP4a3LIal/VZFi942bB7f97Jy+HtZNoS7kkIJXozOnnGH2ORhqurPJ
B9lqETiirfMTg06wYXGihU/Ded3Y+/J/K5auoo9Pc5IbVM//CMxd1sBT06vpEznDMLHAquovBOrPeday1gCwELVm+doxah2KqR2xkH2itH
PiuxOTf2w4JykIhcs38G3yK5mUQL2P1SkdKOuymwCwJJbI3YW1Oel1gXDaYRbUF9RAF41KRQ1fWW7eXoEtY50kDyuBglW2V8j "
    }
  }
}
```


A.1.1.2.1 Overview of covered scenarios

The section below presents a selection of baseline scenarios that cover the key flows in the digital euro settlement process, taking into account:

- the type of transaction ((de)funding, (combined) payment, reservation, refund);
- the party that initiates the process (payer or payee);

- the role a PSP performs in the process (e.g. the same PSP performing different roles for one transaction, or multiple PSPs for different parts of the transaction);

The description of API calls includes information on whether the steps in the process are conditional (e.g. for funding and defunding).

A.1.1.2.1.1 Reservations

A.1.1.2.1.1.1 Payee-initiated reservation creation with open funding

The sections below describe the reservation creation process initiated by the payee PSP in which the payer and payee PSPs are different, and funding of the payer's digital euro payment account is required.

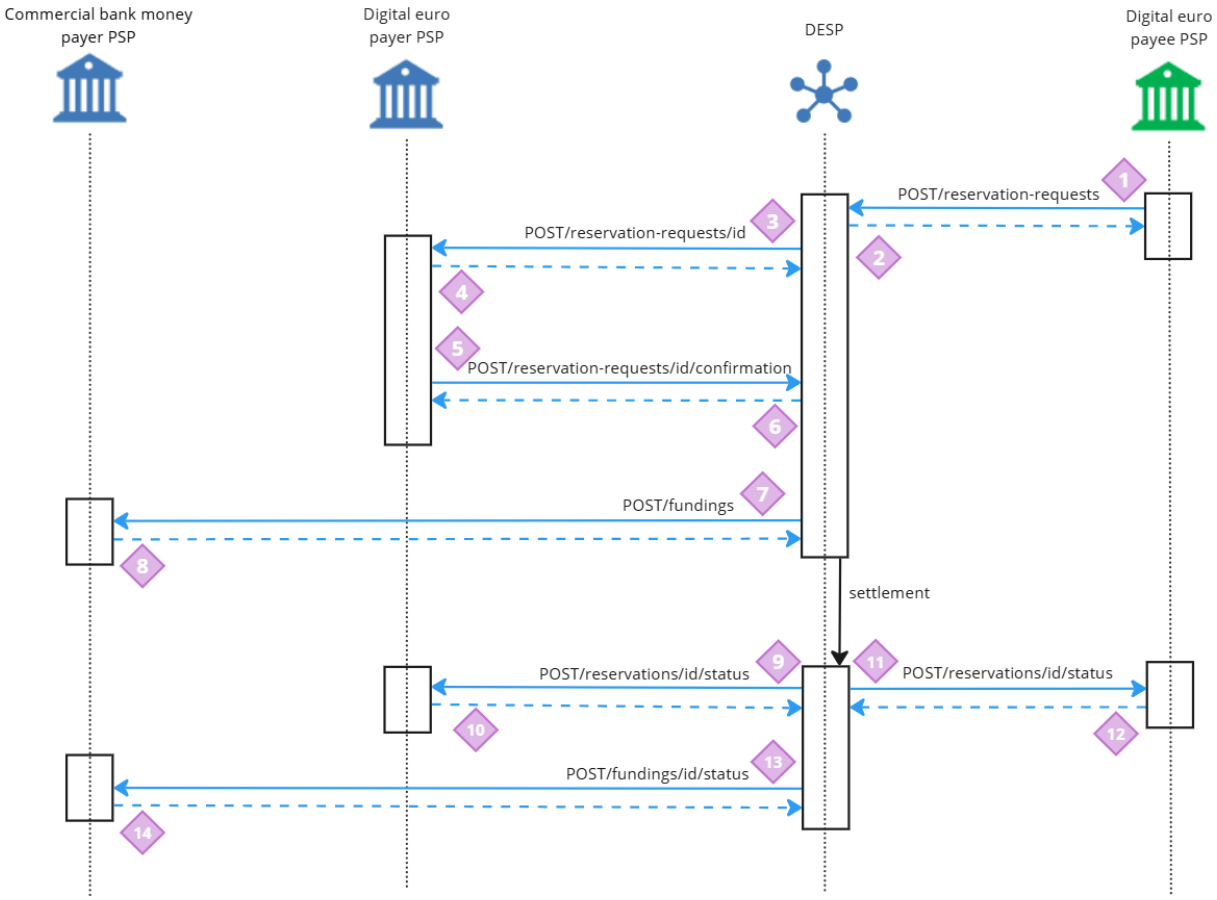


Figure 1 Payee initiated reservation creation with open funding

API call	Description	Covered in section

1	Digital euro payee PSP sends a request with the reservation object with partial settlement data.	DESP API POST /reservation-requests - Request
2	Synchronous response from DESP to confirm the receipt of the request sent in API call 1.	DESP API POST /reservation-requests - Response
3	DESP forwards the request which contains reservation object from API call 1 to digital euro payer PSP.	PSP API POST /reservation-requests – Request
4	Synchronous response from digital euro payer PSP to confirm the receipt of the request received at API 3.[40]	PSP API POST /reservation-requests - Response
5	Asynchronous response from the digital euro payer PSP to send back the validation result and (if the validation result is positive) the remaining settlement data for reservation object and partial settlement data in the funding object..	DESP API POST /reservation-requests/{id}/confirmation - Request
