EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook

IMPORTANT NOTICE:

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

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

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

Version:	0.91
Status:	DRAFT
Date:	02/07/2026

DISCLAIMERS FOR DRAFT RULEBOOK v0.91

Preliminary and non-binding nature of version 0.91

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

No reliance for implementation

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

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

PREAMBLE

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

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

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

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

The purpose of the current draft is to update the RDG and its constituencies on the progress made following the market consultation, coordinated by the RDG and concluded on 31 October 2025, and to serve as a basis for the further development of the draft rulebook.

This document represents a preliminary draft version which has not yet been subject to a general language and editorial review.

Table of contents

0 Document information

0.1 References

This section lists the legal documents referred to in the digital euro scheme rulebook, including relevant regulations and directives, as amended over time. The convention used throughout is to provide the reference number only, enclosed in square brackets. Square brackets are used exclusively for this purpose.

N°	Document Number	Title
[1]	COM/2023/369 final	Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro
[2]	COM/2023/368 final	Proposal for a regulation of the European Parliament and of the Council on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro
[3]	CON/2023/34	Opinion of the European Central Bank of 31 October 2023 on the digital euro
[4]	2015/2366	Directive of the European Parliament and of the Council of 25 November 2015 on payment services in the internal market (PSD2)
[5]	2022/2554	Regulation of the European Parliament and of the Council of 14 December 2022 on digital operational resilience for the financial sector (DORA)
[6]	2015/849	Directive of the European Parliament and of the Council of 20 May 2015 on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing (AMLD)
[7]	2016/679	Regulation of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (GDPR)
[8]	2013/575	Regulation (EU) the European Parliament and of the Council of 26 June 2013 on prudential requirements for credit institutions and investment firms
[9]	2009/110/EC	Directive of the European Parliament and of the Council of 16 September 2009 on the taking up, pursuit and prudential supervision of the business of electronic money institutions

[10]	2014/910	Regulation (EU) of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market
[11]	EBA/GL/2018/05	Guidelines on fraud data reporting applicable to Payment Service Providers
[X]	XX	Directive (EU) 2019/882 of the European Parliament and of the Council of 17 April 2019 on the accessibility requirements for products and services

Table 0-1 - Documents referenced

0.2 List of annexes

- A1: Testing, certification and approval
- B1: Illustrative User Journeys and minimum UX requirements
- B2: End-to-end flows
- C1: Reporting requirements
- D1 Front-end implementation specifications
- D2. Back-end implementation specifications
- E1: Risk management requirements - CONFIDENTIAL
- G1: Rulebook change request form

0.3 Change history

Until the delivery of draft rulebook version 0.8, incremental changes were made with each RDG meeting. Since version 0.8, reviews in form of new version numbers are made in line with commenting rounds.

Version 1.0 will describe the first draft version as approved by the Governing Council of the ECB and only after the adaptation of the digital euro regulation [1].

A public consultation will be conducted on this first draft following alignment with the EU Regulation, prior to its adoption by the Governing of Council of the ECB.

After finalisation of version 1.0 the versions included in the change history will be reset and subsequently follow updates according to the rulebook change management process (see Section 9).

Issue number	Dated	Change overview
V0.1	22 February 2023	Creation of the document.
V0.2	3 April 2023	First draft of end-to-end flows.
V0.3	4 May 2023	Updated end-to-end flows, section on actors.
V0.4	13 June 2023	Updated end-to-end flows, section on generic flows, section on scheme scope.
V0.5	11 July 2023	Updated digital euro scheme scope and interplay section, update functional model section (update to end-to-end flows as well as including draft paragraphs in the identification and authentication sections), included content on technical scheme requirements, updated defined terms ("Glossary").
V0.6	15 September 2023	Inclusion of a preamble, of Section 5 (technical scheme requirements), editorial adjustments to Section 2 and inclusion of high-level flows to Section 3, along with removal of detailed E2E flows moved to a dedicated annex.
V0.7	25 September 2023	Update of Sections 1 (editorial), 2 (mainly editorial) and 3 (inclusion of paragraph on dispute management principles).
V0.8	6 December 2023	Edits and adjustments to Sections 2, 5, and 8. Updates of Section 3 (inclusion of business rules), Section 4 (Adherence Model) and high-level E2E flows added.
V0.9	30 June 2025	Restructuring of rulebook sections. Implementation of rule-based format. Inclusion of Sections 5 (Risk management requirements), 6 (Dispute management requirements), 7 (Minimum UX requirements, 8 (Brand rules). Update of all remaining sections in view of RDG feedback on v0.8 as well as further project progress.

V0.91	24 April 2026	Restructuring of rulebook sections. Integration of Section 7 (Minimum UX requirements) into Section 3, Annex D1.2 into Annex D1 and Annex F1 into B1. Update of all sections in view of RDG feedback on v0.9 as well as further project progress.

Table 0-2 History of changes made to the rulebook

0.4 Defined terms

The digital euro scheme rulebook makes reference to various defined terms which have a specific meaning in the context of this rulebook. Section 10 provides a glossary with the list of defined terms.

0.5 Ownership of the document

The digital euro scheme rulebook is owned by the Central Banks that constitute the Eurosystem.

0.6 Intellectual property

The participants acknowledge that any copyright in the rulebook belongs to the ECB. The participants shall not assert contrary claims, or deal with the rulebook in a manner that infringes or is likely to infringe the copyright held by the ECB in the rulebook.

0.7 Governing law

[Placeholder].

0.8 Rulebook rule numbering convention

The following table outlines the structure of the rule numbering used throughout the digital euro scheme rulebook. Note that the rule numbering convention is specific for the business rules outlined in Section 3 and dispute management rules in Section 6 follow a separate convention as also specified in the below table.

Rulebook section	Rule numbering convention
Participation and Adherence Requirements	PAR.XX
Functional Requirements (including user experience)	FUR.XX
Business rules – Access Management	AM-XXX-XXX
Business rules - Liquidity Management	LM-XXX-XXX
Business rules – Transaction Management	TM-XXX-XXX

Technical Requirements	TER.XX
Risk Management Requirements	RMR.XX
Dispute Management Requirements	DMR.XX
Brand Rules	BRR.XX
Digital euro Fees, Limits and Threshold Requirements	DFR.XX
Scheme Rulebook Management	SRM.XX

Table 0-3 Rule numbering convention per chapter

1 Scheme rulebook scope

1.1 Section overview

This section articulates the objectives of the digital euro scheme rulebook and delineates its scope. The section specifies the scope of the rulebook in terms of geographical coverage, actors and their relationships, offered services and solutions. It also clarifies its interaction with other digital euro documentation.

1.2 Objectives

In accordance with article 5(2) of chapter II of draft regulation [1], the digital euro scheme rulebook provides a single set of measures, rules, and standards for the provision of digital euro payment services.

The digital euro rulebook ensures a standardised digital euro payment experience across all Member States of the euro area, irrespective of the country or the payment service providers (PSPs) used. It leverages, to the extent possible, on existing industry standards and procedures to improve interoperability and promote harmonisation within the European payments infrastructure.

1.3 Geographical scope

In accordance with article 13(1) of chapter IV of draft regulation [1], the digital euro scheme rulebook covers the provision of digital euro payment services by PSPs to natural and legal persons residing or established in the Member States whose currency is the euro, natural and legal persons who opened a digital euro payment account at the time they resided or were established in the Member States whose currency is the euro, but no longer reside or are established in such Member States as well as visitors. Additionally, subject to agreements or arrangement between the European Central Bank and respective central banks, services may be provided to natural and legal persons residing or established in EU member states outside the euro area[2] or other thirdcountries[3]. The geographical scope allows for the provision of both domestic and cross-border digital euro payment transactions.

1.4 Actor scope

1.4.1 Actors

The provision and usage of digital euro payment services involve the following actors, acknowledging that an actor may serve as another actor depending on the context (e.g., a payer may also act as a payee):

[2] Subject to article 18 of proposed regulation [1] and proposed regulation [2].
[3] Subject to article 19 and 20 of proposed regulation [1].

- **Payer,** which is ’a natural or legal person who holds a digital euro payment account and allows a payment order from that digital euro payment account’[4].
- **Payee,** which is ’a natural or legal person who is the intended recipient of funds which have been the subject of a digital euro payment transaction’[5].
  Note: Payer and payee can be an individual or business digital euro user:
  - An **individual digital euro user** is a natural person who is acting for purposes which are outside his or her trade, business, craft or profession and is allowed to open a digital euro payment account
  - A **business digital euro user** is a natural or legal person, who is acting for purposes of his or her trade, business, craft or profession and is allowed to open a digital euro payment account.
- **Payment service providers (PSPs)** participating to the digital euro scheme. These can be either:
  - **Payer PSP**: the PSP providing digital euro payments services to the payer[6]. The rulebook and its annexes occasionally refer to the Payer PSP as the ‘’payer distributing PSP’’ or ‘’digital euro individual user PSP’’, depending on context, or
  - **Payee PSP:** the PSP providing digital euro payments services to the payee. In case the payee is a digital euro business user, this actor can be referred to as the **acquiring PSP**
  - **Payer’s commercial bank money PSP**: the PSP which holds the payer’s linked non-digital euro payment account which can be used for funding and defunding of a digital euro payment account. The payer’s commercial bank money PSP is required for reverse waterfall transactions. The payer’s commercial bank money PSP can be or cannot be the same PSP as the payer PSP, or
  - **Payee’s commercial bank money PSP** is the PSP which holds the payee’s linked non-digital euro payment account which can be used for funding and defunding of a digital euro payment account. The payee’s commercial bank money PSP is required for waterfall transactions. The payee’s commercial bank money PSP can be or cannot be the same PSP as the payee PSP.
- **Third-party Service Providers (TPSPs)** are the parties contracted by one or several of the PSPs defined above to support their provision of digital euro payments services. Third-party service providers are not bound to a specific service and may support PSPs on services related to the digital euro based on a contractual agreement.
- **Digital euro Scheme Governing Authority (SGA)** is the decision-making entity responsible for the governance of the digital euro payment scheme.

---

4 As defined in the regulation proposal [1] (and amended over time)
5 As defined in regulation proposal [1] (and amended over time)
6 As defined in Section 1.5 Services in scope of this rulebook

- **Provider(s) of the Digital Euro Service Platform (DESP)** which are organisations, comprising Eurosystem members and private legal entities, tasked with developing, maintaining, and operating the core infrastructure of the digital euro.
- **TARGET services operator(s)** relevant to the provision of the digital euro payment services. These are the legal and/or organisational entity/entities that operates/operate the TARGET Services.

1.4.2 Scheme participants

Article 13 of draft regulation [1] specifies the types of PSPs required to enable their clients, upon request, to use their accounts for funding and defunding their digital euro payment accounts. These PSPs are, therefore, participants in the digital euro scheme, acting at a minimum as ‘’commercial bank money PSP’’.

Article 14 of draft regulation [1] defines the types of credit institutions required to provide digital euro payment services at their clients' request. These institutions are digital euro scheme participants, acting at least as ‘’(payer/) distributing PSP’’.

Other PSPs may choose to join the digital euro scheme voluntarily, provided they meet the eligibility criteria and complete the adherence process outlined in Section 2 of the rulebook. These institutions are digital euro scheme participants.

The **payer PSPs**, **payee PSPs**, the **payer’s commercial bank money PSP** and the **payee’s commercial bank money PSP** are all digital euro scheme participants. Scheme participants are also referred to as ‘participants’ in the rulebook.

1.4.3 Relationships between actors

Figure 1.1 illustrates, in a simplified manner, the actors mentioned in Section 1.4.1 and involved in digital euro payment services and their relationships, categorised into six types.

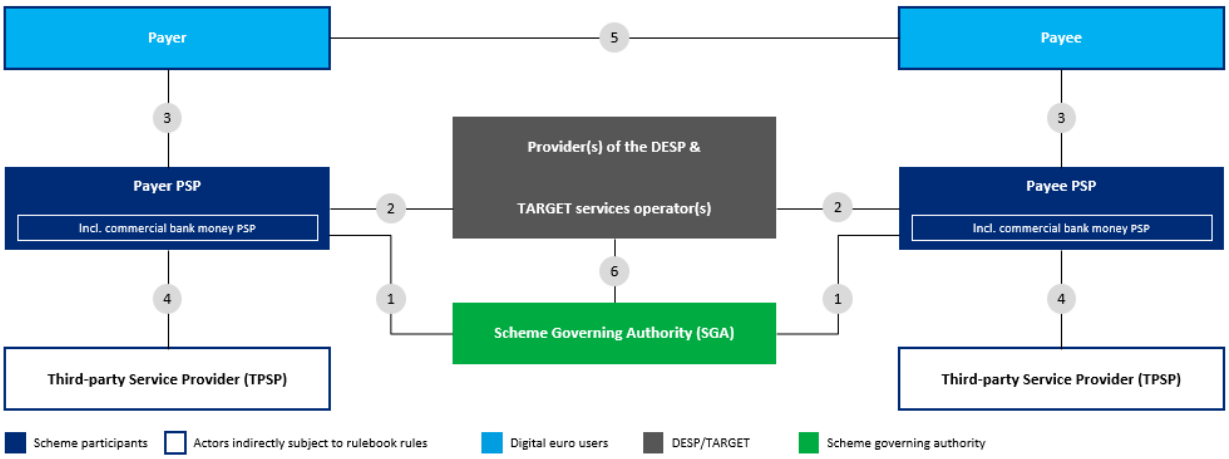

Figure 1-1 Scheme actors model

(1) The relationship between a PSP participating in the scheme and the digital euro Scheme Governing Authority (SGA) is defined in the digital euro scheme rulebook to which the participants need to adhere to.

(2) The relationship between a participating PSP and the provider(s) of DESP and TARGET services is not governed by the digital euro scheme rulebook. The DESP services provided to PSPs by the Eurosystem will be detailed in the respective DESP legal framework. Please note, Figure 1-1 is a simplified picture and although not shown in the picture, e.g. indirect TARGET participants are also included in this relationship.

(3) The relationship between the digital euro user (payer, payee) and their PSP for digital euro payment services is outlined in the respective PSP's Terms and Conditions, which are not directly governed by the digital euro scheme rulebook. However, participating PSPs will be expected to reflect, in their Terms and Conditions, their obligations under the digital euro scheme rulebook as well as under the draft regulation [1] to ensure harmonised provision of basic digital euro payment services.

(4) The relationship between a participating PSP and its third-party service provider is governed by their bilateral contractual arrangements and not directly by the digital euro scheme rulebook. Participating PSPs are responsible for incorporating relevant rulebook provisions into these contracts to ensure the PSP's continued compliance with the rulebook in delivering digital euro payment services.

(5) The relationship between the payer and payee falls under national private law and is outside the scope of the rulebook, with its validity having no impact on the final settlement of digital euro transactions within the scheme.

(6) The relationship between the Provider(s) of the DESP / TARGET services operator(s) and the SGA is not in scope of the rulebook.

For the offline digital euro payment transactions, PSPs are not directly involved since holdings are transferred directly between users' offline digital euro devices. PSPs handle funding and defunding requests. A participation model specific to offline digital euro use cases will be included in a future version of the rulebook.

1.5 Services in scope

The rulebook provides a set of unified measures, rules and standards for the provision of digital euro payment services as defined in Annex I and II of draft regulation [1]. Annex I lists the following services to be offered by PSPs:

1. Enabling digital euro users to access and use the digital euro, without prejudice to possible limitations set by the European Central Bank in accordance with Article 16 of draft regulation [1];
2. Enabling digital euro users to initiate and receive digital euro payment transactions and providing digital euro users with digital euro payment instruments;
3. Managing digital euro users' digital euro payment accounts;
4. Conducting funding and defunding operations in accordance with Article 13 of draft regulation [1]; and
5. Providing additional digital euro payment services on top of basic digital euro payment services pursuant to Annex II for natural persons:.

   Basic digital euro payment services for natural persons consist of:

   a. Opening, holding and closing of a digital euro payment account;
   b. Consulting balances and transactions;
   c. Non-automated funding and defunding from a non-digital euro payment account;
   d. Funding and defunding from/into cash;

e. Initiation and reception of digital euro payment transactions by means of an electronic payment instrument, to the exclusion of conditional digital euro payment transactions other than standing orders, in the following use cases:

   i. Person-to-person digital euro payment transactions;

   ii. Point-of-interaction digital euro payment transactions, including point-of-sale and e-commerce;

   iii. Government-to-person and person-to-government digital euro payment transactions.

f. Digital euro payment transactions referred to in Article 13(4) of draft regulation [1][7] and

g. Provision of at least one electronic payment instrument for the execution of digital euro payment transactions such as referred to in letter (e).

Throughout the rest of the rulebook, these services are categorised into three categories: transaction management, access management, and liquidity management. See also Section 3.5 - Figure 3-1 - for a more detailed services overview.

Access management includes services 1, 3, 5.a, 5.b, and 5.g.

Liquidity management includes services 4, 5.c, and 5.d.

Transaction management includes services 2, 5.e, and 5.f.

1.6 Payment instruments, acceptance solutions and communication technologies

1.6.1 Payment instruments

A payment instrument is a personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order.

