EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital euro pilot

Frontend implementation specifications

Acceptance instruments

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

Introduction

The detailed implementation specifications for the different domains and interactions between actors are presented in the diagram below. The current document is dedicated to the business end user domain and is aimed at describing what must be implemented in the acceptance instruments to offer pilot payment services.

Offline transactions are out of scope of the current document.

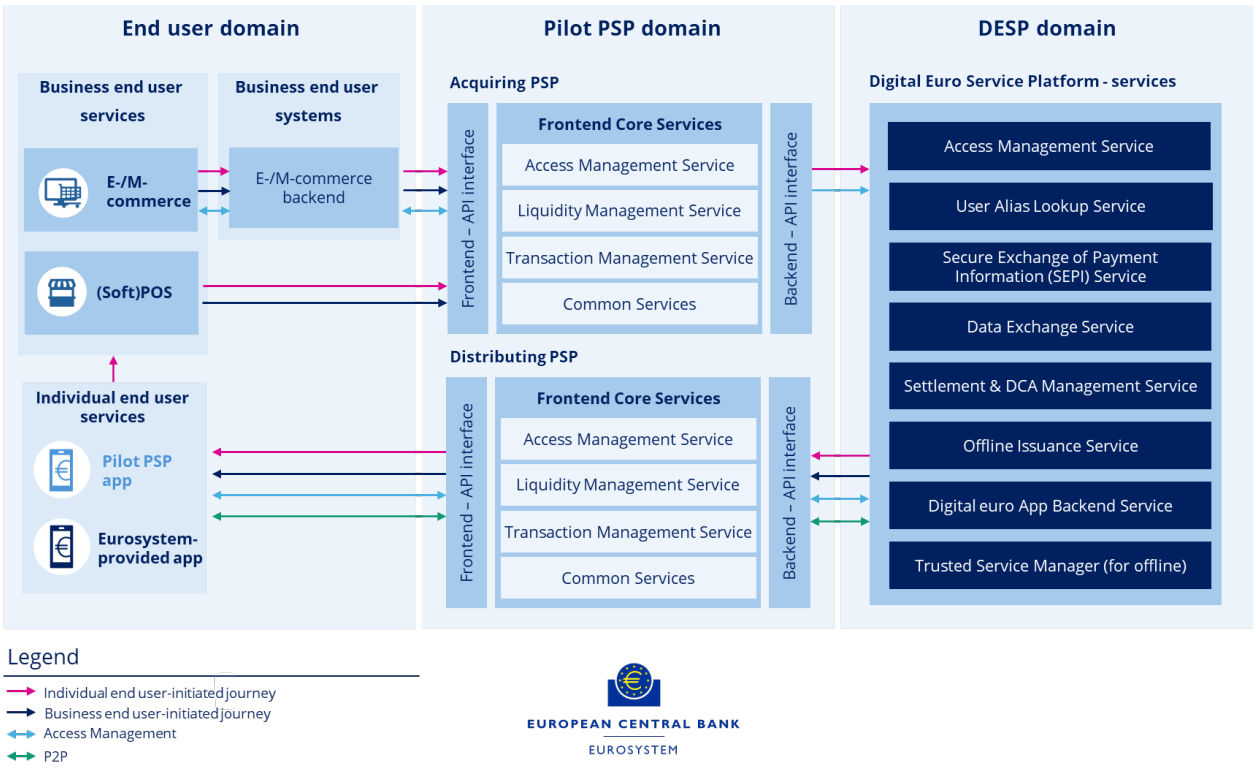

Figure 1 Digital euro pilot - functional architecture

Structure of the document

The **business end user** domain covers several types of acceptance instruments:

- Remote environments:
  - E-Commerce
  - M-Commerce
- Proximity environments
  - SoftPOS

1. E-commerce requirements

This chapter provides detailed implementation specifications for digital merchant point of interaction to allow business end users and acquiring PSPs to offer online beta digital euro dedicated functions.

The chapter is organised as follows:

- General requirements that are not “process specific“, that frame the application and define its characteristics (functional or not).
- Process requirements that describe the specificities of the beta digital euro functions that the application must satisfy.

1.1. General Requirements

This section provides general functional and non functional requirements for digital merchant point of interaction implementation. General requirements are related to the characteristics of the application, applicable independently of the processes.