6	Synchronous response from DESP to confirm receipt of the request received in API call 5.	DESP API POST /reservation-requests/{id}/confirmation - Response
7	DESP forwards funding request from API call 5 to commercial bank money payer PSP.	PSP API POST /fundings - Request
8	Synchronous response from commercial bank money payer PSP that includes the validation result and settlement data (if the validation result is positive).	PSP API POST /fundings - Response
9	DESP sends status of the reservation transaction simultaneously with API call 11 back to digital euro payer PSP.	PSP API POST /reservations/{id}/status - Request

[40] Between API call 4 and API call 5, digital euro PSP might need to contact other services for example, to decode a surrogate value in case of an NFC payment, or to gather the risk score. At synchronous response at API call 4, the PSP could also already reject the transaction based on technical validation result.

10	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /reservations/{id}/status – Response
11	DESP sends status of the reservation transaction simultaneously with API call 9 back to digital euro payee PSP.	PSP API POST /reservations/{id}/status - Request
12	Synchronous response from digital euro payee PSP to confirm receipt of the status notification	PSP API POST /reservations/{id}/status – Response
13	DESP sends status of the funding back to commercial bank money payer PSP.	PSP API POST /fundings/{id}/status - Request
14	Synchronous response from commercial bank money payer PSP to confirm receipt of the status notification.	PSP API POST /fundings/{id}/status - Response

A.1.1.2.1.1.2 Reservation lifecycle management

Management of a reservation may involve decreasing or increasing the reserved amount and shortening or extending an expiry date. In case of an increase of the amount, an additional funding from the commercial bank money payer PSP may be required. In case the reservation transaction needs to be cancelled, the new amount should be set to 0. The diagram below depicts the scenario in which the digital euro PSP and commercial bank money PSP are different (open funding).

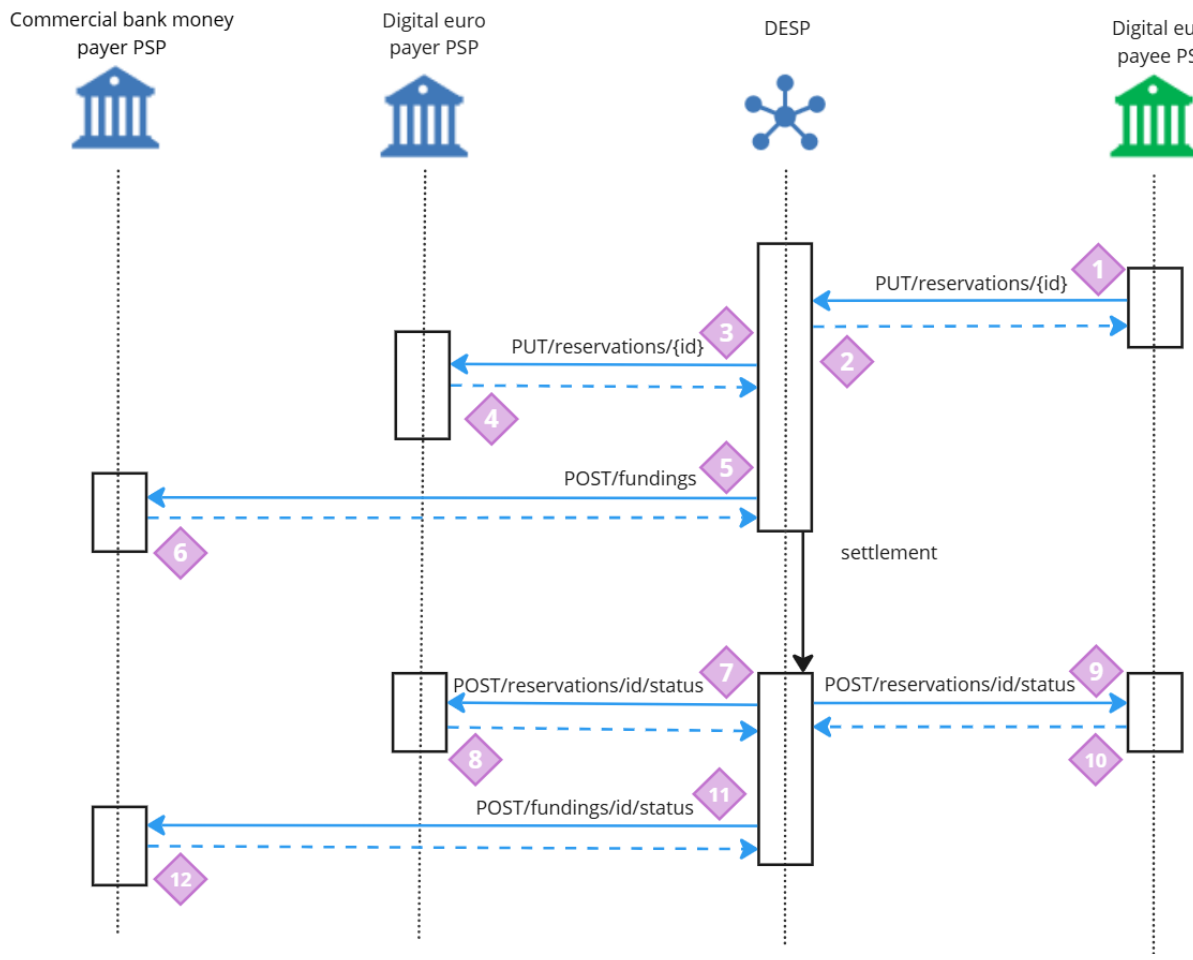


Figure 2 Reservation lifecycle management

API call	Description	Covered in section
1	Digital euro payee PSP sends the request with a reservation object including updated amount and/or updated expiry date.	DESP API PUT /reservations/{id} - Request