The set of rules, standards, and procedures included in the rulebook for the provision of digital euro payment services covers the following payment instruments:

- Mobile application (PSP) - for online and offline digital euro

[7] Payment service providers providing account servicing payment services within the meaning of Directive [4] shall enable digital euro users: (a) to have their digital euros in excess of any limitations the European Central Bank may adopt in accordance with Article 16 automatically defunded to a non-digital euro payment account, where an online digital euro payment transaction is received; (b) to make an online digital euro payment transaction where the transaction amount exceeds their digital euro holdings.

- Digital Euro mobile application[8] - for online and offline digital euro
- Online banking (PSP) - for online digital euro
- Physical card - for online and offline digital euro
- Battery-powered card - for offline digital euro

1.6.2 Acceptance solutions

An acceptance solution is a combination of a digital euro user device, a user interface and communication technology, used by the payee which enables the acceptance of digital euro payment transactions. For the provision and acceptance of digital euro payments services the rulebook covers the following acceptance solutions:

- Software[9] Point-of-Sale (SoftPOS) & Point-of-sale (POS) terminals and devices – for online and offline digital euro
- E-Commerce check-out web pages – for online digital euro
- M-commerce check-out applications – for online digital euro
- ATMs – for online and offline digital euro
- Mobile app(lication) (PSP) – for online and offline digital euro
- Digital euro app(lication) (ECB) – for online and offline digital euro
- Battery-powered cards – for offline digital euro
- Bridge-device (for card) – for offline digital euro

1.6.3 Communication technologies

Communication technology is technology used for the transmission of data between two devices. This includes proximity and remote methods. The rulebook covers the following communication technologies:

- Near-field communication (NFC) (contactless)
- Card (chip) (contact)

---

[8] Requirements for the digital euro app will be detailed further in future versions of the rulebook and/or other documentation.

[9] Traditional POS (Point-of- Sale) systems are dedicated hardware terminals, e.g. used at a check-out counter. SoftPOS or Software POS converts NFC-enabled devices (e.g. smartphones or tablets) into a payment terminal via an app

- Internet (i.e., payment with alias, DEAN, QR Codes and/or pay-by-link)

1.7 DESP and TARGET

The Eurosystem's provision of DESP services (including the sub services) and Digital Euro Service Platform Dedicated Cash Accounts (DESP DCAs) are not covered by this rulebook and addressed in separate documentation. However, the rulebook will consider requirements from DESP to Scheme participants where this is considered necessary for consistency and completeness.

The DESP services provided to PSPs by the Eurosystem are detailed in distinct DESP legal documents. The provision of DESP DCAs is governed by the TARGET Guidelines.

2 Participation and adherence requirements

2.1 Section overview

This section outlines the requirements for participation in the digital euro scheme. It includes the eligibility criteria and the process for becoming a scheme participant. The section details the liability regime between PSPs and the Eurosystem.

In addition, it informs on the requirement to comply with rulebook provisions at all times and the consequences of a scheme participant's non-adherence with the rulebook requirements, while also addressing potential exemptions and SGA rights. Finally, it describes the procedure for a scheme participant's withdrawal from the scheme, ensuring scheme participants understand their obligations and rights.

2.2 Scheme participation

The onboarding to scheme and related participation management of a PSP is supported by an online tool provided by the Eurosystem. Further details on the onboarding process will be provided in dedicated scheme and DESP onboarding guides, available in the tool. For the offline digital euro, certain rules may differ, and next version(s) of the rulebook will provide details on this.

As outlined in Section 1.4.2, of the rulebook, certain institutions are mandated to join the scheme, while others may do so voluntarily. All PSPs joining the scheme shall meet the eligibility criteria defined in Section 2.2.1.

2.2.1 Eligibility Criteria

PAR.01 In order to be eligible to become a scheme participant, a digital euro scheme applicant shall fulfil the following eligibility criteria and demonstrate them when requesting participation and during their onboarding process to the scheme:

(1) the digital euro scheme applicant shall be an account servicing payment service provider under Directive [4], be authorised by a relevant EU regulatory body and be supervised by competent authorities incorporated in EU Member States. Or be incorporated and appropriately authorised by a relevant regulatory body and supervised by competent authorities incorporated in third countries which have signed an agreement with the EU under Art 19 or amended an existing monetary agreement under Art 20 of the [draft regulation].

(2) the digital euro scheme applicant needs to have direct or indirect access to a DESP DCA, i.e. being able to be debited/credited in a DESP DCA as part of a funding/defunding operation.

(3) the digital euro scheme applicant is not required to own or to be able to directly instruct a DESP DCA.

PAR.02 An applicant/scheme participant shall meet the eligibility criteria at all times, i.e. also after having been granted scheme participation.

PAR.03 An applicant/scheme participant shall notify the SGA of any matter that does or could affect its eligibility to participate without delay. These matters include, but are not limited to, insolvency, mergers, acquisitions, licensing processes, and other relevant operational or legal developments. The notification to the SGA shall be done via the online tool provided by the Eurosystem.

PAR.04 In the event a scheme participant does not fulfil eligibility criteria PAR.01(1) any longer, the SGA will terminate the participation in the scheme.

PAR.05 In the event a scheme participant does not fulfil eligibility criteria PAR.01(2) or PAR.01(3), the SGA may terminate the participation in the scheme (see) PAR.45.

PAR.06 The SGA must inform a scheme participant about matters affecting their participation status. The SGA must notify, via the online tool or register of participants, other scheme participants or digital euro users about a change in a participant's status or loss of eligibility.

2.2.2 Becoming a scheme participant

PAR.07 To become a scheme participant an applicant shall undergo the onboarding process to the scheme, including the necessary processes required to meet eligibility criteria PAR.01(2) and PAR.01(3). The applicant shall further conduct an initial self-assessment of adherence with rulebook requirements in line with the eligibility criteria under Section 2.2.1. Applicants shall submit the applications with the self-assessment to the SGA via the online tool and follow the process described in the below Sections 2.2.2.1 to 2.2.2.6.

Figure 2-1 - PSP onboarding process overview

2.2.2.1 PSP initiation of scheme participation

PAR.08 To initiate the application process, the applicant shall contact the SGA to request access to the online tool and the registration documentation required to start the participation request process. The SGA may proactively share the relevant documentation with PSPs subjected to mandatory provision of digital euro services.

PAR.09 The applicant shall submit a completed and signed participation request form along with all necessary documentation to the SGA via the online tool.

PAR.10 In any step of the process, the applicant shall reply to any request of the SGA for additional information and documentation without delay.

2.2.2.2 Validation of the PSP request to scheme participation

PAR.11 The SGA validates the participation request and reviews the completeness of the necessary documentation for the PSP application against the eligibility criteria set in Section 2.2.1 within XX calendar days of receiving the participation request form. If validated, within the same time frame, the SGA provides PSPs access to the online portal.

2.2.2.3 Submission of application to participate by the PSP

PAR.12 Once the applicant's request is validated, the applicant shall be notified of such via the online portal by the SGA. The applicant shall then follow the [scheme onboarding guide] provided by the SGA via the online portal and submit the required documentation.

2.2.2.4 PSP solution(s)[10] certification

PAR.13 The applicants are required to successfully partake in the digital euro testing and meet certification requirements, necessary for scheme participation and DESP access. This includes: (i) front-end technical solution certification, (ii) back-end testing and certification, and (iii) end-to-end certification.

PAR.14 The applicant shall ensure that its solutions meet all certification requirements necessary for providing digital euro payment services. These shall be appropriately tested and implemented as per Annex D1 Front-end implementation specifications.

The details of the processes for (i) front-end testing and certification and (iii) end-to-end testing and certification are described in Annex A1 Testing, certification and approval. The processes for (ii) back-end testing and certification are defined in the [DESP onboarding guide for PSP], available in the online tool.

2.2.2.5 PSP solution(s) approval

PAR.15 The [Certification Entity] of the SGA shall prepare a technical solution certificate summary report based on the front-end, end-to-end and DESP certificates for the applicant and submit it to the SGA, which is responsible for approving the PSP's solution(s). This approval process is based on the verification that the PSP solution(s) meets all certification requirements necessary for providing digital euro payment services.

PAR.16 The applicant shall at all times cooperate in the process of approval and provide additional documentation or undergo any additional activities (e.g. re-testing) as reasonably required by the SGAor the certification entity of the SGA. Non-compliance with the solution(s) approval requirements can lead to the non-completion or delay of the onboarding process and possibly result in not being able to provide digital euro services as required by the draft regulation [1]. The details for PSP solution(s) approval are described in Annex A1 Testing, certification and approval.

2.2.2.6 PSP operationally ready to offer digital euro payment services

PAR.17 An applicant becomes a scheme participant once it has been confirmed by the SGA that it meets all eligibility criteria and has successfully undergone the onboarding process, including the

[10] A solution is a combination of technical or functional factors which enable the initiation and the acceptance of digital euro payment transactions. Digital euro solutions are certified by certifying entities either as acceptance solutions or as distributing solutions.

certification and approval for its solutions by the SGA. Upon such confirmation, the SGA shall notify the PSP of its effective participation via the established online tool. This information will also be publicly communicated by updating the list of digital euro scheme participants available on the ECB website.

2.2.3 Register of digital euro scheme participants

The SGA maintains and regularly updates the register of digital euro scheme participants, accessible via the ECB website. The register details: (i) the legal name of the PSPs and their participating status to the scheme (as defined in Table 2-1), (ii) the PSP identifier; (iii) type of entity/license owned, (iv) the certified and approved digital euro solutions it provides, and (v) the date on which each digital euro scheme applicant acquired Participant status.

PAR.18 By submitting an application to become a scheme participant, a digital euro scheme applicant consents to the publication of the details outlined in this section.

PAR.19 In the event of changes to an applicant's / scheme participant's public registry and/or licence information, resulting in inaccuracies in the register of scheme participants, the scheme participant shall inform the SGA without undue delay.

Status	Legend
Active	PSP providing digital euro payment services.
Onboarding in progress	PSP undergoing onboarding to the digital euros scheme. [planned date for onboarding to be completed]
Inactive	PSP used to be but is no longer able to provide digital euro payment services. [date when participation was finalised]
Suspended	PSP participation to the scheme is suspended. [date when participation was suspended]
Terminated	PSP participation to the scheme is terminated. [date when participation was terminated]

Table 2-1 Status of PSPs' participation to the scheme

2.3 Liability regime

[Placeholder]

This section will cover the liability regime of the SGA and PSPs.

2.4 Adherence to the rulebook

PAR.20 A scheme participant shall ensure full compliance with all applicable rulebook provisions throughout its participation. This obligation also applies in case of outsourcing and use of third-party service providers.

PAR.21 Furthermore, scheme participants shall ensure that the compliance requirements applicable to their digital euro users (individual digital euro users and business digital euro users) are reflected in the contracts that the scheme participants will conclude with their customers.

PAR.22 A scheme participant shall conduct self-assessments of compliance with rulebook requirements initially, at the point of onboarding in line with Section 2.2.2., and continuously afterwards, whenever a change occurs in the rulebook. A scheme participant shall communicate the outcome of the self-assessments to the SGA. For the purpose of conducting self-assessments, an assessment methodology and templates will be provided by the SGA to scheme participants.

PAR.23 A scheme participant must submit an annual attestation of compliance with the rulebook requirements via the online tool, using the dedicated form provided for this purpose. This obligation does not apply where the scheme participant has carried out a self-assessment in the same year due to a rulebook change.

PAR.24 A scheme participant must promptly report any identified breach with a rulebook rule to the SGA. In case a scheme participant has identified a breach with a rulebook rule, irrespective of its origin, the scheme participant may request a temporary exemption from the SGA in line with the exemption requirements outlined in Section 2.5.

PAR.25 If the SGA confirms non-compliance, upon report from the scheme participant, any eventual exemption request will be assessed and the scheme participant will be informed and asked to refrain from actions resulting in non-adherence and/or take any appropriate remedial action.

PAR.26 The SGA will also assess a scheme participant's adherence to the rulebook. Other stakeholders may report potential non-compliance with rulebook requirements by a scheme participant to the SGA, through pre-defined forms based on established criteria and via defined complaint mechanism[11].

PAR.27 If the SGA confirms non-adherence, either through its own assessment or based on information provided by other stakeholders, the scheme participant will be informed and asked to refrain from actions causing non-adherence and/or take any appropriate remedial action.

[11] Complaint mechanism will be further defined in later versions of the rulebook.

PAR.28 The response of the SGA to non-adherence is commensurate with the severity and impact of the compliance breach, ensuring a balanced, fair and effective approach to scheme participants' non-adherence. The measures outlined in the paragraphs PAR.36 – PAR.44 are neither cumulative nor sequential. Any timeframes for the measures are indicative and dependent on the application of the principle of proportionality.

PAR.29 Upon verification of non-adherence, the SGA will issue an initial notice of non-adherence to the scheme participant. The notice will be addressed to the management body of the scheme participant.

PAR.30 The written non-adherence notice from the SGA will:

1. Specify the exact rulebook requirements and corresponding rules that are not complied with.

2. Assign a severity level (high, medium, low)[12] to the non-adherence, based on the nature of rulebook requirement(s) breached, the materiality of the breach(es), any persistent or cumulative instance(s) of non-adherence and any other relevant circumstances.

3. Set a deadline (30 calendar days) for the scheme participant to submit a remediation plan in writing. This deadline may be adjusted depending on the level of severity of the non-adherence.

    a. The remediation plan shall be assessed by the SGA within 5 calendar days of receipt.

    b. Where the remediation plan is not approved, the SGA shall require the scheme participant to amend and resubmit the plan within 10 calendar days.

4. Require the scheme participant to report back to the SGA once remediation measures have been implemented or upon expiry of the remediation deadline, whichever occurs first.

    a. The SGA shall verify full remediation within XX calendar days following such notification. This verification timeline may be adjusted depending on the severity of the non-adherence.

[12] The severity levels will be further defined in later versions of the Rulebook, including what type of breaches of the rulebook requirements would fall under each severity level.

5. Inform the scheme participant of its right to object to the notice where it considers it wholly or partially unfounded or unjustified.

    a. The objection shall be submitted in writing within XX calendar days following the issuance of the notice, including adequate reasoning and, where relevant, supporting evidence.

    b. The SGA shall assess, within XX calendar days, the objection and, where it is rejected, provide a reasoned written decision.

    c. In such cases, the SGA shall also reiterate the applicable obligations and timelines referred to in points (3) to (4).

PAR.31 Upon receipt of the non-adherence notice, the scheme participant shall submit a remediation plan within the deadline specified in the notice, unless PAR.32 or PAR.33 applies. The plan shall detail corrective actions, implementation timelines and expected outcomes, demonstrating the scheme participant's commitment to remedy the non-adherence.

PAR.32 In cases of low severity, the scheme participant may, instead of submitting a remediation plan, request a temporary exemption based on duly justified exceptional circumstances. This shall be in line with the exemption requirements outlined in Section 2.5.

PAR.33 In cases of high severity, the scheme participant may be required by the SGA to take immediate corrective measures to resolve the non-adherence, without prejudice to the subsequent submission of a remediation plan where appropriate.

PAR.34 Where a scheme participant fails to comply with the deadlines set in the non-adherence notice or in the approved remediation plan, the SGA shall issue a second non-adherence notice. The SGA may extend the remediation deadline where justified, contingent upon:

- The severity and complexity of the non-adherence and
- Objective reasons provided by the scheme participant for missing the initial deadline.

PAR.35 If the remediation plan is deemed inadequate. the SGA shall issue a written request requiring the scheme participant to amend and resubmit the plan within a specified timeframe.

2.4.1 Penalty mechanism

PAR.36 Failure to act in line with the non-adherence notice within the imposed deadlines or in line with the remediation plan may result in further actions being taken by the SGA against the scheme participant in the form of pecuniary fines or contractual penalties. The SGA will issue a notice to the scheme participant of the impending probability of a fine or penalty. The scheme participant has the possibility to react to the notice, in writing, notifying of the scheme participants planned or existing remediation measures or with a request for more time in order to address the non-adherence.

PAR.37 In cases of continued non-adherence – repeated or ongoing failure to comply with rulebook requirements, whether due to unresolved breaches after remediation deadlines, repeated non-compliance despite prior remediation efforts, or the accumulation of multiple non-adherence instances over a period of time – the SGA may impose effective, proportionate and dissuasive penalties or fines, taking into account the scheme participant's size, activity and non-adherence's impact.

PAR.38 Continued non-adherence may result in further increases in penalties or fines, emphasising the need for resolution. Depending on the timelines (see Table 2-2), failure to meet deadlines may result in additional fines, which may continue monthly/bi-weekly up until a maximum fine is imposed.

		Measure		
	Severity	**Low**	**Medium**	**High**
Duration	Day 1	Warning	Warning	Warning
	Day + X (e.g. 1 month)	Fine	Fine ↗	Fine ↗↗
	Day +XX (e.g. 2 months)	Increased or repeated fine	Increased or repeated fine ↗	Increased or repeated fine ↗↗
	Continuously (e.g. Monthly/bi-weekly)	Maximum fine	Maximum fine ↗	Maximum fine ↗↗

Table 2-2 – Proposed penalty and timeline per severity level

PAR.39 In cases of low severity non-adherence, in order to apply the principle of proportionality, the SGA may provide guidance rather than impose fines, focusing on corrective actions.