1.1.1. Functional requirements

1.1.1.1. Beta digital euro payment method

The digital merchant point of interaction shall allow the individual end users to pay goods and services with beta digital euro.

1.1.1.2. User experience

The digital merchant point of interaction shall comply with minimum UX requirements as defined in **Digital euro pilot – User journeys & minimum UX requirements.**

1.1.2. Non-functional requirements

1.1.2.1. Supported operating systems

Business end users must ensure that mobile apps, web interfaces, and hardware are compatible with operating systems and browsers that remain within the official support lifecycle of their respective vendors. For security and compliance reasons, platforms that no longer receive vendor-issued security updates must not be supported. Compatibility must be limited to devices such as smartphones and tablets that receive ongoing security updates, support secure communication protocols, are not rooted or jailbroken, and include necessary hardware-level security features where applicable. This is to ensure data integrity, protection of sensitive information, and alignment with prevalent industry regulations and certifications.

1.2. E-commerce payments

E-commerce payments cover electronic payments between two end users for the purchase of goods or services via the internet. The individual end user (payer) should be presented with all possible payment instruments accepted by the business end user (payee) for payments in beta digital euro.

Assumptions

The existing functions related to end user management (registration, personal data, address management) and shopping experience are not impacted by the beta digital euro. The storage of the e-commerce transactions and corresponding status is not expected to be impacted and is not described either.

The digital point of interaction includes both the presentation layer (frontend) and the execution of functions (backend) and does not differentiate between them.

Only the rules applicable to the digital point of interaction are detailed. Rules related to actions performed outside of the digital point of interaction are out of scope of this chapter.

1.2.1. Overview of e-commerce payments

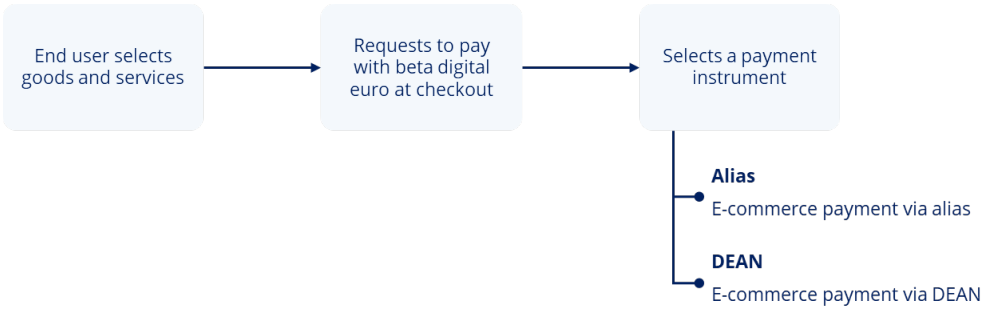

Figure 2 - Overview of e-commerce payments

1.2.2. E-commerce payment with alias

The payment is initiated by the individual end user (payer) who requests to pay at checkout through alias.

E2E flow reference: TM-2.2 E-commerce payment with alias or DEAN

Pre-requisites

1. The individual end user (payer) and the business end user (payee) have a beta digital euro account.
2. Alias is proposed as a payment instrument by the business end user (compliant with alias types usable in beta digital euro context).

#	Mandatory Optional Conditional	Business rules description
1	Conditional	- Alias option is presented to the individual end user only if this payment instrument is offered by the business end user.
2	Conditional	- If the individual end user is not acting as a "guest", and if the individual end user's alias has been stored previously by the business end user, the digital point of interaction must display it.
3	Conditional	- If the alias is not displayed, the individual end user must provide relevant information. - The individual end user must select the type of alias among the list of possible alias. - The individual end user must enter the alias value corresponding to the selected alias type. - The alias value format must be consistent with the alias type.
4	Conditional	- If the alias is not correct, the individual end user must be able to provide relevant information. - The individual end user must be able to use same alias type and update only the alias value. - The individual end user must be able to select a new type of alias among the list of possible alias. - The individual end user must enter the alias value corresponding to the new selected alias type. - The alias value format must be consistent with the alias type.
5	Mandatory	- The individual end user must confirm that the alias displayed or just entered is correct.
6	Optional	- The individual end user should be able to enter a message intended for the business end user to be informed about the transaction.
7	Optional	- The individual end user should be able to enter a Transaction Reference (End to End Identification).
8	Conditional	- The individual end user, if not acting as a "guest", must be able to choose if the business end user is allowed to store the alias provided for future purchases. - The digital point of interaction may only store the individual end user's data in a secure and compliant environment. (placeholder for reference to security framework)
9	Optional	- The merchant digital point of interaction can submit an alias validity check request to the payee PSP. Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.1 - alias validity check)**.
10	Conditional	- After submitting the alias validity check request, the business end user application receives the DEAN together with the corresponding PSP ID.
11	Optional	- The DEAN can then be displayed in a masked format, alongside the PSP ID, in the transaction detail summary.
12	Mandatory	- The payment request is generated only if the alias is confirmed. - The transaction request must include all the transaction details to process properly the payment. Refer to **Digital euro pilot – Frontend specifications – Acquiring PSP (section 7.1 - Payment initiation service - Business end user payment request initiation validation)**. - If the alias is not confirmed, the process must be discontinued.
13	(Placeholder)	- The individual end user consent and authentication (placeholder).

