



EUROPEAN CENTRAL BANK  
EUROSYSTEM

# Digital euro pilot

## Frontend implementation specifications

### Acquiring PSP



**Disclaimer:** This document is indicative and may be subject to modifications. The design, features, and scope of a digital euro may also differ if issued in the future.



EUROPEAN CENTRAL BANK

EUROSYSTEM

## Table of Contents

<b>1</b>	<b>Introduction</b>	<b>5</b>
<b>2</b>	<b>Structure of the document</b>	<b>6</b>
<b>3</b>	<b>Overview of processes</b>	<b>7</b>
3.1	Access Management Service	7
3.1.1	<i>Business end user onboarding</i>	7
3.1.2	<i>Business end user life cycle management</i>	7
3.1.3	<i>Business end user offboarding</i>	8
3.2	Transaction Management Service	9
3.2.1	<i>E/M-commerce transactions</i>	9
3.2.1.1	<i>E-commerce payment via alias</i>	9
3.2.1.2	<i>E-commerce payment via DEAN</i>	11
3.2.1.3	<i>M-commerce payment via mobile app</i>	12
3.2.2	<i>Refund Transactions</i>	13
3.2.2.1	<i>Refund on e-commerce</i>	13
3.2.3	<i>Transactions at (Soft)POS</i>	14
3.2.3.1	<i>NFC mobile payment</i>	14
<b>4</b>	<b>List of services</b>	<b>15</b>
<b>5</b>	<b>Access Management Service</b>	<b>18</b>
5.1	Business end user access management service	19
5.1.1	<i>Functions description</i>	19
5.1.1.1	<i>New business end user registration request validation</i>	19
5.1.1.1.1	<i>Pre-requisite</i>	19
5.1.1.1.2	<i>Requirements</i>	19
5.1.1.1.3	<i>Interface description</i>	20
5.1.1.1.3.1	<i>Message structure</i>	20
5.1.1.1.3.2	<i>Return code</i>	21
5.1.1.1.3.3	<i>Functional error description (reason code)</i>	21
5.1.1.2	<i>New business end user registration</i>	21
5.1.1.2.1	<i>Requirements</i>	21
5.1.1.2.2	<i>Interface description</i>	22
5.1.1.2.2.1	<i>Message structure</i>	22
5.1.1.2.2.2	<i>Return code</i>	23



## EUROPEAN CENTRAL BANK

### EUROSYSTEM

5.1.1.2.2.3	<i>Functional error description (reason code)</i>	23
5.1.1.3	<i>Business end user offboarding request validation</i>	23
5.1.1.3.1	<i>Requirements</i>	23
5.1.1.3.2	<i>Interface description</i>	24
5.1.1.3.2.1	<i>Message structure</i>	24
5.1.1.3.2.2	<i>Return code</i>	25
5.1.1.3.2.3	<i>Functional error description (reason code)</i>	25
5.1.1.4	<i>Business end user deregistration</i>	26
5.1.1.4.1	<i>Requirements</i>	26
5.1.1.4.2	<i>Interface description</i>	26
5.1.1.4.2.1	<i>Message structure</i>	26
5.1.1.5	<i>Business end user offboarding by acquiring PSP</i>	27
5.2	Acceptance solutions service	28
5.2.1	<i>Functions description</i>	28
5.2.1.1	<i>Acceptance solutions settings</i>	28
5.2.1.2	<i>Acceptance solutions deactivation</i>	28
5.3	Notification settings service	29
5.3.1	<i>Functions description</i>	29
5.3.1.1	<i>Notification settings request validation</i>	29
5.3.1.1.1	<i>Pre-requisite</i>	29
5.3.1.1.2	<i>Requirements</i>	29
5.3.1.1.3	<i>Interface description</i>	30
5.3.1.1.3.1	<i>Message structure</i>	30
5.3.1.1.3.2	<i>Return code</i>	33
5.3.1.1.3.3	<i>Functional error description (reason code)</i>	33
5.3.1.2	<i>Notification settings storage</i>	33
5.3.1.2.1	<i>Requirements</i>	33
5.3.1.2.2	<i>Interface description</i>	33
5.3.1.2.2.1	<i>Message structure</i>	33
5.3.1.2.2.2	<i>Return code</i>	34
5.3.1.2.2.3	<i>Functional error description (reason code)</i>	34
5.3.1.3	<i>Notification settings removal</i>	34
5.3.1.3.1	<i>Requirements</i>	34
5.3.1.3.1.1	<i>Message structure</i>	35



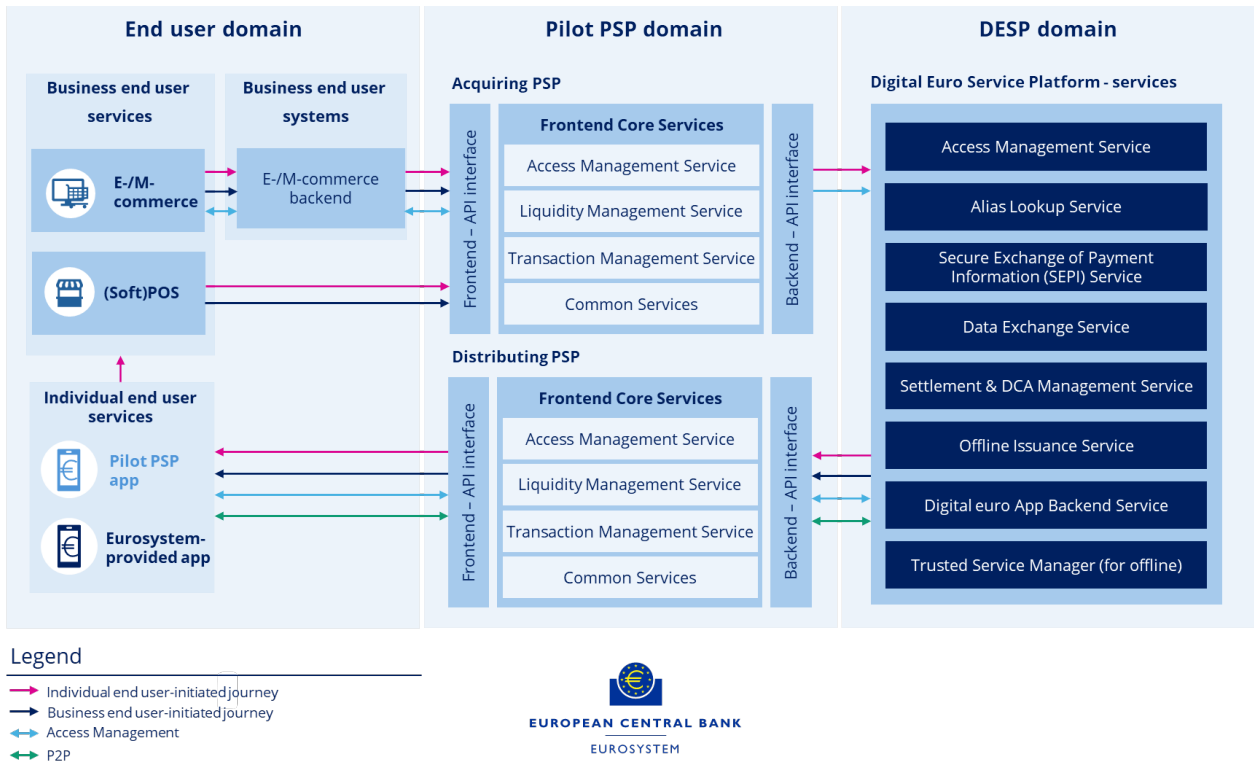
EUROPEAN CENTRAL BANK

EUROSYSTEM

5.3.1.3.1.2	<i>Return code</i>	36
5.3.1.3.1.3	<i>Functional error description (reason code)</i>	36
5.4	Linked account settings service	36
5.5	Beta digital euro account service	37
5.6	Commercial bank money account service	37
<b>6</b>	<b>Liquidity Management Service</b>	<b>39</b>
6.1	Commercial bank money account funds management service	39
6.2	Beta digital euro account funds management service	39
<b>7</b>	<b>Transaction Management Service</b>	<b>41</b>
7.1	Payment initiation service	41
7.1.1	<i>Functions description</i>	41
7.1.1.1	<i>Alias validity check</i>	41
7.1.1.2	<i>Alias look-up dispatch</i>	42
7.1.1.3	<i>PSP ID look-up dispatch</i>	42
7.1.1.4	<i>Business end user payment request initiation validation</i>	42
7.1.1.4.1	<i>Requirements</i>	42
7.1.1.4.2	<i>Interface description</i>	43
7.1.1.4.2.1	<i>Message structure</i>	43
7.1.1.4.2.2	<i>Return Code</i>	47
7.1.1.4.2.3	<i>Functional error description (reason code)</i>	48
7.1.1.5	<i>Refund request initiation validation</i>	48
7.1.1.5.1	<i>Requirements</i>	48
7.1.1.5.2	<i>Interface description</i>	49
7.1.1.5.2.1	<i>Message structure</i>	49
7.1.1.5.2.2	<i>Return Code</i>	50
7.1.1.5.2.3	<i>Functional error description (reason code)</i>	50

# 1 Introduction

The implementation specifications describe the different domains and interactions between actors as presented in the diagram below. This document focuses on the frontend implementation specifications for acquiring PSPs.