2	Synchronous response from DESP to confirm receipt of the message sent in API call 1.	DESP API PUT /reservations/{id} – Response
3	DESP forwards the request which contains payment object from API call 1 to digital euro payer PSP.	PSP API PUT /reservations/{id} - Request

4	Synchronous response from the digital euro payer PSP to send back validation result and settlement data. The funding object can be included if the new reservation amount is higher than the previous one and funding is required.	PSP API PUT /reservations/{id} - Response
5	DESP forwards funding request from API call 4 to commercial bank money payer PSP.	PSP API POST /fundings - Request
6	Synchronous response from commercial bank money payer PSP that includes the validation result and settlement data (if the validation result is positive).	PSP API POST /fundings - Response
7	DESP sends status of the reservation transaction simultaneously with API call 9 back to digital euro payer PSP.	PSP API POST /reservations/{id}/status - Request
8	Synchronous response from digital euro payer PSP to confirm receipt of the status notification.	PSP API POST /reservations/{id}/status – Response
9	DESP sends status of the reservation transaction simultaneously with API call 7 back to digital euro payee PSP.	PSP API POST /reservations/{id}/status - Request
10	Synchronous response from digital euro payee PSP to confirm receipt of the status notification	PSP API POST /reservations/{id}/status – Response
11	DESP sends status of the funding back to commercial bank money payer PSP.	PSP API POST /fundings/{id}/status - Request
12	Synchronous response from commercial bank money payer PSP to confirm receipt of the status notification.	PSP API POST /fundings/{id}/status - Response

A.1.1.2.1.1.3 Settlement – claiming a reservation

The settlement of a reservation follows the same process as the settlement of a payee-initiated payment transaction.

If the total amount of settlement is higher than the reserved amount (partially using reserved money, partially using money authorised in a normal payment transaction), the process of the settlement can be either payer-initiated or payee-initiated, depending on the payment instrument used to initiate the transaction[41].

