EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook – Annex D1 Front-end implementation specification #2 Acquiring PSP requirements

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

1	**Document information**	**6**
1.1	Change history	6
2	**Introduction**	**7**
3	**Structure of the document**	**9**
4	**Overview of processes**	**10**
4.1	Access Management Service	10
4.1.1	*Business user onboarding*	*10*
4.1.2	*Business user lifecycle management*	*10*
4.1.3	*Business user offboarding*	*11*
4.2	Transaction Management Service	12
4.2.1	*E/M-commerce transactions*	*12*
4.2.2	*Recurring e/m-commerce transactions*	*16*
4.2.3	*Pre-authorisation service on e/m-commerce*	*22*
4.2.4	*Refund Transactions*	*27*
4.2.5	*Transactions at POS*	*28*
5	**List of services**	**29**
6	**Access Management Service**	**34**
6.1	Business user access management service	34
6.1.1	*Functions description*	*34*
6.2	Acceptance solutions service	41
6.2.1	*Functions description*	*42*
6.3	Notification settings service	42
6.3.1	*Functions description*	*43*
6.4	Linked account settings service	50
6.5	Digital euro payment account service	51
6.6	Non-digital euro payment account service	51
7	**Liquidity Management Service**	**52**
7.1	Non-digital euro payment account funds management service	52
7.2	Digital euro payment account funds management service	52

8 Transaction Management Service 53
8.1 Payment initiation service 53
8.1.1 Functions description 54
8.2 Recurring payment service 62
8.2.1 Description of function 62

Table of figures

Figure 1 - Business user onboarding 10
Figure 2 - Business user offboarding 11
Figure 3 - E-commerce payment via QR code 12
Figure 4 - E-commerce payment via alias 13
Figure 5 - E-commerce payment via DEAN 14
Figure 6 - M-commerce payment via mobile app 15
Figure 7 - Recurring e-commerce payment via QR code - Set-up 16
Figure 8 - Recurring e-commerce payment via alias - Set-up 17
Figure 9 - Recurring m-commerce payment via mobile app - Set-up 18
Figure 10 – Recurring e/m-commerce payment - periodic processing 19
Figure 11 - Recurring payment parameters update 20
Figure 12 - Recurring payment termination 21
Figure 13 - Pre-authorisation service on e-commerce via QR code 22
Figure 14 - Pre-authorisation service on e-commerce with alias 23
Figure 15 - Pre-authorisation service on m-commerce 24
Figure 16 - Pre-authorisation service on e/m-commerce - final check out 25
Figure 17 - Modification of a pre-authorisation 26
Figure 18 - Refund on e-commerce 27
Figure 19 - Transactions at POS - NFC mobile payment 28

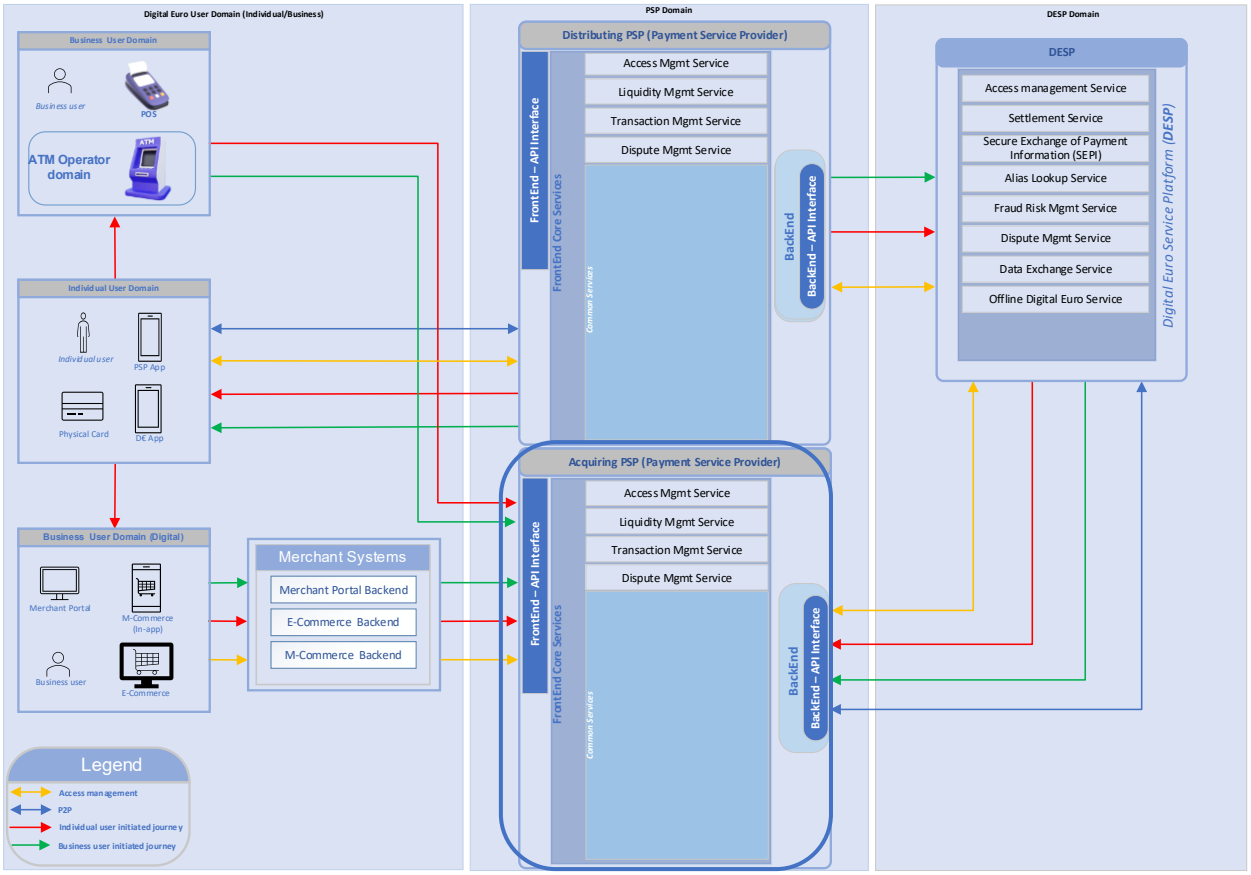
1 Document information

1.1 Change history

Version number	Date	Reason for revision
V0.1	20/02/2025	• Initiation of the document
V0.2	13/03/2025	• Update after workstream participants review
V0.3	20/05/2025	• Update to ensure consistency with G1-2-3 holistic approach sprint
V0.4	15/10/2025	• New functions and messages description to support a new use case • Transaction at POS: NFC mobile payment
V0.5	01/12/2025	• New functions and messages to address new use cases: onboarding and offboarding of business users • Refinement of services to provide additional details about the triggers of functions. • Realignment of data elements description (format, standardised name)
Version renumbering to ensure strict alignment with the rulebook's versioning		
V0.91	26/03/2025	March release

2 Introduction

Annex D to the rulebook will provide detailed implementation specifications for the different domains and interactions between actors as presented in the diagram below.



This document, corresponding to specification#2, is dedicated to acquiring PSP requirements.

The current version focuses only on the following scope:

- Onboarding of business user
- Offboarding of business user
- E-commerce payment via QR code
- E-commerce payment via alias
- E-commerce payment via DEAN
- E-commerce payment via pay-by-link
- M-commerce payment via mobile app
- Recurring e-commerce payment via QR code
- Recurring e-commerce payment via alias
- Recurring e-commerce payment via pay-by-link
- Recurring m-commerce payment via mobile app
- Recurring payment management
- Pre-authorisation service on e-commerce via QR code
- Pre-authorisation service on e-commerce with alias

- Pre-authorisation service on e-commerce via pay-by-link
- Pre-authorisation service on m-commerce
- Modification of a pre-authorisation
- Refund on e-commerce

3 Structure of the document

The current document is organised according to core services as outlined in the Digital Euro Scheme Rulebook.

- Access management service
- Liquidity management service
- Transaction management service

Core services are split into more granular services, and each service contains a set of unitary functions that must be implemented by PSPs to support the digital euro. For each function, applicable business rules, supported message types and data elements are detailed.

Data are described according to the following information

Element	Definition, annotation and example
Data element	Name of data element
Description	Detailed presentation of the data that can include examples. If applicable, a set of possible values for data (attribute) is provided
Type (Format)	Format of the data allowing the system to interact with the data and its value
Length	Maximum number of characters
Presence indicator	Indicator defining if a data is mandatory or not in a specific context: - M: Mandatory - O: Optional - C: Conditional
Standardised name	Name formatted according to a predefined conventions to ensure consistency and uniformity (ISO 20022) **Note:** No standard name is currently assigned to the data created for the needs of the digital euro *(new for digital euro)*

The list of possible types is presented below

Data type	Description
String (STR)	Sequence of characters that can be a letter, a digit, a blank space, a punctuation mark (alphanumeric)
Number (NUM)	Numeric characters only
Boolean (BOOL)	Represents the value True and False
String set (SSET)	List of applicable attributes
Number set (NSET)	List of applicable numbers
Number range	A numeric range for a data
Date	Date format: YYYY-MM-DD
UTC Time	UTC time including milliseconds: HHMMSSsss
Datetime UTC	Date and time format in UTC: YYYY-MM-DDThh:hh:sssZ
Binary (BIN)	Method of encoding data using sequences of bits
UUID	Universally Unique Identifier xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx

4 Overview of processes

For better context understanding, graphical representations illustrate the use cases and introduce the services and unitary functions.
The diagrams presented below:

- are conceptual views centred on flow initiators (individuals & businesses)
- show responsibility split across users, intermediaries, and DESP
- highlight key capabilities (e.g. initiation, validation, settlement, risk & dispute handling)

Their purpose is not to be sequence diagrams. The sequences are reflected in the end-to-end flows.

4.1 Access management service

4.1.1 Business user onboarding

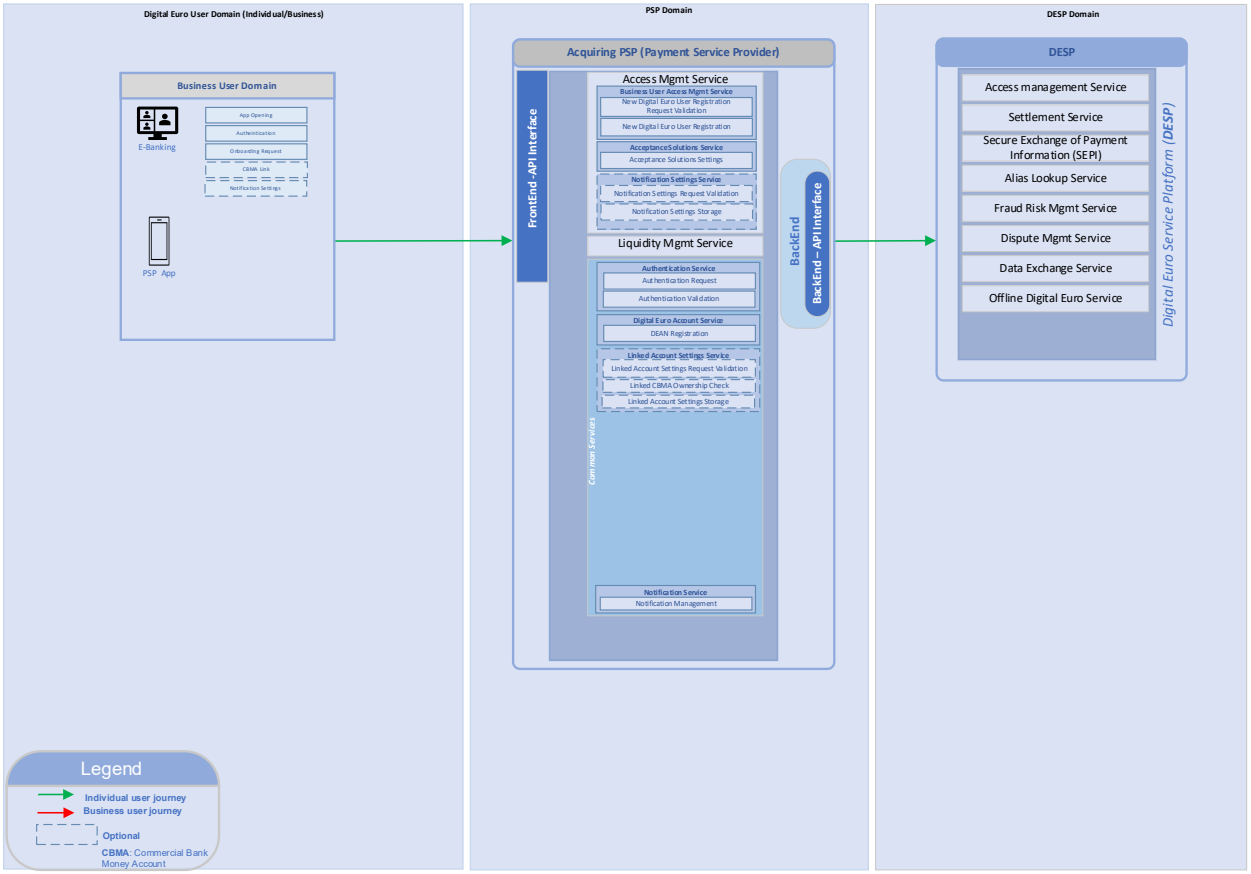


Figure 1 - Business user onboarding

4.1.2 Business user lifecycle management

(placeholder for a future version of specifications)