**Figure 1 - Digital euro pilot - functional architecture**

This document is dedicated to acquiring PSP requirements. The current version focuses on the following scope applicable to the digital euro pilot.

- Onboarding of business end user
- Offboarding of business end user
- E-commerce payment via alias
- E-commerce payment via DEAN
- M-commerce payment via mobile app
- Refund on e-commerce



## 2 Structure of the document

This document is organised according to Core Services, as described in **Digital euro pilot – Frontend specifications – Core Services**.

- Access Management Services
- Liquidity Management Services
- Transaction Management Services

Core services are split into more granular services, and each service contains a set of unitary functions that must be implemented by pilot PSPs to support the pilot payment services. 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: <ul style="list-style-type: none"> <li>- M: Mandatory</li> <li>- O: Optional</li> <li>- C: Conditional</li> </ul>
Standardised name	Name formatted according to a predefined conventions to ensure consistency and uniformity (ISO 20022). <b>Note</b> : No standard name is currently assigned to the data created for the needs of the digital euro ( <i>New for beta digital euro</i> ).

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

### 3 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 (individual end users & business end users).
- show responsibility split across end users, pilot PSPs, and DESP.
- highlight key capabilities (e.g., initiation, validation and settlement)

Their purpose is not to be sequence diagrams. The sequences are reflected in the **Digital euro pilot - End-to-end process flows**.

#### 3.1 Access Management Service

##### 3.1.1 Business end user onboarding

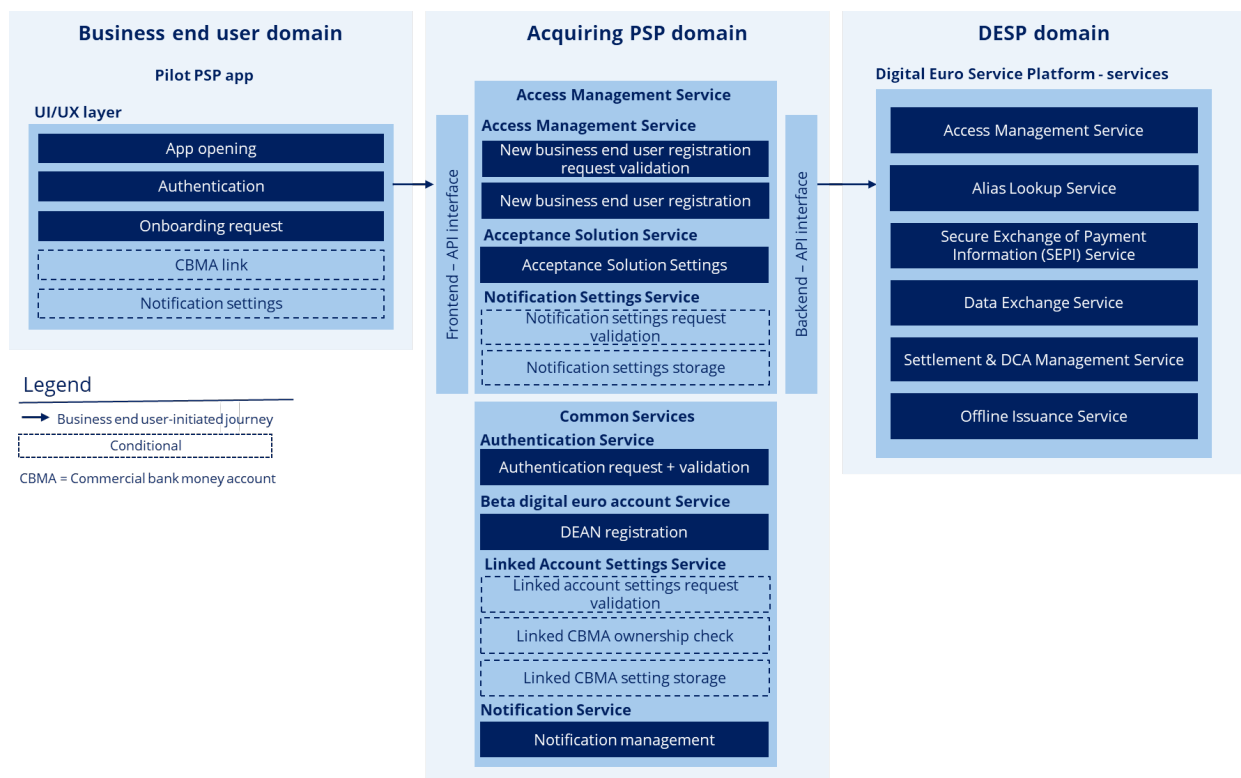


Figure 2 - Business end user onboarding

##### 3.1.2 Business end user life cycle management

Placeholder for a next version of this document.