A.1.1.2.2 Overview of API endpoints

A.1.1.2.2.1 DESP API endpoints for PSPs to send requests to DESP

API nr	Description	Sending partySending party	Exposing party	Covered in section
6	Digital euro payer PSP submits reservation instruction to digital euro payee PSP. If both payer and payee have the same PSP, the reservation instruction is to be submitted directly at this endpoint with complete settlement data.	Digital euro payer PSP	Digital euro payee PSP (via DESP) or DESP*	POST /reservation-instructions
7	Digital euro payer PSP provides asynchronous response to POST /reservation-requests endpoint.	Digital euro payer PSP	DESP	POST /reservation-requests/{id}/confirmation
10	Digital euro payer PSP OR digital euro payee PSP queries status of a reservation transaction.	Digital euro payer PSP or digital euro payee PSP	DESP	GET /reservations/{id}/status

[41] For details on the supported payment instruments please refer to E2E flows in Annex B.

*When the instructing PSP is the same PSP as the PSP instructed for payment transaction, reservation transaction, funding transaction or defunding transaction, and the full settlement data is in the request, then the exposing party will be DESP.

A.1.1.2.2.2 PSP API endpoints for PSPs to receive requests from DESP

API nr	Description	Sending partySending party	Exposing party	Covered in section
9	DESP forwards reservation request to digital euro payer PSP.	DESP	Digital euro payer PSP	POST /reservation-requests
10	DESP sends status of a reservation transaction (initiated at POST /reservation-instructions endpoint) to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /reservation-instructions/{id}/status
11	DESP sends status of a reservation transaction (initiated at POST /reservation-requests endpoint) to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /reservation-requests/{id}/status
12	DESP forwards request to change a reservation transaction to digital euro payer PSP.	DESP	Digital euro payer PSP	PUT /reservations/{id}
13	DESP sends status of a reservation update to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /reservations/{id}/status

A.1.1.2.3 DESP API for PSPs to send requests to DESP

In this section, all API endpoints for PSPs to submit requests to DESP (hereafter **DESP API**) are described in detail.

A.1.1.2.3.1 POST /reservation-instructions

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-instructions	Reservation	Endpoint for reservation initiation from payer PSP

A.1.1.2.3.1.1 POST /reservation-instructions - Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation object	See the table below.	-	-	M
Funding object	See the table below. This object is mandatory to be included if funding is needed.	-	-	O

Reservation object data elements – unencrypted part

Data element	Element description	Type	Length	Presence indicator
Payer PSP ID	Unique identification of the payer's PSP (BIC).	STR	11	M
Payee PSP ID	Unique identification of the payee's PSP (BIC).	STR	11	M
Payment type	Placeholder field for fee calculation related data.	SSET	tbd	tbd
Amount	The amount to be transferred from the payer to the payee.	STR	14.3	M
Currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code.	STR	3	M
Payer entry	Unique identification of the payer's digital euro holding in the ledger.	STR	tbd	M
Payee entry	Unique identification of the payee's digital euro holding in the ledger. This field must be included if payer and payee have the same digital euro PSP.	STR	tbd	O
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M

Reservation object data elements – encrypted part

The encrypted part is only required if payer and payee have different digital euro PSP.

Same as '**Payment object data elements – encrypted part**' in DESP API POST /payment-instructions.

Funding object data elements - unencrypted part

Same as '**Funding object data elements – unencrypted part**' in DESP API POST /payment-instructions.

Funding object data elements - encrypted part

The encrypted part is required for the open funding case, where the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part** in DESP API POST /fundings.

A.1.1.2.3.1.2 POST /reservation-instructions – 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 201.

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation ID	Resource ID for the reservation transaction.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Funding ID	Newly created resource ID for the funding part of the payment transaction.	STR	36	C, only required if funding object is present in the request and if validation result is positive as

				indicated in the field ‘reservation transaction status’
Funding status	Indication of the success or failure of the request.	SSET	4	C, only required if funding object is present in the request
Status reason code	Code providing details about the negative validation result.	SSET	4	C, mandatory in case of failure as indicated in the field ‘reservation transaction status’
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.3.2 POST /reservation-requests/{id}/confirmation

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	https://{server_region}.ecb.europa.eu/v1/reservation-requests/{id}/confirmation	Reservation	Endpoint for asynchronous response to PSP API POST /reservation-requests from the instructed payer PSP. Server is dependent on the parameter which is sent to PSP API POST /reservation-requests.