2.4.2 Suspension

PAR.40 The SGA may suspend the scheme participant's involvement in the digital euro scheme, for some or all services and for a defined period (maximum 6 months). The SGA must notify, via the online tool, the management body of the scheme participant in writing, indicating the grounds, the starting date and the duration of the suspension. In these cases, the scheme participant must support the process, by facilitating a smooth transition of services for digital euro users, supporting switching and minimising disruption. The scheme participant will have the opportunity to contest the suspension by submitting an objection to the SGA within XX days from the notification. The scheme participant must provide valid and sufficient grounds to support their objection.

PAR.41 Upon the suspension of a scheme participant’s participation, the SGA must publicly announce the suspension, having confirmed that appropriate steps were taken to ensure a smooth transition of services for digital euro users. This transparency ensures that all stakeholders are adequately informed and can take necessary actions to protect their interests.

2.4.3 Termination

PAR.42 The SGA may terminate a scheme participant's participation in the digital euro scheme in severe cases and due to continued non-adherence. In this case, upon notification by the SGA of the termination, indicating the grounds and the date of termination, the scheme participant will also have the opportunity to contest the termination, prior to it taking effect, providing adequate grounds to the SGA in case of objection.

PAR.43 In clearly and narrowly defined exceptional circumstances, immediate exclusion of a scheme participant from the digital euro scheme by the SGA may be possible. A scheme participant may be withdrawn from the digital euro scheme in specific cases such as high severity of the non-adherence with the digital euro scheme rulebook requirements, where there are immediate risks for digital euro users and the scheme or other cases such as opening of insolvency proceedings or withdrawal of a credit institution license. In these cases, the decision for the termination of a scheme participant’s participation from the digital euro scheme would lie with the SGA, and will take into account, amongst others, the remaining operational capabilities of the scheme participant.

PAR.44 Upon the termination of a scheme participant's participation in the scheme, the SGA must publicly announce its termination, having confirmed that appropriate steps were taken to ensure a smooth transition of services for digital euro users. The communication is done via the register of digital euro scheme participants. This transparency ensures that all stakeholders are informed and can take necessary actions to protect their interests.

2.5 Exemptions

[Placeholder]

2.6 Withdrawal of voluntary participation

PAR.45 A scheme participant that is not subject to the obligation of mandatory provision of the digital euro services under the [draft regulation] may voluntarily withdraw its participation from the digital euro scheme. Where a scheme participant decides to withdraw from the scheme, a scheme participant must give written notice in due time (6 months in advance of withdrawal) to the SGA.

PAR.46 The scheme participant shall inform its digital euro users of the withdrawal, within XX calendar days after submitting the written notice, and of the process of digital euro payment account switching.

PAR.47 Where a scheme participant provides written notice of its intention to withdraw its participation, it must ensure continued access to digital euro services for their existing digital euro users until the end of the scheme participant's participation.

PAR.48 The scheme participant needs to ensure adherence with all rulebook requirements and remains responsible until the end of its participation.

PAR.49 The scheme participant shall, following the end of its participation, continue to support potential dispute cases, processing of reservation of funds, ensure the storage and availability of relevant data, and perform any outstanding fee settlement obligations, for at least the period necessary to comply with its obligations under Union law, in particular: (a) the rights of digital euro users and the corresponding scheme participant obligations under the Payment Services Regulation (PSR) relating to unauthorised or incorrectly executed payment transactions, including the time limits for notification and refund claims; and (b) applicable Union law requirements on record-keeping and data retention, including those laid down in the AML/CTF framework..

PAR.50 The scheme participant shall facilitate, in advance of the technical offboarding from the DESP, the switching of digital euro payment accounts of digital euro users to other scheme participants.

PAR.51 The withdrawal of a scheme participant's participation in the scheme, including the last day of the scheme participant's operations shall be publicly communicated by the SGA at least 30 calendar days before the day on which the withdrawal enters into effect, via updating the register of digital euro scheme participants.

3 Functional requirements

3.1 Section overview

This section defines the functional and operational model of the different services in scope of the digital euro scheme. The functional and operational model is intended to support the provision of digital euro services as described in the illustrative user journeys, available in Annex B1 - User Journeys and Minimum UX Requirements, on which basis the end-to-end (E2E) process flows pertaining to the digital euro have been designed. Summarised process flows are included in this section while detailed process flows are included in Annex B2 – E2E flows.

3.2 User journeys and minimum User experience (UX) requirements

User journeys illustrate how the various functions and features of the digital euro are utilised from a digital euro user perspective and user journeys provide an overview of specific user-related processes.

The user journeys are illustrative of the intended outcomes and are not directly binding for scheme participants.

Scheme participants may offer additional use cases not included in the illustrative user journeys, as long as these comply with the rulebook.

The illustrative user journeys are included in Annex B1 - User Journeys and Minimum UX Requirements . This annex reflects the progress at a specific point in time, so the number of use cases and user journeys may evolve over time.

The minimum user experience (UX) requirements are the set of requirements for user experience that scheme participants must comply with when developing and offering digital euro services.

Minimum UX requirements include both generic and specific UX requirements. Generic UX requirements are requirements that are applicable to all user journeys. Specific UX requirements are requirements that are organised by user journey and only apply to that specific user journey.

Minimum UX requirements are considered mandatory for scheme participants. Optional UX requirements are suggestions to further enhance the UX and are marked as [optional].

Minimum UX requirements apply to all scheme participants, and if other comparable digital means of payment exceed these requirements, scheme participants must ensure that the digital euro UX is at least equivalent to their respective proprietary solutions. This is known as the equivalence principle.

3.2.1 Generic UX requirements

3.2.1.1 Authentication

FUR.01 Scheme participants shall ensure that authentication methods for digital euro payment services are equivalent to those made available for other means of payment.

FUR.02 Scheme participants shall ensure that authentication can be completed in no more steps than required for other means of payment.

FUR.03 Scheme participants shall provide multi-modal authentication methods, including at least one option that does not require a smartphone unless the payment instrument is itself a smartphone.

FUR.04 Digital euro users shall have the option to enable or disable available authentication methods.

FUR.05 Participants shall ensure that at least one authentication method is enabled at all times.

FUR.06 Scheme participants shall ensure end-users are able to use their European Digital Identity Wallet to authenticate, if supported by the payment instrument.

FUR.07 Scheme participants shall offer end-users the option to retry authentication or select an alternative authentication method if the initial attempt fails.

FUR.08 Scheme participants shall provide a secure fallback authentication method when the primary authentication method is unavailable.

FUR.09 Scheme participants shall ensure that active user sessions are not terminated while the end-user is interacting with the frontend solution.

FUR.10 If authentication times out, scheme participants shall notify end-users and provide them with the opportunity to reauthenticate.

FUR.11 If authentication is about to time out, scheme participants shall notify end-users, and indicate the action required to maintain the session.

FUR.12 Scheme participants shall provide end-users with the choice to be redirected to their default digital-euro-supporting frontend solution when redirection is required.

FUR.13 Scheme participants shall require renewed authentication if the transaction amount or payee is changed.

FUR.14 Scheme participants shall require successful end-user authentication before displaying any personal data, including account balances, transaction history, or identifiers.

FUR.15 Scheme participants shall indicate to end-users that identity verification is required before accessing digital euro payment services.

FUR.16 When a session is resumed on a different device, scheme participants shall prompt the end-users to reauthenticate before granting access and inform the end-user that the previous session will be logged out automatically for security reasons.

FUR.17 Scheme participants shall display the result of the authentication process as successful or unsuccessful.

3.2.1.2 Accessibility

FUR.18 All front-end solutions and payment services offered shall comply with the requirements outlined in the European Accessibility Act.

3.2.1.3 Branding

FUR.19 All front-end solutions and payment services offered shall comply with the branding requirements outlined in Section 7 of the rulebook.

3.2.1.4 Controllability

FUR.20 Scheme participants shall provide functionality for end-users to select a default digital-euro-supporting frontend solution.

FUR.21 Scheme participants shall provide functionality allowing payers to cancel a transaction before authentication starts.

FUR.22 Scheme participants shall ensure that payers can return to the previous step at any time before authentication starts.

FUR.23 [Optional] Payers may be able to refuse incoming payment by blocking users based on their DEAN or alias.

FUR.24 Scheme participants shall ensure that end-users can log out of digital euro services at any time. Logging out shall terminate the active session and require reauthentication before further access.

FUR.25 Scheme participants shall ensure that each button or link in the frontend solution is labelled with a descriptive action name (e.g., “Confirm Payment”, “Cancel”) and leads to a screen or outcome that matches the label’s intent.

FUR.26 Digital euro users shall not be logged out while actively interacting with the front-end solution.

3.2.1.5 Error handling

FUR.27 Scheme participants shall, where the user interface allows it, inform end-users of the high-level functional reason for an error (e.g., “Insufficient funds”).

FUR.28 Scheme participants shall provide actionable guidance or inform end-users of the steps to resolve an error such as retrying an action, correcting input, or contacting support.

FUR.29 Scheme participants shall not expose internal system details or technical diagnostics to end-users.

FUR.30 Scheme participants shall use neutral, non-specific language for errors related to fraud, risk, or security.

FUR.31 Scheme participants shall use plain, everyday language and avoid technical jargon.

FUR.32 Scheme participants shall display critical errors prominently, ensuring they cannot be missed by end-users.

FUR.33 Scheme participants shall allow end-users to retry failed actions without re-entering all data, where technically feasible.

FUR.34 Scheme participants shall display error messages as soon as the issue is detected.

FUR.35 [Optional] Error messages may follow this structure: [What went wrong.] [Why it happened, if known.] [What End-Users can do next.]

FUR.36 [Optional] Scheme participants may use visual indicators (e.g., red text, icons) alongside text to help end-users quickly identify errors.

FUR.37 [Optional] Scheme participants may keep messages under 200 characters.

FUR.38 [Optional] Scheme participants may avoid including error codes unless required for end-user support.

FUR.39 [Optional] Scheme participants may use sentence case and proper punctuation.

FUR.40 [Optional] Scheme participants may acknowledge the inconvenience caused by the error and reassure end-users.

3.2.1.6 Feedback and information

FUR.41 Scheme participants shall inform end-users when they are being redirected to another frontend solution.

FUR.42 If field validation is performed, scheme participants shall ensure it occurs before allowing the end-user to proceed to the next screen.

FUR.43 Scheme participants shall specify which field has failed validation.

FUR.44 [Optional] Scheme participants may perform field validation immediately after end-users complete the corresponding field.

FUR.45 Scheme participants shall present all information required to complete the current step within the same screen, avoiding the need for end-users to recall details from previous steps.

FUR.46 Information provided by scheme participants shall be understandable and shall not exceed the B2 (upper intermediate) complexity level of the Council of Europe's Common European Framework of Reference for Languages.

FUR.47 [Optional] Scheme participants may display a progress indicator in multi-step flows to inform the end-user about the number of steps in the process (e.g. for onboarding).

FUR.48 Scheme participants shall provide tactile feedback when appropriate to reinforce end-user actions, such as during NFC interactions or other relevant use cases.

FUR.49 Scheme participants shall provide functionality enabling end-users to set a user-defined nickname for each account, which shall be displayed alongside the account or the offline device identifier to support user recognition.

FUR.50 Whenever an amount is displayed in the frontend solution, scheme participants shall display the corresponding currency.

3.2.1.7 Positioning

FUR.51 Digital euro services shall be accessible via the main page of the front-end solution equivalent to non-digital euro payment services.

3.2.1.8 Transactions

FUR.52 Scheme participants shall provide functionality enabling end-users to select a default mode for using either online or offline digital euro to initiate a payment.

FUR.53 Scheme participants shall display, before authentication of the transaction, whether the transaction is being conducted using online or offline digital euro and shall, if applicable, offer payers the option to switch.

FUR.54 [Optional] Scheme participants may provide end-users with access to a shortcut (e.g. via a button or link) for funding if a payment fails due to insufficient funds.

FUR.55 If a transaction is made using open funding, the transaction amount using open funding shall be displayed distinctively.

FUR.56 For transactions made using reverse waterfall, the transaction amount using reverse waterfall shall be made available for the payer.

FUR.57 For payments or (de)funding transactions, scheme participants shall display the origin account (where funds are withdrawn) before authentication starts.

FUR.58 Scheme participants shall inform end-users when a transaction would cause their balance to exceed the holding limit by displaying the limit and explaining the consequences (e.g., failed incoming payments, automated defunding).

3.2.1.9 User support

FUR.59 Scheme participants shall ensure that end-users can access accurate help and documentation in an easily accessible manner, equivalent to other means of payment.

FUR.60 Scheme participants shall provide customer support for digital euro services equivalent to that offered for other means of payment.

FUR.61 Scheme participants shall provide customer support in an inclusive and accessible manner, using different methods of communication (e.g., visual and auditory) to and offering it through more than one channel.

FUR.62 Scheme participants shall provide contextual help, such as tooltips or information icons, for concepts that are specific to the digital euro services.

3.2.2 Specific UX requirements

Specific UX requirements are organised by illustrative user journey (Annex B1) and only apply to that specific user journey. Annex B1 details, for a selection of user journeys, such specific UX requirements and accompanying wireframes. The wireframes are illustrative in nature and only serve to support the UX requirements.

Additional specific UX requirements, including for other user journeys, will be added in future iterations of the draft rulebook.

3.3 Identification of digital euro users

3.3.1 Unique Identifier

A unique identifier created by a payment service provider distributing the digital euro that unambiguously differentiates, for online digital euro purposes, digital euro users but that is not attributable to an identifiable

natural or legal person by the European Central Bank and the national central banks. This unique identifier facilitates PSP switching, the opening of new accounts and the management of holding limits.

FUR.63 When requesting to create a new digital euro payment account for an individual user, scheme participants shall provide a digital euro user unique identifier. The characteristics of this unique identifier are still being defined.

FUR.64 When requesting to create a new digital euro payment account for a business user, scheme participants shall provide a digital euro user unique identifier. The characteristics of this unique identifier are still being defined.

FUR.65 Upon successful provision of the unique identifier, the scheme participant shall assign a DEAN to the end user by either requesting one from the DESP or by assigning one already requested upfront via a bulk request (see Annex D2).

3.3.2 Digital Euro Account Number

A digital euro account number (DEAN) is the unique account number assigned to an end-user's digital euro payment account, enabling identification of the user's account, and facilitating transactions with individuals or businesses.

FUR.66 A DEAN shall be requested by a scheme participant from the DESP either upfront (in a bulk) or following an end-user request. The DESP generates the DEAN and then provides it to the requesting scheme participant. The scheme participant then assigns the DEAN provided by the DESP to the digital euro user that wishes to open a digital euro payment account.

FUR.67 The DEAN is independent of the requesting PSP and does not rely on country identification.

FUR.68 Since the DEAN is PSP agnostic, scheme participants can request the PSP ID associated to a DEAN via the alias look-up service (see Annex D2).

FUR.69 Digital euro account numbers (DEANs) are composed of 18 alphanumerical characters and respect a specific structure:

1. The first two characters are the Latin alphabetic characters 'E' and 'U'.

2. The third and fourth characters are two check digits generated using the ISO/IEC 7064, MOD 97-10 algorithm.
3. The fifth character is an indicator digit that provides specific information about the DEAN. Only the following values allowing to distinguish DEAN types are authorised for this indicator digit:
    1. “0” is attributed to DEANs used for individual users (personal or household capacity)
    2. “1”’ is attributed to DEANs used for business users (commercial or professional purposes)
4. The sixth to eighteenth characters form a 13-digit serial number.
5. The fifth to eighteenth characters (including the indicator digit and the serial number) are known as the Basic European Account Number (BEAN).

FUR.70 When using a physical card as a payment instrument, the DEAN shall be printed on the card to identify users.

3.3.3 Alias

The DEAN is the mandatory basic account identifier, yet it can be accompanied by alternative identification means – an alias. The alias could be used in the same way as the DEAN for identifying the account in the payment process if the alias is registered.

FUR.71 The provision of an alias by the user is voluntary. If a user chooses to use an alias, he/she will have to provide one to its PSP.

FUR.72 Scheme participants shall support the alias registration.

FUR.73 Individual users can use an alias, mapped to their corresponding DEAN, for identifying themselves and using digital euro services.

FUR.74 An alias shall only be a phone number that is linked to the individual digital euro user.

FUR.75 There is only a one-to-one relationship between the alias and DEAN.

FUR.76 Scheme participants shall perform an alias validation when registering an alias (e.g. sending a one-time password to the phone number provided by the user and the user needs to enter it in

the app or the internet banking application). Should the alias provided by the user already be registered and validated by the scheme participant for other purposes (e.g. contact purposes), alias validation is not required.

FUR.77 In case an individual user's phone number changes, then the user should be able within the set of access management features offered by his/her PSP, to request the change of the alias. His/her PSP should then take the request further to the DESP component as described in Annex8 D2 – following the alias validation as outlined above.

FUR.78 Business users are not able to use an alias as an identification method.

3.4 Authentication of digital euro users

3.4.1 Users onboarded on the digital euro app

FUR.79 Scheme participants shall implement and make available seamless authentication for online digital euro transactions and online access to digital euro payment accounts, as further specified in Annex D1. Front-end implementation specifications. Seamless authentication relies on public key cryptography and the use of biometrics or alternatively a PIN to allow the authentication to take place within the digital euro app in which the user action is initiated without any redirection to another app.