### 3.1.3 Business end user offboarding

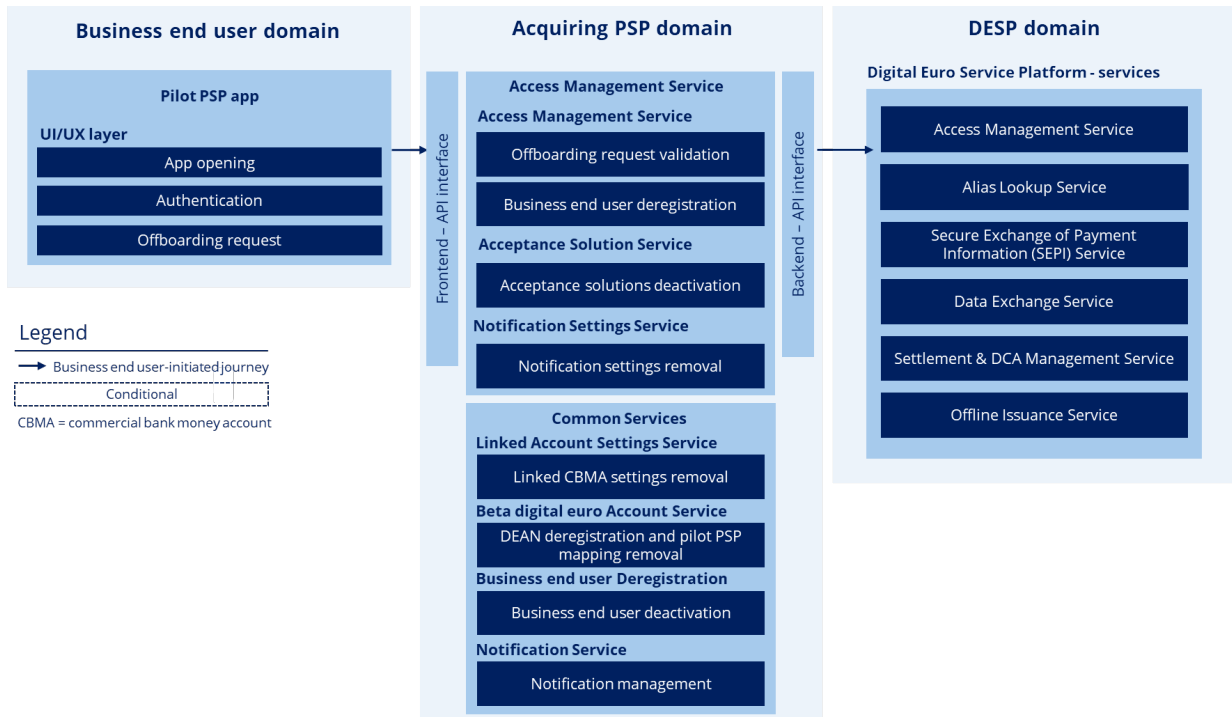


Figure 3 Business end user offboarding



**EUROPEAN CENTRAL BANK**

EUROSYSTEM

## **3.2 Transaction Management Service**

### **3.2.1 E/M-commerce transactions**

#### **3.2.1.1 E-commerce payment via alias**



# EUROPEAN CENTRAL BANK

## EUROSYSTEM

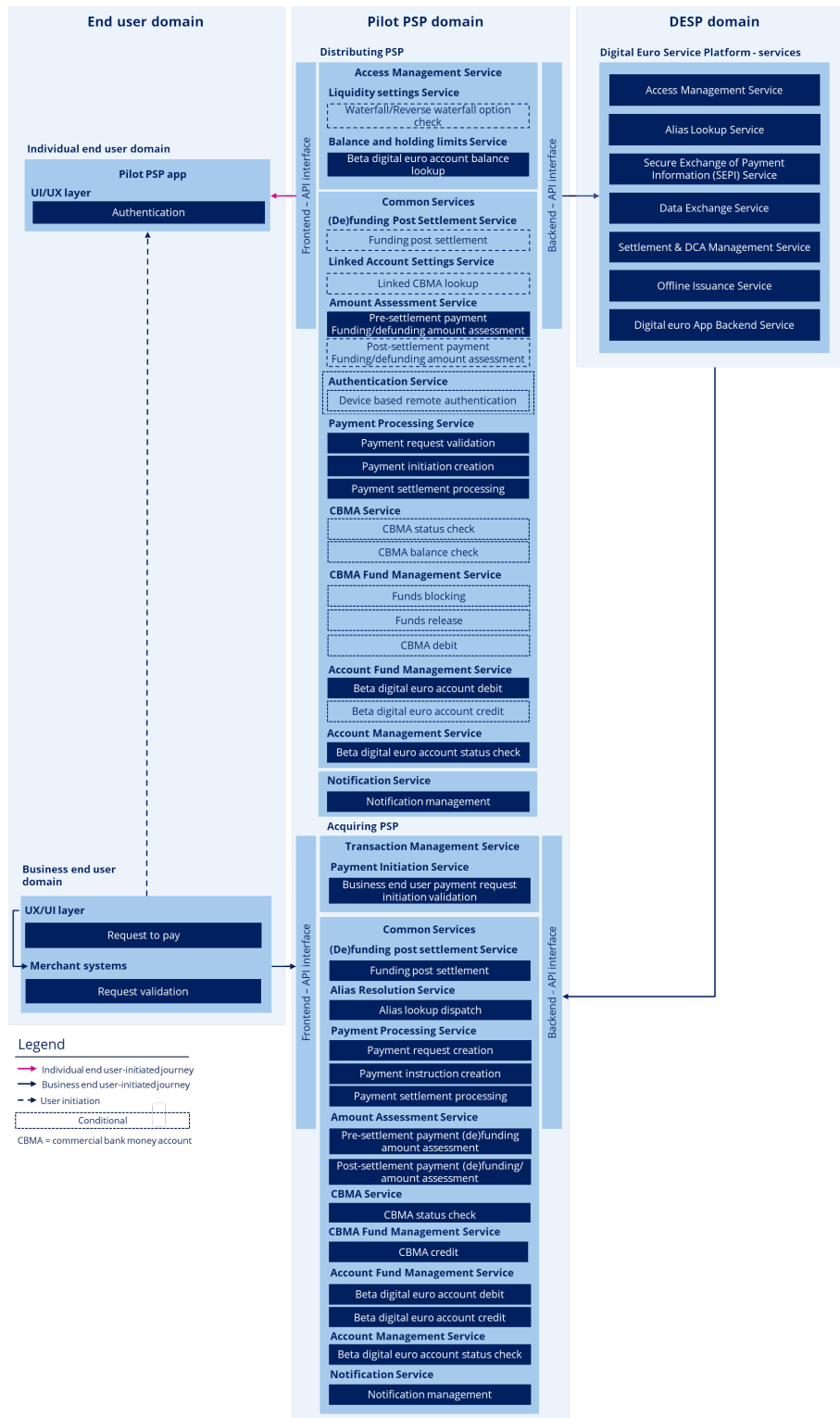
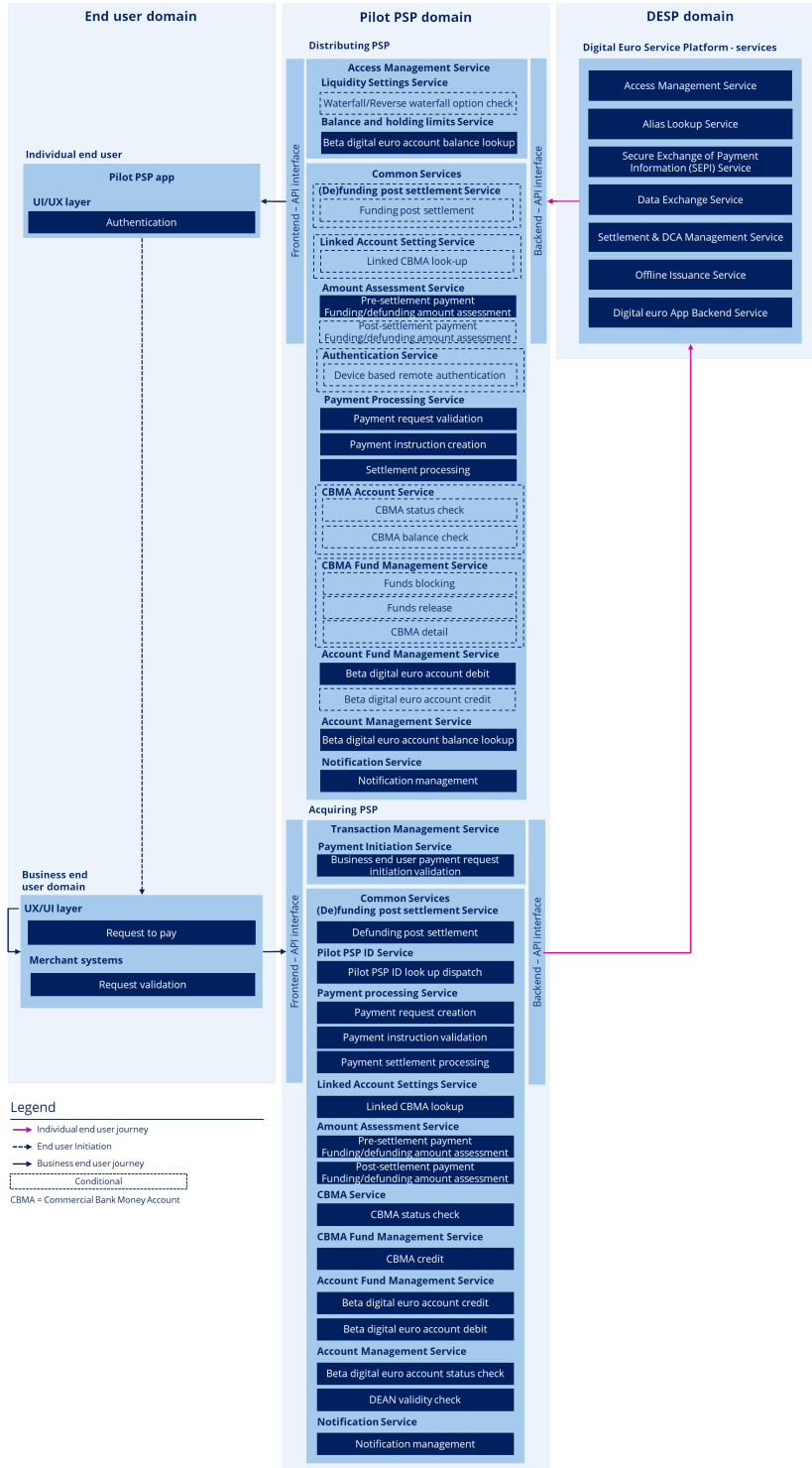