4.1.3 Business user offboarding

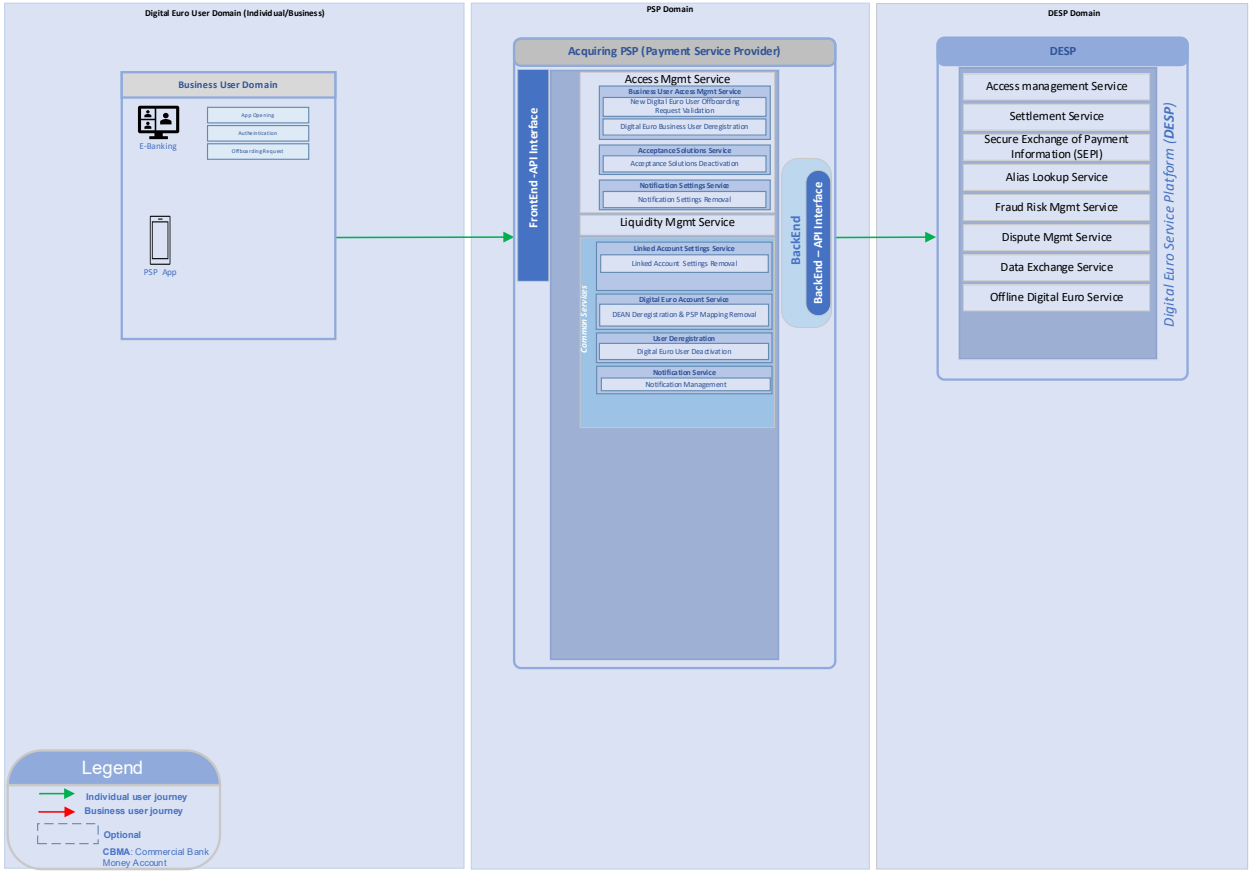


Figure 2 - Business user offboarding

4.2 Transaction management service

4.2.1 E/M-commerce transactions

4.2.1.1 E-commerce payment via QR code

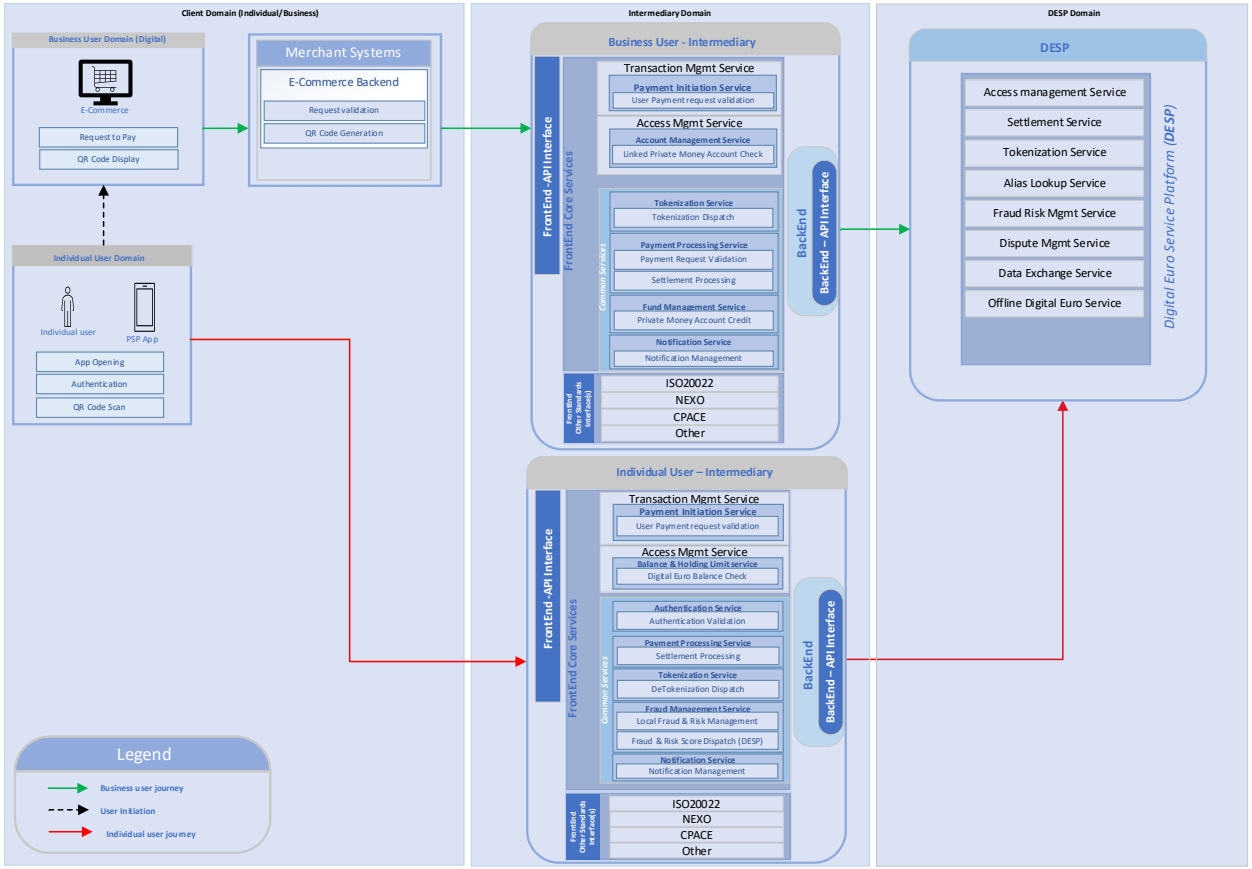


Figure 3 - E-commerce payment via QR code

4.2.1.2 E-commerce payment via alias

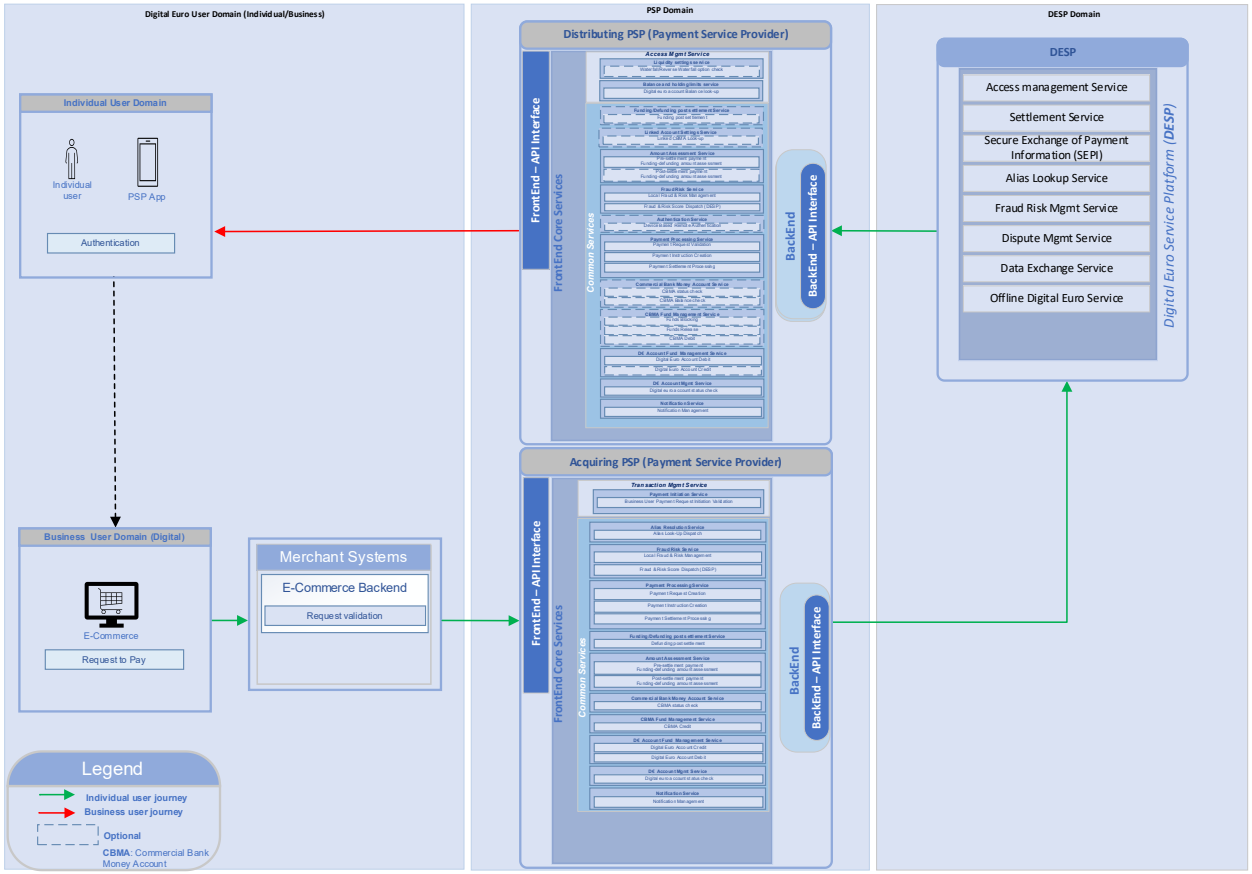


Figure 4 - E-commerce payment via alias

4.2.1.3 E-commerce payment via DEAN

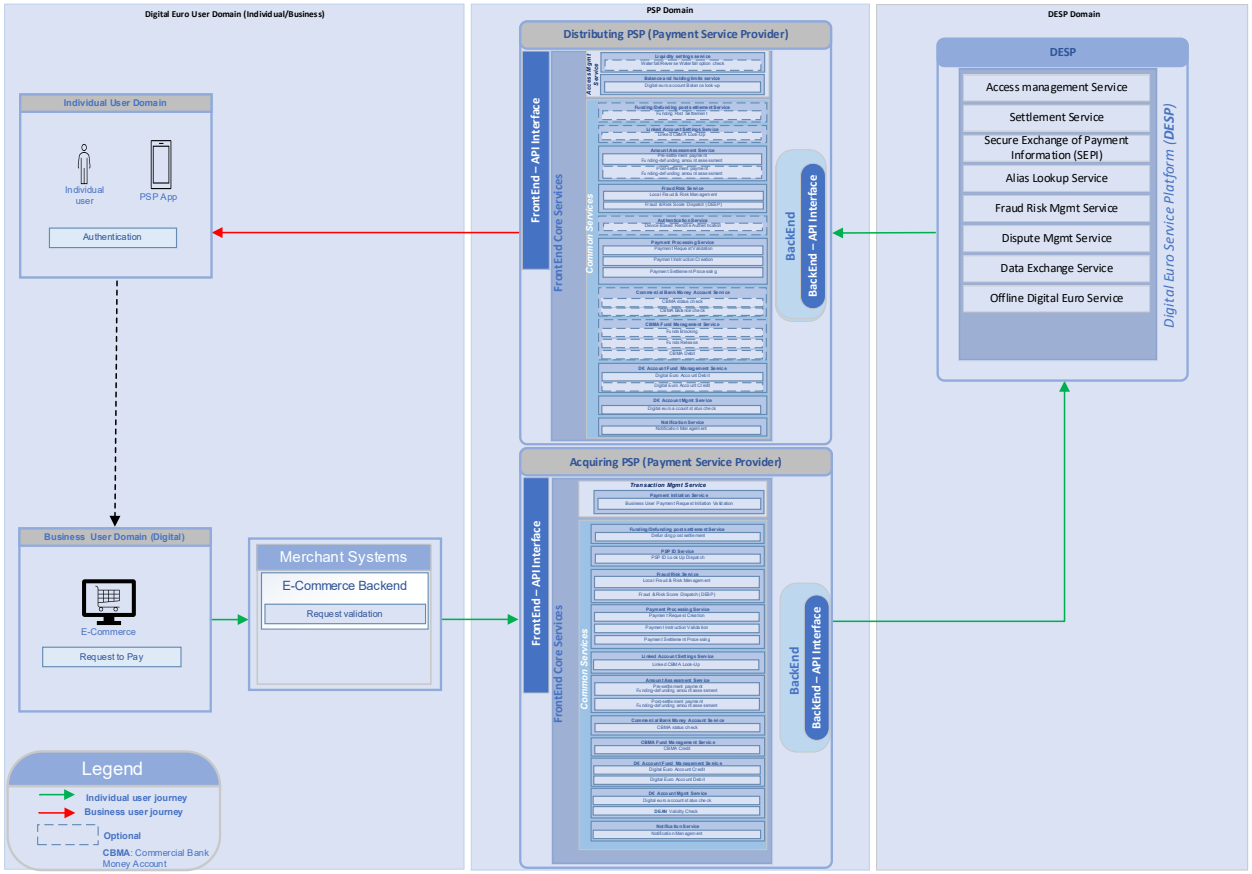


Figure 5 - E-commerce payment via DEAN

4.2.1.4 E-commerce payment via pay-by-link

(Placeholder for a future version of specifications)