FUR.80 Scheme participants shall enrol users into the seamless authentication solution when the user onboards on the digital euro app. It is expected that seamless authentication will be the default way to authenticate users that are onboarded on the digital euro app, with redirection offered as a fallback solution if seamless authentication is temporarily unavailable.

FUR.81 For e-commerce transactions, decoupled authentication - using biometrics or a PIN via a notification in the user's digital euro app or PSP app - is the preferred authentication method.

3.4.2 Users relying on PSPs' digital interfaces

FUR.82 Scheme participants are free to implement their preferred strong customer authentication (SCA) method when users rely on their digital interfaces. The authentication method shall comply with all applicable regulatory frameworks and associated security requirements.

FUR.83 cheme participants must abide by the minimum user experience standards set in Section 3.2 Illustrative user journeys and minimum User experience (UX) requirements and Annex B1 - User Journeys and Minimum UX Requirements.

3.4.3 Authentication for offline digital euro

FUR.84 Authentication for offline payment transactions (Person-to-person (P2P), POS) relies on the device's local authentication mechanisms for both the digital euro app and PSP app. For offline digital euro operations that require internet connectivity, such as (de)funding and device deactivation, the same authentication approach used for online digital euro transactions is applied (refer to Sections 3.4.1 and 3.4.2).

3.4.4 Inclusive authentication

FUR.85 Without prejudice to the accessibility requirements of the European Accessibility Act and as per the requirements of the future Payment Services Regulation, scheme participants shall ensure that all their customers, including persons with disabilities, older persons, persons with low digital skills and persons who do not have access to digital channels or digital payment instruments, have at their disposal at least a means of authentication adapted to their specific situation.

3.4.5 Authentication in “open PSP”

FUR.86 The distributing PSP shall enable one single authentication of the user in situations where the user is using a different PSP for the funding of the digital euro payment account – a situation referred to as “open PSP situation”.

3.5 Digital euro services - steps and requirements

This section describes the digital euro focus areas:

- **Access management – registration and management of digital euro users**: describes the processes for onboarding, offboarding, lifecycle management and switching for digital euro users (see Section 3.5.2).
- **Liquidity management – distribution of digital euro**: details funding/defunding of the user’s digital euro payment account from and to a non-digital euro payment account and describes the digital euro user’s holding limit. Funding/defunding shall be possible both manually or automatically at a pre-defined moment in time or at the breach of a threshold, other than the holding limit, defined

by the user (including reverse waterfall and waterfall triggered at the breach of the holding limit). Funding/defunding shall also be possible from and to cash manually via ATM or scheme participant's branch according to its respective service hours, if provided by the scheme participant,as part of its non-digital euro payment services (see Section 3.5.3).

- **Transaction management – processing of digital euro transactions**: describes the services that enable users to make transactions in digital euro (through a one-off or recurring payment, standing order or a pre-authorisation service). It comprises activities including authentication, transaction initiation and payment confirmation/rejection, as well as refund processes (see Section 3.5.4).

Figure 3-1 shows an overview of the described focus areas, listing digital euro user services.

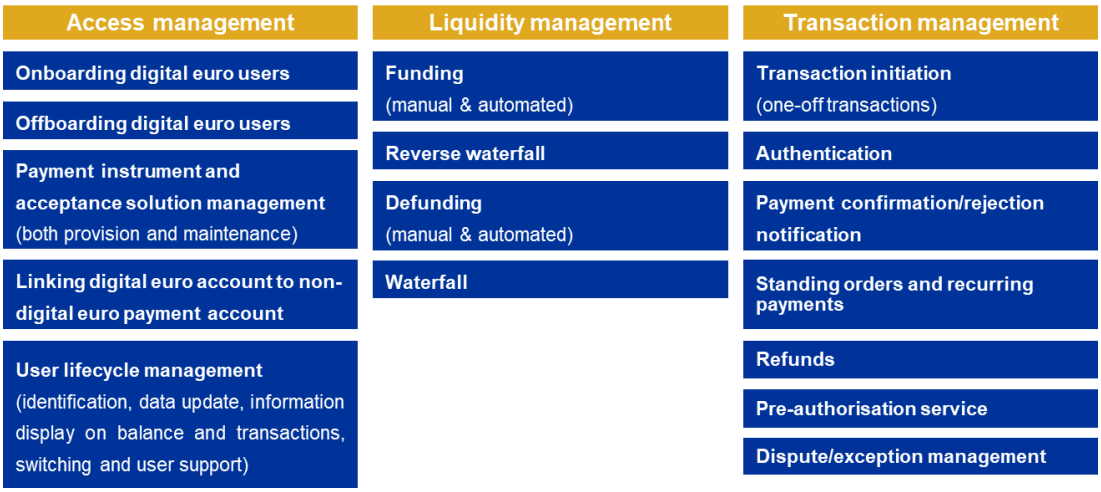

Figure 3-1 - Overview of digital euro services

3.5.1 Functional requirements specific naming conventions

This section describes the naming conventions used.

The descriptions are based on the concepts of process and process-step:

- A **process** refers to an end-to-end completion of the major business functions/a major business function carried out by (one of) the different parties involved.
- A **process-step** is defined as the realisation of each step of one process executed by the parties involved in that step.

3.5.2 Access management

3.5.2.1 Onboarding

FUR.87 Scheme participants are responsible for the onboarding of digital euro users.

FUR.88 Scheme participants shall comply with the applicable business rules and end-to-end process flows for the onboarding of a user as defined in this subsection.

High-level overview

Onboarding can take place online within a scheme participant's remote environment, or through the digital euro app offered by the Eurosystem, or in person during the scheme participant's service hours, if such onsite services are provided by the scheme participant as part of its non-digital euro payment services[13]. Onboarding consists of activities that provide a digital euro user access and ability to use the digital euro online and offline, including the allocation of digital ero account number(s) (DEAN(s)) and the user's payment instrument(s) or acceptance solution(s).

Individual digital euro users can ask for a (voluntary) registration of an alias to receive online payments, in addition to being addressable via a DEAN.

A high-level flow for the onboarding of a user is shown in Figure 3-2.

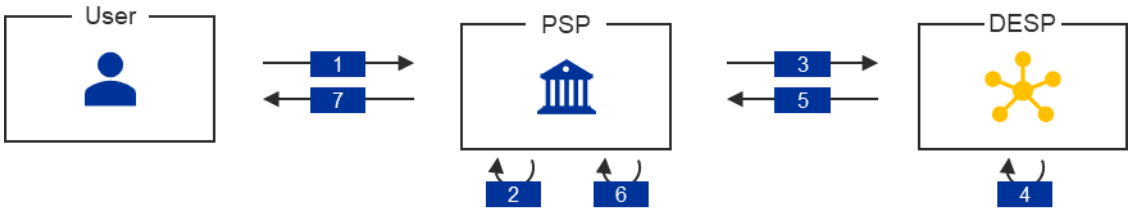

Figure 3-2 - High-level flow for the onboarding of a digital euro user

Description of steps:

1. The user requests its PSP to provide access to digital euro services
2. The PSP onboards (only if the user is yet unknown) and/or authenticates the user (if already known) according to its processes and applicable regulations

[13] Offering these two options is crucial to promote financial inclusion. Indeed, a full remote onboarding could strengthen the accessibility of the digital euro to people facing geographical and social barriers while an onboarding with live human interaction could benefit those people less confident with digitalisation including the elderly.

3. The PSP requests the DESP to generate a DEAN mapped to the PSP
4. The DESP generates a DEAN and maps it to the PSP The DESP returns the generated DEAN and confirms to the PSP the updated mapping
5. The PSP receives and links the DEAN to the digital euro user, activates the user's payment instrument(s) or acceptance solution(s) and sets up liquidity management and notification preferences (if requested by the user)
6. The PSP informs the user about successful onboarding and shares the DEAN associated with the digital euro payment account

A detailed description of the end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules - Onboarding	
Individual user business rules:	
AM-011-001	An individual user can have only one digital euro payment account.
AM-011-002	An individual user can have only one offline digital euro device.
AM-011-003	Upon receipt of an onboarding request from an individual user, the PSP shall check whether the user already holds a digital euro payment account.
AM-011-004	If an individual user already holds a digital euro payment account, the PSP should offer the user to switch the existing account instead (see Section 0).
AM-011-005	When opening a new digital euro payment account upon the individual user's onboarding request, the PSP must request a DEAN and registration of the user in the DESP, including the mapping to itself as the corresponding PSP and including a potential alias.
AM-011-006	The PSP must share the DEAN and technical proof with the individual user when onboarding is completed successfully.
AM-011-007	The PSP must comply with the provisions in Section 5 when providing an individual user with a digital euro payment instrument(s) (either during onboarding or afterwards).
Business user business rules:	
AM-012-001	A business user can have an unlimited number of digital euro payment accounts either with the same PSP or with multiple PSPs that are scheme participants.
AM-012-002	A business user can have an unlimited number of offline digital euro devices.
AM-012-003	When opening a new account upon an onboarding request from a business user, the PSP must request a DEAN and registration of the user in the DESP, including the mapping to itself as the corresponding PSP.
AM-012-004	The PSP must share the DEAN(s) and the technical proof(s) with the business user when onboarding is completed successfully.
AM-012-005	The PSP must comply with the provisions in Section 5 when providing a business user with (a) digital euro acceptance solution(s) (either during onboarding or afterwards).

End-to-end flows – Onboarding	
AM-1.1	Onboarding of an individual user part I (online)
AM-1.2	Onboarding of a business user (online and offline)
AM-1.3	Digital euro app configuration and onboarding of an individual user
AM-1.4	Bulk DEAN request

Table 3-1 - Applicable business rules and end-to-end flows Onboarding

3.5.2.2 Switching

FUR.89 Scheme participants are responsible for the switching function enabling individual users to seamlessly transfer their digital euro payment account, digital euro holdings as well as all basic digital euro payment services and where applicable value added services (see Annexes I and II of draft regulation [1]), depending on if the new PSP already offers these additional services, functionalities) while maintaining the same DEAN.

FUR.90 Scheme participants shall ensure a seamless transition of digital euro payment accounts when requested by users. They shall provide clear guidance and support, including comprehensive instructions for initiating the switch. Additionally, they shall offer multiple channels for users to initiate the switching service, such as online platforms, PSP and Digital Euro apps, and in-person customer service (depending on the current PSP channel offering).

FUR.91 Upon receiving a switching request, the new PSP shall gather the necessary data and conduct a due diligence procedure to verify the user's identity and account status. These verification procedures should align with the new PSP's existing regulatory processes to ensure compliance with all relevant regulations.

FUR.92 Individual users shall not be charged fees for switching - including transferring transaction history, standing orders links to non-digital euro payment accounts and recurring payments. A remediation period of at least 90 days shall be granted to resolve any issues arising from the switch.

FUR.93 Scheme participants shall comply with the business rules and end-to-end process flows for the switching of digital euro users as defined in this subsection.

Emergency account switching

As outlined in the draft legislation [1], in cases of prolonged service disruption or data loss by a PSP, the Eurosystem may declare an emergency situation along the rules set by the legal framework, allowing users to switch their account to a new PSP without requiring support from the previous PSP. This ensures that individual users maintain access to their online digital euro holdings.

FUR.94 Scheme participants shall have internal procedures and processes in place to facilitate emergency switching, utilising the technical proof provided by users. The technical proof is generated during onboarding (see Section 3.5.2.1).

FUR.95 In the event of an emergency situation activated by the Eurosystem, scheme participants acting as new PSPs, after conducting due diligence and verification procedures similar to those for standard account switching, shall be able to grant individual users access to their digital euro holdings using the technical proof. In such cases, data from the previous PSP, such as transaction history, linked non-digital euro payment accounts and waterfall/reverse waterfall cannot be recovered. Therefore, the new PSPs should clearly communicate this limitation to the user, confirm the completion of the process, provide the new technical proof and provide any necessary follow-up information.

<u>High-level switching overview</u>

Scheme participants shall enable individual digital euro users to switch their digital euro payment accounts to another scheme participant upon request while maintaining the same account identifiers. After the new PSP accepts a switching request from an individual user (e.g. after conducting due diligence procedure), it initiates all required procedures and processes to provide access to digital euro online holdings and can, upon individual user consent, obtain additional individual user's data from the previous PSP (e.g., transaction history, recurring payments and standing orders). The individual user also receives an updated PSP identifier and technical proof that is needed for emergency situations in which the current account-providing scheme participant would be unable to support digital euro services for a prolonged time.

In emergency situations, the emergency switching function will ensure an individual user's undisputed accessibility to their digital euro holdings. Such a procedure will allow digital euro users to switch to another scheme participant even without the support of the previous scheme participant. Therefore, in case of a failure of the scheme participant and complete loss of its data used to access and manage digital euro holdings, a user will be provided with an emergency switching to another scheme participant. Upon the Eurosystem's declaration of an emergency case for a specific PSP, the new PSP will be able to access the

user's digital euro holdings via the technical proof the individual user received during onboarding to the digital euro (or during successful switching cases thereafter). The main difference to the standard switching scenario is that the individual user's data from the previous PSP (e.g. transaction history) cannot be restored from previous PSP's data in the emergency case.

Account switching does not cover the switching of individual users' offline digital euro holdings. Since offline digital euro holdings are locally stored on the offline device, prior to deactivating the offline device – required for switching - any offline digital euro holdings can be defunded to either online digital euro holdings, non-digital euro payment account holdings or cash, or can be transferred to another offline device.

A detailed description of the related end-to-end flows is included in Annex B2.

Technical aspects related to the transfer of recurring payments and standing orders from one scheme participant to another are still under investigations and will be developed in the next iteration of this section.

Applicable business rules and end-to-end flows

Business rules – Switching	
Individual user business rules:	
AM-031-001	An individual user may request the switching (while maintaining the same DEAN) across PSPs at any time. Such a request can only be refused by the current (previous) PSP for the following reasons: • Some or all of the user's digital euro holdings are reserved by pre-authorisation(s) (see Section **Error! Reference source not found.**) • There is a (pre-)dispute(s) related to a transaction(s) from or to the account that has (have) not been resolved yet • The user's digital euro payment account is blocked by the PSP for, e.g. compliance or fraud reasons
AM-031-002	Both the previous and the new PSP must enable the individual user to transfer the user's transaction history of (at least) 13 months in the past and/or the user's recurring payments and standing orders when switching.
AM-031-003	If the individual user chooses to switch without transferring the transaction history, the previous PSP must allow the user to retrieve the transaction history for (at least) 13 months after the switching.
AM-031-004	If the individual user chooses to move the transaction history and/or the recurring payments and standing orders, the previous PSP sends to the new PSP: • The transaction history that the new PSP must make available to the user, and/or • The recurring payment and standing order parameters that the new PSP must use, in accordance with Section **Error! Reference source not found.**, after o btaining one single explicit consent to seamlessly continue all such arrangements without requiring the user to re-authorise each payment individually**Error! Reference source not found.**

AM-031-005	The previous and new PSP must authenticate the individual user and obtain approval for the switching request, including for moving the transaction history and/or the recurring payments and standing orders, before executing it. The previous and new PSP shall require a single, comprehensive consent from the user for the switching, rather than separate consent for each operation.
AM-031-006	After accepting the switching request, the previous PSP must refrain from processing any further payment, funding or defunding requests involving the digital euro payment account that is to be switched.
AM-031-008	After accepting the switching request, the new PSP is responsible for initiating all necessary procedures and processes to grant the user access to their online digital euro holdings.
AM-031-009	The new PSP shall confirm the switching and must share the new technical proof with the individual user when switching is completed successfully.
AM-031-007	Offline digital euro devices and holdings cannot be automatically transferred from previous to new PSP as part of switching. Any digital euro offline device must be deactivated prior to switching.
Business user business rules:	
AM-032-001	A business user cannot switch their digital euro payment account(s) nor their offline devices and holdings.
End-to-end flows – Switching	
AM-2.1	Individual user account switching (standard procedure)
AM-2.2	Individual user account switching (emergency procedure)

3.5.2.3 Lifecycle management

FUR.96 Scheme participants are responsible for the lifecycle management of digital euro users and for enabling a user to interact with the digital euro environment.

FUR.97 Scheme participants shall comply with the business rules and end-to-end process flows for the lifecycle management of a digital euro user as defined in this subsection.