Figure 4 E-commerce payment via alias



**EUROPEAN CENTRAL BANK**  
**EUROSYSTEM**

**3.2.1.2 E-commerce payment via DEAN**



**Figure 5 E-commerce payment via DEAN**



EUROPEAN CENTRAL BANK  
EUROSYSTEM

### 3.2.1.3 M-commerce payment via mobile app

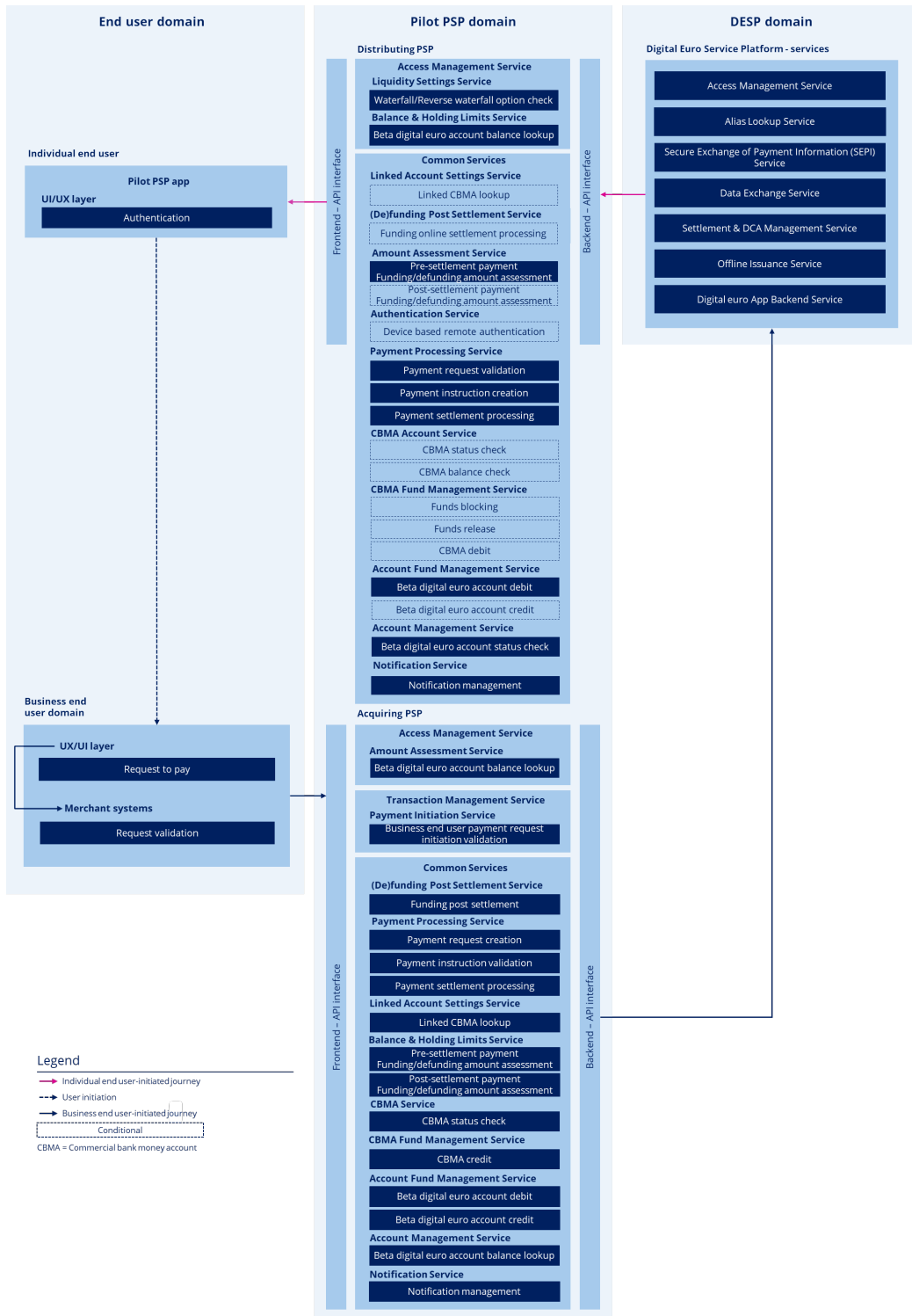


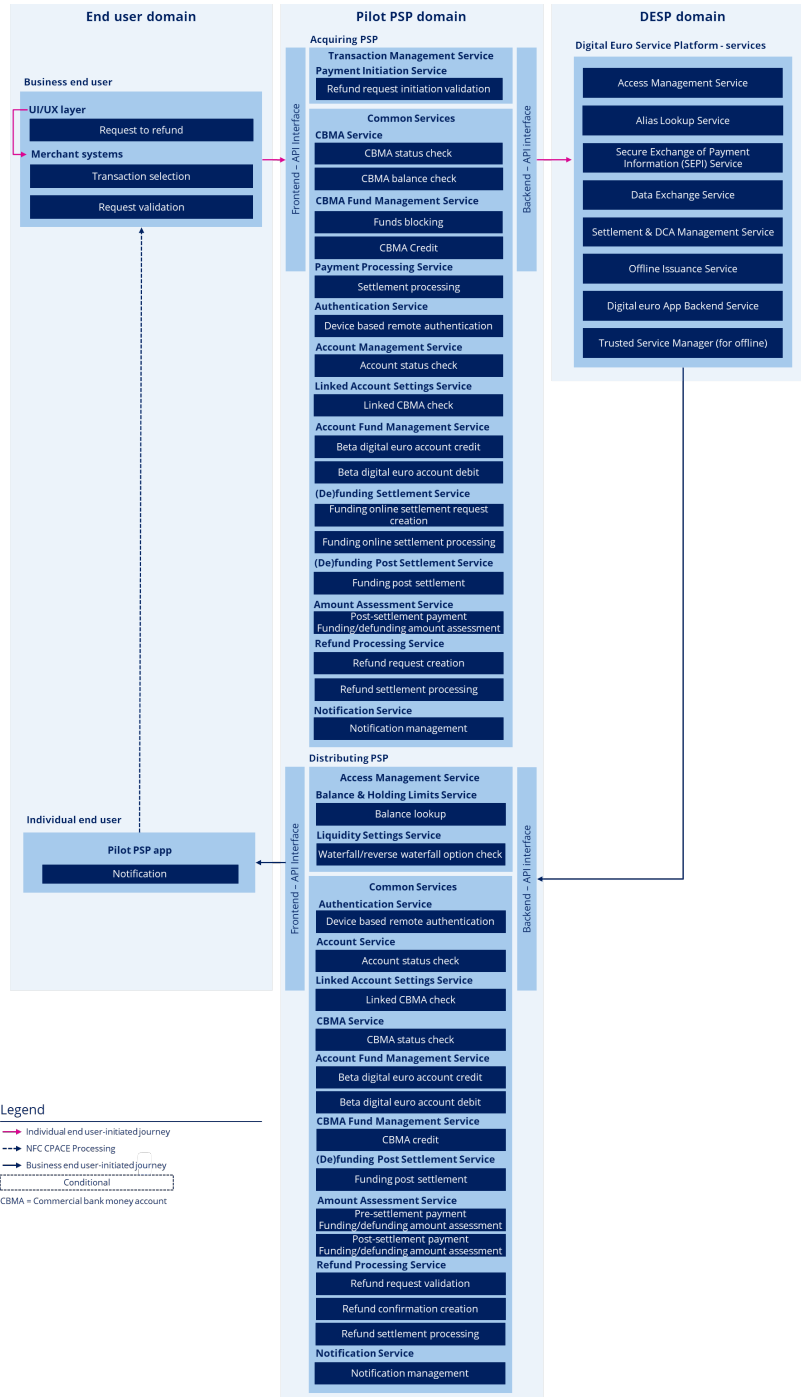
Figure 6 M-commerce payment via mobile app