4.2.1.5 M-commerce payment via mobile app

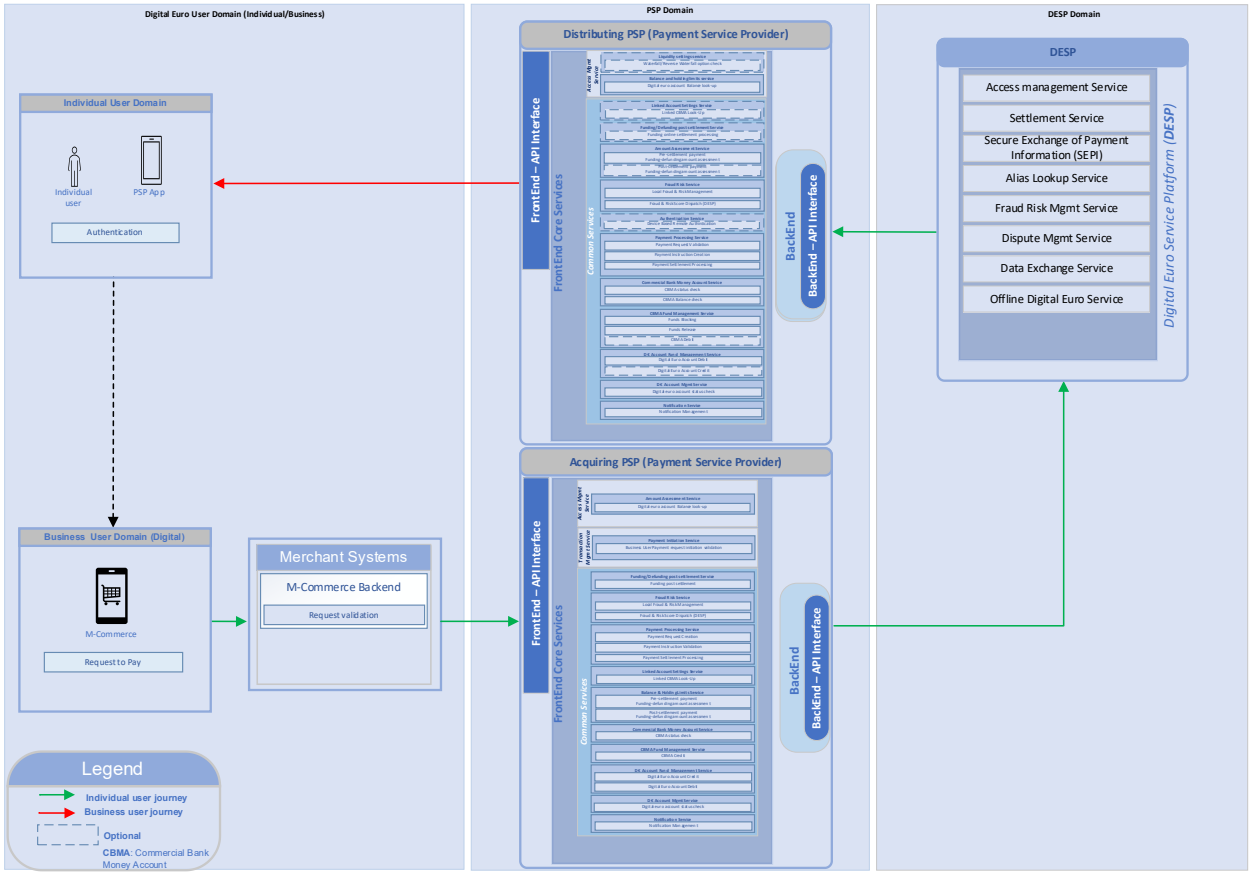


Figure 6 - M-commerce payment via mobile app

4.2.2 Recurring e/m-commerce transactions

4.2.2.1 Recurring e-commerce payment via QR code (set-up)

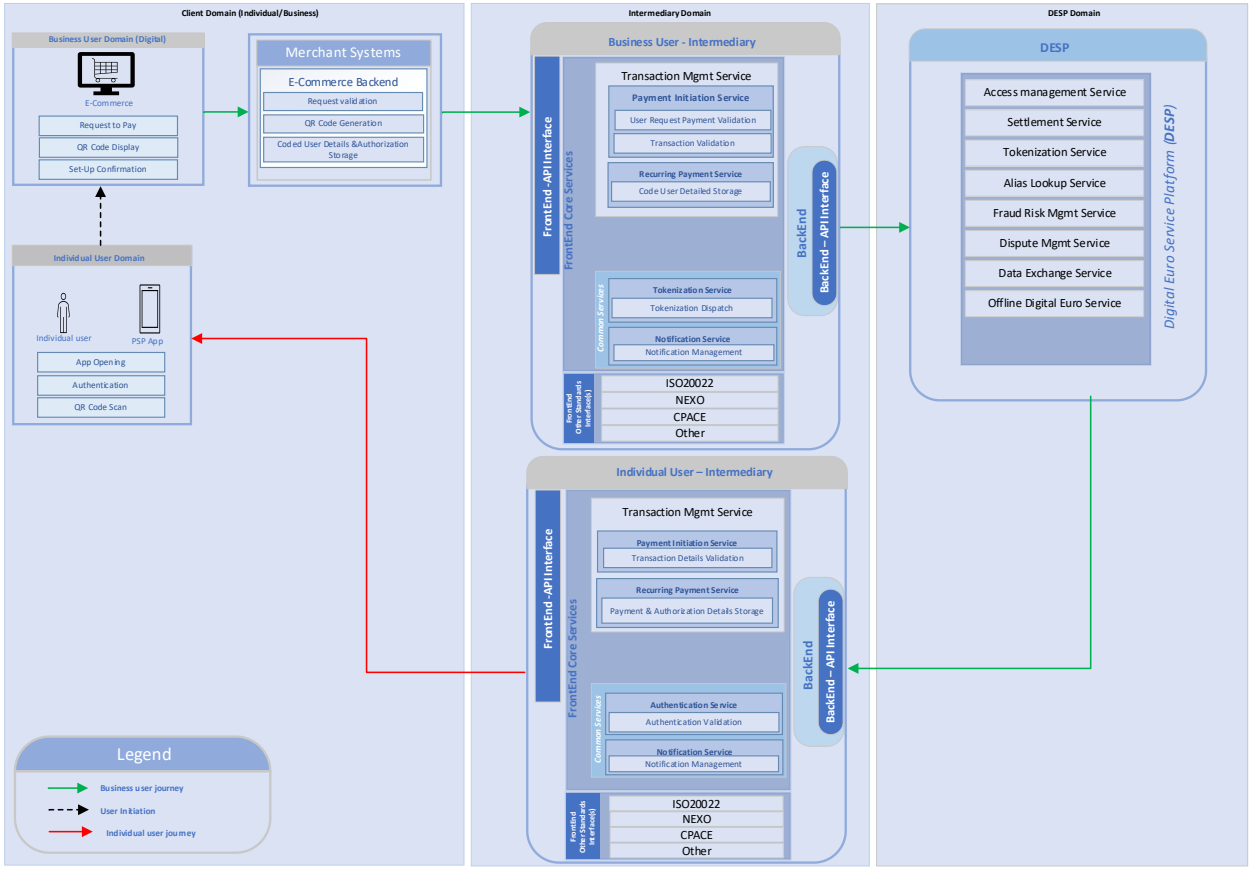


Figure 7 - Recurring e-commerce payment via QR code - Set-up

4.2.2.2 Recurring e-commerce payment via alias (set-up)

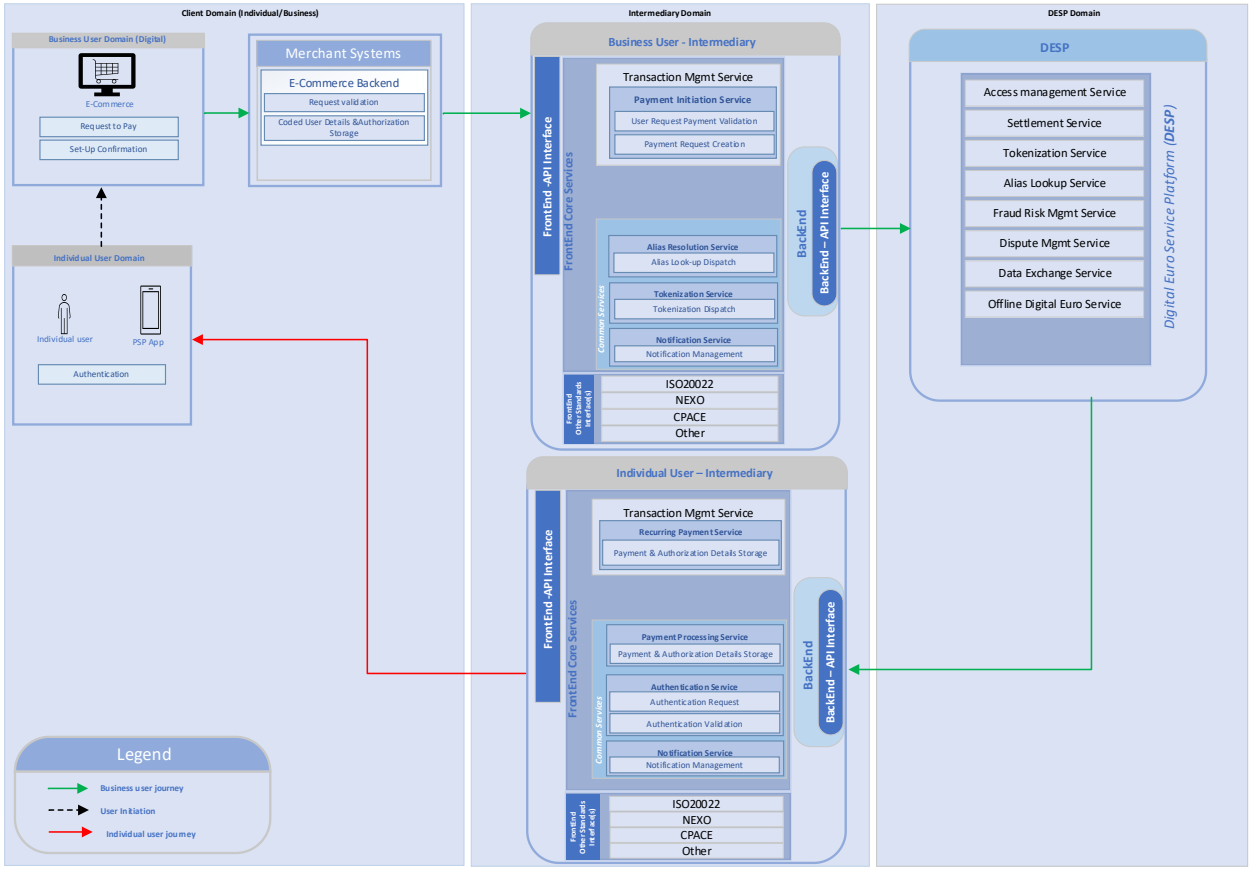


Figure 8 - Recurring e-commerce payment via alias - Set-up

4.2.2.3 Recurring e-commerce payment via pay-by-link (set-up)

(placeholder for a future version of specifications)

4.2.2.4 Recurring m-commerce payment via mobile app (set-up)

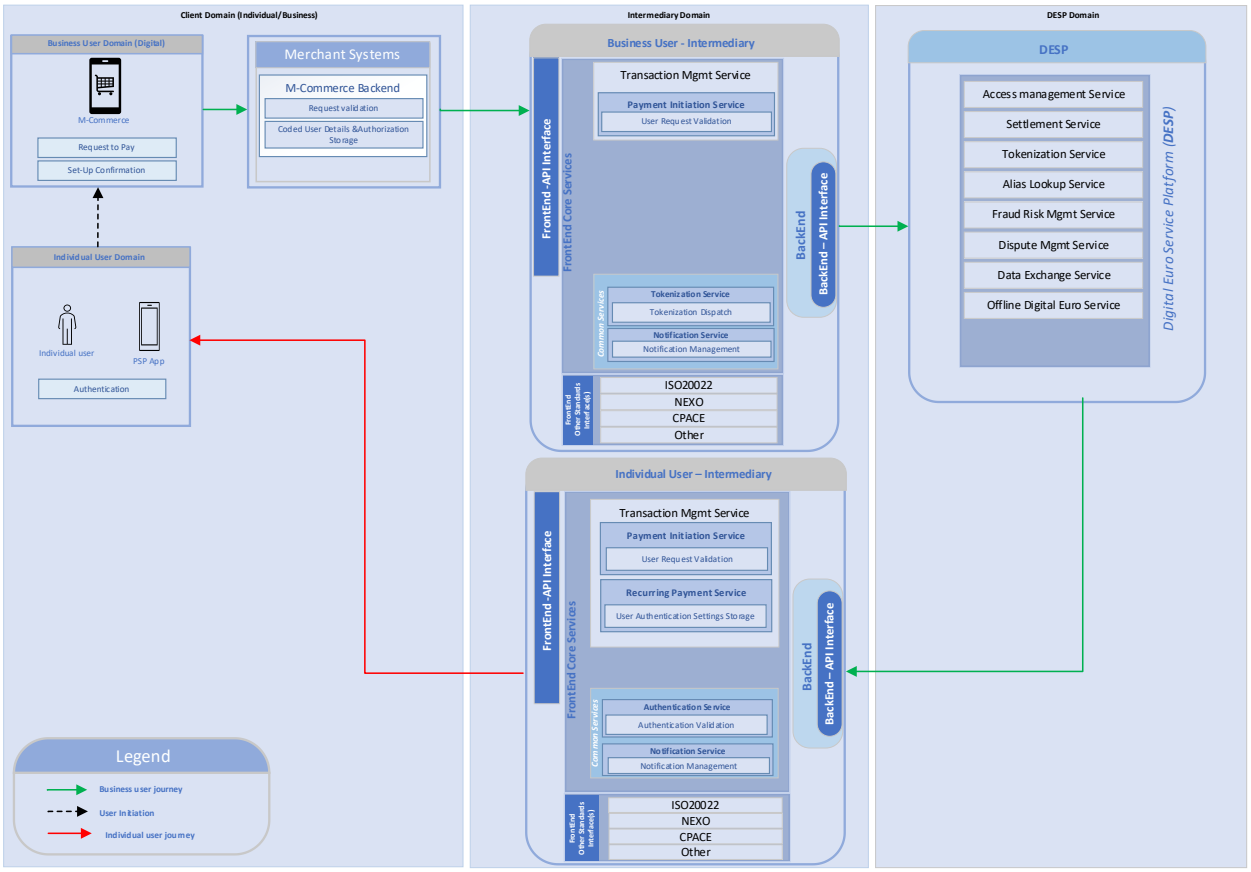


Figure 9 - Recurring m-commerce payment via mobile app - Set-up

4.2.2.5 Recurring e/m-commerce payment – periodic processing

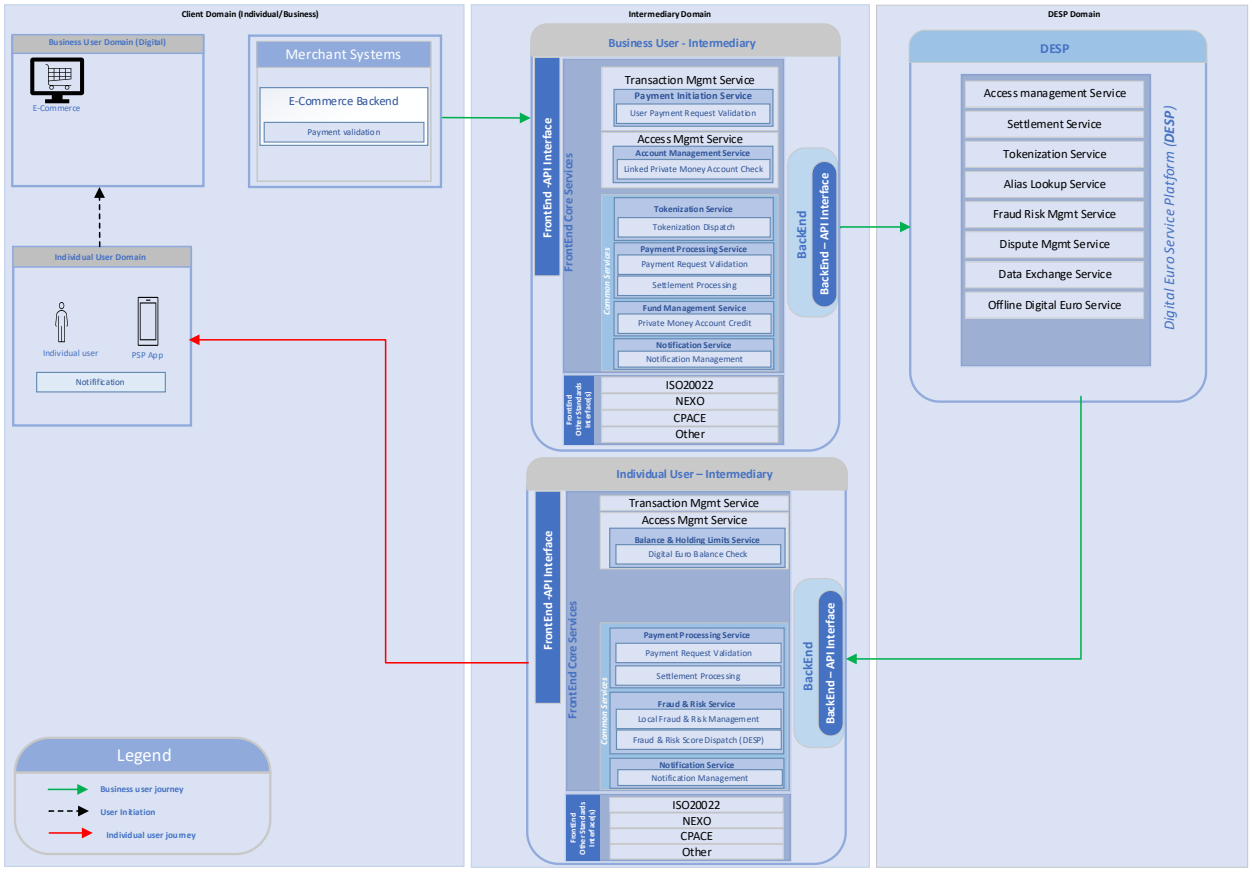


Figure 10 – Recurring e/m-commerce payment - periodic processing

.

4.2.2.6 Recurring payment management

Recurring payment management covers, active recurring payments parameters update and recurring payments termination. Update and termination are initiated by the merchant (potentially on user's request).