<u>High-level lifecycle management overview</u>

Managing the lifecycle of digital euro users and enabling users to interact with the digital euro environment includes the following options:

- Manage digital euro payment account(s)
- View, register or edit profile settings such as alias(-es)

- Enable/disable different types of notifications
- View and add/remove linked non-digital euro payment accounts used for funding/defunding/waterfall/reverse waterfall
- View and edit different types of automated funding/defunding
- Checking digital euro balance and transaction history
- Block and unblock digital euro payment instrument(s) or acceptance solution(s)

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules - Managing digital euro payment account(s)	
Individual user business rules:	
AM-021-001	The PSP must give individual users the possibility to block and unblock their digital euro payment account. Individual users can only unblock their account if they have blocked it themselves (i.e. if it was not blocked by the PSP for, e.g. compliance or fraud reasons). Blocking of the user's digital euro payment account shall not prevent the settlement of reservation(s) on the user's account (see Section 3.5.4.5), unless the blocking was imposed by the PSP for, e.g. compliance or fraud reasons.
Business user business rules:	
AM-022-001	The PSP must allow business users to open new digital euro payment account(s) (see Section 3.5.2.1) or close existing digital euro payment account(s).
AM-022-002	If the digital euro payment account to be closed happens to be the last digital euro payment account of that business user with the PSP, the PSP must initiate the offboarding of the digital euro business user (see Section 3.5.2.4).
AM-022-003	The PSP must ensure that a digital euro payment account of a business user is maintained for the period of (to be defined) after closure for refunds and claims.
Business rules - Viewing, registering or editing profile settings such as alias(-es)	
Individual user business rules:	
AM-021-002	The PSP is only allowed to register an alias for an individual user to whom it provides digital euro services.
AM-021-003	The PSP is only allowed to register an alias for an individual user.
AM-021-004	The PSP must give individual users the possibility to register, change or disable an alias. Users can choose not to register an alias.
AM-021-005	Registration of an alias, changes to an alias registration and disablement of an alias are executed at the request of the individual user.
AM-021-006	Only one alias can be registered per digital euro payment account.

AM-021-007	The PSP must verify that the alias provided is available to the individual user.
AM-021-008	The PSP must manage its individual user's alias by promptly updating, amending and deactivating them as soon as a change is required by the user.
AM-021-009	The PSP is responsible for the correctness of the association between the alias and the individual user's DEAN.
AM-021-010	The PSP is not permitted to use the registered alias received as part of a digital euro payment instruction/request for any other purpose than the initiation of a digital euro payment transaction, unless the user has explicitly requested and/or agreed for other purposes.
Business rules - Enabling/disabling different types of notifications	
Individual user business rules:	
AM-021-011	The PSP must allow individual users to specify for which events they wish to receive notifications. At least the following notifications shall be offered: • A credit to their digital euro payment account • A debit to their digital euro payment account • Execution of a waterfall transaction • Execution of a reverse waterfall transaction • Execution of any other automated funding transaction • Execution of any other automated defunding transaction • Rejections/unsuccessful digital euro transactions • Rejections/unsuccessful funding/defunding transactions • Rejections/unsuccessful waterfall/reverse waterfall transactions
AM-021-012	The PSP must allow individual users to select the means of notification.
AM-021-013	The PSP must allow individual users to modify their notification settings at any point in time.
Business user business rules:	
AM-022-004	The PSP must allow business users to specify for which events they wish to receive notifications. At least the following notifications shall be offered: • A credit to their digital euro payment account • A debit to their digital euro payment account • Execution of a waterfall transaction • Execution of a reverse waterfall transaction • Execution of an offline funding transaction • Execution of an offline defunding transaction • Rejections/unsuccessful digital euro transactions • Rejections/unsuccessful funding/defunding transactions • Rejections/unsuccessful waterfall/reverse waterfall transactions • Aggregated notifications for specific event types
AM-022-005	The PSP must allow business users to select the means of notification.
AM-022-006	The PSP must allow business users to modify their notification settings at any point in time.
Business rules - Viewing and adding/removing linked non-digital euro payment account(s)	

General business rules:	
AM-020-001	The non-digital euro payment account to be linked to a digital euro payment account can be any payment account at either the same PSP which services the user's digital euro payment account or at another PSP that is a scheme participant.
Individual user business rules:	
AM-021-014	The PSP must allow individual users to link a non-digital euro payment account to their digital euro payment account for funding and defunding purposes including waterfall and reverse waterfall transactions (see Section 3.5.3), either during onboarding or at any later point in time. If an account is linked, this non-digital euro payment account shall be presented by the PSP as the default source account for manual and/or automated funding.
AM-021-015	The PSP must allow individual users to change or remove the link to a non-digital euro payment account at any point in time. If the user chooses to remove the linked non-digital euro payment account, all automated liquidity management options (including waterfall and reversed waterfall) must be disabled as well.
Business user business rules:	
AM-022-007	The PSP must ensure that a business user links a non-digital euro payment account(s) to their digital euro payment account(s) and must allow to change the link to (a) non-digital euro payment account(s), while ensuring that a business user's digital euro payment account has a non-digital euro payment account linked to it at all times.
Business rules - Viewing and editing different types of limits and thresholds	
Individual user business rules:	
AM-021-016	The PSP must allow an individual user to set up, change and terminate different types of automated funding and defunding, including to schedule regularly recurring funding/defunding operations as well as minimum/maximum thresholds (see Sections 3.5.3.1 and 0).
Business rules - Checking digital euro balance and transaction history	
General business rules:	
AM-020-002	For online digital euro holdings, the PSP must inform the user of the current online digital euro balance and transaction history at the user's request.
Business rules - Blocking and unblocking digital euro payment instrument(s) or acceptance solution(s)	
General business rules:	
AM-020-003	When an offline digital euro device connects online, the PSP must check whether the offline digital euro device has been reported lost or stolen and if so, the status of the offline digital euro device shall be set as disabled.
Individual user business rules:	
AM-021-017	The PSP must give individual users the possibility to block, unblock, add or remove their payment instrument(s) (e.g. card, PSP app / digital euro app, offline digital euro device). Individual users can only unblock their payment instrument(s) if it was blocked

	on their behalf (i.e. if it was not blocked by the PSP for, e.g. compliance or fraud reasons).
AM-021-018	The PSP must verify that the individual user reporting a stolen or lost payment instrument is indeed the authorised user of the payment instrument.
AM-021-019	The PSP must ensure that a disabled payment instrument is not allowed to initiate or receive transactions, to fund or defund or to query transactions.
AM-021-020	The PSP must change the status of the payment instrument from disabled to enabled when it is reported found or recovered by the authorised individual user.
Business user business rules:	
AM-022-008	The PSP must give business users the possibility to block, unblock, add or remove their acceptance solution(s) (e.g. POS terminal, offline device). Business users can only unblock their acceptance solution(s) if blocked on their behalf (i.e. if not blocked by the PSP for, e.g. compliance or fraud reasons).
AM-022-009	The PSP must verify that the business user reporting a stolen or lost acceptance solution is indeed the authorised user of the acceptance solution.
AM-022-010	The PSP must ensure that a disabled acceptance solution is not allowed (to initiate refunds or) receive transactions.
AM-022-011	The PSP must change the status of the acceptance solution from disabled to enabled when it is reported found or recovered by the authorised business user.
End-to-end flows – Lifecycle management	
AM-4.1.1	End user (individual) amendments - account linkage
AM-4.1.2	End user (individual) amendments - liquidity management settings
AM-4.1.3	End user (individual) amendments - online notifications management
AM-4.1.4	End user (individual) amendments (offline notification preferences)
AM-4.1.5	End user (individual) amendments (un-blocking digital euro account payment instrument(s))
AM-4.1.6	End user (individual) amendments -un-blocking digital euro account
AM-4.1.7	End user (individual) amendments (de-activate payment instrument(s))
AM-4.1.8	End user (individual) amendments - (user data)
AM-4.1.9	End user (individual) amendments (alias registration)
AM-4.2.1	End user (business) amendments - account linkage
AM-4.2.2	End user (business) amendments (user registration)
AM-4.2.3	End user (business) amendments (notification preferences)
AM-4.2.4	End user (business) amendments (close account)
AM-4.2.5	End user (business) amendments (un-blocking digital euro account)
AM-4.2.6	End user (business) amendments (acceptance solution management)
AM-4.2.7	End user (business) amendments -user data
AM-4.2.8	End user (business) amendments (new account)

3.5.2.4 Offboarding

FUR.98 As scheme participants, PSPs are responsible for the offboarding of digital euro users.

FUR.99 Scheme participants shall comply with the business rules and end-to-end process flows for the offboarding of a digital euro user as defined in this subsection.

High-level offboarding overview

The offboarding is a procedure initiated when a digital euro user chooses to close their digital euro payment account. The PSP shall be able to return the funds associated with a DEAN or an offline digital euro device to the offboarding user (online and offline defunding), deactivate recurring payments and standing orders (if activated), resolve pending disputes, close all open transactions and disable access to payment instruments or acceptance solutions.

A high-level flow for the offboarding of a user is shown in Figure 3-3.

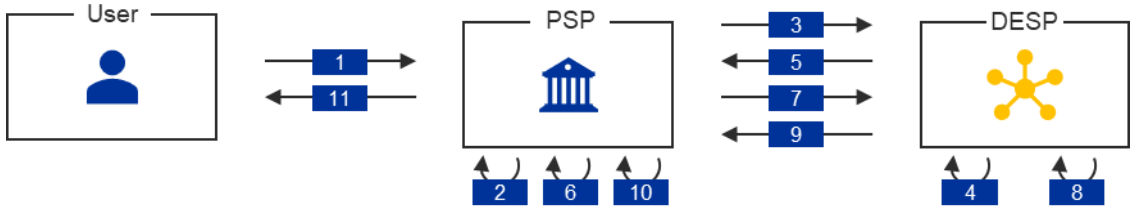

Figure 3-3 – High-level flow for the offboarding of a digital euro user

Description of steps:

1. The user requests the PSP to be offboarded from digital euro services
2. The PSP authenticates the user, locks the digital euro payment account and payment instrument(s) or acceptance solution(s)
3. If the user's digital euro payment account has a positive balance (online and/or offline), the PSP sends a defunding instruction to DESP to defund the digital euro holdings (for online the defunding is triggered by the PSP, while for offline defunding is triggered by the user)
4. The DESP validates and defunds the user's digital euro payment account
5. The DESP confirms the defunding to the PSP
6. The PSP credits the non-digital euro payment account or provides cash (according to the user's preferences)

7. The PSP requests the DESP to close the user's' digital euro payment account and deactivates the user registration
8. The DESP deactivates the user registration and closes the user's digital euro payment account
9. The DESP confirms the deactivation of the user registration and the closing of the user's digital euro payment account to the PSP
10. The PSP disables the digital euro services and payment instrument(s) or acceptance solution(s) for the offboarded user
11. The PSP informs the user about successful offboarding

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules - Offboarding	
General business rules:	
AM-040-001	Users can request their PSPs to be offboarded from digital euro services at any point in time. A PSP can only reject such a request for any of the following reasons: • Some or all of the user's digital euro holdings are reserved by pre-authorisation(s) (see Section **Error! Reference source not found.**) • There is a (pre-)dispute(s) related to a transaction(s) from or to the account that has (have) not been resolved yet • The user's digital euro payment account(s) is (are) blocked by the PSP for, e.g. compliance or fraud reasons
AM-040-002	Upon offboarding of a digital euro user, the PSP shall generate and provide the user with a final account statement.
Individual user business rules:	
AM-041-001	The PSP accepting the offboarding of an individual user must ensure that the user can neither receive nor send any further digital euro payments and that the individual user's online and/or offline digital euro holdings are defunded and offline device is deactivated prior to the completion of the offboarding.
Business user business rules:	
AM-042-001	The PSP accepting the offboarding of a business user must ensure that the user can neither receive nor send any further digital euro payment (refund)s and that the offline device(s) is (are) deactivated prior to the completion of the offboarding.
AM-042-002	The PSP accepting the offboarding of a business user must ensure that a digital euro payment account of a business user is maintained for the period of (to be defined) after the closure for refunds and claims.

End-to-end flows - Offboarding	
AM-3.1	Offboarding of an individual user (online and offline)
AM-3.2	Offboarding of a business user (online and offline)

3.5.3 Liquidity management

Scheme participants shall support liquidity management of digital euro users within the digital euro holding limit (see Section 3.5.3.5), supporting the full range of methods for users to fund (see Section 3.5.3.1) and/or defund (see Section 3.5.3.2) their digital euro holdings.

To maximise payment convenience, an individual user may choose to link an online digital euro payment account to a non-digital euro payment account to pay with digital euro even though available digital euro holdings do not suffice (see Section 3.5.3.3) or receive a digital euro payment that would exceed the holding limit and defund the amount in excess (see Section 3.5.3.4). In these cases, the user has the option to set up reverse waterfall and waterfall functionalities, which require linking an existing non-digital euro payment account with the online digital euro payment account.

Neither a non-digital euro payment account nor a link between such an account and an online digital euro payment account are prerequisites for individual users to receive access to digital euro services. A business user shall always link the digital euro payment account(s) to a non-digital euro payment account, enabling (at least) the waterfall function necessary to enforce the business user`s holding limit.

A high-level flow for a funding and defunding operation is shown in Figure 3-4.

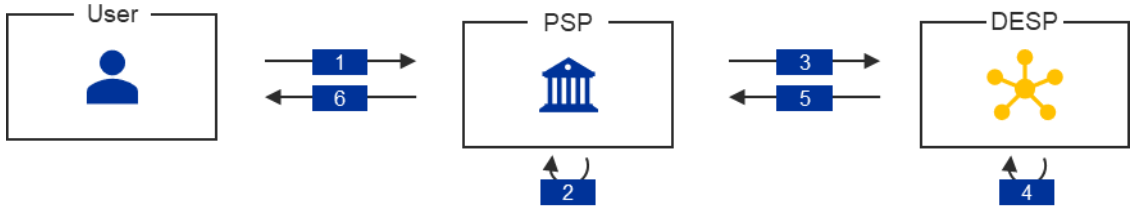

Figure 3-4 High-level flow for a manual (de)funding operation[14]

Description of steps:

1. The user initiates (de)funding of the digital euro payment account

[14] A (de)funding operation might involve a different PSP in case the PSP providing the digital euro payment account and the PSP providing the non-digital euro payment account are not the same.

2. The PSP assures the user is authenticated and that sufficient funds are available for (de)funding
3. The PSP sends the (de)funding instruction to the DESP
4. The DESP validates and (de)funds the user's digital euro payment account
5. The DESP confirms completion of the (de)funding operation to the PSP
6. The PSP confirms the (de)funding of the digital euro payment account to the user

3.5.3.1 Funding

FUR.100 Scheme participants shall support the full range of funding functionalities for users to fund their digital euro holdings.

FUR.101 Scheme participants shall comply with the applicable business rules and end-to-end process flows for funding as defined in this subsection.

High-level overview

The funding functionalities allow digital euro users to fund their online and offline digital euro holdings. Funding of the online digital euro holdings can be done from a non-digital euro payment account held at the scheme participant of the users choice, from the offline digital euro holdings or from cash. Funding of the offline digital euro holdings can be done, beside the previously mentioned possibilities, also from an online digital euro holding. Funding functionalities from non-digital euro payment accounts shall be available in line with the availability requirement as defined in Section 4.3.1. Funding from cash via ATM or PSP's branch(es) of scheme participants shall be supported according to their respective service hours if provided by a scheme participant as part of its non-digital euro payment services.

Scheme participants may offer manual and automated funding functionalities as per the following combinations:

Online digital euro funding

- Online digital euro manual funding from a non-digital euro payment account or cash
- Online digital euro manual funding from offline holdings
- Online digital euro automated funding from a non-digital euro payment account

Offline digital euro funding

- Offline digital euro manual funding from a non-digital euro payment account or cash
- Offline digital euro manual funding from online digital euro holdings
- Offline digital euro automated funding from a non-digital euro payment account or online digital euro holdings

Manual funding from a non-digital euro payment account can be triggered by the user from any non-digital euro payment account at either the same scheme participant which services the user's digital euro payment account or at another PSP that is a scheme participant. Manual funding from cash requires an existing relationship with the scheme participant if provided by the participant as part of its non-digital euro payment services. In the case of funding by cash, users would either access an ATM or go to a branch of their PSP and hand the cash to an employee (or be assisted in the use of the ATM).

Automated funding functionality for offline digital euro can be activated by the user as for the online digital euro functionality. The source of funds can also be the user's online digital euro payment account. An individual user has the options to schedule regularly recurring funding operations with a set amount and frequency and/or to set a minimum threshold (within the holding limit), which is automatically maintained by funding the missing amount if the set threshold is breached after a debit transaction[15].

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules – Funding	
General business rules:	
LM-020-001	The PSP shall ensure that the manual and automated funding functionalities from a non-digital euro payment account are available to digital euro users in line with the availability requirement as defined in Section 4.3.1. Without prejudice to compliance with holding limits, the manual and automated funding shall be executed immediately. The non-digital euro payment account can be any non-digital euro payment account at either the same PSP which services the user's digital euro payment account or at another PSP that is a scheme participant.
LM-020-002	In the case of funding by cash, users would either access an ATM or go to a branch of their PSP and hand the cash to an employee (or be assisted in the use of the ATM) ccording to their respective service hours if provided by the PSP..
Individual user business rules:	

[15] The check of whether automated funding needs to be initiated is performed either by the PSP for online automated funding or by the PSP app or digital euro app for offline automated funding whenever the offline device comes online.