**EUROPEAN CENTRAL BANK**  
**EUROSYSTEM**

**3.2.2 Refund Transactions**

**3.2.2.1 Refund on e-commerce**



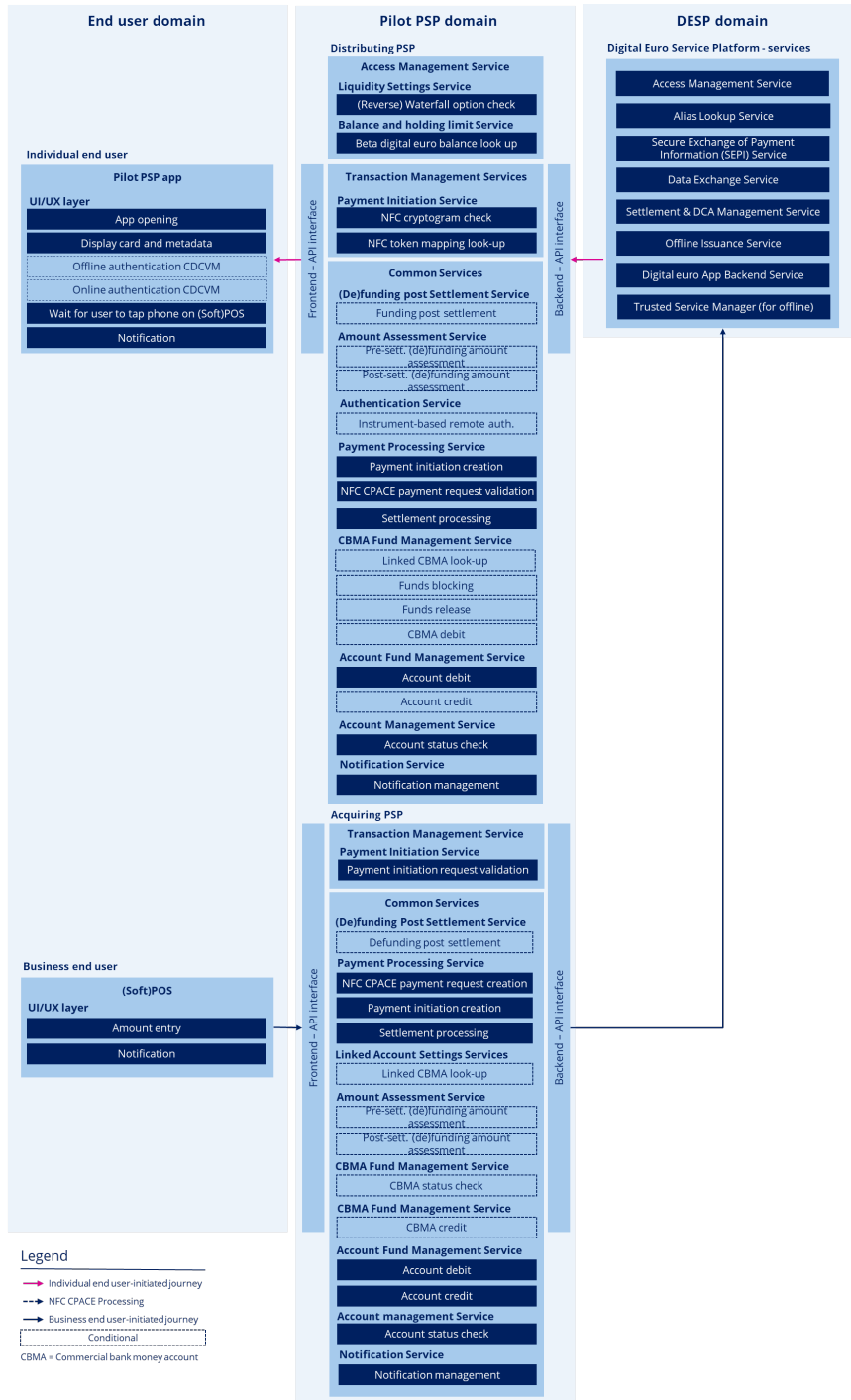
**Figure 7 Refund on e-commerce**



**EUROPEAN CENTRAL BANK**  
**EUROSYSTEM**

**3.2.3 Transactions at (Soft)POS**

**3.2.3.1 NFC mobile payment**



**Figure 8 NFC mobile payment**



## 4 List of services

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

Service	Function	Description of function	Core Service
<b>Business end user access management service</b>  <i>Management of requests initiated by a business end user who:</i> - wants to be onboarded as a business end user - wants to close their beta digital euro account  <i>Management of requests initiated by a pilot PSP</i>	New business end user registration request validation	The acquiring PSP checks if the registration request sent by the business end user is valid.	Access Management Service
	New business end user registration	The acquiring PSP registers the business end user as an end user.	Access Management Service
	New business end user offboarding request validation	The acquiring PSP checks if the offboarding request sent by the business end user is valid.	Access Management Service
	Business end user deregistration	The acquiring PSP orchestrates the final steps as part of the offboarding request.	Access Management Service
	Business end user offboarding by acquiring PSP	The acquiring PSP initiates the business end user offboarding and orchestrates the required steps.	Access Management Service
<b>Acceptance solutions services</b>  <i>Management of acceptance solutions (configuration and deactivation)</i>	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 beta 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
<b>Commercial bank money account service</b>  <i>Management of the commercial bank money account involved in beta digital euro processes.</i>	Commercial bank money account status check	The pilot PSP servicing the commercial bank money account verifies the operational status of a commercial bank money account. It ensures that the account is active, valid, and ready for transactions.	Common Service



EUROPEAN CENTRAL BANK

EUROSYSTEM

Service	Function	Description of function	Core Service
<b>Beta digital euro account service</b>  <i>Management of beta digital euro account settings and life cycle</i>	Beta digital euro account (un)blocking request validation	The pilot PSP checks if the beta digital euro account blocking or beta digital euro account unblocking request sent by the business end user device is valid.	Common Service
	Beta digital euro account blocking	The pilot PSP blocks the beta digital euro account.	Common Service
	Beta digital euro account unblocking	The pilot PSP unblocks the beta digital euro account.	Common Service
	DEAN registration	The pilot PSP requests a DEAN to DESP and stored it.	Common Service
	DEAN registration and pilot PSP mapping removal	The pilot PSP requests a DEAN registration and pilot 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
<b>Notification settings service</b>  <i>Management of parameters defined by the end user to receive notifications</i>	Notification settings request validation	The acquiring PSP validates if the notification settings request sent by the business end user 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 business end user offboarding.	Access Management service
<b>Payment Initiation service</b>  <i>Management of payment requests initiated by a business end user (covering all form factors)</i>	Alias validity check	The pilot PSP checks the alias consistency and triggers the alias look-up dispatch function.	Common Service
	Alias look-up dispatch	The pilot PSP servicing beta digital euro account requests an alias resolution to DESP to retrieve DEAN and pilot PSP ID.	Common Service
	PSP ID look-up	The pilot PSP servicing beta digital euro account requests the pilot PSP ID corresponding to the DEAN to DESP for routing purpose.	Common Service
	Business end user payment request initiation validation	The pilot PSP servicing beta digital euro account checks the payment request sent by the business end user is consistent and contains mandatory information.	Transaction Management Service



EUROPEAN CENTRAL BANK

EUROSYSTEM

Service	Function	Description of function	Core Service
	Refund request initiation validation	The pilot PSP servicing beta digital euro account checks the refund request is consistent and contains mandatory information.	Transaction Management Service
<b>Linked account settings service</b>  <i>Management of the link between a commercial bank money account and the beta digital euro account</i>	Linked account settings request validation	The pilot PSP checks if the linked account settings request is valid.	Common Service
	Linked account settings storage	The pilot PSP stores the information related to linked commercial bank money account (new link, updated link, link removal).	Common Service
	Linked account settings removal	The pilot PSP removes the link between the commercial bank money account and the beta digital euro account as part of the business end user offboarding.	Common Service
	Linked commercial bank money account ownership validation	The pilot PSP receives proof of commercial bank money account ownership and validates it.	Common Service
	Linked commercial bank money account look-up	The pilot PSP checks whether the business end user has linked a commercial bank money account to the beta digital euro account.	Common Service
	Linked commercial bank money account check	During a payment transaction that requires a waterfall or reverse waterfall process, the pilot PSP checks whether the beta digital euro account is linked to a commercial bank money account and, if so, returns the IBAN of that linked account.	Common Service
	<b>Payment processing service</b>  <i>Management of payment after request initiation – in relation to DESP</i>	Payment request creation	The pilot PSP servicing beta digital euro account generates a payment request to DESP.
Payment request validation		The pilot PSP servicing beta digital euro account receives a payment request from DESP and validates its consistency.	Common service
Payment instruction creation		The payer PSP sends the request with a payment instruction (single or combined transaction).	Common service
Payment instruction validation		The pilot PSP servicing beta digital euro account receives a payment instruction from DESP, validates its consistency and complements it.	Common service