4.2.2.6.1 Recurring payment parameters update

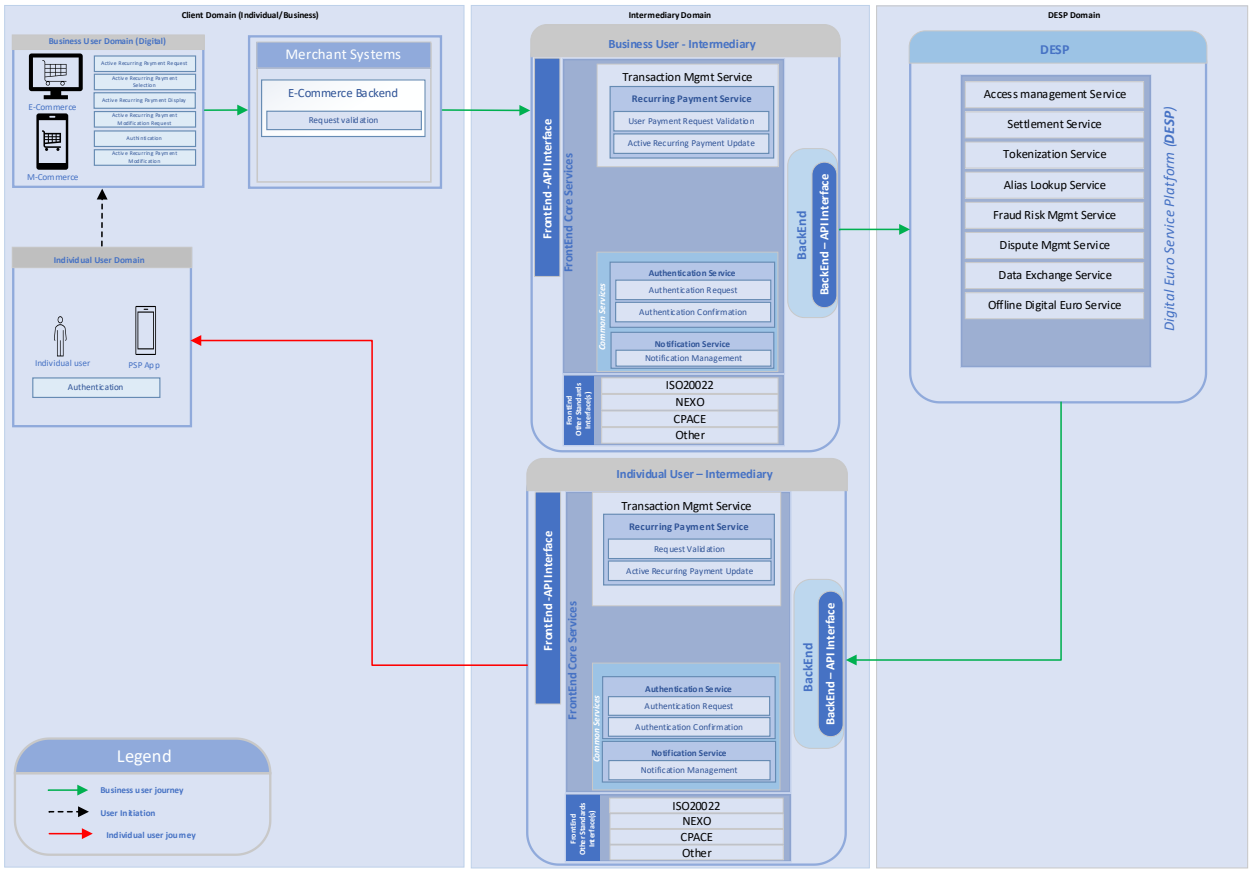


Figure 11 - Recurring payment parameters update

4.2.2.6.2 Recurring payment termination

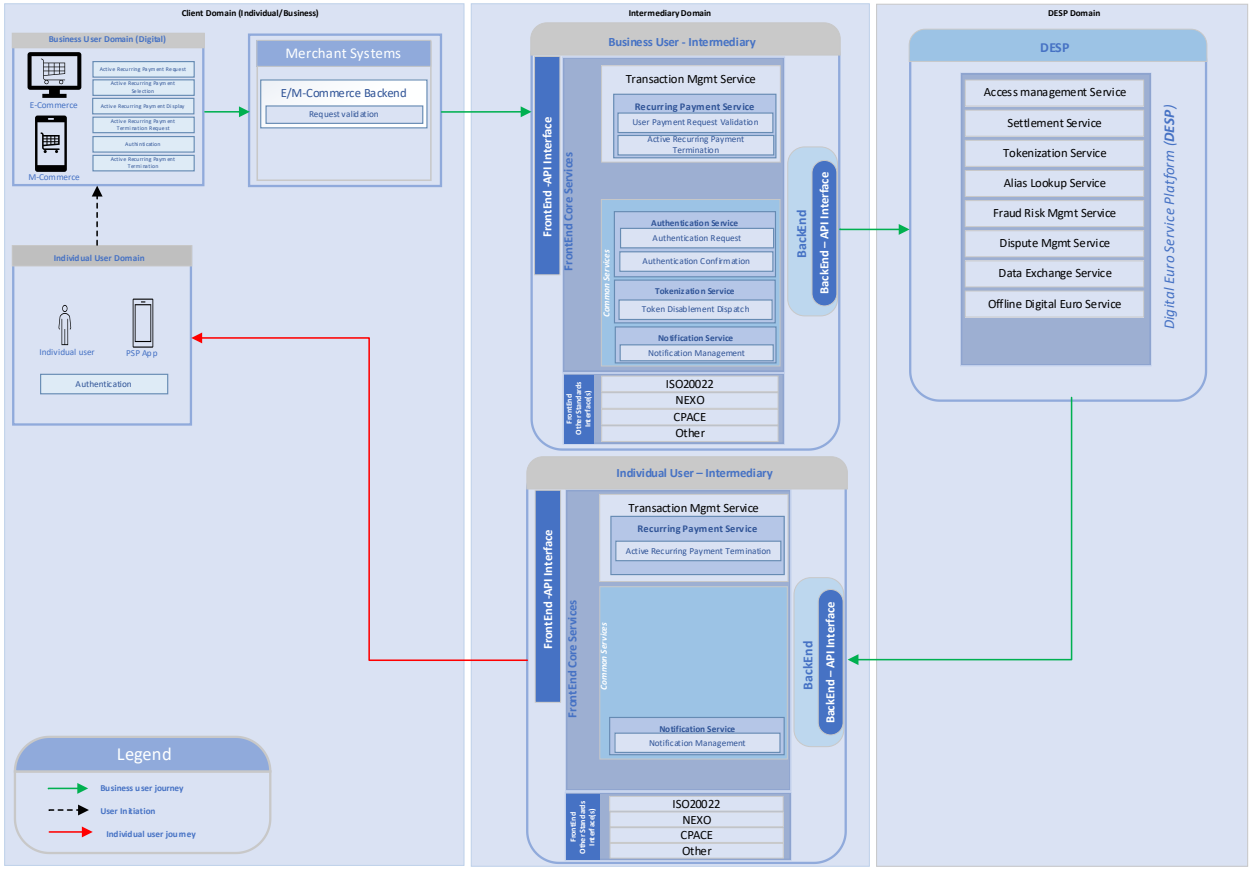


Figure 12 - Recurring payment termination

4.2.3 Pre-authorisation service on e/m-commerce

4.2.3.1 Pre-authorisation service on e-commerce via QR code

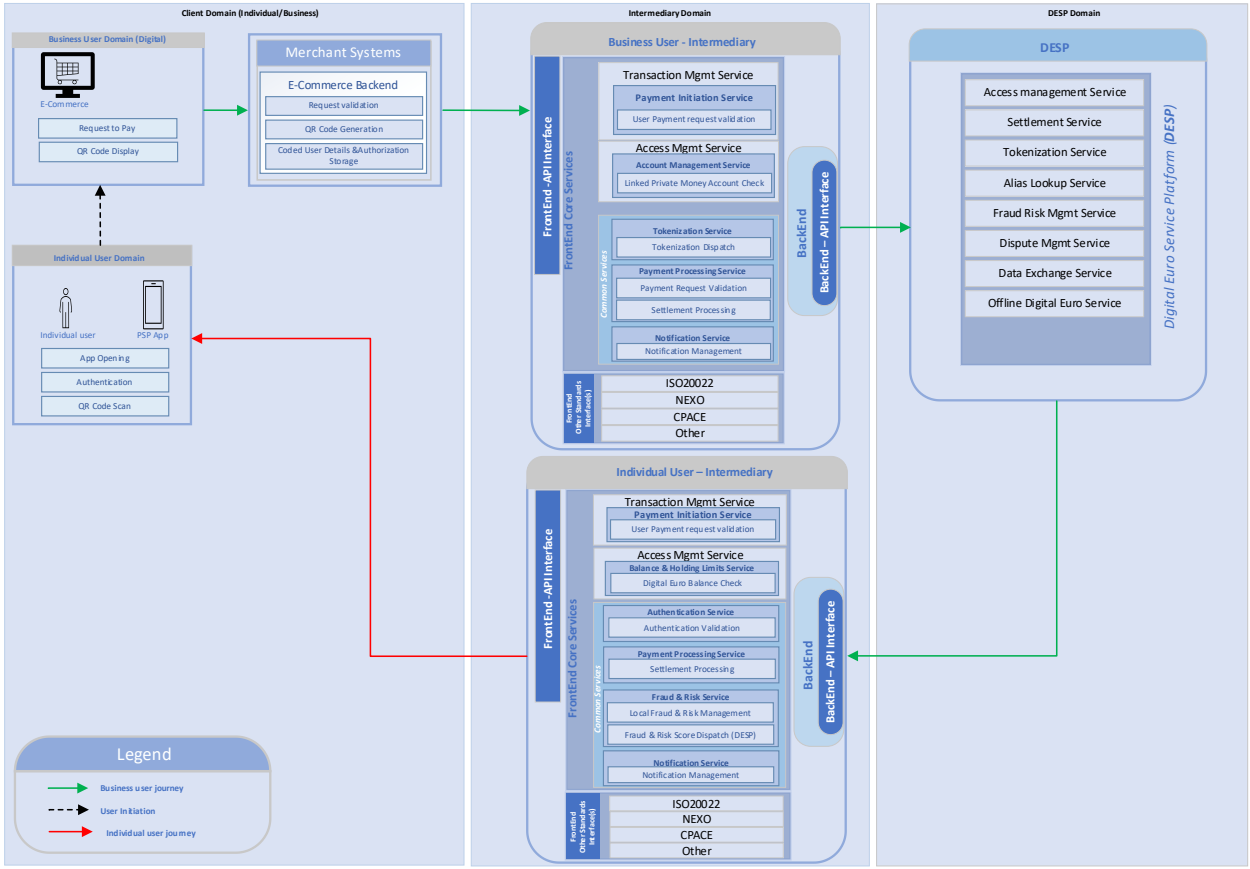


Figure 13 - Pre-authorisation service on e-commerce via QR code

4.2.3.2 Pre-authorisation service on e-commerce with alias

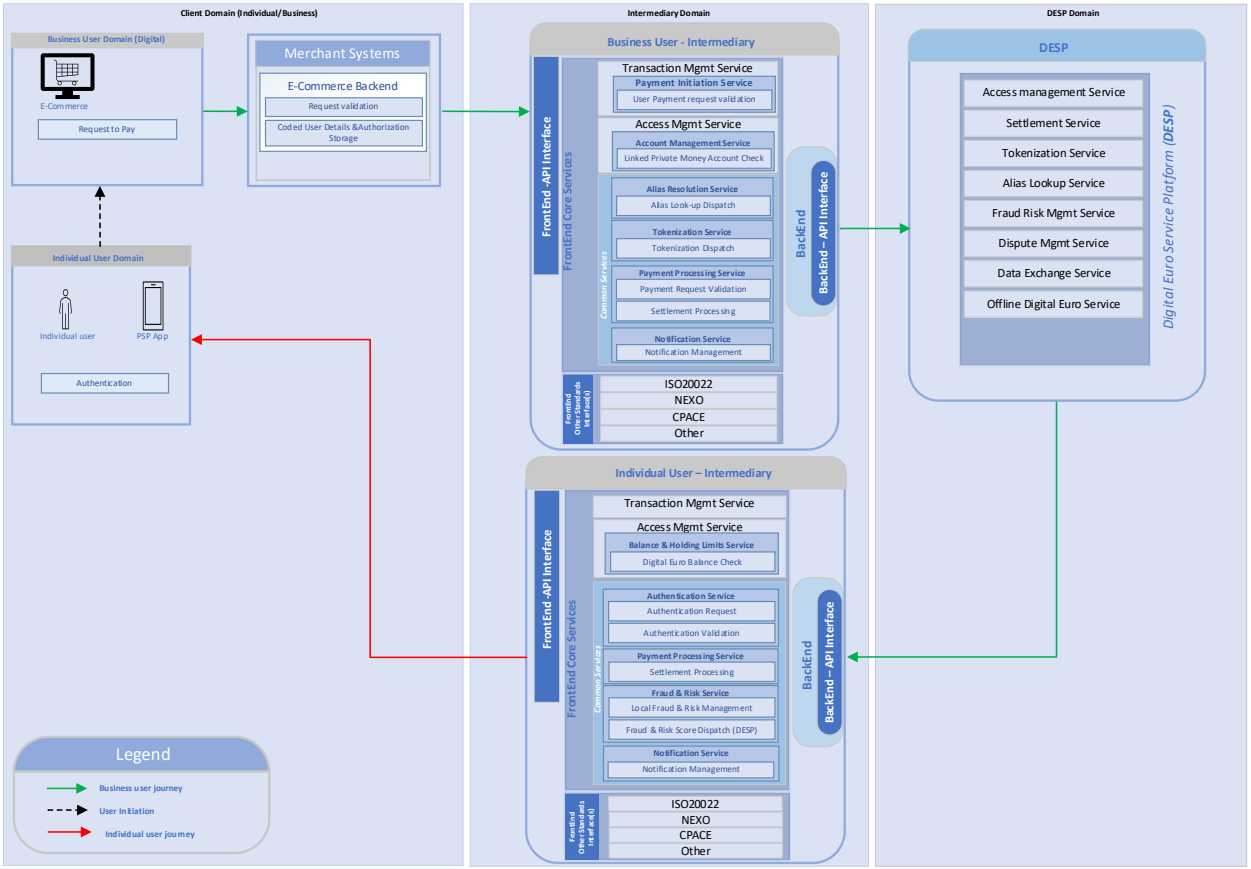


Figure 14 - Pre-authorisation service on e-commerce with alias

4.2.3.3 Pre-authorisation service on e-commerce via pay-by-link

(Placeholder for a future version of specifications)