LM-021-001	The PSP must offer individual users the possibility to fund its offline digital euro device from online digital holdings. This requires the PSP to request defunding first (see Section 0), followed by a funding request (see Section 3.5.3.1).
LM-021-002	The PSP must allow individual users to set up, change and terminate automated funding. The user must be allowed to specify: • The starting date, funding frequency, and funding amount, and/or • The funding account, and/or • The minimum threshold (within the holding limit), which is to be automatically maintained by the PSP by funding the missing amount if the set minimum threshold is breached after a debit transaction
LM-021-003	If the individual user has set up automated funding and the funding amount is not available on either the non-digital euro payment account (for online and offline funding) or the online digital euro holdings (for offline funding only), the funding process must be aborted, and the PSP must inform the user.
LM-021-004	Automated funding can only be applied if the non-digital euro payment account holds sufficient balance, within the financial agreement specified between the user and the PSP providing the non-digital euro payment account.
LM-021-005	If the individual user has linked a non-digital euro payment account to the digital euro payment account, this linked non-digital euro payment account should be presented by the PSP as the default source account for manual and/or automated funding. However, the user should be offered the possibility to specify another non-digital euro payment account instead of the linked non-digital euro payment account, provided that the user is able to prove he/she is the owner of the alternative non-digital euro payment account.
LM-021-006	After having made any debit to the individual user's digital euro payment account (see Section 3.5.4), the PSP must check if the available balance on the online digital euro payment account has dropped below the minimum threshold specified by the individual user for automated funding (if applicable). If it has, the PSP must initiate the funding of the account as per the individual user's liquidity management settings.

End-to-end flows – Funding	
Online end-to-end flows:	
LM-1.1	Online manual funding from non-digital euro payment account – same PSP
LM-1.2	Online manual funding from non-digital euro payment account – different PSPs
LM-1.3	Online scheduled/automated funding from non-digital euro payment account same PSP
LM-1.4	Online scheduled/automated funding from non-digital euro payment account – different PSPs
LM-1.5	Online manual funding from cash at ATM with QR code
LM-1.6	Online manual funding with cash deposit at ATM through card (contact and contactless) or smartphone
LM-1.7	Online manual funding from cash at PSP branch
Offline end-to-end flows:	
LM-1.8	Offline digital euro manual funding from non-digital euro payment account via app – same PSP
LM-1.9	Offline digital euro manual funding from online digital euro account via app – same PSP
LM-1.10	Offline digital euro manual funding of offline card from online digital euro account via app & NFC device

LM-1.11	Offline digital euro manual funding from cash at ATM with card (contact and contactless) or smartphone
LM-1.12	Offline scheduled/automated funding from non-digital euro payment account via app – same PSP
LM-1.13	Offline scheduled/automated funding from online digital euro account via app

3.5.3.2 Defunding

FUR.102 Scheme participants shall support the full range of methods for users to defund their digital euro holdings.

FUR.103 Scheme participants shall comply with the applicable business rules and end-to-end process flows for defunding as defined in this subsection.

High-level overview

The defunding functionalities allow digital euro users to defund their online and offline digital euro holdings. Defunding of the online digital euro holdings can be done to a non-digital euro payment account at the scheme participant of the user's choice or to cash. Defunding of the offline digital euro holdings can be done, besides the previously mentioned possibilities, also to online digital euro holdings. Defunding functionalities to a non-digital euro payment account shall be available in line with the availability requirement as defined in Section 4.3.1. Defunding to cash at ATM or PSP branch can be used according to the respective service hours, if provided by the scheme participant.

PSPs may offer manual and automated defunding functionalities as per the following combinations:

Online digital euro defunding:

- Online digital euro manual defunding to a non-digital euro payment account or cash (also including Payment with Cash Back (PwCB) at the POS)
- Online digital euro manual defunding to offline digital euro holding
- Online digital euro automated defunding to a non-digital euro payment account

Offline digital euro defunding:

- Offline digital euro manual defunding to a non-digital euro payment account or cash
- Offline digital euro manual defunding to online digital euro holdings

- Offline digital euro automated defunding to a non-digital euro payment account or the online digital euro holdings

Manual defunding to a non-digital euro payment account can be triggered by the user to any non-digital euro payment account at either the same PSP which services the user's digital euro payment account or at another PSP that is a scheme participant. In the case of defunding to cash, users would either access an ATM and withdraw banknotes or receive cash from an employee at a branch of their PSP if provided by the PSP as part of its non-digital euro payment services (or be assisted in the use of the ATM).

Automated defunding functionalities can be activated at the individual user's choice to a non-digital euro payment account (the linked payment account or another payment account indicated by the user)[16]. Additionally, in case of offline, automated defunding functionalities can be activated to online digital euro holdings. An individual user has the option to schedule regularly recurring defunding operations with an amount and a defunding frequency, and/or to set a maximum threshold (within the holding limit), which is automatically maintained by defunding the surplus amount if the set maximum threshold is breached after an incoming transaction[17].

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules – Defunding	
General business rules:	
LM-040-001	The PSP must ensure that manual and automated defunding functionalities to a non-digital euro payment account are available to digital euro users in line with the availability requirement as defined in Section 4.3.1. Without prejudice to compliance with holding limits, manual and automated defunding shall be executed immediately. The non-digital euro payment account can be any non-digital euro payment account at either the same PSP which services the user's digital euro payment account or at another PSP that is a scheme participant.
LM-040-002	The PSP must ensure that the manual defunding functionalities to cash are available to digital euro users via ATM and/or PSP's branch, according to their respective service hours if provided by the PSP. Manual defunding to cash via ATM does not require an existing relationship between the end user and the PSP operating the ATM.
LM-040-003	The PSP must credit the user's non-digital euro payment account immediately after receiving the confirmation from DESP that the defunding instruction has been settled.

[16] The non-digital euro payment account can be any payment account either at the same PSP which services the user's digital euro payment account or at another PSP that is a scheme participant.
[17] The check of whether automated defunding needs to be initiated is performed either by the PSP for online automated defunding or by the app for offline automated defunding whenever the offline device comes online.

Individual user business rules:	
LM-041-001	The PSP must offer individual users the possibility to defund its offline digital euro device to online digital euro holdings. This requires the PSP to request defunding first (see Section 3.5.3.2), followed by a funding request (see Section 3.5.3.1).
LM-041-002	The PSP must allow individual users to set up, change and terminate automated defunding. The user must be allowed to specify: • The starting date, defunding frequency, and defunding amount, and/or • The defunding non-digital euro payment account, and/or • The maximum threshold (within the holding limit), which is to be automatically maintained by the PSP by defunding the surplus amount if the set maximum threshold is breached after an incoming transaction
LM-041-003	If the individual user has set up automated defunding and the defunding amount is not available on the digital euro payment account, the defunding process must be aborted, and the PSP must inform the user.
LM-041-004	If the individual user has linked a non-digital euro payment account to the digital euro payment account, this linked non-digital euro payment account shall be presented by the PSP as the default destination account for manual defunding. However, the user shall be offered the possibility to indicate another non-digital euro payment account instead of the linked non-digital euro payment account, provided that the user is able to prove he/she is the owner of the alternative non-digital euro payment account.
LM-041-005	When processing an incoming transaction to the user's digital euro payment account (see Section 3.5.4**Error! Reference source not found.**), the PSP shall check if the i ncoming transaction would breach the maximum threshold specified by the user on the online digital euro payment account (if applicable). If it would breach the maximum threshold, the PSP must initiate the defunding as per the user's automated defunding settings.
End-to-end flows - Defunding	
Online end-to-end flows:	
LM-2.1	Online manual defunding to non-digital euro payment account same PSP
LM-2.2	Online manual defunding to non-digital euro payment account - different PSPs
LM-2.3	Online scheduled or automated defunding to non-digital euro payment account same PSP
LM-2.4	Online scheduled or automated defunding to non-digital euro payment account - different PSPs
LM-2.5	Online manual defunding with cash withdrawal at PSP branch
LM-2.6	Online manual defunding with cash withdrawal at ATM through QR code & app
LM-2.7	Online manual defunding with cash withdrawal at ATM through card (contact and contactless) or smartphone
LM-2.8.1	Online purchase with Cash Back at POS (PwCB) with NFC through card (contact and contactless) or mobile device
LM-2.8.2	Online purchase with Cash Back at POS (PwCB) with QR code
Offline end-to-end flows:	
LM-2.10	Offline manual defunding to non-digital euro payment account via app – same PSP
LM-2.11	Offline digital euro manual defunding to online digital euro account via app

LM-2.12	Offline digital euro manual defunding to online digital euro account via app and NFC card
LM-2.13	Offline digital euro manual defunding to cash at ATM with card (contact and contactless) or smartphone
LM-2.14	Offline scheduled/automated defunding to non-digital euro payment account via app – same PSP
LM-2.15	Offline scheduled/automated defunding to online digital euro account via app

3.5.3.3 Reverse waterfall

FUR.104 For the event that digital euro holdings are not sufficient to complete a digital euro payment transaction, scheme participants shall provide users with the option to allow automatic transfers of funds via a reverse waterfall functionality from the linked non-digital euro payment account. The activation of the reverse waterfall functionality is mandatory for business users.

FUR.105 Scheme participants shall comply with the applicable business rules and end-to-end process flows for the reverse waterfall functionality as defined in this subsection.

High-level overview

Via a reverse waterfall functionality an individual user may allow automatic transfers of funds from the linked non-digital euro payment account if digital euro holdings are not sufficient to complete a digital euro payment transaction. The activation of the reverse waterfall is mandatory for business users.

The reverse waterfall is solely available for online digital euro payment transactions.

In case the user does not have sufficient digital euro holdings, the reverse waterfall (if activated by the user) will be triggered to cover for the insufficient digital euro holdings to perform the outgoing digital euro payment transaction. The check whether reverse waterfall is required is integrated into the pre-settlement validation of an online digital euro payment transaction (so called 'balance pre-check', executed by the payer's PSP). Likewise, the settlement of reverse waterfall is fully integrated into the settlement of an online digital euro payment transaction.

If the reverse waterfall is not activated, or if it fails due to, e.g. insufficient funds on the linked non-digital euro payment account (within the financial agreement specified between the user and the PSP providing the non-digital euro payment account), both the digital euro payment transaction and the reverse waterfall will be rejected.

A detailed description of the related end-to-end flows is included in Annex B2.

Further details on the management of digital euro transactions can be found under Section 3.5.4.

Applicable business rules and end-to-end flows

Business rules – Reverse Waterfall	
General business rules:	
LM-030-001	The PSP must ensure that the reverse waterfall functionality is available to digital euro users in line with the availability requirement as defined in Section 4.3.1.
LM-030-002	If reverse waterfall is activated by the user and required, the PSP must instruct the funding of the transaction amount deducted with the digital euro user's current digital euro balance.
LM-030-003	If a transaction including reverse waterfall fails, the PSP must immediately reverse the debit or reservation made on the user's non-digital euro payment account.
Individual user business rules:	
LM-031-001	The PSP must allow individual users to activate or deactivate the reverse waterfall option.
LM-031-002	The PSP must allow individual users to specify reverse waterfall. The reverse waterfall can only be applied if - within the financial agreement specified between the user and the PSP providing the non-digital euro payment account - the linked non-digital euro payment account holds sufficient balance.
Business user business rules:	
LM-032-001	The PSP must ensure that a business user has always activated the reverse waterfall option.
End-to-end flows – Reverse Waterfall	
The reverse waterfall is directly integrated into the following end-to-end flows that are part of the digital euro pre-transaction processing:	
sTM-31	Balance pre-check payer sub-flow

3.5.3.4 Waterfall

FUR.106 For the event that the online digital euro holding limit is reached, an individual user is provided the option to allow automatic transfer of funds to the linked non-digital euro payment account via a waterfall functionality. The activation of the waterfall functionality is mandatory for business users.

FUR.107 Scheme participants shall comply with the applicable business rules and end-to-end process flows for the waterfall functionality as defined in this subsection.

High-level overview

Via a waterfall functionality an individual user may allow automatic transfers of funds to the linked non-digital euro payment account if the online digital euro holding limit is reached. The activation of the waterfall is mandatory for business users to enforce business users online holding limit when accepting digital euro payments.

The waterfall functionality is solely available for online digital euro transactions.

In case an incoming digital euro payment transaction would exceed the holding limit on the user's digital euro payment account, the waterfall (if activated by the user) will be triggered for the excess amount above the holding limit (current digital euro balance plus transaction amount minus holding limit). The check whether waterfall is required is integrated into the pre-settlement validation of an online digital euro payment transaction (so called 'balance pre-check' executed by payee's PSP). Likewise, the settlement of waterfall is integrated into the settlement of an online digital euro payment transaction.

If the waterfall is not activated, or if it fails, with an incoming digital euro payment transaction exceeding the holding limit, both the digital euro payment transaction and the waterfall will not be processed.

Further details on the management of digital euro payment transactions can be found under Section 3.5.4

An additional waterfall may be necessary aft er settlement confirmation to handle the following scenario (so-called post-settlement holding limit check):

- Incoming digital euro payment transaction 1 is received. The check is performed to verify if it would result in a breach of the holding limit. This is not the case. Waterfall is not triggered.
- Incoming digital euro payment transaction 2 is received while transaction 1 has not yet been settled. The check is performed to verify if it would result in a breach of the holding limit. This is not the case at this point in time. However, after settlement of incoming transaction 1, transaction 2 would breach the holding limit. Waterfall is not triggered by the standard validation. To ensure the holding limit, the additional waterfall step is performed after settlement. Further details can be found in the relevant end-to-end flows.

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules – Waterfall	
General business rules:	
LM-050-001	The PSP must ensure that the waterfall functionality is available to digital euro users in line with the availability requirement as defined in Section 4.3.1.

LM-050-002	If waterfall is active the PSP must instruct the defunding of the excess amount above the holding limit (current digital euro balance plus digital euro payment transaction amount minus holding limit).
LM-050-003	The PSP must credit the user's non-digital euro payment account immediately after receiving the confirmation from DESP that the waterfall instruction has been settled.
Individual user business rules:	
LM-051-001	The PSP must allow individual users to activate or deactivate the waterfall option.
Business user business rules:	
LM-052-001	The PSP must ensure that a business user has the waterfall activated at all times.
End-to-end flows – Waterfall	
The waterfall is integrated into the digital euro (post-) transaction processing and is represented by the following end-to-end flows:	
sTM-33	Balance pre-check payee sub-flow
sTM-32	Post-settlement holding limit check (waterfall) sub-flow – same PSP
sTM-41	Post-settlement holding limit check (waterfall) sub-flow – different PSPs

3.5.3.5 Holding limit

[Section on the functioning and enforcement of the holding limit to be detailed out in further iterations of the Rulebook.]

FUR.108 Scheme participants shall comply with the business rules applicable to enforcing the digital euro holding limits for user's digital euro payment accounts as defined in this subsection.

Business rules – Holding Limit	
General business rules:	
LM-010-001	The PSP is responsible for enforcing the user's online digital euro holding limit.
Individual user business rules:	
LM-011-001	At no point in time shall the total sum of digital euro held by an individual user exceed the individual user's holding limit.
LM-011-002	An online digital euro payment account owned by an individual user has a holding limit assigned to it. This holding limit can never be exceeded.
LM-011-003	An offline device owned by an individual user has a holding limit assigned to it. This holding limit can never be exceeded.
Business user business rules:	

LM-012-001	An online digital euro payment account owned by a business user has a holding limit of zero. Any online digital euros received by a business user shall be defunded combined with the digital euro transaction via the waterfall functionality (see Section 3.5.3.4).
LM-012-002	An offline device owned by a business user has a holding limit assigned to it. Offline digital euro holdings received by a business user shall be defunded as soon as technically possible, down to the defined threshold. The business user's offline device shall initiate a defunding operation towards the linked non-digital euro payment account as soon as a network connection is available (see Section 0).

3.5.4 Transaction management

FUR.109 Scheme participants shall be responsible for the transaction management outlining the ways of digital euro users paying and receiving online payments according to the availability defined in Section 4.3.1.

FUR.110 Scheme participants shall comply with the business rules applicable to the general management and processing of digital euro payment transactions as defined in this subsection.

High-level overview

Scheme participants are responsible for the transaction management outlining the ways of digital euro users paying and receiving payments according to the availability defined in Section 4.3.1. This involves providing a variety of payment instruments and acceptance solutions, such as cards and PSP apps for individual users, and physical or virtual points of interaction for business users, like POS or e-commerce/m-commerce systems. These instruments and solutions are supported by different communication technologies. The digital euro can be used in various transactions:

- (Online and offline) P2P payment transactions (see Section 3.5.4.1)
- (Online) e-commerce payment transactions[18] (see Section 3.5.4.2), and
- (Online and offline) POS payment transactions[19] (see Section 3.5.4.3)

Digital euro users will also be able to use a digital euro for recurring payments and standing orders (see Section 3.5.4.4), in full or partial refunds (see Section 3.5.4.6), and in payments enabled via the pre-authorisation service (see Section 3.5.4.5).

[18] Including m-commerce payments, person/business-to-government (X2G) payments, and government-to-person/business (G2X) payments.
[19] Including person/business-to-government (X2G) payments and government-to-person/business (G2X) payments.

Digital euro users will also have the right to dispute an (un-)successful digital euro payment transaction. The dispute management principles, processes and rules are described in Section 6.

Offline digital euro payment transactions occur directly between payer and payee devices, enforcing any relevant rules locally on the device. Since PSPs are not involved in these transactions, details about offline transactions will not be further covered in this section, except for references to the offline end-to-end flows.

Online digital euro payment transaction processing depends on the payment instruments and acceptance solutions used and can fall into two categories with regard to the required interactions between the involved parties (payer, payee, payer's PSP, payee's PSP and DESP). The payment process begins when the first instruction, containing payment information (and settlement details, if initiated by the payer's digital euro payment service provider), reaches the DESP:

- If the initial request with payment information is sent by the payee's digital euro payment service provider, it is considered a payee-initiated payment
- If the initial request comes from the payer's digital euro payment service provider, it is a payer-initiated payment and also includes settlement details

A high-level flow of a payer-initiated online digital euro payment transaction using the example of a simplified P2P payment is shown in Figure 3-5.