Service	Function	Description of function	Core Service
	Payment settlement processing	The pilot PSP manages the life cycle of a payment instruction or payment request in alignment with the settlement phase status.	Common service
<b>Commercial bank money account funds management service</b>  <i>Management of rules to manage funds in commercial bank money accounts (debit, credit, block, release)</i>	Commercial bank money account debit	The pilot PSP servicing commercial bank money account defunds commercial bank money account.	Common service
	Commercial bank money account credit	The pilot PSP servicing commercial bank money account funds commercial bank money account.	Common service
	Funds blocking	The pilot PSP servicing commercial bank money account blocks funds on commercial bank money account if reverse waterfall is needed for transaction proper execution.	Common service
	Funds release	The pilot PSP servicing commercial bank money account releases funds blocked on commercial bank money account if the transaction is discontinued.	Common service
<b>Beta digital euro funds management service</b>  <i>Management of rules to handle funds in beta digital euro account (debit, credit)</i>	Beta digital euro account debit	The pilot PSP servicing the beta digital euro account debits the beta digital euro account	Common Service
	Beta digital euro account credit	The pilot PSP servicing the beta digital euro account credits the beta digital euro account.	Common Service

All the services, functions identified as Common Service are described in **Digital euro pilot – Frontend specifications – Common Services**.

## 5 Access Management Service

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

## 5.1 Business end user access management service

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

Business end users can only be registered as a new end user if they are already a customer of the pilot PSP.

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

Service	Function/sub-functions	Description
Business end user access management service	New business end user registration request validation	The acquiring PSP checks if the registration request sent by the end user's device is valid
	New business end user registration	The acquiring PSP registers the business end user as an end user.
	Business end 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.

### 5.1.1 Functions description

#### 5.1.1.1 New business end user registration request validation

##### 5.1.1.1.1 Pre-requisite

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

The business end user could use:

- The pilot PSP app and is already connected to the acquiring PSP through a Strong Customer Authentication process specific to that pilot PSP.
- The pilot PSP web browser is already authenticated and connected to the acquiring PSP.

##### 5.1.1.1.2 Requirements

A new business end user request is sent by the pilot PSP app 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.



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

### 5.1.1.1.3 Interface description

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

#### 5.1.1.1.3.1 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: "Business end 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 beta digital euro account to open	Number of DEAN the business end user wants to open.	NUM	3	O	<b>(New for beta digital euro)</b>

Outgoing message

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



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:ssZ	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

#### 5.1.1.1.3.2 Return code

#	Description
0	Successful
1	Failure

#### 5.1.1.1.3.3 Functional error description (reason code)

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

### 5.1.1.2 New business end user registration

#### 5.1.1.2.1 Requirements

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

#	Mandatory Optional Conditional	Business rules description
1	M	The acquiring PSP must create the business end user data envelop that is: <ul style="list-style-type: none"> <li>- complemented during the onboarding process,</li> <li>- updated during amendment process and offboarding process</li> </ul>
2	M	The business end user data envelop must contain the following data <ul style="list-style-type: none"> <li>- Business end user <b>identifier</b></li> <li>- Technical proof</li> <li>- Entry identifier</li> </ul>



#	Mandatory Optional Conditional	Business rules description
		<ul style="list-style-type: none"> <li>- Business end user <b>type</b></li> <li>- Business end user <b>creation date</b></li> <li>- Business end user <b>status</b></li> <li>- Business end user <b>country</b></li> <li>- Business end user <b>language</b></li> </ul>
3	M	The distributing PSP has to link the business end user <b>identifier</b> with the <b>PSP App ID</b> associated with the app that initiated the request.
4	M	The business end user <b>identifier</b> 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 business end user <b>creation date</b> must be equal to the current date
7	M	The business end user status must be initiated according to the end user life cycle. <ul style="list-style-type: none"> <li>- <b>PENDING</b>: the customer is registered but has not yet opened a beta digital euro account.</li> </ul>
7	M	The business end 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.

### 5.1.1.2.2 Interface description

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

The result of the new business end user registration function is sent through an outgoing message.

#### 5.1.1.2.2.1 Message structure

Incoming message

The incoming message is the request received from the device and validated by the new business end user request validation function. Refer to **paragraph 5.1.1.1**.

#### 5.1.1.1 New business end user registration request validation

Outgoing message

Data element	Description	Type	Length	Presence indicator	Standardised name
Identifier of the message	Unique identifier of outgoing message	STR	36	M	MessageIdentification



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	36	O	OriginalMessageIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:sssZ	DATE TIME UTC	24	M	CreationDateTime
Identifier of the business end user	Unique identifier of the end user Populated if the process is successful	STR	TBD	O	<i>(New for beta digital euro)</i>
Technical proof	Cryptographic root key used to prove the ownership of holdings. Populated if the process is successful	STR	TBD	O	<i>(New for beta digital euro)</i>
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

#### 5.1.1.2.2.2 Return code

#	Description
0	Successful
1	Failure

#### 5.1.1.2.2.3 Functional error description (reason code)

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

### 5.1.1.3 Business end user offboarding request validation

#### 5.1.1.3.1 Requirements

- The business end user intends to close their beta digital euro account and has submitted a request to the acquiring PSP servicing the beta digital euro accounts through their device.
- The acquiring PSP must validate the request is consistent and valid and that the pre-requisites are fulfilled.
- All the beta digital euro accounts owned by the business end user will be closed.



#	Mandatory Optional Conditional	Business rules 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 <ul style="list-style-type: none"> <li>- there aren't any pre-disputes, and/or disputes still not closed</li> <li>- Any beta digital euro account has been previously blocked by the pilot PSP blocked.</li> </ul> If the conditions are not met, the request must be rejected.
5	C	If the offboarding request is valid, <ul style="list-style-type: none"> <li>- the status of the business end user must be updated to indicate the ongoing offboarding.</li> <li>- the contract target closing date must be defined and entered into the system to schedule further steps (acceptance solution disablement and beta digital euro account blocking).</li> </ul>
6	M	The function must provide a return code. In case of failure, a reason code must be provided.

### 5.1.1.3.2 Interface description

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

#### 5.1.1.3.2.1 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 end user offboarding"	STR	35	M	EventIdentification
Date of the message	Date time of the message creation YYYY-MM-DDThh:hh:ssZ	DATETIME UTC	24	M	CreationDateTime
Identifier of the end user	Unique identifier of the end user	STR	TBD	M	<i>(New for beta digital euro)</i>



**EUROPEAN CENTRAL BANK**  
EUROSYSTEM

Data element	Description	Type	Length	Presence indicator	Standardised name
Beta digital euro contract identifier	Unique identifier of the contract to be closed	STR	35	M	RegisteredContractIdentification

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:ssZ	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

5.1.1.3.2.2 *Return code*

#	Description
0	Successful
1	Failure

5.1.1.3.2.3 *Functional error description (reason code)*

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.



#### 5.1.1.4 Business end user deregistration

##### 5.1.1.4.1 Requirements

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

#	Mandatory Optional Conditional	Business rule description
1	M	The acquiring PSP must check if a commercial bank money account is still linked to the beta digital euro account. Refer to <b>Digital euro pilot – Frontend specifications – Common Services (section 1.5 - Linked account settings service)</b> .
2	C	If a commercial bank money account is still linked to a beta digital euro account, the acquiring PSP must remove the existing link. Refer to <b>Digital euro pilot – Frontend specifications – Common Services (section 1.5 - Linked account settings service)</b> .
3	M	The acquiring PSP must remove the notification settings still defined for the business end user. Refer to <b>Digital euro pilot – Frontend specifications – Acquiring PSP (section 5.3 - Notification settings service)</b> .
4	M	The acquiring PSP must request the business end user deactivation. Refer to <b>Digital euro pilot – Frontend specifications – Common Services (section 1.7 - End user deactivation)</b> .
5	C	If the deactivation is successful, the following data must be updated: <ul style="list-style-type: none"><li>- Business end user status is updated and switched to “CLOSED”.</li><li>- Business end user closing date is populated with the current date.</li></ul>
6	M	The function must provide the return code. In case of failure, a reason code must be provided.