#	Mandatory Optional Conditional	Business rules description
14	Mandatory	- The digital merchant point of interaction must display the final status of the payment. - In case of rejection, the digital merchant point of interaction must provide the reason of the rejection.

1.2.3. E-commerce via DEAN

The payment is initiated by the individual end user (payer) who requests to pay at checkout with DEAN.

E2E flow reference: TM-2.2 E-commerce payment with alias or DEAN

Pre-requisites

1. Both the individual end user (payer) and the business end user (payee) have a beta digital euro account.
2. DEAN is proposed as a payment instrument by the business end user.

#	Mandatory Optional Conditional	Business rules description
1	Mandatory	- The digital merchant point of interaction must allow the individual end user acting as a payer to select a payment with DEAN.
2	Conditional	- If the individual end user is not acting as a "guest", they must be able to select a DEAN already used in a previous payment and stored by the digital point of interaction.

3	Mandatory	- The digital merchant point of interaction must allow the individual end user acting as a payer to enter manually a DEAN.
		- An initial format check must be performed. The DEAN must:
		  - Contain 18 characters
		  - Start with "EU"
		  - Include 16 numeric characters
		  - Indicate that the payer is an individual end user: the fifth character of the DEAN must be equal to "0".
		- The digital merchant point of interaction must request a DEAN validity check to the acquiring PSP.
		Refer to **Digital euro pilot – Frontend specifications – Common Services (section 1.4 - Beta digital euro account service/*DEAN validity check*)**.

4	Mandatory	- If the DEAN is not valid, the individual end user must be informed and must be allowed to retry.
5	Optional	- If the DEAN is valid, the corresponding PSP ID (PSP of the payee) could be displayed.
6	Optional	- The payer should be able to enter a message intended for the payee to be informed about the transaction.
7	Optional	- The payer should be able to enter a Transaction Reference (End to End Identification).

#	Mandatory Optional Conditional	Business rules description
8	Mandatory	- The pilot PSP app must allow the individual end user acting as a payer to confirm the transaction details. - The pilot PSP app must allow the individual end user acting as a payer to reject the transaction details.
9	Mandatory	- The digital merchant point of interaction must be able to generate a payment request that is transmitted to the acquiring PSP core system. Refer to **Digital euro pilot – Frontend specifications – Acquiring PSP (section 7.1 - Payment initiation service/Business end user payment request inititiation validation)**.
10	(Placeholder)	- The individual end user consent and authentication (placeholder).
11	Mandatory	- The digital merchant point of interaction must be able to receive the final status of the payment request execution.
12	Mandatory	- The digital merchant point of interaction must display the final status of the payment. - In case of rejection, the digital merchant point of interaction provide the reason of the rejection.

1.3. Refund on e-commerce

An individual end user can initiate a refund by requesting a refund from the business end user. The business end user can also initiate a refund if the goods or service are not delivered. A refund transaction is always linked to the original transaction. This section describes the rules dedicated to refund.