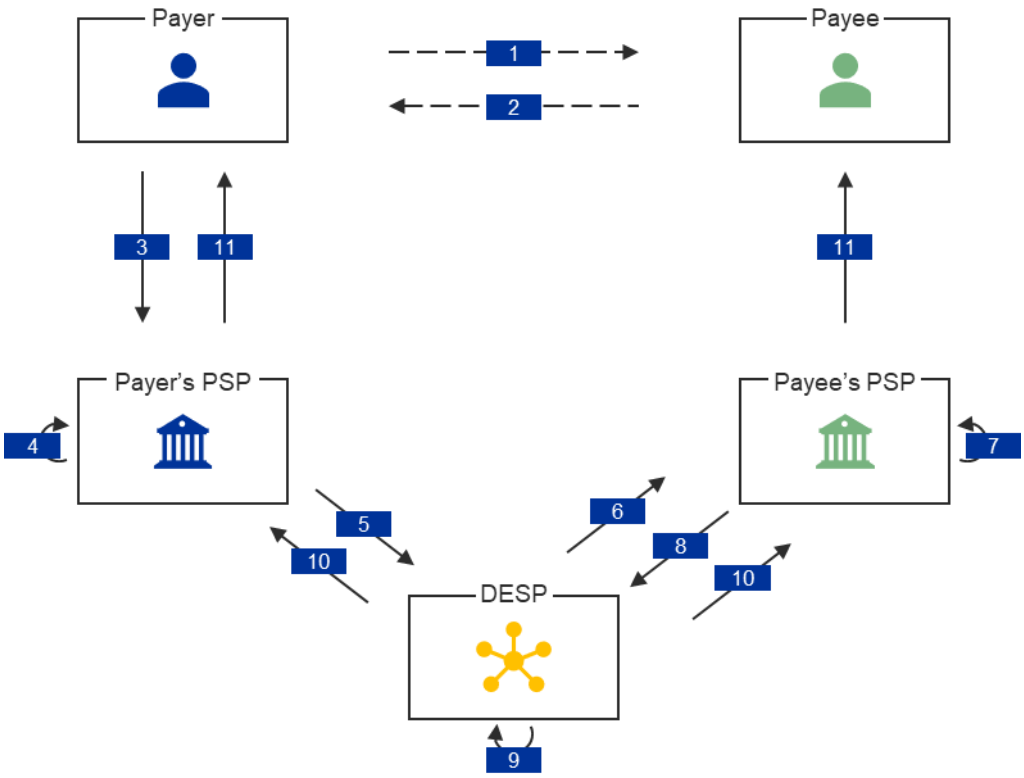

Figure 3-5 High-level flow of a payer-initiated online transaction - P2P payment[20]

Description of steps:

1. and 2. The payer and payee agree on the payment details and amount *(optional depending on the payment method used)*
3. The payer initiates the digital euro payment transaction with its PSP
4. The payer's PSP validates the digital euro payment transaction
5. The payer's PSP submits the digital euro payment transaction to the DESP
6. The DESP forwards the digital euro payment transaction to the payee's PSP for validation
7. The payee's PSP validates the digital euro payment transaction
8. The payee's PSP sends the validation response to the DESP

[20] A payment transaction might involve the initiation of both reverse waterfall on payer's side and waterfall on payee's side as well as different PSP(s) in case the PSP(s) providing the digital euro payment account(s) and the PSP(s) providing the non-digital euro payment account(s) are not the same.

9. The DESP initiates the settlement, after the involved PSPs have confirmed and provided the settlement information, and settles the transaction

10. The DESP confirms the settlement to the involved PSPs

11. The involved PSPs confirm the settlement to the payer and the payee respectively

A high-level flow of a payee-initiated online digital euro payment transaction using the example of a simplified POS payment is shown in Figure 3-6.

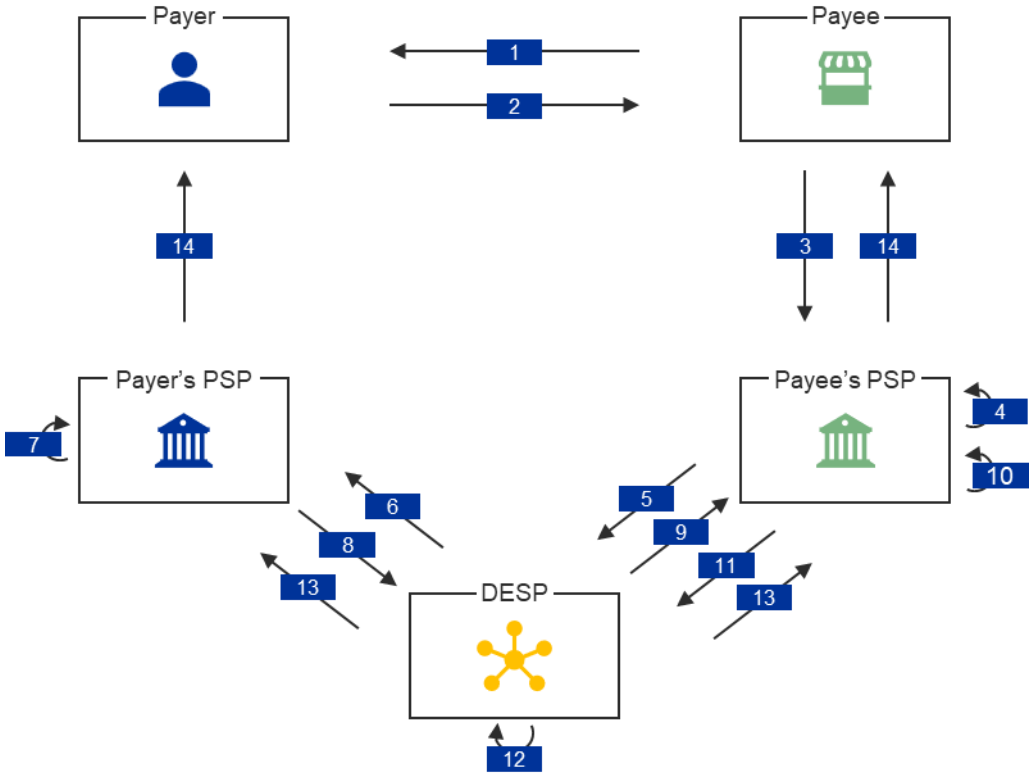

Figure 3-6 High-level flow of a payee-initiated online transaction - POS payment[21]

Description of steps:

1. The payee presents the amount payable to the payer at the POS

2. The payer verifies the payment by authenticating and presenting the payment instrument

[21] A payment transaction might involve the initiation of both reverse waterfall on payer's side and waterfall on payee's side (compulsory for business users) as well as different PSP(s) in case the PSP(s) providing the digital euro payment account(s) and the PSP(s) providing the non-digital euro payment account(s) are not the same.

3. The payee initiates the digital euro payment authorisation request, including consent details with its PSP
4. The payee's PSP validates the digital euro payment authorisation request
5. The payee's PSP submits the digital euro payment authorisation validation request to the DESP
6. The DESP forwards the digital euro payment authorisation validation request to the payer's PSP for validation
7. The payer's PSP validates the digital euro authorisation validation request
8. The payer's PSP submits the digital euro payment transaction to the DESP
9. The DESP forwards the digital euro payment transaction to the payee's PSP for validation
10. The payee's PSP validates the digital euro payment transaction
11. The payee's PSP sends the validation response to the DESP
12. The DESP initiates the settlement, after the involved PSPs have confirmed and provided the settlement information, and settles the transaction
13. The DESP confirms the settlement to the involved PSPs
14. The involved PSPs confirm the settlement to the payer and the payee respectively

The business rules applicable to the general management and processing of digital euro payment transactions are included in the table below.

Business rules – Transaction management	
General business rules:	
TM-000-001	The PSP shall ensure that paying and receiving payments in digital euro is possible for digital euro users in line with the availability requirement as defined in Section 4.3.1.
TM-000-002	The PSP shall perform validations of digital euro payment transactions (including funding/defunding) as per the implementation specifications (see Annexes D1 and D2).
TM-000-003	If the PSP rejects a digital euro payment transaction from its user or receives a rejection notification from DESP, the PSP shall ensure that the reason for the reject is communicated in a clear and easy to understand manner to the digital euro user.
TM-000-006	Upon receipt of the settlement confirmation from the DESP, the PSP immediately updates the user's digital euro balance and notifies the user in accordance with the user's notification preferences (see Section FUR.89).
TM-000-007	The payer PSP must verify that the payer either: • Holds sufficient digital euros to complete the digital euro payment transaction, or

	• Has a linked non-digital euro payment account with an activated reverse waterfall functionality (see Section 0)
TM-000-009	The PSP submitting a digital euro payment transaction to the DESP must ensure that at least one party that is to be debited (payer) or credited (payee) in the transaction is an individual user.
TM-000-010	The payer's PSP must accept all digital euro payment transactions received from either DESP or the payer that conform to the implementation specifications for processing, unless the identified payer account is blocked or closed, invalid or being monitored for compliance or fraud reasons.
TM-000-011	The payee's PSP must accept all digital euro payment transactions received from either DESP or the payee that conform to the implementation specifications for processing, unless the identified payee account is blocked or closed, invalid or being monitored for compliance or fraud reasons.
TM-000-012	The PSP must make the status/result of a digital euro payment transaction known to its digital euro user immediately.
TM-000-014	When processing digital euro payment transactions, PSPs are to interact with the DESP Risk and Fraud Management (RFM) component as required in Section **Error! Reference source not found.**.
TM-000-016	Digital euro payment transactions cannot be cancelled once sent to the DESP.
Individual user business rules:	
TM-001-001	If the payee is an individual user, the payee's PSP must verify that the digital euro payment transaction either: • Would not result in the payee's digital euro balance exceedance of the holding limit, or • Would result in the triggering of the waterfall functionality, if activated (see Section 3.5.3.4)
TM-001-002	If the payee is an individual user and the payee does not have a linked non-digital euro payment account with an activated waterfall option, the payee's PSP must ensure that while processing the incoming payments, the holding limit is not breached at any time.
Business user business rules:	
TM-002-001	If the payee is a business user, the payee's PSP must trigger the waterfall mechanism upon receipt of each incoming digital euro payment transaction (see Section 3.5.3.4).

3.5.4.1 Person-to-person payment

FUR.111 Individual users may use the digital euro for initiating one-off P2P digital euro payment transactions.

FUR.112 Scheme participants shall comply with the end-to-end process flows for P2P digital euro payment transactions as stated in this subsection.

A detailed description of the related end-to-end flows is included in Annex B2.

End-to-end flows – P2P payment	
Online end-to-end flows:	
TM-3.1	P2P payment with QR code in-app (payee-initiated)
TM-3.2	P2P payment with NFC (online), payer-initiated
TM-3.3	P2P payment with NFC (online), payee-initiated
TM-3.5	P2P payment with alias (payerinitiated)
TM-3.6	P2P payment with alias (payeeinitiated)
TM-3.7	P2P payment with payment request by link
TM-3.10	P2P payment with DEAN (payerinitiated) – same PSP
TM-3.11	P2P payment with DEAN (payerinitiated) – different PSPs
TM-3.12	P2P payment with DEAN (payee initiated)
Offline end-to-end flows:	
TM-3.4	Offline contactless P2P payment – mobile device to mobile device
TM-3.8	Offline P2P payment with smartcards using bridge device
TM-3.9	Offline P2P payment between battery powered cards

3.5.4.2 E-commerce & m-commerce payment

FUR.113 Individual and business users may use the digital euro for initiating one-off e-commerce and m-commerce digital euro payment transactions.

FUR.114 Scheme participants shall comply with the end-to-end process flows for e-commerce and m-commerce digital euro payment transaction as stated in this subsection.

A detailed description of the related end-to-end flows is included in Annex B2.

End-to-end flows e-Commerce & m-Commerce payment	
Online end-to-end flows:	
TM-2.1	E-commerce (including C2G) payment with QR code
TM-2.2	E-commerce payment with alias or DEAN
TM-2.3	E-commerce payment with pay by link
TM-2.4	M-Commerce payment (in-app)

3.5.4.3 (Soft)Point-of-sale payment

FUR.115 Individual and business users may use the digital euro for initiating one-off (Soft)POS digital euro payment transactions.

FUR.116 Scheme participants shall comply with the end-to-end process flows for (Soft)POS digital euro payment transactions as stated in this subsection.

A detailed description of the related end-to-end flows is included in Annex B2.

End-to-end flows – (Soft)Point-of-Sale payment	
Online end-to-end flows:	
TM-1.1	POS payments with payee-generated QR code
TM-1.2	Online contact and contactless POS payment with mobile device, card or wearable – same PSP
TM-1.3	Online contact and contactless POS payment with mobile device, card or wearable – different PSPs
TM-1.6	Online contactless SoftPOS payment with mobile device or wearable – same PSP
Offline end-to-end flows:	
TM-1.4	Offline contact and contactless POS payment with smartcard
TM-1.5	Offline contactless POS payment with smartphone

3.5.4.4 Standing order and recurring payment

FUR.117 Individual users may set standing orders for automatically initiating digital euro payment transactions.

FUR.118 Business users may set up recurring payments to be accepted and authorised by the individual user for automatically initiating digital euro payment transactions.

FUR.119 Scheme participants shall comply with the business rules and end-to-end process flows for standing orders and recurring digital euro payment transactions, if offered, as stated in this subsection.

High-level overview

Individual users may set standing orders for automatically initiating digital euro payment transactions to other (individual or business) digital euro users. Once set up, individual users can access active standing orders to either modify or terminate them.

Business users may set up recurring payments for automatically initiating digital euro payment transactions by specifying recurring payment parameters such as the amount and frequency. These parameters, as defined by the business user during the setup process, shall be accepted and authorised by the individual user. Once set up, both individual and business users can access and view active recurring payments. However, only business users are permitted to modify or terminate recurring payments prior to their expiration. Any modifications of a recurring payment made by a business user must also be accepted and authorised by the individual user.

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules – Standing order and Recurring payment	
Individual user business rules:	
TM-041-001	When receiving a recurring payment and/or standing order setup or modification, the payer's PSP must store the recurring payment and/or standing order parameters authorised by the individual user for the purpose of validating subsequent payments.
TM-041-002	When receiving a recurring payment request from a payee's PSP for one of its individual users, the payer's PSP must validate the recurring payment against the recurring payment parameters authorised by the individual user.
TM-041-006	The payer's PSP must reject any (subsequent) payments received for a terminated recurring payment.
TM-041-003	The payer PSP shall allow an individual user to terminate a standing order.
TM-041-004	The payer PSP shall allow an individual user to modify a standing order and shall store the modifications authorised by the individual user for the purpose of initiating subsequent payments.
TM-041-005	The PSP shall allow individual users to set up standing orders with a fixed amount and fixed frequency.
Business user business rules:	
TM-042-001	For the purpose of initiating recurring payments, the payee's PSP must ensure that the business user stores the payer's details in coded form.
TM-042-002	When setting up and initiating recurring payments, the payee's PSP is not allowed to share any non-coded payer details of an individual user with the business user.
TM-042-003	For the purpose of initiating recurring payments, the payee's PSP must ensure that the business user obtains consent from the payer regarding: • The storage of coded payer's details

	• The recurring payment fixed amount • The recurring payment fixed frequency • Whether or not the payer's consent is required for each subsequent transaction • Expiry date/end date of the recurring payments (optional)
TM-042-004	The payee's PSP shall allow a business user to terminate a recurring payment.
TM-042-005	The payee's PSP shall allow a business user to modify a recurring payment. Any modifications of a recurring payment made by a business user must also be accepted and authorised by the individual user via the payer's PSP.
End-to-end flows – Standing order and Recurring payment	
Online end-to-end flows:	
TM-4.1.1	Recurring e-commerce payment via QR code
TM-4.1.2	Recurring e-commerce payment with pay by link
TM-4.1.3	Recurring e-commerce payment via alias or DEAN
TM-4.2	Recurring m-commerce payment (in-app)
TM-4.3	Standing order
TM-4.5	Recurring payment management by business user
TM-4.6	Standing order management by individual user

3.5.4.5 Pre-authorisation

FUR.120 Individual and business users may use the digital euro in services requiring a payment pre-authorisation[22] where the payable amount and payment time are not known at the checkout.

FUR.121 Scheme participants shall comply with the applicable business rules and end-to-end process flows for the pre-authorisation service as stated in this subsection.

High-level overview

Individual and business users may use the digital euro in services requiring a payment pre-authorisation where the payable amount and payment time are not known at the checkout. In this instance, a business user requires payment certainty to offer the service. A pre-authorisation service is offered to the business user to ensure that the individual user pays for consumed goods or services[23]

[22] A payment "pre-authorisation" in the front-end solution equals to "reservation" of digital euro holdings in the DESP.
[23] The business user may submit more than one partial settlement instruction of the pre-authorised amount, while the reservation remains active. These partial settlements are not considered recurring payments because they do not depend on a defined periodicity.