A.1.1.2.3.2.1 POST /reservation-requests/{id}/confirmation – 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
Reservation ID	Resource identification for the reservation transaction.	STR	36	M

Request body data elements:
Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

Reservation object	See the table below.	-	-	C, mandatory in case of a positive validation result as indicated at the field 'reservation transaction status'
Funding object	See the table below. This object is mandatory to be included if funding is needed.	-	-	O

Reservation object, non-encrypted part

Data element	Element description	Type	Length	Presence indicator
Payer entry	Unique identification of the user's digital euro holding in the ledger.	STR	Tbd	M

Funding object data elements – non-encrypted part

Same as '**Funding object data elements – encrypted part**' in DESP API POST /payment-instructions.

Funding object data elements – encrypted part

The encrypted part is required for open defunding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part** in DESP API POST /fundings.

A.1.1.2.3.2.2 POST /reservation-requests/{id}/confirmation – Response

Response 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
Reservation ID	The reservation ID received at PSP API POST /reservation-requests API call	STR	36	M

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
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'

Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.3.3 GET /reservations/{id}/status

This endpoint is used for PSPs to query statuses of reservation request, instruction and update.

Applicable endpoint and method:

Method	Endpoint	Resource	Description
GET	/v1/reservations/{id}/status	Reservation	Endpoint for Digital euro payer PSP OR Digital euro payee PSP to query the status of a reservation transaction

A.1.1.2.3.3.1 GET /reservations/{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
Reservation ID	Unique identification of the reservation transaction for which the status is requested.	STR	36	M

A.1.1.2.3.3.2 GET /reservations/{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.

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Settlement timestamp	Time and date of the moment the settlement was recorded in DESP when the funds were reserved for the reservation transaction.	ISODate Time	26	C, in case of a positive validation result as indicated in the field 'reservation transaction status'
Remaining reserved amount	The amount to be transferred from the payer to the payee.	STR	14.3	C, in case of a positive validation result as indicated in the field 'reservation transaction status'
Remaining reserved amount currency	The currency in which the remaining reserved amount is expressed. ISO 4217 three-letter code.	STR	3	C, in case of a positive validation result as indicated in the field 'reservation transaction status'

Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer	ISODate Time	26	C, in case of a positive validation result as indicated in the field 'reservation transaction status'
Reservation transaction status	Indication of the success or failure of the request	SSET	4	M
Funding status	Indication of the success or failure of the request	SSET	4	C, mandatory if funding object is present in the request
Funding ID	Resource ID generated by the DESP for the funding part of the payment transaction.	STR	36	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field 'payment transaction status'
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.4 PSP API for PSPs to receive requests from DESP

This section describes in detail all API endpoints for PSPs to receive requests from DESP (hereafter **PSP API**).

A.1.1.2.4.1 POST /reservation-requests

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-requests	Reservation	Endpoint for reservation requests

A.1.1.2.4.1.1 POST /reservation-requests – 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
Call Back Server	Call back URL https://{server_region}.ecb.europa.eu/v1/reservation-requests/{id}/confirmation	STR	tbd	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be	STR	36	M

	located at any time, by any of the parties in the chain. Set by the instructing PSP.			
Reservation object	See the table below.	-	-	M

Reservation object data elements – unencrypted part

The payee entry that was specified by the payee PSP will not be forwarded to the payer PSP.

Data element	Element description	Type	Length	Presence indicator
Reservation ID	Newly created resource ID for the reservation transaction.	STR	36	M
Payer PSP ID	Unique identification of the payer's PSP (BIC).	STR	11	M
Payee PSP ID	Unique identification of the payee's PSP (BIC).	STR	11	M
Payment type	Placeholder field for fee calculation related data. The discussion on fee is still open, therefore it serves as a placeholder at this moment.	SSET	tbd	tbd
Amount	The amount to be transferred from the payer to the payee.	STR	14.3	M
Currency	The currency in which the amount is expressed. ISO 4217 three-letter code.	STR	3	M
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M

Reservation object data elements - encrypted part

Same as the content '**Reservation object data elements – encrypted part**' included in the request DESP API POST /reservation-requests Acquiring PSP section.

A.1.1.2.4.1.2 POST /reservation-requests – 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.

Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.4.2 POST /reservation-instructions/{id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-instructions/{id}/status	Reservation	Endpoints for DESP to provide status of a reservation instruction to a PSP.