1.3.1. Overview of refund on e-commerce

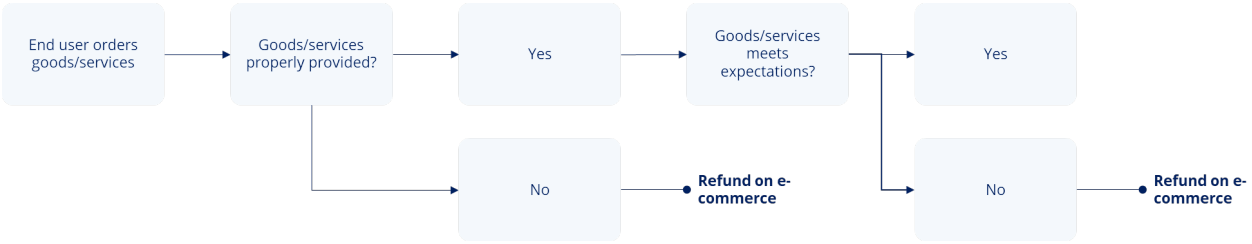

Figure 3 - Overview of refund on e-commerce

1.3.2. Refund on e-commerce

The refund is initiated by the business end user on individual end user's request or by their own decision if the goods/service is not delivered.

For the purpose of simplification, the rules are presented for the digital point of interaction even if another system (application) could be used instead by the business end user to proceed with the refund.

The existing refund process is not impacted by the beta digital euro.

E2E flow reference : TM-7.2 Refund e-commerce

Pre-requisites

1. The individual end user ordered good/services, the transaction is settled and the good/services are sent back to the business end user (partially or totally).
2. The individual end user ordered good/service and good/service is not delivered or does not meet expectations.
3. The terms and conditions stipulate that a refund request can be made.

#	Mandatory Optional Conditional	Business rules description
1	Conditional	- The refund request is allowed only if the refund conditions are met.

2	Mandatory	- The business end user must be able to filter existing transactions already settled according to several criteria.
		  - Transaction identifier
		  - Transaction date
		  - Product/Service identifier
		- The list of corresponding transactions must be displayed accordingly.

3	Mandatory	- The digital point of interaction must allow the business end user to select the initial transaction only if it has not been already refunded.
4	Mandatory	- When the initial transaction is selected, the digital point of interaction must allow the business end user to enter additional information to provide reason for the refund and request a confirmation. - The business end user must be able to ask a refund for the same amount, or to adjust the amount (greater or lower than the original transaction amount).
5	Conditional	- According to countries regulation, the refund must use the same payment method used in the original transaction.
6	Conditional	- If the refund is confirmed, the digital point of interaction must generate a refund request to the payee's acquiring PSP. Refer to **Digital euro pilot – Frontend specifications – Acquiring PSP (section 7.1 - Payment Initiation Service/Refund request initiation validation)**.
7	Mandatory	- The digital point of interaction must be able to receive the status of the refund request and close the process accordingly.
8	Mandatory	- The digital merchant point of interaction must display the final status of the refund. - The notification must provide clear and easy to understand messages and contain the reason of the rejection. - The notification message must be in the business end user's preferred language as defined by the pilot PSP.

2. M-commerce requirements

This chapter provides detailed implementation specifications for business end user mobile application used by an individual end user to buy goods and services.
This chapter is structured as follows:

- General requirements that are not specific to any single process, but that define and frame the application and its functional characteristics.
- Process-specific requirements describing the particular features of the beta digital euro functions that the application must support.

In the context of the beta digital euro, m-commerce is involved in transaction management processes. The requirements presented below cover the following use case:

- M-commerce payment – app-to-app

Assumptions

The existing functions related to individual end user management (registration, address management) and shopping experience are not impacted by the beta digital euro. The storage of the m-commerce transactions and corresponding status is not expected to be impacted and is not described either.

Business end user mobile application is considered in the current document as a whole system without any differentiation between the presentation layer (frontend) and the execution of functions (backend).

Only the rules applicable to the business end user mobile app are detailed out. Rules related to actions performed outside of the business end user mobile app are out of scope of this chapter specification. **Offline transactions are out of scope of the current document.**

2.1. General requirements

This section provides general functional and non functional requirements for business end user's mobile application implementation. General requirements are related to the characteristics of the application, applicable independently of the processes.

2.1.1. Functional requirements

2.1.1.1. Beta digital euro payment method

The business end user mobile application (app) shall allow the individual end user to pay for goods and services with beta digital euro.