4.2.3.4 Pre-authorisation service on m-commerce

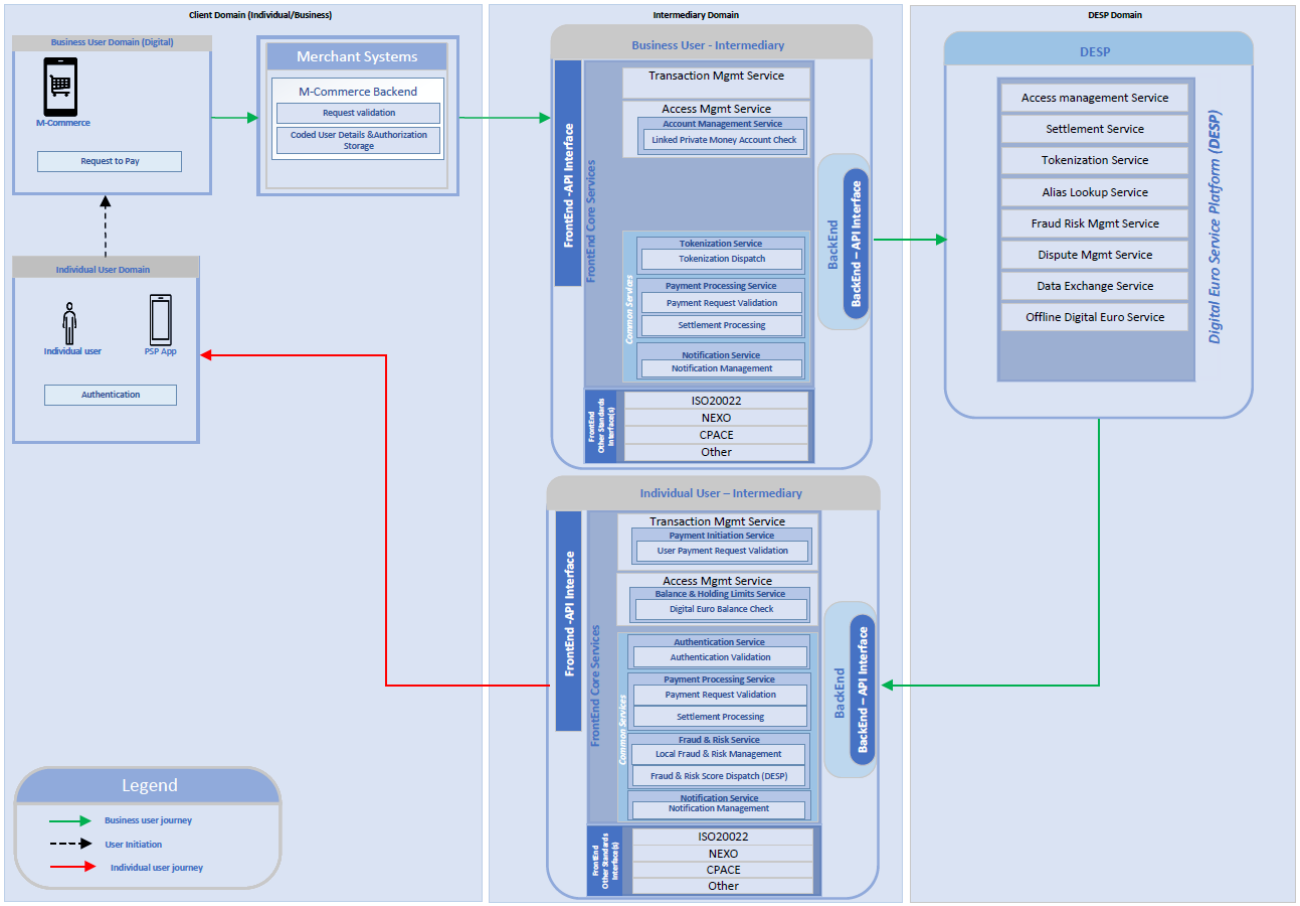


Figure 15 - Pre-authorisation service on m-commerce

4.2.3.5 Pre-authorisation service on e/m-commerce: final check out

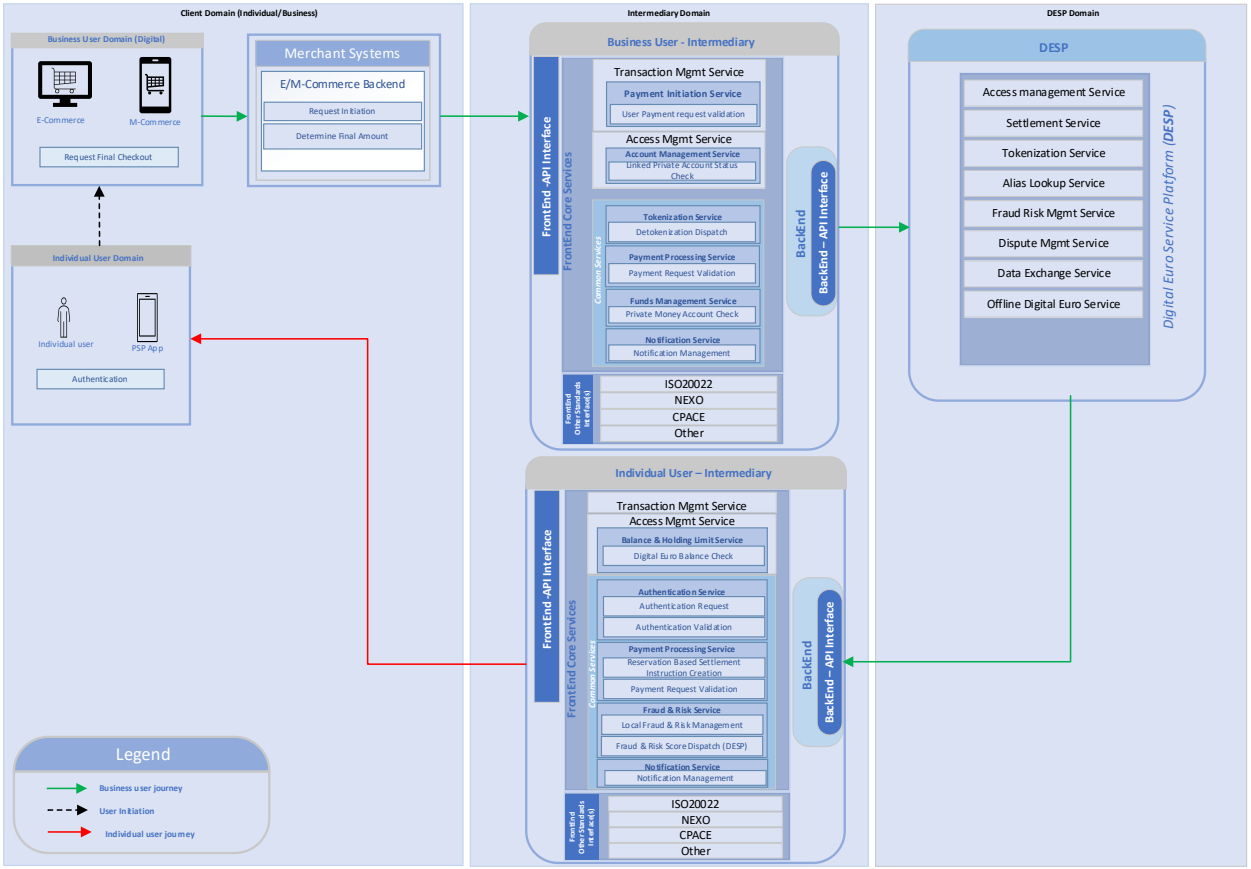


Figure 16 - Pre-authorisation service on e/m-commerce - final check out

4.2.3.6 Modification of a pre-authorisation

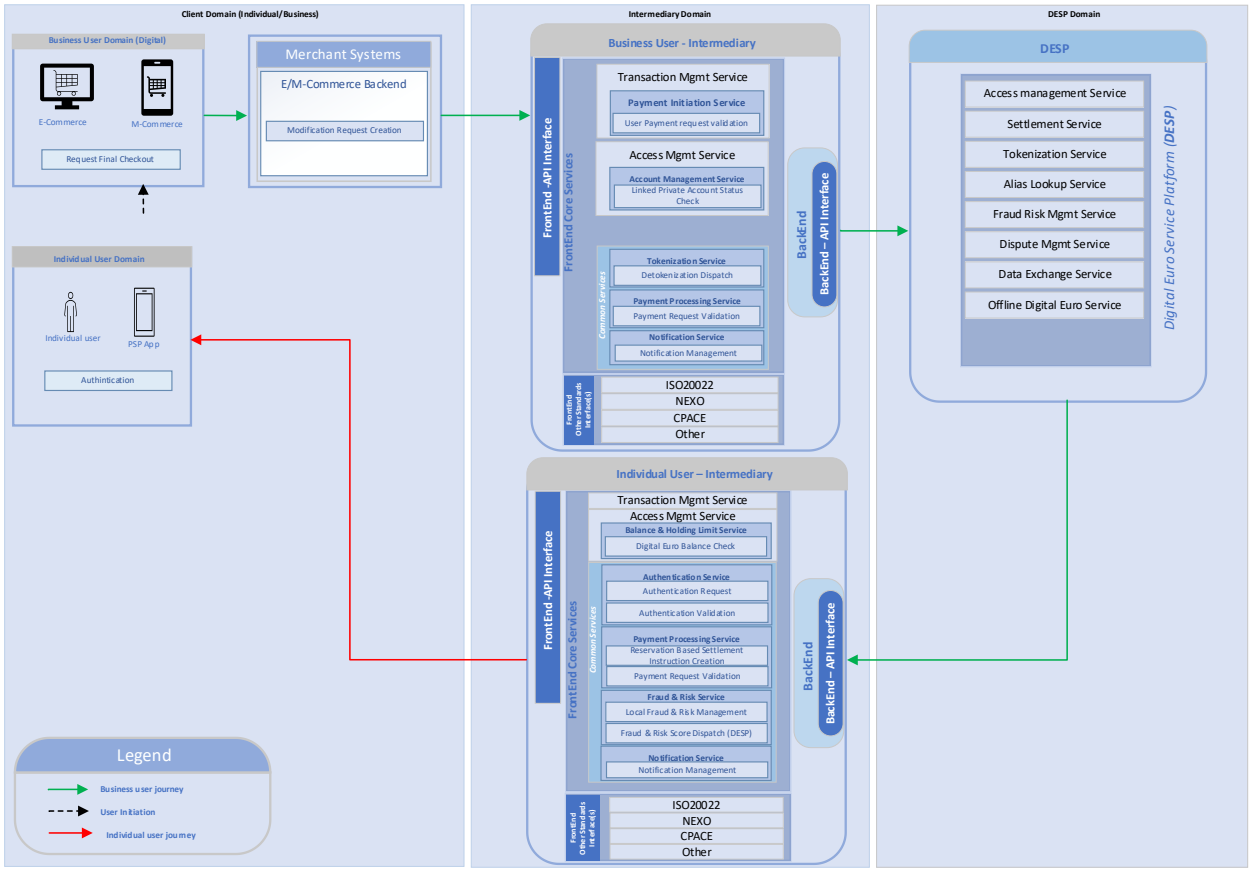


Figure 17 - Modification of a pre-authorisation

4.2.4 Refund Transactions

4.2.4.1 Refund on e-commerce

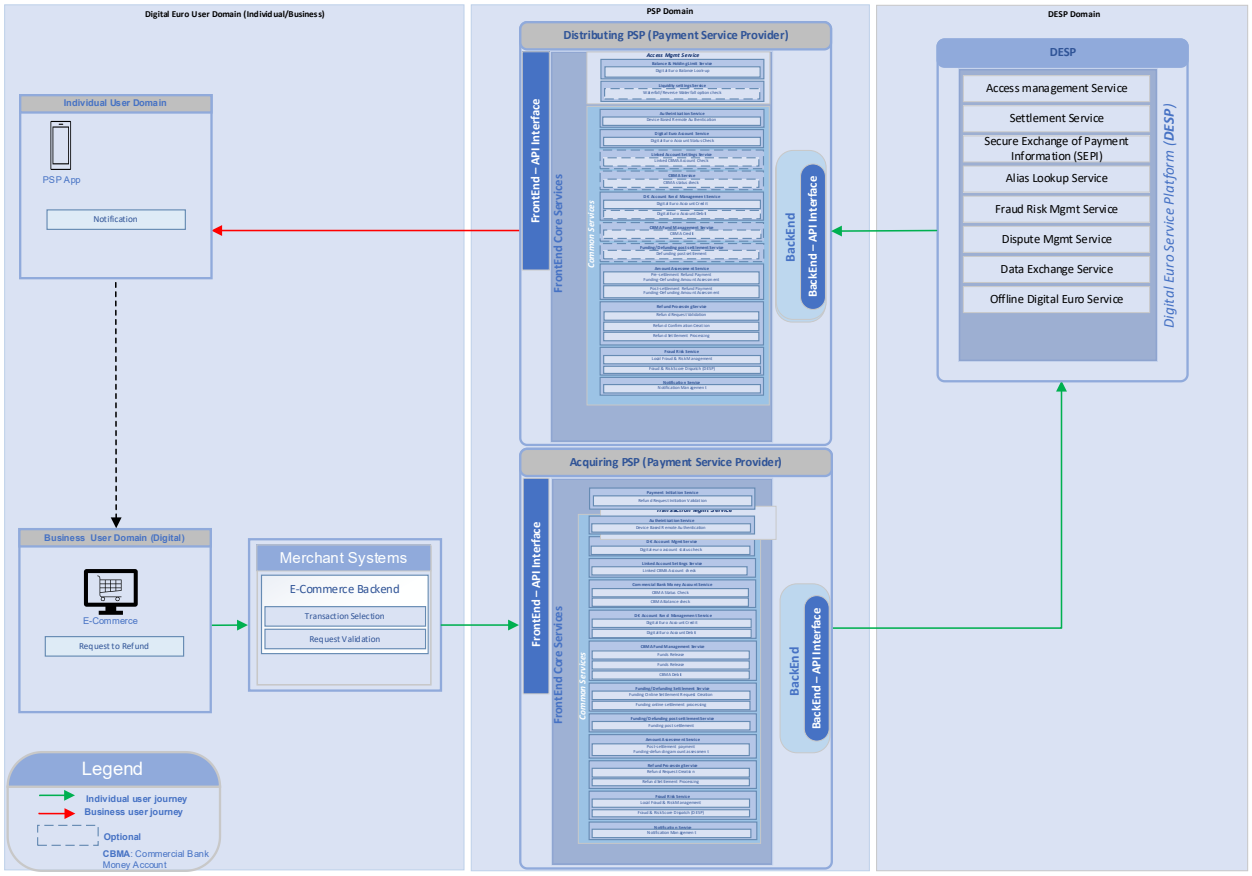


Figure 18 - Refund on e-commerce

4.2.5 Transactions at POS

4.2.5.1 NFC mobile payment

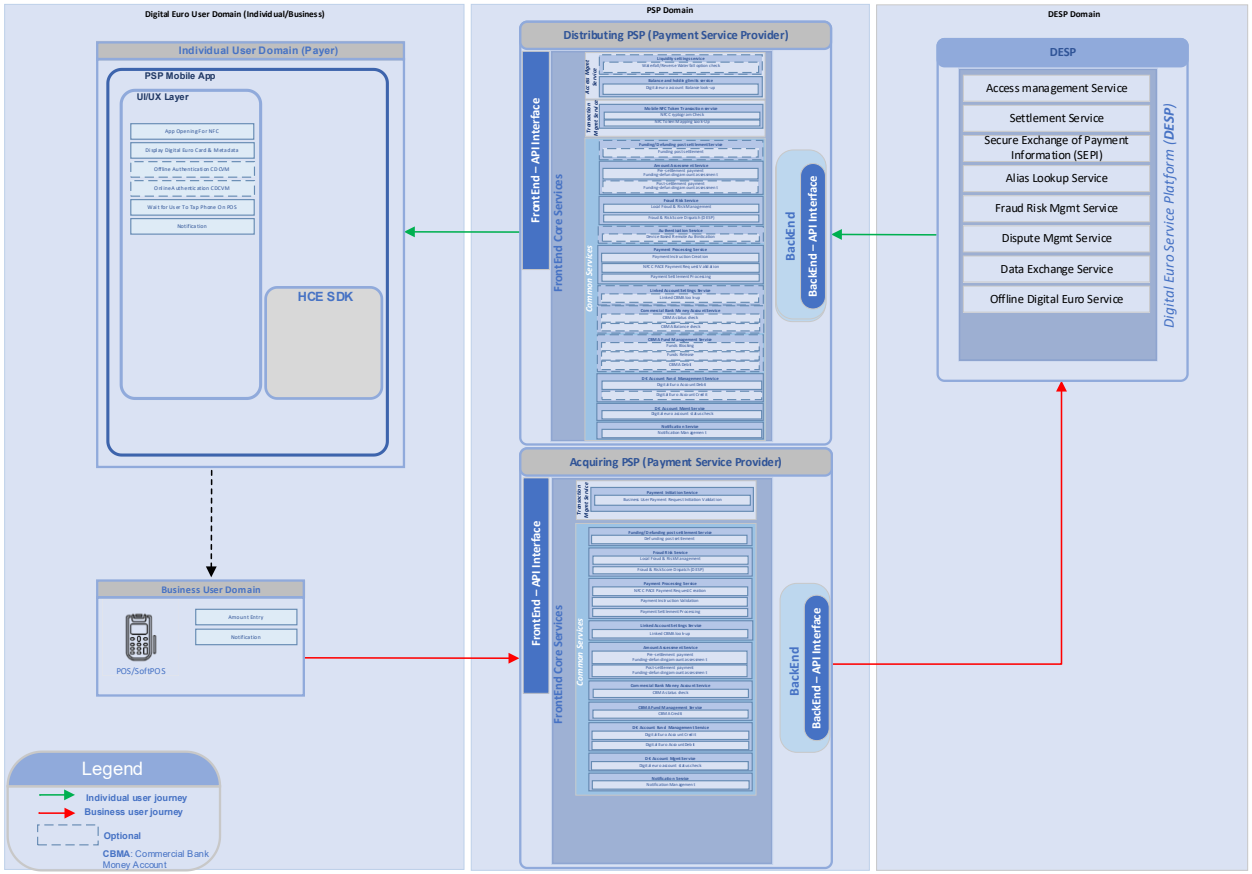


Figure 19 - Transactions at POS - NFC mobile payment

5 List of services

The graphical representations shown in the previous section list services and functions needed to support e/m-commerce transactions. They are described in this document.

Service	Function	Description of function	Core service
Business user access management service *Management of requests initiated by a business user who:* - *wants to be onboarded as a digital euro user* - *wants to close their Digital euro payment account* *Management of requests initiated by a PSP*	New digital euro business user registration request validation	The acquiring PSP checks if the registration request sent by the end-user is valid	Access management service
	New digital euro business user registration	The acquiring PSP registers the business user as a digital euro user.	Access management service
	New digital euro business user offboarding request validation	The acquiring PSP checks if the offboarding request sent by the end-user is valid	Access management service
	Digital euro business user deregistration	The acquiring PSP orchestrates the final steps as part of the offboarding request	Access management service
	Digital euro business user offboarding by acquiring PSP	The acquiring PSP initiates the business user offboarding and orchestrates the required steps	Access management service
Acceptance solutions services *Management of acceptance solutions (configuration and deactivation)*	Acceptance solutions settings	The acquiring PSP ensures that all payment channels (in-store POS, e-commerce gateway, omnichannel features) are properly parameterised to accept payments in digital euro.	Access management service
	Acceptance solutions deactivation	The acquiring PSP manages the deactivation of the acceptance solution as part of the offboarding process	Access management service
Non-digital euro payment account service *Management of the non-digital euro payment account involved in digital euro processes.*	Non-digital euro payment account status check	The PSP servicing the non-digital euro payment account verifies the operational status of a non-digital euro payment account. It ensures that the account is active, valid, and ready for transactions.	Common service
Digital euro payment account service *Management of digital euro payment account*	Digital euro payment account (un)blocking request validation	The PSP checks if the digital euro payment account blocking or digital euro payment account unblocking request sent by the end-user's device is valid	Common service
	Digital euro payment account blocking	The PSP blocks the Digital euro payment account	Common service

Service	Function	Description of function	Core service
settings and lifecycle	Digital euro payment account unblocking	The PSP unblocks the Digital euro payment account	Common service
	DEAN registration	The PSP requests a DEAN to DESP and stored it.	Common service
	DEAN registration and PSP mapping removal	The PSP requests a DEAN registration and PSP mapping removal to DESP as part of the offboarding process	Common service
	DEAN validity check	The acquiring PSP checks the DEAN provided by the payer is consistent	Common service
Fraud and compliance risks service *Management of central score and local fraud and sanction controls to block litigious or suspicious transactions according to the current regulation*	Fraud and risk score dispatch	The PSP servicing the digital euro payment account requests a risk score to DESP to perform the local fraud and risk check	Common service
	Local fraud and sanction check	The PSP servicing the digital euro payment account receives score risk from DESP and combines it with its own score risk to block or proceed with the payment	Common service
Notification settings service *Management of parameters defined by the end-user to receive notifications*	Notification settings request validation	The acquiring PSP validates if the notification settings request sent by the end-user's device is valid	Access management service
	Notification settings storage	The acquiring PSP stores the parameters	Access management service
	Notification settings removal	The acquiring PSP removes the notification settings as part of the individual user offboarding	Access management service
Payment Initiation service *Management of payment requests initiated by an end-user (covering all form factors)*	Alias validity check	The PSP checks the alias consistency and triggers the alias look-up dispatch function.	Common service
	Alias look-up dispatch	The PSP servicing digital euro payment account requests an alias resolution to DESP to retrieve DEAN and PSP ID	Common service
	PSP ID look-up	The PSP servicing digital euro payment account requests the PSP ID corresponding to the DEAN to DESP for routing purpose	Common service
	Tokenisation service	The PSP servicing digital euro payment account requests tokenisation or detokenisation to DESP to process QR code or Pay-by-Link payments.	Common service

Service	Function	Description of function	Core service
	Link creation	The PSP servicing digital euro payment account generate a link for pay-by-link transactions	Common service
	Business user payment request initiation validation	The PSP servicing digital euro payment account checks the payment request sent by the end-user is consistent and contains mandatory information	Transaction management service
	Refund request initiation validation	The PSP servicing digital euro payment account checks the refund request is consistent and contains mandatory information	Transaction management service
Linked account settings service *Management of the link between a non-digital euro payment account and the digital euro payment account*	Linked account settings request validation	The PSP checks if the linked account settings request is valid	Common service
	Linked account settings storage	The PSP stores the information related to linked non-digital euro payment account (new link, updated link, link removal)	Common service
	Linked account settings removal	The PSP removes the link between the non-digital euro payment account and the digital euro payment account as part of the business user offboarding	Common service
	Linked non-digital euro payment account ownership validation	The PSP receives proof of non-digital euro payment account ownership and validates it	Common service
	Linked non-digital euro payment account look-up	The PSP checks whether the end-user has linked a non-digital euro payment account to the digital euro payment account.	Common service
	Linked non-digital euro payment account check	During a payment transaction that requires a waterfall or reverse waterfall process, the PSP checks whether the digital euro payment account is linked to a non-digital euro payment account and, if so, returns the IBAN of that linked account.	Common service
Recurring payment service *Management of recurring payment (set-up, modification, termination, periodic payment transaction)*	Recurring payment set-up request validation	The PSP servicing digital euro payment account checks the set-up request sent by the end-user (merchant) is valid	Transaction management service
	Recurring service update request validation	The PSP servicing digital euro payment account checks the update request sent by the end-user is valid	Transaction management service
	Recurring service termination request validation	The PSP servicing digital euro payment account checks the termination request sent by the end-user is valid	Transaction management service
	Active recurring payments parameters storage	The PSP servicing digital euro payment account stores the recurring payments parameters (after an initial set-up or an update request)	Transaction management service