##### 5.1.1.4.2 Interface description

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

###### 5.1.1.4.2.1 Message structure

Incoming message

Detailed in **Digital euro pilot - Backend 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

#### 5.1.1.5 Business end user offboarding by acquiring PSP

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

- Schedules the contract cancellation
- Disables acceptance solutions. Refer to **paragraph 5.2.1.2**.
- Blocks the beta digital euro accounts. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.4 - beta digital euro account service)**.
- Removes the linked commercial money account settings. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.5 – linked account settings service)**.
- Removes the notifications settings. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.
- Requests DEAN(s) deregistration and PSP ID mapping removal. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.4 - beta digital euro account service)**.
- Requests business end user deactivation. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.7 - End user deactivation)**.

## 5.2 Acceptance solutions service

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

Service	Function/sub-functions	Description
Acceptance solutions service	Acceptance solutions settings	The acquiring PSP performs the settings of acceptance solutions during the onboarding process or business end user life cycle management.
	Acceptance solutions disablement	The acquiring PSP disables the acceptance solutions during the offboarding process.

### 5.2.1 Functions description

#### 5.2.1.1 Acceptance solutions settings

The acquiring PSP is responsible for configuring and activating the payment acceptance solutions according to the business end user'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 beta digital euro. This includes activating the necessary payment methods and the communication technology.

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

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

#### 5.2.1.2 Acceptance solutions deactivation

When a business 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 end 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 business end users.



### 5.3 Notification settings service

Once a business end user has successfully opened at least a beta digital euro 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 business 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 service	Notification settings request validation	The acquiring PSP checks if the notification settings request sent by the business end user device is valid.
	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 end user is offboarded.

#### 5.3.1 Functions description

##### 5.3.1.1 Notification settings request validation

###### 5.3.1.1.1 Pre-requisite

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

###### 5.3.1.1.2 Requirements

The business 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 beta digital euro account, which must verify that the request is valid and consistent.

#	Mandatory Optional Conditional	Business rules 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: <ul style="list-style-type: none"><li>- CREATE → Initial set-up</li><li>- UPDATE → Set-up amendment</li></ul>



#	Mandatory Optional Conditional	Business rules description
		- 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 beta digital euro <i>Account credit</i> event aggregation indicator is set to 'Yes', the corresponding frequency must be defined.
7	C	If the beta digital euro <i>Account debit</i> event aggregation indicator is set to 'Yes', the corresponding frequency must be defined.
8	C	If the <i>Waterfall</i> event aggregation indicator is set to 'Yes', the corresponding frequency must be defined.
9	C	If the <i>Reverse Waterfall</i> event aggregation indicator is set to 'Yes', the corresponding frequency must be defined.
10	C	If the <i>Aggregated notifications</i> 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 beta digital euro account.
12	M	The function must provide a return code. In case of failure, a reason code must be provided.
13	C	If the function execution is successful, the acquiring PSP must trigger <i>Notification settings</i> storage function. Refer to <b>paragraph 5.3.1.2</b> .

### 5.3.1.1.3 Interface description

A dedicated interface received from a business end user device (incoming message) triggers the *Notification settings request* validation. The function generates an outgoing message providing the result of the function execution.

#### 5.3.1.1.3.1 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's device.	SSET	4	M	RequestType



EUROPEAN CENTRAL BANK

EUROSYSTEM

Data element	Description	Type	Length	Presence indicator	Standardised name
	<ul style="list-style-type: none"> <li>- <b>CRED - CREATE</b></li> <li>- <b>UPDT - UPDATE</b></li> <li>- <b>DELT - DELETE</b></li> </ul>				
Communication channel type	Method by which the notification is delivered <ul style="list-style-type: none"> <li>- <b>EMAL</b> (transmission by email)</li> <li>- <b>ONLI</b> (transmission online – e.g., in app)</li> <li>- <b>MBNO</b> (transmission by mobile phone)</li> <li>- <b>FILE</b> (transmission by file transfer)</li> </ul>	SSET	4	M	CommunicationMethodCode
Communication channel value	Detailed information of the method chosen to receive notification.	STR	140	M	CommunicationMethodValue
Beta digital euro account credit event indicator	Specifies whether a notification is triggered when the beta digital euro account is credited.	BOOL	1	O	<i>(New for beta digital euro)</i>
Beta digital euro account credit event aggregation indicator	Specifies whether the business end user requests aggregated notifications for beta digital euro account credit event.	BOOL	1	O	<i>(New for beta digital euro)</i>
Beta digital euro account credit event aggregation frequency	Specifies the applicable frequency for aggregated beta digital euro credit event notifications (ISO Frequency7Code).	SSET	4	O	Frequency
Beta digital euro account debit event indicator	Specifies whether a notification is triggered when the beta digital euro account is debited.	BOOL	1	O	<i>(New for beta digital euro)</i>
Beta digital euro account debit event aggregation indicator	Specifies whether the business end user requests aggregated notifications for beta digital euro <i>account debit</i> event.	BOOL	1	O	<i>(New for beta digital euro)</i>
Digital euro account debit event aggregation frequency	Specifies the applicable frequency for aggregated beta digital euro <i>Account debit</i> event notifications (ISO Frequency7Code).	SSET	4	O	Frequency
Waterfall transaction event indicator	Specifies whether a notification is triggered when a waterfall process affects the beta digital euro account.	BOOL	1	O	<i>(New for beta digital euro)</i>
Waterfall event aggregation indicator	Specifies whether the business end user requests aggregated notifications for <i>Waterfall</i> event.	BOOL	1	O	<i>(New for beta digital euro)</i>



Data element	Description	Type	Length	Presence indicator	Standardised name
Waterfall aggregation frequency	Specifies the applicable frequency for aggregated <i>Waterfall</i> 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 beta digital euro account.	BOOL	1	O	<i>(New for beta digital euro)</i>
Reverse waterfall event aggregation indicator	Specifies whether the business end user requests aggregated notifications for reverse waterfall event.	BOOL	1	O	<i>(New for beta digital euro)</i>
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 business end user requests aggregated notifications compiling all the events.	BOOL	1	O	<i>(New for beta digital euro)</i>
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 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

#### 5.3.1.1.3.2 Return code

#	Description
0	Successful
1	Failure

#### 5.3.1.1.3.3 Functional error description (reason code)

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

### 5.3.1.2 Notification settings storage

#### 5.3.1.2.1 Requirements

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

#	Mandatory Optional Conditional	Business rules 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

#### 5.3.1.2.2 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.

##### 5.3.1.2.2.1 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 **paragraph 5.3.1.1**.



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:ssZ	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

5.3.1.2.2.2 *Return code*

#	Description
0	Successful
1	Failure

5.3.1.2.2.3 *Functional error description (reason code)*

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

**5.3.1.3 Notification settings removal**

**5.3.1.3.1 Requirements**

When a business 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 end user.



EUROPEAN CENTRAL BANK

EUROSYSTEM

#	Mandatory Optional Conditional	Business rules 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.

#### 5.3.1.3.1.1 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 access number	Identification of the beta digital euro account.	STR	18	M	<b>(New for beta digital euro)</b>

##### 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



Data element	Description	Type	Length	Presence indicator	Standardised name
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

#### 5.3.1.3.1.2 Return code

#	Description
0	Successful
1	Failure

#### 5.3.1.3.1.3 Functional error description (reason code)

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

## 5.4 Linked account settings service

A business end user who has successfully opened a beta digital euro account must have the ability to link a commercial bank money account to their beta digital euro 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 pilot PSP checks if the linked account settings request is valid.
	Linked account settings storage.	The pilot PSP stores the information related to linked commercial bank money account (new link, updated link, link removal) upon end user request.
	Linked account settings removal.	The pilot PSP clears the linked account when the end user is offboarded.
	Linked commercial bank money account ownership validation.	The pilot PSP receives proof of commercial bank money account ownership and validates it.
	Linked commercial bank money account look-up.	The pilot PSP checks whether the business end user has linked a commercial bank money account to the beta digital euro account.



Service	Function/sub-functions	Description
	Linked commercial bank money account check.	During a payment transaction that requires a waterfall or reverse-waterfall process, the pilot PSP checks whether the beta digital euro account is linked to a commercial bank money 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 in **Digital euro pilot – Frontend specifications – Common Services**.

### 5.5 Beta digital euro account service

The beta digital euro account service is triggered during the onboarding of a business end user, throughout the beta digital euro account life cycle management. It also offers some functions to validate that the conditions are met for a beta digital euro transaction’s proper execution.