2.1.1.2. User experience

The business end user mobile app shall comply with minimum UX requirements as defined in **Digital euro pilot – User journeys & Minimum UX requirements.**

2.1.2. Non-functional requirements

2.1.2.1. Supported operating systems

Business end users must ensure that mobile apps, web interfaces, and hardware are compatible with operating systems and browsers that remain within the official support lifecycle of their respective vendors. For security and compliance reasons, platforms that no longer receive vendor-issued security updates must not be supported. Compatibility must be limited to devices such as smartphones and tablets that receive ongoing security updates, support secure communication protocols, are not rooted or jailbroken, and include necessary hardware-level security features where applicable. This is to ensure data integrity, protection of sensitive information, and alignment with prevalent industry regulations and certifications.

2.2. M-commerce payments via mobile app

M-commerce payments consist in payments sent by the business end user app to the individual end user. The individual end user, after shopping online and requesting the checkout in a business end user app, performs the transaction payment through the pilot PSP app or the Eurosystem-provided app.

2.2.1. Overview of m-commerce payments

Figure 4 - Overview of m-commerce payments

2.2.2. M-commerce payment in app

The payment is initiated by the individual end user (payer) who requests to pay at checkout in the business end user app.

E2E flow reference: TM-2.4 M-commerce payment via mobile app

Pre-requisites

1. Both the individual end user (payer) and the business end user (payee) have a valid beta digital euro account.
2. The individual end user has installed the business end user app on their device.
3. The business end user app is able to manage redirection to either pilot PSP app or Eurosystem-provided app.
4. If both the pilot PSP app and Eurosystem-provided app are installed on the individual end user device, one app must be set as the default app.

#	Mandatory Optional Conditional	Business rules description
1	Conditional	- The business end user app must allow the individual end user to pay at checkout if the prerequisites are met.
2	Mandatory	- The business end user app must collect the minimum mandatory data elements of the payment transaction.
3	Mandatory	- The business end user app must generate a payment request based on the details retrieved after the individual end user completes the checkout process. - The individual end user must be automatically redirected to either the pilot PSP app or the Eurosystem-provided app depending on which is installed or set as default application.
4	Mandatory	- Placeholder for re-direction rules between both applications (Business end user app and individual end user app)
5	Mandatory	- If authentication fails, a rejection notification must be sent to the business end user app, which must then stop the payment process.

3. (Soft)POS requirements

This chapter provides detailed implementation specifications for merchant points of interaction in physical environments, enabling business end users and acquiring PSPs to offer pilot payment services for in-person payments.

3.1. General Requirements

This section provides general functional requirements for the implementation of digital merchant points of interaction in physical environments. These general requirements relate to the characteristics of the application and apply independently of specific transaction processes.

3.1.1. Functional requirements

3.1.1.1. Beta digital euro payment method

The physical point of interaction shall enable individual end users to pay for goods and services using beta digital euro through proximity payment technologies such as mobile NFC.

3.1.1.2. User experience

The merchant physical point of interaction shall comply with minimum UX requirements as described in **Digital euro pilot – User journeys & minimum UX requirements**.

3.1.2. Design decisions

3.1.2.1. Scope of Applicability – Payment Terminal Types

This specification applies to software-only solutions installed on commercial off-the-shelf (COTS) devices such as smartphones or tablets, enabling contactless payments without additional hardware. In this specification, the term 'POS' refers to both hardware-based terminals and software-based terminals (SoftPOS).

3.1.2.2. NFC 'point of acceptance'

In this document, the term 'point of acceptance' refers to the complete acceptance environment, encompassing both the POS terminal (acceptance instrument) and its associated acceptance infrastructure (e.g., acceptation-hosted backend systems), without distinction between frontend and backend components.

3.1.2.3. POS Protocol for beta digital euro account payment

The POS protocol for beta digital euro account payments, used for NFC transactions, is based on the CPACE-Terminal-Kernel-Specification (Kernel 2E).

3.1.2.4. POS notifications to the individual end user

The POS shall provide clear and easy to understand messages in the language as set in the language preferences offered to the individual end user. The business end user can offer messages in different languages, but payment-related messages must be in the individual end user's preferred language as defined by the pilot PSP.
At minimum, messages shall contain the result of the transaction or request initiated by the business end user via the merchant physical point of interaction. In the case of a rejection, the message shall provide the reason for the rejection.