Service	Function	Description of function	Core service
	Active recurring payment termination	The PSP servicing digital euro payment account terminates an active recurring payment according to the request received from the user	Transaction management service
	Active recurring payment parameters update	The PSP servicing digital euro payment account updates an active recurring payment parameter according to the request received from the user	Transaction management service
	Recurring payment coded user and authorisation details storage	The PSP servicing digital euro payment account stores the details of a recurring payment	Transaction management service
	Recurring payment transaction validation	The PSP servicing digital euro payment account checks the periodic transaction sent by the end-user (merchant) is valid	Transaction management service
Payment processing service *Management of payment after request initiation – in relation to DESP*	**Payment request creation**	The digital euro payee PSP servicing digital euro payment account generates a payment request to DESP	Common service
	Payment request validation	The PSP servicing digital euro payment account receives a payment request from DESP and validates its consistency	Common service
	Payment instruction creation	The digital euro payer PSP sends the request with a payment instruction (single or combined transaction)	Common service
	Payment instruction validation	The PSP servicing digital euro payment account receives a payment instruction from DESP, validates its consistency and complements it.	Common service
	Payment settlement processing	The PSP manages the lifecycle of a payment instruction or payment request in alignment with the settlement phase status	Common service
Non-digital euro payment account funds management service *Management of rules to manage funds in* non-digital euro payment account*s (debit, credit, block, release)*	Non-digital euro payment account debit	The PSP servicing non-digital euro payment account defunds non-digital euro payment account	Common service
	Non-digital euro payment account credit	The PSP servicing non-digital euro payment account funds non-digital euro payment account	Common service
	Funds blocking	The PSP servicing non-digital euro payment account blocks funds on non-digital euro payment account if reverse waterfall is needed for transaction proper execution	Common service
	Funds release	The PSP servicing non-digital euro payment account releases funds blocked on non-digital euro payment account if the transaction is discontinued.	Common service

Service	Function	Description of function	Core service
Digital euro funds management service *Management of rules to handle funds in digital euro payment account (debit, credit)*	Digital euro payment account debit	The PSP servicing the digital euro payment account debits the digital euro payment account	Common service
	Digital euro payment account credit	The PSP servicing the digital euro payment account credits the digital euro payment account	Common service

All the services, functions identified as common service are described in **Specifications#5 common services.**

6 Access management service

Access management core services are dedicated to functions needed for users and accounts management.

6.1 Business user access management service

The business user access management service is triggered during onboarding, offboarding, and throughout the user lifecycle. It offers a set of functions dedicated to digital euro user management, which are executed at specific stages of various use cases.

Business users can only be registered as a new digital euro user if they are already a client of the PSP.

As the creation of a new client is carried out in compliance with the current regulations and following the established process, the corresponding steps are not detailed in the current document.

Service	Function/sub-functions	Description
Business user access management service	New digital euro business user registration request validation	The acquiring PSP checks if the registration request sent by the end-user's device is valid
	New digital euro business user registration	The acquiring PSP registers the individual user as a digital euro user.
	Business user offboarding request validation	The acquiring PSP checks if the registration request sent by the end-user's device is valid, the pre-requisites are met and schedule contract cancellation.

6.1.1 Functions description

6.1.1.1 New digital euro business user registration request validation

6.1.1.1.1 Pre-requisite

The business end user is an existing customer of the acquiring PSP.

The business user could use:

- the PSP app and is already connected to the acquiring PSP through a strong customer authentication process specific to that PSP.
- The PSP web browser is already authenticated and connected to the acquiring PSP.

6.1.1.1.2 Requirements

A digital euro user request is sent by the PSP app or web browser to the acquiring PSP to trigger the onboarding process. The acquiring PSP must validate the request is consistent enough to proceed properly with the registration.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent.
2	M	The following data must be provided: - Account type (DEUR) And the PSP must directly trigger digital euro payment account creation and related steps.
3	M	The function must provide a return code. In case of failure, a reason code must be provided.

6.1.1.1.3 Interface description

A dedicated interface received from a user's device (incoming message) triggers the request validation function. The function generates an outgoing message providing the result of the function execution.

6.1.1.1.3.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Digital euro user registration"	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Type of the new account	Type of account to be opened "DEUR" (to be confirmed)	SSET	4	M	AccountType
Number of digital euro payment account to open	Number of DEAN the business user wants to open	NUM	3	O	***(New for digital euro)***

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification

Data element	Description	Type	Length	Presence indicator	Standardised name
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC		M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	SSET	4	O	StatusReason

6.1.1.1.3.2 Return code

#	Description
0	Successful
1	Failure

6.1.1.1.3.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.1.1.2 New digital euro business user registration

6.1.1.2.1 Requirements

The acquiring PSP creates a new digital euro user and stores minimum set of data. The function is triggered when the “new digital euro user registration request validation” function is successfully executed.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The acquiring PSP must create the digital euro user data envelop that is: - complemented during the onboarding process, - updated during amendment process and offboarding process
2	M	The digital euro user data envelop must contain the following data: - Digital euro user identifier - Technical proof - Entry identifier - Digital euro user type - Digital euro user creation date - Digital euro user status - Digital euro user country - Digital euro user language
3	M	The acquiring PSP has to link the digital euro user identifier with the PSP app ID associated with the app that initiated the request.

#	Mandatory Optional Conditional	Description
4	M	The digital euro user identifier must be generated according to the following rules (placeholder)
5	M	The technical proof must be generated according to the following rules (placeholder)
6	M	The entry identifier must be generated according to the following rules (placeholder)
6	M	The digital euro user creation date must be equal to the current date
7	M	The digital euro user status must be initiated according to the digital euro user lifecycle. - **PENDING**: the client is registered but has not yet opened a Digital euro payment account
7	M	The digital euro user type must be “Business” (BUSI)
8	M	The function must provide a return code. In case of failure, a reason code must be provided.

6.1.1.2.2 Interface description

This function is triggered without any interface exchanged between the end-user’s device and the acquiring PSP.

The result of the new digital euro individual user registration function is sent through an outgoing message.

6.1.1.2.2.1 Message structure

- Incoming message

The incoming message is the request received from the device and validated by the new digital euro business user request validation function. [Refer to Section 6.1.1.1.3.1]

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	36	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	36	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Identifier of the digital euro user	Unique identifier of the digital euro user. Populated if the process is successful	STR	TBD	O	***(New for digital euro)***
Technical proof	Cryptographic root key used to prove the ownership of holdings.	STR	TBD	O	***(New for digital euro)***

Data element	Description	Type	Length	Presence indicator	Standardised name
	Populated if the process is successful				
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	M	StatusReason

6.1.1.2.2.2 Return code

#	Description
0	Successful
1	Failure

6.1.1.2.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.1.1.3 Digital euro business user offboarding request validation

6.1.1.3.1 Requirements

The digital euro business user intends to close their digital euro payment account and has submitted a request to the acquiring PSP servicing the digital euro payment accounts through their device.

The acquiring PSP must validate the request is consistent and valid and that the pre-requisites are fulfilled.

All the digital euro payment accounts owned by the business user will be closed.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The request must contain the user ID
3	M	The request must contain the reference of the contract to be cancelled
4	M	The acquiring PSP must check the following conditions: - there aren't any pre-disputes, and/or disputes still not closed - Any digital euro payment account has been previously blocked by the PSP blocked. If the conditions are not met, the request must be rejected
5	C	If the offboarding request is valid, - the status of the digital euro user must be updated to indicate the ongoing offboarding

#	Mandatory Optional Conditional	Description
		- the contract target closing date must be defined and entered into the system to schedule further steps (acceptance solution disablement and digital euro payment account blocking)
6	M	The function must provide a return code. In case of failure, a reason code must be provided.

6.1.1.3.2 Interface description

A dedicated interface received from a user's device (incoming message) triggers the request validation function. The function generates an outgoing message providing the result of the function execution.

6.1.1.3.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Individual user offboarding"	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Identifier of the digital euro user	Unique identifier of the digital euro user	STR	TBD	M	***(New for digital euro)***
Digital euro contract identifier	Unique identifier of the contract to be closed	STR	35	M	RegisteredContractIndentification

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

6.1.1.3.2.2 Return code

#	Description
0	Successful
1	Failure

6.1.1.3.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.1.1.4 Digital euro business user deregistration

6.1.1.4.1 Requirements

As part of business user offboarding process, the final steps must be orchestrated by the acquiring PSP servicing the digital euro payment account. The user deregistration function is activated once the DESP has confirmed the DEAN deregistration and PSP mapping removal.

Business rules

#	Mandatory Optional Conditional	Description
1	M	- The acquiring PSP must check if a non-digital euro payment account is still linked to the digital euro payment account **Refer to [Specifications#5 – Linked account settings service]**
2	C	- If a non-digital euro payment account is still linked to a digital euro payment account, the acquiring PSP must remove the existing link **Refer to [Specifications#5 – Linked account settings service]**
3	M	- The acquiring PSP must remove the notification settings still defined for the digital euro user **Refer to [Specifications#2 – Notification settings service]**
4	M	- The acquiring PSP must request the digital euro user deactivation **Refer to [Specifications#5 – Digital euro user deactivation]**
5	C	If the deactivation is successful, the following data must be updated: - Digital euro user status is updated and switched to “CLOSED” - Digital euro user closing date is populated with the current date
6	M	- The function must provide the return code. In case of failure, a reason code must be provided.

6.1.1.4.2 Interface description

The function is activated by the confirmation message sent by DESP after DEAN deregistration and PSP mapping successful removal.

6.1.1.4.2.1 Message structure

- Incoming message

[[Refer to Digital Euro scheme rulebook v0.91 - Annex D2 - Back-end implementation specifications ➔ POST /DEANs-deactivations – Response]

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message Populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode

6.1.1.5 Digital euro business user offboarding by acquiring PSP

The offboarding process of a business user can be directly initiated by the acquiring PSP which then orchestrates the various steps:

- Schedules the contract cancellation
- Disables acceptance solutions [Refer to Section 6.3.1.2]
- Blocks the digital euro payment accounts [Refer to Specifications#5/Digital euro payment account service]
- Removes the linked non-digital euro payment account settings [Refer to specifications#5/Linked account settings service]
- Removes the notifications settings [Refer to Section 6.4.1.3]
- Requests DEAN(s) deregistration and PSP ID mapping removal [Refer to Specifications#5/Digital euro payment account service]
- Requests Digital euro user deactivation [Refer to Section 6.1.1.4]

6.2 Acceptance solutions service

A business user who has successfully opened a digital euro payment account must have the ability to enable acceptance solutions. At offboarding process, a business user must have the ability to disable acceptance solutions.

Service	Function/sub-functions	Description
	Acceptance solutions settings	The acquiring PSP performs the settings of acceptance solutions during the onboarding process or business user lifecycle management

Service	Function/sub-functions	Description
Acceptance solutions service	Acceptance solutions disablement	The acquiring PSP disables the acceptance solutions during the offboarding process

6.2.1 Functions description

6.2.1.1 Acceptance solutions settings

The acquiring PSP is responsible for configuring and activating the payment acceptance solutions according to the merchant's preferences. The acquiring PSP ensures that all payment channels (in-store POS, e-commerce gateway, omnichannel features) are properly parameterised to accept payments in digital euro. This includes activating the necessary payment methods and the communication technology.

Depending on the payment method, ECB may provide a configuration kit. The acquiring PSP must comply with the instructions in the kit (e.g. configuring the CPACE Kernel).

As such acceptance solution settings depends on the merchant's IT system and their payment gateway capabilities, **the deployment of configurations is determined by each acquiring PSP** and includes its providers and merchants.

6.2.1.2 Acceptance solutions deactivation

When an end-user initiates an offboarding request, all previously applied acceptance solution settings must be removed. This specific step in the offboarding process is carried out under the coordination of the acquiring PSP and is triggered once the contract cancellation date (defined when the business user onboarding request is received), is reached.

The deactivation of acceptance solutions, just like their configuration, **is determined by each acquiring PSP** and includes its providers and merchants.

6.3 Notification settings service

Once a business user has successfully opened at least a Digital euro payment account, they must be able to configure the events that trigger notifications. This service enables the definition, modification, or removal of notification configuration parameters.

Assumptions: Settings are managed at the level of the digital euro end user. The functions and the business rules are defined accordingly. Same settings are applied to all the DEANs.

Service	Function/sub-functions	Description
	Notification settings request validation	The acquiring PSP checks if the notification settings request sent by the end-user's device is valid

Service	Function/sub-functions	Description
Notification settings service	Notification settings storage	The acquiring PSP stores the new or updated parameters and confirms the settings
	Notification settings removal	The acquiring PSP clears all the parameters when the business user is offboarded

6.3.1 Functions description

6.3.1.1 Notification settings request validation

6.3.1.1.1 Pre-requisite

The business end user has been provided with a device either after completing a KYC process as a prospective client, or as an existing customer of the acquiring PSP.

6.3.1.1.2 Requirements

The end-user must be able to request dedicated notification settings through their own device. The corresponding request is received by the acquiring PSP servicing the Digital euro payment account, which must verify that the request is valid and consistent.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The request must contain the user ID
3	M	The request must contain the type of request - CREATE ➔ Initial set-up - UPDATE ➔ Set-up amendment - DELETE ➔ Set-up removal
4	M	The request can be set to 'CREATE' only if no existing parameters are already defined
5	C	If the request type is set to “CREATE”, at least one parameter must be populated
6	C	If the digital euro payment account credit event aggregation indicator is set to ‘Yes’, the corresponding frequency must be defined.
7	C	If the digital euro payment account debit event aggregation indicator is set to ‘Yes’, the corresponding frequency must be defined.
8	C	If the Waterfall event aggregation indicator is set to ‘Yes’, the corresponding frequency must be defined.
9	C	If the reverse waterfall event aggregation indicator is set to ‘Yes’, the corresponding frequency must be defined.
10	C	If the aggregated notifications indicator is set to ‘Yes’, the corresponding frequency must be defined.
11	M	The request can be set to UPDATE” or “DELETE” only if a configuration already exists for the Digital euro payment account.
12	M	The function must provide a return code. In case of failure, a reason code must be provided.

#	Mandatory Optional Conditional	Description
13	C	If the function execution is successful, the acquiring PSP must trigger notification settings storage function **(refer to Section 6.3.1.2)**

6.3.1.1.3 Interface description

A dedicated interface received from a user's device (incoming message) triggers the notification settings request validation. The function generates an outgoing message providing the result of the function execution.