A.1.1.2.4.2.1 POST /reservation-instructions/{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
Reservation ID	Resource ID generated by DESP to identify a reservation transaction.	STR	36	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M

Settlement timestamp	Time and date of the moment the settlement was recorded in DESP when the funds were reserved for the reservation transaction.	ISODateTime	26	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Remaining reserved amount	The amount to be transferred from the payer to the payee.	STR	14.3	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Remaining reserved amount currency	The currency in which the remaining reserved amount is expressed. ISO 4217 three-letter code.	STR	3	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M

Funding status	Indication of the success or failure of the request.	SSET	4	C, mandatory if funding object is present in the request
Funding ID	Resource ID generated by the DESP for the funding part of the payment transaction.	STR	36	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field 'reservation transaction status'
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.4.2.2 POST /reservation-instructions/{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, without response body.

A.1.1.2.4.3 POST /reservation-request/{id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-requests/{id}/status	Reservation	Endpoints for DESP to provide status of a reservation request.

A.1.1.2.4.3.1 POST /reservation-request/{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
Reservation ID	Resource ID generated by DESP to identify a reservation transaction.	STR	36	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator

UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Settlement timestamp	Time and date of the moment the settlement was recorded in DESP when the funds were reserved for the reservation transaction.	ISODateTime	26	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Remaining reserved amount	The amount to be transferred from the payer to the payee.	STR	14.3	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Remaining reserved amount currency	The currency in which the remaining reserved amount is expressed. ISO 4217 three-letter code.	STR	3	C, in case of a positive validation result as indicated in the field ‘reservation transaction status’
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	C, in case of a positive validation result as indicated in

				the field ‘reservation transaction status’
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Funding status	Indication of the success or failure of the request.	SSET	4	C, mandatory if funding object is present in the request
Funding ID	Resource ID generated by the DESP for the funding part of the payment transaction.	STR	36	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field ‘reservation transaction status’
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field ‘reservation transaction status’
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.4.3.2 POST /reservation-request/{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, without response body.

A.1.1.2.4.4 PUT /reservations/{id}

Applicable endpoint and method:

Method	Endpoint	Resource	Description
PUT	/v1/reservation /{id}	Reservation	This endpoint is for DESP to forward modification of an existing reservation request from payee PSP to payer PSP.

A.1.1.2.4.4.1 PUT /reservations/{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
Reservation ID	Resource ID generated by DESP to identify a reservation transaction.	STR	36	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the reservation modification process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation object	See the table below.	-	-	M

Reservation object data elements - unencrypted part

Same as the content '**Reservation object data elements – unencrypted part**' included in the request DESP API PUT /reservations/{id} Acquiring PSP section.

Reservation object data elements - encrypted part

Same as the content '**Reservation object data elements – encrypted part**' included in the request DESP API PUT /reservations/{id} Acquiring PSP section.

A.1.1.2.4.4.2 PUT /reservations/{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.

Response Body

Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Request status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'request status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

Funding object	See the table below. This object is mandatory to be included when the new reservation amount is higher than the latest reserved amount and funding is required as a result.	-	-	O

Funding object data elements – unencrypted part

Same as '**Funding object data elements – unencrypted part**' in DESP API POST /reservation-instructions.

Funding object data elements – encrypted part

The encrypted part is required for open funding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part** in DESP API POST /fundings.

A.1.1.2.4.5 POST /reservations/{id}/status

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservations /{id}/status	Reservation	Endpoints for DESP to provide status of a reservation transaction to a PSP after completion of reservation modification process via PUT/reservations/{id} endpoint, or after the expiry date of a reservation transaction.

A.1.1.2.4.5.1 POST /reservations/{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
Reservation ID	Resource ID generated by DESP to identify a reservation transaction.	STR	36	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Settlement timestamp	Time and date of the moment the settlement was recorded in DESP when additional funds were reserved or released for the reservation transaction.	ISODateTime	26	C, mandatory in case of positive validation as indicated at the field 'request status'
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	C, in case of a positive validation result as indicated in the field 'request status'
Reservation modification object.	See the table below.	-	-	C, mandatory in case of a update following PUT/reservations/{id} request

Reservation modification object data elements – unencrypted part

Data element	Element description	Type	Length	Presence indicator
Request status	Indication of the success or failure of the request.	SSET	4	M
Funding status	Indication of the success or failure of the request.	SSET	4	C, mandatory if funding object is present in the request
Funding ID	Resource ID generated by the DESP for the funding part of the reservation transaction.	STR	36	C, mandatory if funding object is present in the request and in case of positive validation as indicated at the field 'request status'
Remaining reserved amount	The amount to be transferred from the payer to the payee.	STR	14.3	C, in case of a positive validation result as indicated in the field 'request status'
Remaining reserved amount currency	The currency in which the remaining reserved amount is expressed. ISO 4217 three-letter code.	STR	3	C, in case of a positive validation result as indicated in the field 'request status'
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'payment transaction status'

Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.1.2.4.5.2 POST /reservations/{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, without response body.