3.1.2.5. CPACE Terminal Kernel

The terminal must implement the **CPACE Terminal Kernel**, which is identified by Kernel ID 2E (assigned by EMVCo). This kernel ensures compatibility with CPACE-compliant mobile applications.

3.1.2.6. NFC Payment UX at the POS with a beta digital euro account

For NFC payments involving a beta digital euro account, the objective is to avoid requiring cashier intervention to activate a specific POS configuration prior to initiating the transaction. The POS should be ready to accept such payments without manual setup.

3.1.3. POS configuration: CPACE KERNEL

3.1.3.1. CPACE KERNEL configuration

The acquiring PSP is responsible for implementing CPACE acceptance for the beta digital euro. The ECB only provides the data that must be configured in the CPACE terminal, as well as the data that must be transmitted from the POS to the acquiring PSP, which then forwards it to the DESP.

Each pilot PSP is free to define and implement its own acceptance solution, taking into account the specific characteristics of its commercial environment, such as:

- the type of business end user (small retailers, large chains, e-commerce platforms, etc.),
- the industrial partners involved (terminal providers, integrators, payment service providers), and the technical and operational constraints specific to each setup.

This flexibility is granted provided that the solution:

- complies with the latest official version of the CPACE kernel.
- is configured in accordance with the table below:

CPACE POS configuration for beta digital euro NFC payment

Name	Description
Kernel ID	2E
Type of trigger for authorization request	Automatic and systematic
Country code	PSP country depending
Currency Code	978
AID (RIX et PIX)	A0000009580110
Terminal capabilities	In accordance with EMVCo standards and based on the capabilities supported by the terminal, the following tags must be configured to enable CPACE HCE transactions with CDCVM support. Byte 2 Bit 8: EMV contactless Bit 5: Mobile functionality Bit 3: Consumer device CVM Byte 3 Bit 8: Contactless EMV mode
PDOL (eligibles tags)	9F66049F1A02
Maximum accepted transaction amount (CENTS)	99999999
Minimum accepted transaction amount (CENTS)	00000001
Terminal Action Code (TAC) Denial	00 00 00 00 00 (no bits set → never decline locally).
Terminal Action Code (TAC) Online	FF FF FF FF FF (all bits set → any issue forces online
Terminal Action Code (TAC) Default	00 00 00 00 00 → no fallback
POS Rejection Codes and Display Messages	See below — to be translated into the language of the acceptance instrument.

POS rejection codes and display messages

Code Meaning	Explanation	POS Display Message
001	Merchant not recognized or authorized	Invalid Merchant
002	Issuer refused the transaction without reason	Do Not Honor
003	General processing error	Error
004	Unsupported or malformed transaction	Invalid Transaction
005	Amount is zero, negative, or unacceptable	Invalid Amount
006	Token is not valid or recognized	Invalid Token
007	Card issuer could not be identified	No Such Issuer
008	Message format is incorrect or corrupted	Format Error
009	Not enough balance in the account	Insufficient Funds
011	Card not linked to a checking account	No Checking Account

Code Meaning	Explanation	POS Display Message
012	Card has expired	Expired Card
013	Card not found in issuer's system	No Card Record
014	Cardholder not allowed to perform this transaction	Transaction Not Permitted to Cardholder
015	Terminal not authorized for this transaction	Transaction Not Permitted to Terminal
016	Transaction flagged as potentially fraudulent	Suspected Fraud
017	A security rule was breached	Security Violation
018	Issuer or network is unavailable	Issuer or Switch Inoperative
019	Transaction could not be routed correctly	Routing Error
020	Transaction blocked due to legal restrictions	Violation of Law
021	Same transaction submitted more than once	Duplicate Transmission
022	Technical failure in the processing system	System Malfunction

3.2. NFC CPACE Mobile Payment with a beta digital euro account

Below specification follows the end-to-end process flow "**TM-1.6 Online Contactless SoftPOS Payment with mobile device – same pilot PSP**". However, there are some discrepancies that will be worked out in a next version of end-to-end process flows. Below, the E2E Flow Discrepancies in NFC/Chip-Based Online Payments via Mobile Devices.

- Authentication is performed prior to the payment tap, either by launching the pilot PSP app or through an initial "tap" that emulates the app launch.
- Authentication can be local to the device (offline authentication) or executed via an online connection to the app's backend (online authentication).