6.3.1.1.3.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Notification settings request"	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Type of request	Type of request sent by the end-user' device. - **CRED - CREATE** - **UPDT - UPDATE** - **DELT - DELETE**	SSET	4	M	RequestType
Communication channel type	Method by which the notification is delivered - **EMAL** (transmission by email) - **ONLI** (transmission online – e.g. inApp) - **MBNO** (transmission by mobile phone) - **FILE** (transmission by file transfer)	SSET	4	M	CommunicationMethodCode
Communication channel value	Detailed information of the method chosen to receive notification	STR	140	M	CommunicationMethodValue
Digital euro payment account credit event indicator	Specifies whether a notification is triggered when the digital euro payment account is credited.	BOOL	1	O	***(New for digital euro)***
Digital euro payment account credit event aggregation indicator	Specifies whether the end-user requests aggregated notifications for digital euro payment account credit event	BOOL	1	O	***(New for digital euro)***
Digital euro payment account credit event aggregation frequency	Specifies the applicable frequency for aggregated digital euro credit event notifications (ISO Frequency7Code)	SSET	4	O	Frequency

Data element	Description	Type	Length	Presence indicator	Standardised name
Digital euro payment account debit event indicator	Specifies whether a notification is triggered when the digital euro payment account is debited.	BOOL	1	O	***(New for digital euro)***
Digital euro payment account debit event aggregation indicator	Specifies whether the end-user requests aggregated notifications for digital euro payment account debit event	BOOL	1	O	***(New for digital euro)***
Digital euro payment account debit event aggregation frequency	Specifies the applicable frequency for aggregated digital euro debit event notifications (ISO Frequency7Code)	SSET	4	O	Frequency
Waterfall transaction event indicator	Specifies whether a notification is triggered when a waterfall process affects the Digital euro payment account.	BOOL	1	O	***(New for digital euro)***
Waterfall event aggregation indicator	Specifies whether the end-user requests aggregated notifications for waterfall event	BOOL	1	O	***(New for digital euro)***
Waterfall aggregation frequency	Specifies the applicable frequency for aggregated waterfall event notifications (ISO Frequency7Code)	SSET	4	O	Frequency
Reverse waterfall transaction event indicator	Specifies whether a notification is triggered when a reverse waterfall process affects the Digital euro payment account.	BOOL	1	O	***(New for digital euro)***
Reverse waterfall event aggregation indicator	Specifies whether the end-user requests aggregated notifications for reverse waterfall event	BOOL	1	O	***(New for digital euro)***
Reverse waterfall aggregation frequency	Specifies the applicable frequency for aggregated reverse waterfall event notifications (ISO Frequency7Code)	SSET	4	O	Frequency
Aggregated notifications indicator	Specifies whether the end-user requests aggregated notifications compiling all the events	BOOL	1	O	***(New for digital euro)***
Aggregated notifications frequency	Specifies the applicable frequency for aggregated notifications (ISO Frequency7Code)	SSET	4	O	Frequency

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the	Unique identifier of the corresponding incoming message	STR	35	O	OriginalMessageIdentification

Data element	Description	Type	Length	Presence indicator	Standardised name
incoming message	Populated if the function is triggered by an incoming message.				
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

6.3.1.1.3.2 Return code

#	Description
0	Successful
1	Failure

6.3.1.1.3.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.3.1.2 Notification settings storage

6.3.1.2.1 Requirements

Once the acquiring PSP validates the notification settings request initiated by the end-user through device, the new or updated parameters are stored.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The acquiring PSP must store the notification parameters provided by the end-user.
2	M	Only new or updated information must be stored.
3	M	An amendment date must be stored. It must be in accordance with the current date
4	C	If the event parameter is set to “False”, it should be interpreted as opting out.
5	C	If the event parameter is set to “True”, it should be interpreted as opting in.
6	M	The function must provide a return code to confirm or reject the notification settings

6.3.1.2.2 Interface description

This function is triggered without any interface exchanged between the payer device and the acquiring PSP. It is triggered by the acquiring PSP during the notification settings process.
The result of the storage function is sent through an outgoing message.

6.3.1.2.2.1 Message structure

- Incoming message

The incoming message is the request received from the device and validated by the notification settings request validation function. [Refer to Section 6.3.1.1.3.1]

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the	Unique identifier of the corresponding incoming message	STR	35	O	OriginalMessageIdentification

Data element	Description	Type	Length	Presence indicator	Standardised name
incoming message	Populated if the function is triggered by an incoming message.				
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

6.3.1.2.2.2 Return code

#	Description
0	Successful
1	Failure

6.3.1.2.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.3.1.3 Notification settings removal

6.3.1.3.1 Requirements

When an end-user initiates an offboarding request, any previous notification settings must be removed.

This dedicated step of the offboarding process is executed under the coordination of the acquiring PSP.

This function can be executed as many times as needed to consider all the DEAN of the business user.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The request must contain the DEAN
3	M	The acquiring PSP must remove all the notification settings defined for the DEAN
4	O	An amendment date could be stored. It must be in accordance with the current date
5	M	The function must provide a return code. In case of failure, a reason code must be provided.

6.3.1.3.1.1 Message structure

- Incoming message

The incoming message is generated by the acquiring PSP and contains the following data

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: “Notification settings removal””	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Digital euro payment account Number	Identification of the digital euro payment account	STR	18	M	***(New for digital euro)***

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

6.3.1.3.1.2 Return code

#	Description
0	Successful
1	Failure

6.3.1.3.1.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

6.4 Linked account settings service

An end-user who has successfully opened a digital euro payment account must have the ability to link a non-digital euro payment account to their digital euro payment account for funding and defunding purposes. The link between both accounts is a pre-requisite to waterfall and reverse waterfall processes. This service is activated to define, update or remove the link.

Service	Function/sub-functions	Description
Linked account settings service	Linked account settings request validation	The PSP checks if the linked account settings request is valid
	Linked account settings storage	The PSP stores the information related to linked non-digital euro payment account (new link, updated link, link removal) upon end-user request.
	Linked account settings removal	The PSP clears the linked account when the individual user is offboarded
	Linked non-digital euro payment account ownership validation	The PSP receives proof of non-digital euro payment account ownership and validates it
	Linked non-digital euro payment account look-up	The PSP checks whether the end-user has linked a non-digital euro payment account to the digital euro payment account.
	Linked non-digital euro payment account check	During a payment transaction that requires a waterfall or reverse-waterfall process, the PSP checks whether the digital euro payment account is linked to a non-digital euro payment account and, if so, returns the IBAN of that linked account.

Those functions are used by several processes performed by both distributing and acquiring PSPs and are described as a common function. **[Refer to Specifications#5 – Common services].**

6.5 Digital euro payment account service

The digital euro payment account service is triggered during the onboarding of an end-user, throughout the digital euro payment account lifecycle management. It also offers some functions to validate that the conditions are met for a digital euro transaction proper execution.

Service	Function/sub-functions	Description
Digital euro payment account status	Digital euro payment account status check	The PSP checks the digital euro payment account status
	Digital euro payment account (un)blocking request validation	The PSP checks if the digital euro payment account blocking or digital euro payment account unblocking request sent by the end-user's device is valid
	Digital euro payment account blocking	The PSP blocks the digital euro payment account
	Digital euro payment account unblocking	The PSP unblocks the digital euro payment account
	DEAN registration	The PSP requests a DEAN to DESP and stores it.
	DEAN Validity check	The PSP servicing the digital euro payment account checks if the DEAN provided is consistent
	DEAN registration and PSP mapping removal	The PSP requests to DESP the deregistration of the digital euro account number (DEAN) and the removal of its mapping to the PSP.

Those functions are used by several processes performed by both distributing and acquiring PSPs and are described as a common function. **[Refer to Specifications#5 – Common services].**

6.6 Non-digital euro payment account service

Non-digital euro payment account service is invoked during a payment transaction process by the PSP servicing the non-digital euro payment account of the user. It offers the needed functions to validate that the conditions are met for a digital euro transaction proper execution.

Service	Reference	Function	Description
Non-digital euro payment account service		Non-digital euro payment account status check	The PSP servicing non-digital euro payment account verifies the operational status of a non-digital euro payment account

This function is used by several processes performed by both distributing and acquiring PSPs and is described as a common function. **[Refer to Specifications#5 – Common services].**

7 Liquidity management service

The liquidity management core services are dedicated to functions needed for funding and defunding the digital euro payment account and the non-digital euro payment account.

The following services are identified for the current scope of use cases:

- Non-digital euro payment account funds management service
- Digital euro payment account funds management service

7.1 Non-digital euro payment account funds management service

Non-digital euro payment account funds management service is invoked during a payment or a funding-defunding transaction process by the PSP servicing the non-digital euro payment account of the user. It offers the needed functions to handle the non-digital euro payment account funds.

Service	Reference	Function	Description
Non-digital euro payment account funds management service		Non-digital euro payment account debit	The PSP servicing non-digital euro payment account defunds non-digital euro payment account
		Non-digital euro payment account credit	The PSP servicing non-digital euro payment account funds non-digital euro payment account
		Funds blocking	The PSP servicing non-digital euro payment account blocks funds on non-digital euro payment account if reverse waterfall is needed for transaction execution and in funding processes
		Funds release	The PSP servicing non-digital euro payment account releases funds blocked on non-digital euro payment account if the process is discontinued.

This service is used in several processes and is described as a common function. **[Refer to Specifications#5 – Common services].**

7.2 Digital euro payment account funds management service

Digital euro funds management service is invoked during a payment transaction process (to debit or credit the digital euro payment account) or a funding or defunding process by the PSP servicing the digital euro payment account of the user.

Service	Reference	Function	Description
Digital euro payment account funds management service		Digital euro payment account debit	The PSP servicing the digital euro payment account debits the digital euro payment account
		Digital euro payment account credit	The PSP servicing the digital euro payment account credits the digital euro payment account

This service is used in several processes and is described as a common function. **[Refer to Specifications#5 – Common services].**

8 Transaction management service

Transaction management core services are dedicated to functions needed for paying or receiving payments in digital euro, where digital euros are transferred between two end-user accounts.

In the context of e/m-commerce transactions, two main services are needed to manage e/m-commerce one-time payments and e/m-commerce recurring payments. All the payment methods are covered:

- Payment initiation service
- Recurring payment service

8.1 Payment initiation service

The Payment initiation service offers the functions to initiate the payment process regardless of the form factors.

Service	Reference	Function	
Payment initiation service		DEAN validity check	The PSP servicing digital euro payment account checks if the DEAN is consistent
		Alias validity check	The PSP servicing the digital euro payment account receives an alias validity check from a device, checks the consistency and triggers the alias look-up dispatch
		Alias look-up dispatch	The PSP servicing digital euro payment account requests an alias resolution to DESP to retrieve payee's details
		PSP ID look-up dispatch	The PSP servicing digital euro payment account requests the PSP ID corresponding to the DEAN to DESP for routing purpose
		Tokenisation request	The PSP servicing digital euro receives a payment request through QR or Pay-by-link and requests a token from DESP.
		Pay-by-link creation	The PSP servicing digital euro payment account generates a payment link.
		Business user payment request initiation validation	The PSP servicing digital euro payment account checks the payment request sent by the business user is consistent and contains mandatory information
		Payment refund instruction initiation Validation	This feature allows the business user (through its acquiring PSP) to initiate a refund for a transaction paid by a payer.

8.1.1 Functions description

8.1.1.1 Alias validity check

This function is used by several processes and is described as a common function. **[Refer to Specifications#5 – Common services]**

8.1.1.2 Alias look-up dispatch

This function is used by several processes and is described as a common function. **[Refer to Specifications#5 – Common services]**

8.1.1.3 PSP ID look-up dispatch

This function is used by several processes and is described as a common function. **[Refer to Specifications#5 – Common services]**

8.1.1.4 Tokenisation request

This function is used by several processes and is described as a common function. **[Refer to Specifications#5 – Common services]**

8.1.1.5 Pay-by-link creation

This function is used by several processes and is described as a common function. **[Refer to Specifications#5 – Common services]**

8.1.1.6 Business user payment request initiation validation

8.1.1.6.1 Requirements

In e/m-commerce or proximity payment context, a payment request is sent by the payee to the payee's PSP to trigger the payment processing. The PSP must validate the payment request is complete to proceed with the payment.
The request could be initiated for a one-time payment, for a single pre-authorisation, for a periodic transaction in case of recurring payment, at final check-out after a pre-authorisation.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	Following data must always be provided: - Message identifier - Event identifier - Message date time - Transaction initiation method - Transaction type - Transaction amount - Transaction currency - Transaction date - Payee trade name - Payee DEAN (Merchant DEAN) - Payee location (address) - Payee location (city) - Payee location (postcode) - Payee location (country) - Merchant category code - Transaction identification
3	M	The transaction type must be populated with "PB01" (POI payment – e-com / POS)
4	O/C	Structured remittance information or Unstructured Remittance information could be provided. If Structured remittance information is provided, unstructured remittance information must not be present and vice-versa.
5	C	If the structured remittance information is provided, the reference must at least be present.
6	C	If the transaction initiation method is "Alias" and the transaction type is "Purchase", following data must be provided: - Payer alias type - Payer alias value
7	C	If the transaction initiation method is "Alias" and the transaction type is "Reservation", following data must be provided: - Payer alias type - Payer alias value - Reservation identification - Reservation expiry date time
8	C	If the transaction initiation method is "DEAN", 'QR Code" or "Pay-by-link" and the transaction type is "Purchase", following data must be provided: - Payer DEAN
9	C	If the transaction initiation method is "DEAN", QR Code" or "Pay-by-link" and the transaction type is "Reservation", following data must be provided: - Payer DEAN - Reservation identification - Reservation expiry date time

#	Mandatory Optional Conditional	Description
10	O	The Payer PSP ID can be provided by the digital point of interaction if it was recovered in a previous step.
11	C	For a CPACE transaction, the acquiring PSP is provided with all the information required to generate the EMV cryptogram data envelope (see the interface description below).
12	C	If the function execution is successful, the acquiring PSP must generate the unique identifier providing an end-to-end reference for the payment transaction and store the transaction. This unique identifier (UETR) format must follow the UUID type (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)
13	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.1.1.6.2 Interface description

A dedicated interface received from the merchant digital point of interaction (incoming message) triggers the business user payment request initiation validation function. The function generates an outgoing message providing the result of the function execution.

8.1.1.6.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of Incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: “User payment request”	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATE TIME UTC	24	M	CreationDateTime
Payer PSP ID	Unique identification of the payer’s PSP (BIC).	STR	11	O	DebtorAgent
Transaction initiation method	Method chosen by the individual user to initiate a payment transaction: - QR code - Pay-by-link - Alias - DEAN Code set to be clarified	STR	4	M	PaymentMethod
Transaction type	Type of transaction initiated by the individual user: - PP01: P2P payment - PB01: POI payment – e-com / POS - BP01: B2P payment - FU01: Funding - DF01: Defunding	SSET	4	M	TransactionType
Transaction Amount	Amount of the transaction	NUM	18	M	Amount
Transaction Currency	Currency of the transaction (code set defined in ISO 4217)	STR	3	M	Currency
Transaction Date	Date of the transaction YYYY-MM-DDThh:hh:sssZ	DATE TIME UTC	24	M	CreationDateTime

Data element	Description	Type	Length	Presence indicator	Standardised name
Payee Name	The legal name of the entity receiving the payment.	STR	70	O	Name
Payee Trade Name	The commercial name under which the payee operates, which may differ from their legal name.	STR	35	M	TradingName
Payee location (address)	Full address of the payee, including street name and number.	STR	70	M	StreetName
Payee location (City)	City where the payee is located.	STR	35	M	TownName
Payee location (Postcode)	Postcode corresponding to the payee's address.	NUM	16	M	PostCode
Payee location (Country)	Country where the payee resides or is registered (code defined in ISO 3166)	STR	2	M	CountryCode
Merchant Category Code	Four-digit code that classifies the business type of the merchant code set defined in ISO 18245	NSET	4	M	MerchantCategoryCode
Structured Remittance	Predefined code/value provided by the payee to the payer, facilitating automated reconciliation.			O	StructuredRemittanceInformation
Reference		STR	35		
Reference Type		STR	35		
Reference Issuer		STR	35		
Unstructured Remittance	Free text or code/value provided by the payee to the payer, facilitating reconciliation.	STR	140	O	UnstructuredRemittanceInformation
Transaction Identification	End-to-end identification entered by the end-user at the initiation of the transaction.	STR	35	O	EndToEndId
Payee DEAN	Digital euro payment account number of the payee	STR	18	M	***(New for digital euro)***
Payer alias type	Payer's alias type entered by the payer Code set defined in ISO ExternalProxyAccountType1code	STR	4	O	AccountProxyType
Payer alias value	Payer's alias value entered by the payer	STR	2048	O	AccountProxy
Payer DEAN	Digital euro payment account number of the payer entered by the payer	STR	18	O	***(New for digital euro)***
Reservation identification	Unique identifier of a reservation	UUID	36	O	UETR
Original reservation identification	Unique identifier of the original reservation in case of cancellation or modification	UUID	36	O	OriginalUETR
Reservation expiry date and time	The date and time at which the reservation ends, and any still reserved amount will be released.	DATE TIME UTC	24	O	ExpiryDateTime

- In coming message supplementary data in case of CPACE transaction: EMV Cryptogram Data Envelope
    - Mobile HCE CPACE transaction

Data element	Description	Type	Length	Presence indicator	Standardised name
PAN token (5A)	Provided by CPACE-HCE processing over the contactless interface	NUM	16	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Issuer application data (9F10)	Profile CCI	BIN	1	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
	DKI (Derivation Key Index)	BIN	1		
	CVR	BIN	5		
Application transaction counter (ATC) (9F36)	Two-byte EMV value that counts the number of transactions performed by the card, incrementing with each new transaction to help detect fraud or replay attacks.	NUM	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Cryptogram information Data (9F27)	One-byte EMV field that indicates the type of cryptogram generated by the card and the status of issuer authentication during a transaction	BIN	1	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Application cryptogram (9F26)	Cryptographic code generated by the EMV card to authenticate a transaction with the issuing bank	BIN	8	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Amount, authorised (9F02)	Amount authorised by the distributing PSP	NUM	12	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Amount, other (9F03)	Part of amount authorised reserved for cashback…	NUM	12	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Transaction type (9C)	EMV Transaction type	NUM	2	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Terminal country code (9F1A)	Terminal country code	NUM	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Terminal verification results – TVR	Terminal verification results	BIN	5	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData

Data element	Description	Type	Length	Presence indicator	Standardised name
Transaction currency code (5F2A)	Transaction currency code	NUM	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Terminal transaction date (9A)	Terminal transaction date	NUM	6	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Unpredictable number (9F37)	A unique variable associated with the generation of the ARQC application cryptogram (discriminating element)	BIN	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
Terminal type (9F35)	See possible values in EMV Book 4 — Terminal type	NUM	2	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData
CVM results (9F34)	The CVM (Cardholder Verification Method) result is returned by the card after processing the terminal's CVM list and attempting cardholder verification (e.g. PIN, signature, no CVM required, etc.).	BIN	3	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRltdData

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.1.1.6.2.2 Return code

#	Description

0	Successful
1	Failure

8.1.1.6.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.1.1.7 Refund request initiation validation

8.1.1.7.1 Requirements

This feature allows the business (through its acquiring PSP) to initiate a refund for a transaction paid by a payer.