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

Those functions are used by several processes performed by both distributing and acquiring PSPs and are described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

### 5.6 Commercial bank money account service

Commercial bank money account service is invoked during a payment transaction process by the pilot PSP servicing the commercial bank money account of the business end user. It offers the needed functions to validate that the conditions are met for a beta digital euro transaction’s proper execution.



EUROPEAN CENTRAL BANK

EUROSYSTEM

Service	Function	Description
Commercial bank money account service	Commercial bank money account status check.	The pilot PSP servicing commercial bank money account verifies the operational status of a commercial bank account.

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

## 6 Liquidity Management Service

The liquidity management core services are dedicated to functions needed for funding and defunding the beta digital euro account and the commercial bank money account.

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

- Commercial bank money account funds management service
- Beta digital euro account funds management service

### 6.1 Commercial bank money account funds management service

Commercial bank money account funds management service is invoked during a payment or a funding-defunding transaction process by the pilot PSP servicing the commercial bank money account of the business end user. It offers the needed functions to handle the commercial money account funds.

Service	Function	Description
Commercial bank money account funds management service	Commercial bank money account debit	The pilot PSP servicing commercial bank money account defunds commercial bank money account.
	Commercial bank money account credit	The pilot PSP servicing commercial bank money account funds commercial bank money account.
	Funds blocking	The pilot PSP servicing commercial bank money account blocks funds on commercial bank money account if reverse waterfall is needed for transaction execution and in funding processes.
	Funds release	The pilot PSP servicing commercial bank money account releases funds blocked on commercial bank money account if the process is discontinued.

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

### 6.2 Beta digital euro account funds management service

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



EUROPEAN CENTRAL BANK

EUROSYSTEM

Service	Function	Description
Beta digital euro account funds management service	Beta digital euro account debit	The pilot PSP servicing the beta digital euro account debits the beta digital euro account.
	Beta digital euro account credit	The pilot PSP servicing the beta digital euro account credits the beta digital euro account.

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

## 7 Transaction Management Service

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

In the context of e/m-commerce transactions, one main service is needed to manage e/m-commerce one-time payments:

- Payment initiation service

### 7.1 Payment initiation service

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

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

#### 7.1.1 Functions description

##### 7.1.1.1 Alias validity check

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.



### 7.1.1.2 Alias look-up dispatch

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

### 7.1.1.3 PSP ID look-up dispatch

This function is used by several processes and is described as a Common function in **Digital euro pilot – Frontend specifications – Common Services**.

### 7.1.1.4 Business end user payment request initiation validation

#### 7.1.1.4.1 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 pilot PSP must validate the payment request is complete to proceed with the payment. The request could be initiated for a one-time payment.

#	Mandatory Optional Conditional	Business rules description
1	M	The request format and content must be consistent.
2	M	Following data must always be provided <ul style="list-style-type: none"> <li>- Message Identifier</li> <li>- Event Identifier</li> <li>- Message date time</li> <li>- Transaction initiation Method</li> <li>- Transaction type</li> <li>- Transaction Amount</li> <li>- Transaction Currency</li> <li>- Transaction date</li> <li>- Payee trade Name</li> <li>- Payee DEAN (Merchant DEAN)</li> <li>- Payee location (address)</li> <li>- Payee location (City)</li> <li>- Payee location (Post code)</li> <li>- Payee location (Country)</li> <li>- Merchant Category Code</li> <li>- Transaction Identification</li> </ul>
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



#	Mandatory Optional Conditional	Business rules description
		<ul style="list-style-type: none"> <li>- Payer alias type</li> <li>- Payer alias value</li> </ul>
7	C	If the Transaction initiation method is “DEAN” and the transaction type is “Purchase”, following data must be provided: <ul style="list-style-type: none"> <li>- Payer DEAN</li> </ul>
8	O	The Payer PSP ID can be provided by the digital point of interaction if it was recovered in a previous step.
9	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).
10	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)
11	M	The function must provide the return code. In case of rejection, a reason code must be provided.

#### 7.1.1.4.2 Interface description

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

##### 7.1.1.4.2.1 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 end user to initiate a payment transaction <ul style="list-style-type: none"> <li>- Alias</li> <li>- DEAN</li> </ul>	STR	4	M	PaymentMethod



EUROPEAN CENTRAL BANK

EUROSYSTEM

Data element	Description	Type	Length	Presence indicator	Standardised name
	Code set to be clarified				
Transaction type	Type of transaction initiated by the individual end 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
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 (Post code)	Postal code 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	MerchantCategory Code
Structured Remittance	Predefined code/value provided by the payee to the payer, facilitating automated reconciliation.	STR	35	O	StructuredRemittanceInformation
Reference		STR	35	O	
Reference Type		STR	35	O	
Reference Issuer		STR	35	O	
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



Data element	Description	Type	Length	Presence indicator	Standardised name
Payee DEAN	Digital euro access number of the payee	STR	18	M	<i>(New for beta digital euro)</i>
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	Beta digital euro access number of the payer entered by the payer	STR	18	O	<i>(New for beta digital euro)</i>

Incoming message - supplementary data in case of CPACE transaction: EMV Cryptogram Data Envelope

- o 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 ICCRIttdData
Issuer Application Data (9F10)	Profile CCI	BIN	1	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
	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 ICCRIttdData
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 ICCRIttdData
Application Cryptogram (9F26)	Cryptographic code generated by the EMV card	BIN	8	M	In ISO 20022 EMV data are usually provided in the



EUROPEAN CENTRAL BANK

EUROSYSTEM

Data element	Description	Type	Length	Presence indicator	Standardised name
	to authenticate a transaction with the issuing bank				specific TLV field ICCRIttdData
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 ICCRIttdData
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 ICCRIttdData
Transaction Type (9C)	EMV Transaction type	NUM	2	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
Terminal country code (9F1A)	Terminal country code	NUM	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
Terminal Verification results – TVR	Terminal Verification results	BIN	5	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
Transaction currency code (5F2A)	Transaction currency code	NUM	4	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
Terminal Transaction Date (9A)	Terminal Transaction Date	NUM	6	M	In ISO 20022 EMV data are usually provided in the specific TLV field ICCRIttdData
Unpredictable Number (9F37)	A unique variable associated with the generation of the ARQC application	BIN	4	M	In ISO 20022 EMV data are usually provided in the



Data element	Description	Type	Length	Presence indicator	Standardised name
	cryptogram (discriminating element)				specific TLV field ICCRItData
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 ICCRItData
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 ICCRItData

#### 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

#### 7.1.1.4.2.2 Return Code

#	Description
0	Successful
1	Failure

#### 7.1.1.4.2.3 Functional error description (reason code)

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.

### 7.1.1.5 Refund request initiation validation

#### 7.1.1.5.1 Requirements

This feature allows the business end user (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 pilot 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.

#	Mandatory Optional Conditional	Business rules description
1	M	The pilot 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 PSP is responsible for conducting thorough fraud checks and due diligence procedures related to the business end user it acquires. This includes verifying the legitimacy of the business end user, monitoring transaction patterns for suspicious activity, and implementing appropriate risk mitigation measures to prevent fraudulent behaviour.
4	M	The acquiring PSP is required to perform anti-money laundering (AML) checks on the business end user it acquires. This includes verifying the identity and legitimacy of the business end user, assessing the risk of money laundering based on the business end user'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)



#	Mandatory Optional Conditional	Business rules description
7	M	The function must provide the return code. In case of rejection, a reason code must be provided.

### 7.1.1.5.2 Interface description

The data listed below in the incoming message are incomplete. The interaction between the pilot PSP and the business end user about refund request are not detailed. The pilot PSP must retrieve (at least) the identifier of the transaction that is being refunded and consider the refunded amount.

The pilot PSP can choose whether to retrieve all the information originally used to construct the initial transaction, including settlement data.

#### 7.1.1.5.2.1 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



EUROPEAN CENTRAL BANK  
EUROSYSTEM

Data element	Description	Type	Length	Presence indicator	Standardised name
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

7.1.1.5.2.2 *Return Code*

#	Description
0	Successful
1	Failure

7.1.1.5.2.3 *Functional error description (reason code)*

The functional error descriptions are listed in **Digital euro pilot – Frontend specifications – Common Services (section 4.2 – Notification Service)**.