3.2.1.1. Overview of NFC CPACE Mobile payments at physical (Soft)POS with a beta digital euro account

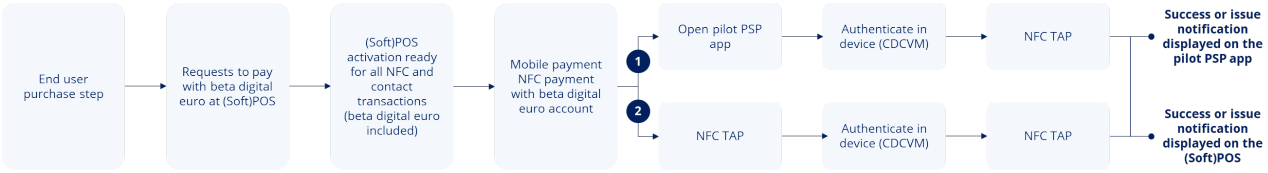

Figure 5 - Overview of NFC CPACE Mobile payments at physical (Soft)POS with a beta digital euro account

3.2.1.2. Mobile Payment NFC CPACE transaction with a beta digital euro account

Mobile NFC payments cover proximity transactions between two end users (an individual end user and a business end user) using NFC contactless technology. The payer should be able to select from all available beta digital euro payment instruments supported by the merchant's physical point of interaction.

The payment is initiated by the business end user (payee) who requests to an individual end user (payer) to pay at POS with their smartphone.

Pre-requisites

1. The individual end user (payer) and the business end user (payee) both have a beta digital euro account.
2. NFC payment with a beta digital euro account is proposed as a communication technology by the business end user.
3. The pilot PSP app used by the individual end user is enrolled with beta digital euro NFC-based mobile payment capabilities.

#	Mandatory Optional Conditional	Business rules description
1	Conditional	NFC payment with beta digital euro option is presented to the individual end user only if this payment instrument is accepted by the business end user.
2	Mandatory	The same AID will be used across both mobile NFC payment and contact/contactless card form factors.
3	Mandatory	For mobile NFC payments involving a beta digital euro account, the objective is to avoid requiring cashier intervention to activate a specific POS configuration prior to initiating the transaction. The POS should be ready to accept such payments without manual setup.
4	Mandatory	The transaction is initiated by the payee's device, and the payment request is transmitted to the DESP via the acquiring PSP through the payee's POS terminal.
5	Conditional	If the transaction request is invalid, the POS must inform the end user of the rejection using a message that accurately reflects the reason for the failure. This notification is displayed based on a reason code, which may be generated by the POS itself or provided by one of the stakeholders involved in the payment process. The notification message must be in the end user's preferred language as defined by the pilot PSP.
6	Mandatory	The HCE SDK stores the Distributing PSP ID in tag A5-BFOC-5F54 (BIC). The POS terminal must recover this tag to provide in the online authorization in accordance with the acquiring PSP's specifications, as defined in **Digital euro pilot – Frontend specifications – Common Services**.
7	Mandatory	The HCE SDK stores the last four digits of the DEAN in tag 9F25. The POS terminal must read this tag and display the value on the payment receipt, preceded by 12 asterisks, in accordance with PCI DSS standards.
8	Mandatory	The POS must be compliant with CPACE-Terminal-Kernel-Specification_V1.2.

#	Mandatory Optional Conditional	Business rules description
9	Conditional	In case of impossibility to go online, the CPACE HCE rejects the transaction by providing an AAC cryptogram in the response of the first generate AC.
10	Mandatory	No velocity checks are applied by the POS or the acquiring PSP regarding the number of NFC transactions performed with the same payment instrument.
11	Mandatory	Terminal Risk Management is to be Performed on CPACE HCE SDK request (This request is mandatory in CPACE HCE specification).
12	This becomes mandatory upon publication of the guideline by the ECB.	Sensory branding is a form of animation and sounds, serving to provide individual end users with auditory and visual cues, enhancing brand recognition, and providing additional audio-visual confirmation upon a successful transaction.
13	Mandatory	After the TAP NFC communication, the POS (Point of Acceptance) has obtained all the information to perform an online authorization in accordance with the acquiring PSP's specifications, as defined in **Digital euro pilot – Frontend specifications – Acquiring PSP (section 7.1 - Payment intitation service/Business end user payment request initiation validation)**.