The validation of a refund instruction consists of ensuring that the request is complete and consistent, correctly linked to the original transaction, and compliant with business rules such as amount, currency, and mandatory data. The PSP checks message integrity, applies any internal controls, and returns at minimum the refund amount and the transaction identifier, along with either a validation status or a rejection with an error code.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The PSP must implement a mechanism to retrieve the original transaction, and its {id}
2	M	The refund amount may be full or partial, and it may even exceed the original amount when additional costs must be reimbursed to the individual end user.
3	M	The acquiring Payment Service Provider (PSP) is responsible for conducting thorough fraud checks and due diligence procedures related to the merchants it acquires. This includes verifying the legitimacy of the merchant, monitoring transaction patterns for suspicious activity, and implementing appropriate risk mitigation measures to prevent fraudulent behaviour
4	M	The acquiring Payment Service Provider (PSP) is required to perform anti-money laundering (AML) checks on the merchants if acquires. This includes verifying the identity and legitimacy of the merchant, assessing the risk of money laundering based on the merchant's profile and activities, and implementing ongoing monitoring procedures to detect and report any suspicious transactions in compliance with applicable AML regulations.
5	M	The currency applied must match the currency used for the original transaction.
6	C	If the function execution is successful, the acquiring PSP must generate the Unique Identifier providing an end-to-end reference for the payment transaction and store the transaction. This unique Identifier (UETR) format must follow the UUID type (xxxxxxxx-xxxx-xxxx-xxxx-xxxxxxxxxxxx)
7	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.1.1.7.2 Interface description

The data listed below in the incoming message are incomplete. The interaction between the PSP and the merchant about refund request are not detailed. The PSP must retrieve (at least) the identifier of the transaction that is being refunded and consider the refunded amount.
The PSP can choose whether to retrieve all the information originally used to construct the initial transaction, including settlement data.

8.1.1.7.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of Incoming message	STR	35	M	MessageIdentification
Identification of the event	Unique identifier of the event that triggers the message: “Refund”	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Original transaction Identification	Unique end-to-end transaction identification of the payment transaction that is being refunded	UUID	36	M	OriginalUETR
Refund Amount	The amount to be refunded by the merchant.	NUM	18	M	Amount
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.1.1.7.2.2 Return code

#	Description
0	Successful
1	Failure

8.1.1.7.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2 Recurring payment service

The recurring payment service is invoked when a payer requests a recurring payment set-up. It is also used during the recurring payment lifecycle.

Service	Reference	Function	
Recurring payment service		Recurring payment set-up request validation	The PSP servicing digital euro payment account checks the set-up request sent by the end-user (merchant) is valid
		Recurring service update request validation	The PSP servicing digital euro payment account checks the update request sent by the end-user is valid
		Recurring service termination request validation	The PSP servicing digital euro payment account checks the termination request sent by the end-user is valid
		Active recurring payment termination	The PSP servicing digital euro payment account terminates an active recurring payment according to the request received from the user
		Active recurring payment parameters update	The PSP servicing digital euro payment account updates active recurring payment parameters according to the request received from the user
		Recurring payment coded user and authorisation details storage	The PSP servicing digital euro payment account stores the details of a recurring payment
		Recurring payment transaction validation	The PSP servicing digital euro payment account checks the periodic transaction sent by the end-user (merchant) is valid

8.2.1 Description of function

8.2.1.1 Recurring payment set-up request validation

8.2.1.1.1 Requirements

The payer can set up a new recurring payment through e-commerce or m-commerce and provide all the parameters for this purpose. This request is sent by the payee (through the merchant's system) to the payee's PSP. The payee's PSP must validate the consistency of the request.
The following payment methods are offered for recurring payments:

- E-commerce via QR Code
- E-commerce via pay-by-link
- E-commerce via alias
- M-commerce via mobile app

The request validation function will consider all payment methods

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The following data must be provided: - Recurring payment plan identifier - Recurring payment amount (fixed or maximum in case of variable amount[2]) - Recurring payment frequency - Recurring payment start date - Authorisation indicator
3	O	The following data could be provided: - Recurring payment end date - Unstructured remittance - Authorisation end date
4	C	If the authorisation indicator is set to 'Yes', an end-date for the authorisation must be specified.
5	C	If the recurring payment is imitated from the merchant website (e-commerce), the payment method must be provided
6	C	The payment method is provided, it must be QR code or alias or pay-by-link
7	C	If the payment method is QR code or pay-by-link, the request must contain the DEAN of the payer
8	C	If the payment method is alias, the request must contain the alias type and the alias value of the payer.
9	C	If the recurring payment set-up is requested from m-commerce application, the request must contain the DEAN of the payer.
10	M	The function must provide the return code. In case of rejection, a reason code must be provided.
11	O	If the incoming message is accepted and the function execution successful, the recurring payment identifier assigned by the PSP can be provided.

8.2.1.1.2 Interface description

A dedicated interface received from a merchant system (incoming message) triggers the recurring payment set-up request check function. The function generates an outgoing message providing the result of the function execution.

8.2.1.1.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Recurring payment set-up request"	STR	35	M	EventIdentification
Date of the message	Date time of the request creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime

[2] Variable amount for recurring payment will not be offered at Digital euro launch. The corresponding data is nevertheless provided.

Data element	Description	Type	Length	Presence indicator	Standardised name
Transaction initiation method	Method chosen by the individual user to initiate a recurring payment transaction: - QR code - Pay-by-link - Alias - DEAN Code set to be defined	SSET	4	M	PaymentMethod
Recurring payment plan identification	Unique identifier of the recurring payment parameters assigned by the merchant	STR	35	M	PlanIdentification
Recurring payment fixed amount[3]	Amount of money to be transferred when a payment instruction is created as a result of a recurring payment	NUM	18	O	CollectionAmount
Recurring payment variable amount[4]	Maximum amount of money to be transferred when a payment instruction is created as a result of a recurring payment	NUM	18	O	MaximumAmount
Recurring payment currency	Currency associated with the recurring payment plan	STR	3	M	Currency
Recurring payment frequency	Time interval considered to create payment instruction as a result of the recurring payment (ISO Frequency7Code)	SSET	4	M	Frequency
Payer alias type	Payer's Alias type entered by the payer Code set defined in ISO ExternalProxyAccountType1code	STR	4	O	AccountProxyType
Payer alias value	Payer's Alias value entered by the payer	STR	2048	O	AccountProxy
Payer DEAN	Digital euro payment account number of the payer	STR	18	O	***(New for digital euro)***
Recurring payment starting date	Date on which the first payment instruction is created as a result of recurring payment	DATE	10	M	FromDate
Recurring payment end date	Date defining the end of the validity period	DATE	10	O	ToDate
Unstructured Remittance	Free-text or code/value provided by the payee to the payer, facilitating reconciliation.	STR	140	O	UnstructuredRemittanceInformation
Authorisation end-date	Date defining the end of the validity period of the authorisation	DATE	10	O	ToDate

[3] At digital euro launch, only fixed amount for recurring payment will be offered. The provision of this field will be mandatory in this context.
[4] Variable amount for recurring payment will not be offered at digital euro launch. The corresponding data is nevertheless provided.

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message. Populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason
Recurring payment PSP Identifier	Unique identifier of the recurring payment parameters assigned by the PSP	STR	35	O	PlanIdentification

8.2.1.1.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.1.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.2 Recurring service update request validation

8.2.1.2.1 Requirements

The merchant can manage recurring payment parameters update (potentially on payer's request) and the corresponding request is transferred to the merchant's PSP. The PSP must validate the consistency of the update request.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The recurring payment plan identifier must be provided to facilitate the identification of the recurring payment involved The recurring payment plan identifier could be the one assigned by the merchant and transmitted to the PSP during initial set-up, or the one assigned by the PSP and communicated to the merchant after set-up finalisation.

#	Mandatory Optional Conditional	Description
3	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.2.2 Interface description

A dedicated interface received from the merchant's site (incoming message) triggers the recurring payment update request check function. The function generates an outgoing message providing the result of the function execution.

8.2.1.2.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	36	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Recurring payment update request"	STR	36	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Recurring payment plan identification	Unique identifier of the recurring payment parameters assigned by the merchant	STR	35	M	PlanIdentification
Recurring payment frequency	Regular occurrence for a recurring payment (refer to ISO Frequency7Code)	SSET	4	O	Frequency
Recurring payment fixed amount[5]	Amount of money to be transferred when a payment instruction is created because of a recurring payment	NUM	18	O	CollectionAmount
Recurring payment variable amount[6]	Maximum amount of money to be transferred when a payment instruction is created as a result of a recurring payment	NUM	18	O	MaximumAmount
Recurring payment update reason code	Specifies the reason for which parameters are modified Code set to be defined	SSET	4	M	PurposeCode

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification

[5] At digital euro launch, only fixed amount for recurring payment will be offered. The provision of this field will be mandatory in this context.

[6] Variable amount for recurring payment will not be offered at digital euro launch. The corresponding data is nevertheless provided.

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.2.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.2.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.3 Recurring payment termination request validation

8.2.1.3.1 Requirements

The merchant can manage recurring payment parameters update (potentially on payer's request) and the corresponding request is transferred to the merchant's PSP.
The PSP must validate the consistency of the termination request.

Business rules

#	Mandatory Optional Conditional	Description
1	M	The request format and content must be consistent
2	M	The recurring payment plan identifier must be provided to facilitate the identification of the recurring payment involved The recurring payment plan identifier could be the one assigned by the merchant and transmitted to the PSP during initial set-up, or the one assigned by the PSP and communicated to the merchant after set-up finalisation.
3	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.3.2 Interface description

A dedicated interface received from the merchant's site (incoming message) triggers the recurring payment termination request check function. The function generates an outgoing message providing the result of the function execution.

8.2.1.3.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Recurring payment termination request"	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Recurring payment plan identifier	Unique identifier of the recurring payment parameters assigned by the merchant	STR	35	M	PlanIdentification
Recurring payment end date	Date defining the end of the validity period.	DATE	10	O	ToDate
Recurring payment termination reason code	Specifies the reason for which a recurring payment is terminated: - **CTAM** Mandate suspended due to amendment of the contract. - **CTCA** Mandate suspended due to cancellation of the contract, requested by the debtor. - **CTEX** Mandate suspended due to the contract that expired. - **MCFC** Mandate suspended as final collection took place. - **MCOC** Mandate suspended as the once off collection took place. - **MSUC** Mandate suspended after 7 consecutive unsuccessful collections Code set defined in ISO ExternalMandateSuspensionReason1code	SSET	4	M	PurposeCode

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification

Data element	Description	Type	Length	Presence indicator	Standardised name
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.3.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.3.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.4 Active recurring payment parameters storage

A validated recurring payment parameters set-up request or a validated recurring payment parameters update request trigger the storage of corresponding details by the payee's PSP. The details will be used to generate the payment request as a result of a recurring payment according to the frequency.

8.2.1.4.1 Requirements

Business rules

#	Mandatory Optional Conditional	Description
1	M	The new or updated data must be stored
2	C	If the storage is triggered by an update request, previous parameters must be kept for history needs
3	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.4.2 Interface description

This function is triggered without any interface exchanged between the payee and the payee's PSP. The result of the function is provided through an outgoing message.

8.2.1.4.2.1 Message structure

- Incoming message

The incoming message could be:

- In case of initial set-up, the request received from the device and validated by the recurring payment set-up request validation function. [Refer to Section 8.2.1.1.2.1]
- In case of update, the request received from the device and validated by the recurring payment update request validation function. [Refer to Section 8.2.1.2.2.1]

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Recurring payment plan identifier	Unique identification of the recurring payment set of parameters assigned by the PSP.	STR	35	M	PlanIdentifier
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.4.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.4.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.5 Active recurring payment termination

A validated recurring payment termination request triggers the termination of the corresponding recurring payment by the payee's PSP.

8.2.1.5.1 Requirements

Business rules

#	Mandatory Optional Conditional	Description
1	M	The following data must be updated: - Recurring plan end date - Reason for the termination

#	Mandatory Optional Conditional	Description
		- Date of the termination
2	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.5.2 Interface description

This function is triggered without any interface exchanged between the payee's device and the payee's PSP. The result of the function is provided through an outgoing message.

8.2.1.5.2.1 Message structure

- Incoming message

The incoming message is the request received from the device and validated by the recurring payment termination request function. [Refer to Section 8.2.1.3.2.1]

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message Populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.5.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.5.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.6 Recurring payment coded user and authorisation details storage

User details are managed via a token, and the corresponding token must be stored by the payee's PSP.

8.2.1.6.1 Requirements

Business rules

#	Mandatory Optional Conditional	Description
1	M	The message format and content must be consistent
2	M	The coded user and authorisation details must be stored for future use. It corresponds to a token identifier.
3	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.6.2 Interface description

The coded user and authorisation message storage function is triggered by the reception of the token provided by DESP. The function generates an outgoing message providing the result of the function execution.

8.2.1.6.2.1 Message structure

- Incoming message

(Placeholder for a reference to Annex D2)

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message Populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.6.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.6.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**

8.2.1.7 Recurring payment periodic transaction validation

The payee (merchant) initiates the payment at the agreed interval and sends it (including coded user details) to the payee's PSP.
The payee's PSP must validate the request.

8.2.1.7.1 Requirements

Business rules

#	Mandatory Optional Conditional	Description
1	M	The message format and content must be consistent
2	M	The function must check that the recurring payment plan is still active
3	M	The function must check that the payment transaction sequence is correct and corresponds to the expected one
4	M	The function must check that the payment transaction amount is consistent with the recurring payment plan
5	M	The function must check that the payment transaction is initiated according to the frequency defined in the recurring payment plan
6	M	The function must provide the return code. In case of rejection, a reason code must be provided.

8.2.1.7.2 Interface description

The recurring payment periodic transaction validation function is triggered by the payment receipt. The function generates an outgoing message providing the result of the function execution.

8.2.1.7.2.1 Message structure

- Incoming message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of incoming message	STR	35	M	MessageIdentification
Identifier of the event	Unique identifier of the event that triggers the message: "Recurring payment periodic transaction"	STR	35	M	EventIdentification
Date of the message	Date time of the request creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Recurring payment plan identification	Unique identifier of the recurring payment parameters assigned by the merchant	STR	35	M	PlanIdentification
Recurring payment sequence number	Indicates the recurring occurrence of the transaction	NUM	18	M	SequenceNumber

Data element	Description	Type	Length	Presence indicator	Standardised name
Recurring payment frequency	Time interval considered to create payment instruction as a result of the recurring payment (ISO Frequency7Code)	SSET	4	M	Frequency
Transaction type	Type of the transaction	SSET	4	M	TransactionType
Transaction amount	Amount of money to be transferred when a payment instruction is created as a result of a recurring payment	NUM	18	M	Amount
Transaction currency	Currency associated with the transaction	STR	3	M	Currency
Token	Unique identifier of coded payer's details including authorisation. Minimum 8 maximum 28 characters	NUM	TBD	M	Token
Merchant identification	Unique identifier of the merchant	STR	35	M	MerchantIdentification
Merchant category code	Specifies the merchant category code, using the ISO 18245	NSET	4	M	MerchantCategoryCode
Merchant digital euro payment account number	Digital euro payment account number of the merchant	STR	18	O	***(New for digital euro)***

- Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	35	M	MessageIdentification
Identifier of the incoming message	Unique identifier of the corresponding incoming message populated if the function is triggered by an incoming message.	STR	35	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATETIME UTC	24	M	CreationDateTime
Return code	Exit code of function providing the status that the process returns when executed.	BOOL	1	M	ReturnCode
Reason code	Populated only in case of rejection and corresponds to the rejection root cause.	NSET	4	O	StatusReason

8.2.1.7.2.2 Return code

#	Description
0	Successful
1	Failure

8.2.1.7.2.3 Functional error description (reason code)

The functional error descriptions are listed in notification service. **[Refer to Specifications#5 – Common services].**