A.1.2 Acquiring PSP requirements

A.1.2.1 Functional description

Please refer to section Functional description.

A.1.2.2 Interface description

A.1.2.2.1 Settlement payload structure

Please refer to section describing Settlement payload structure.

A.1.2.2.2 Overview of API endpoints

A.1.2.2.2.1 DESP API endpoints for PSPs to send requests to DESP

API nr	Description	Sending partySending party	Exposing party	Covered in section
7	Digital euro payee PSP submits reservation request to digital euro payer PSP.	Digital euro payee PSP	Digital euro payer PSP (via DESP)	POST /reservation-requests
8	Digital euro payer PSP provides asynchronous response to POST /reservation-requests endpoint.	Digital euro payer PSP	DESP	POST /reservation-requests/{id}/confirmation
9	Digital euro payee PSP submits a request to change a reservation transaction.	Digital euro payee PSP	Digital euro payer PSP (via DESP)*	PUT /reservations/{id}
13	Digital euro payer OR payee PSP queries status of a reservation transaction.	Digital euro payer or payee PSP	DESP	GET /reservations/{id}/status

*If the instructing PSP is the same PSP as instructed PSP for payment transaction, reservation transaction, funding transaction or defunding transaction, and full settlement data is in the request, then the exposing party will be DESP.

A.1.2.2.2.2 PSP API endpoints for PSPs to receive requests from DESP

API Nr	Description	Sending partySending party	Exposing party	Covered in section
9	DESP forwards reservation instruction to digital euro payee PSP.	DESP	Digital euro payee PSP	POST /reservation-instructions
10	DESP sends status of a reservation transaction (initiated at POST /reservation-	DESP	Digital euro payer and payee PSP	POST /reservation-instructions/{id}/status

	instructions endpoint) to digital euro payer and payee PSP.			
11	DESP sends status of a reservation transaction (initiated at POST /reservation-requests endpoint) to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /reservation-requests/{id}/status
12	DESP sends status of a reservation update to digital euro payer and payee PSP.	DESP	Digital euro payer and payee PSP	POST /reservations/{id}/status

A.1.2.2.3 Overview of covered scenarios

Please refer to section describing Overview of covered scenarios.

A.1.2.2.4 DESP API for PSPs to send requests to DESP

A.1.2.2.4.1 POST /reservation-requests

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-request	Reservation	Endpoint for reservation initiation from Digital euro payee PSP

A.1.2.2.4.1.1 POST /reservation-requests – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation object	See the table below.	-	-	M

Reservation object data elements – unencrypted part

Data element	Element description	Type	Length	Presence indicator
Payer PSP ID	Unique identification of the payer's PSP (BIC).	STR	11	M
Payee PSP ID	Unique identification of the payee's PSP (BIC).	STR	11	M
Payment type	Placeholder field for fee calculation related data.	SSET	tbd	tbd
Amount	The amount to be transferred from the payer to the payee.	STR	14.3	M
Currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code.	STR	3	M
Payee entry	Unique identification of the payee's digital euro holding in the ledger.	STR	tbd	M
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M

Reservation object data elements – encrypted part

The encrypted part is only required if payer and payee have different digital euro PSPs.

Same as '**Payment object data elements – encrypted part**' in DESP API POST /payment-requests.

A.1.2.2.4.1.2 POST /reservation-requests – 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
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation ID	Newly created resource ID for the reservation transaction.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative validation result.	SSET	4	C, mandatory in case of failure as indicated in the field 'reservation

				transaction status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.2.2.4.2 PUT /reservations/{id}

Applicable endpoint and method:

Method	Endpoint	Resource	Description
PUT	/v1/reservations/{id}	Reservation	Endpoint for reservation modification

A.1.2.2.4.2.1 PUT /reservations/{id} – Request

Request header:

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

Data element	Element description	Type	Length	Presence indicator
Reservation ID	Resource identification for the reservation transaction.	STR	36	M

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator

Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the reservation modification process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation object	See the table below.	-	-	M
Funding object	See the table below. This object is mandatory to be included when the new reservation amount is higher than the latest reserved amount and funding is required as a result. Furthermore, this object can only be included when payer and payee have the same digital euro PSP.	-	-	O

Reservation object data elements – unencrypted part

Data element	Element description	Type	Length	Presence indicator
Payer PSP ID	Unique identification of the payer's PSP (BIC).	STR	11	M
Payee PSP ID	Unique identification of the payee's PSP (BIC).	STR	11	M
Payment type	Placeholder field for fee calculation related data.	SSET	tbd	tbd
Latest reserved amount	The remaining reserved amount of the existing reservation.	STR	14.3	M
Latest reserved currency	The currency in which the latest reserved amount is expressed. ISO 4217 three-letter code. Attribute of latest reserved amount.	STR	3	M

New reserved amount	The new reservation amount.	STR	14.3	M
New reserved currency	The currency in which the new amount is expressed. ISO 4217 three-letter code. Attribute of new reserved amount.	STR	3	M
Latest expiry date time	Date and time at which the existing reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M
New expiry date time	Date and time at which the modified reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M

Reservation object data elements – encrypted part

The encrypted part is required if the payer and payee have different digital euro PSPs.

Data element	Element description	Type	Length	Presence indicator
Unstructured remittance information	The field provides additional information about (the purpose of) the transaction in free format text. It is mandatory to include this field if the user provides the remittance.	STR	140	O
Structured remittance information	The fields provide additional information about (the purpose of) the transaction in a standardised and structured format. It may include a type, a reference to a standard and a value. It is mandatory to include this field if the user provides the remittance.	STR (tbd)	tbd	O

Funding object data elements - unencrypted part

Same as '**Funding object data elements – unencrypted part**' in DESP API POST /payment-instructions.

Funding object data elements - encrypted part

The encrypted part is required for open funding case when the digital euro PSP is different from the commercial bank money PSP.

Same as '**Funding object data elements – encrypted part** in DESP API POST /fundings.

A.1.2.2.4.2.2 PUT /reservations/{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.

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Request status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'request status'
Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O

A.1.2.2.5 PSP API for PSPs to receive requests from DESP

A.1.2.2.5.1 POST /reservation-instructions

Applicable endpoint and method:

Method	Endpoint	Resource	Description
POST	/v1/reservation-instructions	Reservation	Endpoint for payee PSP to receive reservation instructions from payer PSP via DESP

A.1.2.2.5.1.1 POST /reservation-instructions – Request

Request header:

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

Request body data elements:

Root

Data element	Element description	Type	Length	Presence indicator
Acceptance timestamp	Date and time. This timestamp will be used for determination of maximum processing time. This is set by the first PSP which starts the settlement process, and should not be altered by other PSPs.	ISODateTime	26	M
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of	STR	36	M

	the parties in the chain. Set by the instructing PSP.			
Reservation object	See the table below.	-	-	M

Reservation object data elements – unencrypted part

The payer entry that was specified by the payer PSP will not be forwarded to the payee PSP.

Data element	Element description	Type	Length	Presence indicator
Reservation ID	Newly created resource ID for the reservation transaction.	STR	36	M
Payer PSP ID	Unique identification of the payer's PSP (BIC).	STR	11	M
Payee PSP ID	Unique identification of the payee's PSP (BIC).	STR	11	M
Payment type	Placeholder field for fee calculation related data.	SSET	tbd	tbd
Amount	The amount to be transferred from the payer to the payee.	STR	14.3	M
Currency	The currency in which the transaction amount is expressed. ISO 4217 three-letter code	STR	3	M
Expiry date time	Date and time at which the reservation expires and any remaining reserved amount is automatically released to the payer.	ISODateTime	26	M

Reservation object data elements – encrypted part

Same as '**Reservation object data elements – encrypted part**' in DESP API POST /reservation-instructions.

A.1.2.2.5.1.2 POST /reservation-instructions – 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.

Response Body

Root

Data element	Element description	Type	Length	Presence indicator
UETR	Unique End-to-end Transaction Reference, a unique, unalterable reference which allows a payment to be located at any time, by any of the parties in the chain. Set by the instructing PSP.	STR	36	M
Reservation transaction status	Indication of the success or failure of the request.	SSET	4	M
Status reason code	Code providing details about the negative business validation result.	SSET	4	C, mandatory in case of negative validation as indicated at the field 'reservation transaction status'

Additional information status reason	Text providing details about the status reason code.	STR	Max 100*70	O
Reservation object	See the table below.	-	-	C, mandatory in case of positive validation as indicated at the field ‘reservation transaction status’

Reservation object data elements – unencrypted part

Data element	Element description	Type	Length	Presence indicator
Payee entry	Unique identification of the user’s digital euro holding in the ledger.	STR	tbd	M