Like recurring e-commerce payments, amendments and terminations of pre-authorisations are performed by the business user before it shares an update with the individual user via their PSPs.

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules – Pre-authorisation	
General business rules:	
TM-050-001	Digital euro holdings reserved by a pre-authorisation can be finally settled as a whole or in part, and it may also be settled for an amount exceeding the existing reservation. Multiple partial settlements are possible. If the final settlement amount exceeds the existing reservation, authorisation by the individual user (payer) via the payer's PSP is required for the amount that exceeds the existing reservation.
TM-050-002	If a reservation for which a reverse waterfall (see Section 3.5.3.3) has been triggered is finally partially settled or fails or expires, the unused digital euro holdings reserved by the pre-authorisation are released and remain on the individual user's digital euro payment account.
TM-050-003	The amount of digital euro holdings reserved by pre-authorisation(s) on the individual user's digital euro payment account contributes to the calculation of the holding limit and cannot, in total, exceed the holding limit.
Individual user business rules:	
TM-051-001	The payer's PSP must notify the individual user (payer) when holdings reserved by pre-authorisation are released due to a (partial) cancellation, by (partial) settlement of the final amount, or when the expiry date and time are reached.
Business user business rules:	
TM-052-001	The payee's PSP must notify the business user (payee) when holdings reserved by pre-authorisation are released due to a (partial) cancellation, by (partial) settlement of the final amount, or when the expiry date and time are reached.
TM-052-002	A payee's PSP must allow a business user (payee) to modify an existing reservation (increase or decrease the amount, change of expiry date). A change increasing the amount or extending the period of an existing reservation requires the authorisation by the individual user (payer) via the payer's PSP. A change reducing the amount or the period does not require authorisation of the individual user (payer).
TM-052-003	The payee's PSP must allow a business user to cancel a (partial) reservation from the moment of the confirmation that the digital euro holdings have been blocked throughout the entire duration of the reservation.
End-to-end flows – Pre-authorisation	
Online end-to-end flows:	
TM-5.1.1	Pre-authorisation service at POS with QR code (lower or equal final amount)

TM-5.1.2	Pre-authorisation service at POS with QR code (higher final amount)
TM-5.1.3	Pre-authorisation service at POS with NFC
TM-5.2.1	Pre-authorisation service on e-commerce with QR code (lower or equal final amount)
TM-5.2.2	Pre-authorisation service on e-commerce with pay by link (lower or equal final amount)
TM-5.2.3	Pre-authorisation service on e-commerce via alias or DEAN (lower or equal final amount)
TM-5.3	Pre-authorisation service on m-commerce (lower or equal final amount)
TM-5.4	Modification of a reservation or pre-authorisation

3.5.4.6 Refund

FUR.122 Business users may use the digital euro for initiating digital euro payment refunds.

FUR.123 Scheme participants shall comply with the business rules and end-to-end process flows for a refund as stated in this subsection.

High-level overview

Business users may use the digital euro for initiating digital euro payment refunds. Refunds might be initiated via POS when an individual user requests the refund physically (e.g. in the store where the purchase took place) or online via the e-commerce website or the m-commerce app.

A detailed description of the related end-to-end flows is included in Annex B2.

Applicable business rules and end-to-end flows

Business rules - Refund	
General business rules:	
TM-060-001	The payee's PSP is not allowed to request decoding of the payer's details received as part of a refund.
Individual user business rules:	
TM-061-001	When the payer's PSP receives a refund, it must verify that the refund either: • Would not result in the individual user's digital euro balance exceedance of the holding limit, or • Would result in the triggering of the waterfall mechanism (see Section 3.5.3.4)
Business user business rules:	
TM-062-001	When initiating a refund, the payee's PSP must ensure that the refund relates to an original digital euro payment that has already been settled.

TM-060-002	The refund amount may be full or partial, and it may even exceed the original digital euro payment transaction amount, when additional costs must be reimbursed to the individual end user.
End-to-end flows - Refund	
Online end-to-end flows:	
TM-7.1	Refund at POS via (contact or contactless) card, mobile device or wearable
TM-7.2	Refund (E-commerce)
Offline end-to-end flows:	
TM-7.3	Refund for purchase in offline digital euro at POS

4 Technical requirements

4.1 Section overview

The purpose of this section is to introduce the technical requirements for participants to offer digital euro payment services. This includes the applicable standards for payment interfaces and corresponding technologies (Section 4.2), non-functional requirements for PSPs' internal systems (Section 4.3), and an overview of the implementation specifications which is provided in Section 4.4 and Section 4.5 while the full specifications are available in Annex D.

The implementation specifications outlined in Section 4.4 and Section 4.5 are systematically organised into the three key domains of the digital euro functional architecture, as depicted in

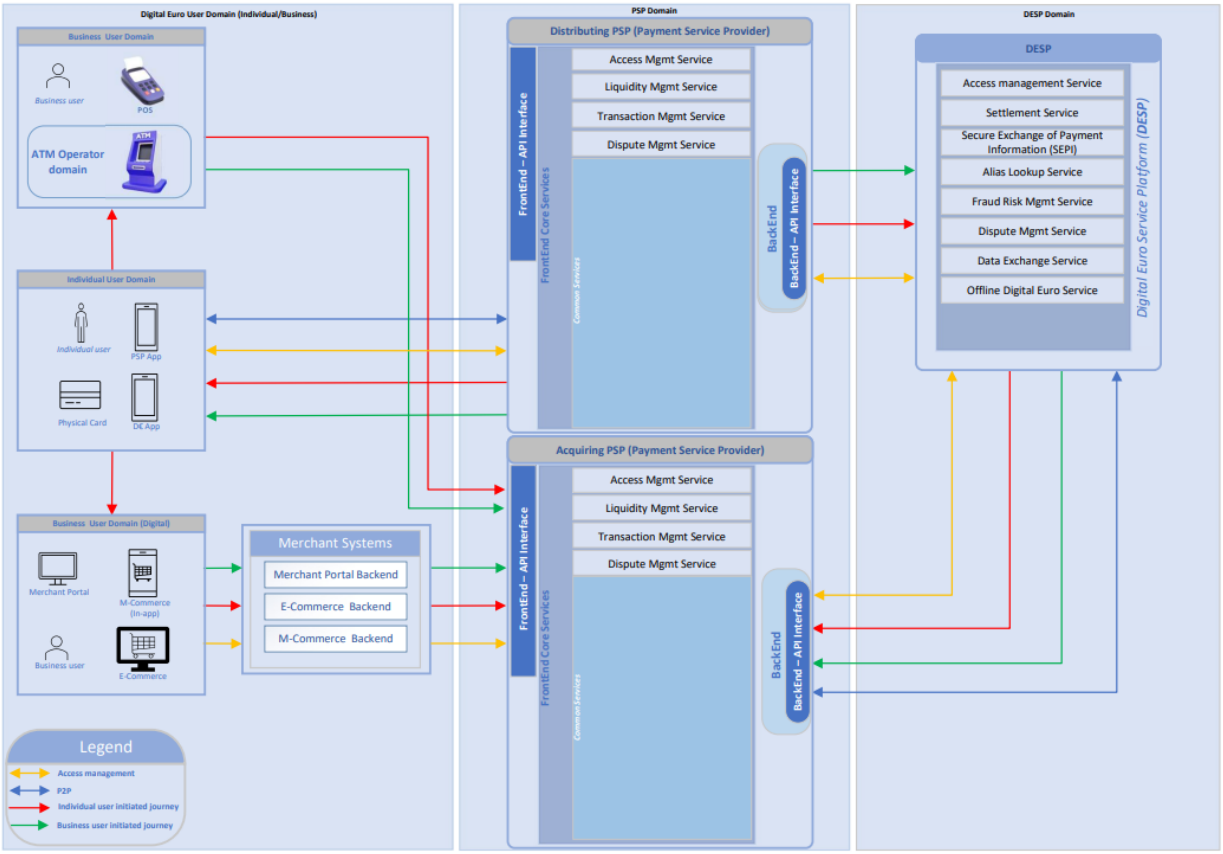

Figure 4-1 below[24]:

[24] Figure 4-1 describes the various domains in line with the terminology applied in the implementation specifications (Annex D), a future version of the rulebook will update the terminology in Annex D accordingly.

- **Digital euro user Domain:** covers payment instruments, user to application interfaces and acceptance solutions
- **PSP Domain:** includes specifications for distributing and acquiring PSPs services and functions
- **DESP Domain:** focuses on integration with DESP interfaces

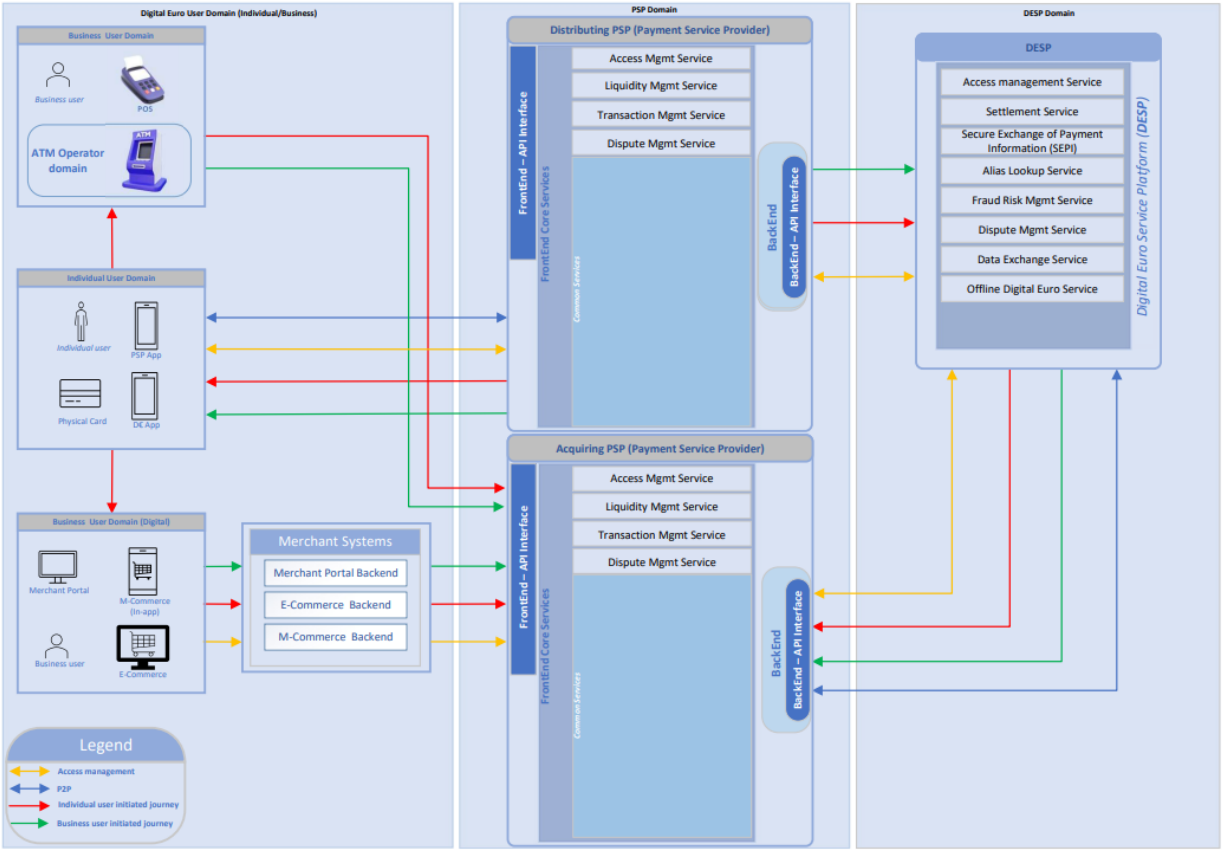

Figure 4-1 The digital euro functional architecture

4.2 Applicable standards

In order to foster a harmonised user experience of the digital euro across scheme participants as well as to support interoperability with existing European payments infrastructure, the digital euro rulebook makes use of existing open market standards where possible. This section introduces the list of envisaged standards in the scope of the digital euro.

TER.01 PSPs and potential third-party service providers shall implement the envisaged rulebook standards outlined in this section.

The standards are presented following the architecture detailed in Section 4.1, i.e., user domain applicable standards (4.2.1), PSP domain applicable standards (4.2.2) and DESP domain applicable standards (4.2.3). Where open standards are being reused for digital euro processes, the related implementation specifications include explicit references to the relevant part of the respective standard, including the source and format. As the standard selection process is ongoing, please consider the following caveats:

- The mentioned selected standards are candidates and preliminary
- Candidate standards may evolve or be added, with the finalised list to be confirmed at a later stage
- The mentioned digital euro implementation specifications are the ones in the Annex D, in the scope of draft version 0.91 of the rulebook
- Security-related standards are under elaboration and review and will be announced at a later stage
- Standards for the offline solution are still being defined and will be communicated at a later stage

4.2.1 User domain applicable standards

The below table introduces the envisaged standards related to the user domain. These standards are preliminary candidates (not yet approved) and may be subject to change.

Solution type	User domain	Payment instrument / acceptance solution	Type	Standard
	Business user domain	E-commerce[25] check-out web pages	QR code	EPC QR[26]
			DEAN	Potential ISO standard, under investigation

[25] The payment interface is, in this case, the business user application running on a computer
[26] EPC governs a number of standards of which several are of interest for the digital euro. The most prominent one is the one for QR-code payments (ISO_QR_193). It will be reused in the acceptance domain for online POS, e- and m-commerce and potential ATM QR-code payments.

Online solution			Alias	ITU-T E.164
		M-commerce[27] check-out application	Not applicable	Digital euro implementation specification
		POS[28]	QR code	EPC QR
			Contactless and contact	CPACE
		ATM	NFC and contact	CPACE
	Individual user domain	Physical card	Contactless and contact	CPACE
		Mobile application	QR code	EPC QR
			NFC	CPACE for P2B and under investigation for P2P
			DEAN	Potential ISO standard, under investigation
			Alias	ITU-T E.164
			Balance and transaction history	Berlin Group under investigation
		PSP website	DEAN	Potential ISO standard, under investigation
			Alias	ITU-T E.164
Offline solution	Offline solution is currently under definition			

[27] The payment interface is, in this case, the business user application running on a smartphone
[28] A POS can be a classic payment terminal or a SoftPOS (Point of sale with a payment application on a smartphone).

Table 4-1 User domain applicable standards

4.2.2 PSP domain applicable standards

The below table introduces the envisaged standards related to the PSP domain. A caveat to note: For ATMs, the Nexo standard is expected to be offered as a reference implementation rather than mandated, with existing domestic implementations also permitted. This will be confirmed at a later stage. These standards are preliminary candidates and may be subject to change.

Solution type	Acceptance solution	Standard
Online solution	E-commerce check-out web pages	Nexo (reference implementation) or upcoming digital euro implementation specifications
	M-commerce check-out application	Digital euro implementation specification
	POS	Nexo (reference implementation) or upcoming digital euro implementation specifications
	ATM	Nexo (reference implementation) or upcoming digital euro implementation specifications
Offline solution	Offline solution is currently under definition	

Table 4-2 PSP domain applicable standards

4.2.3 DESP domain applicable standards

The interfaces facilitating the settlement of transactions between PSPs and the DESP utilises the ISO 20022 data dictionary wherever applicable. Additional elements specific to the digital euro will be defined as needed. The specifications within the DESP domain will adhere to the structure of market-standard RESTful API documentation as for instance specifications developed by Berlin Group.

4.3 Reliability and performance requirements

Non-functional requirements (NFRs) are critical to delivering a seamless digital euro user experience across all scheme participants. These requirements directly impact PSP's underlying system's reliability and performance. The following categories of NFRs are established:

- **Reliability:** Service availability (planned or unplanned downtime) and recoverability capabilities

- **Performance:** Transaction latency

Please note that the current KPIs are aspirational and may be subject to change.

4.3.1 Reliability

TER.02 A scheme participant shall aim at a 99.85% - 99.95% availability of all digital euro transaction, liquidity and access management services that are not dependent on (branch) service hours[29] throughout the entire year on a 24-7-365 basis.

Availability is defined as the period during which digital euro services offered by scheme participants are fully operational[30]. Service availability applies continuously and throughout each day, excluding planned maintenance and services dependent on (physical branch) service hours.

TER.03 A scheme participant shall aim at a recovery time objective (RTO) of 4 hours for digital euro payment services.

RTO is defined as the maximum tolerable amount of time required to restore one or more services to a correct operational state after a failure or disaster event has compromised availability[31].

TER.04 A scheme participant shall aim that planned maintenance [32] and scheduled downtime is communicated 2 days in advance, performed during off-peak hours[33], and does not exceed a cumulative maximum of 4 hours per calendar month.

4.3.2 Performance

TER.05 A payee PSP shall aim at a maximum latency for 99% of online digital euro payment transactions of below 200ms whereby this duration is measured as the elapsed time between the moment a transaction request is received by the payee's PSP and the moment a response is sent to the DESP, with the payee PSP conducting the following tasks in the meantime:

- Check end user balance
- Check whether end user is a business end user
- Waterfall checks, if required

---

29 Including physical onboarding or offboarding (e.g.in-person identity verification or assisted access for vulnerable users).
30 Unavailability of services caused by DESP failure or outage is not considered as non-compliance.
31 More granular incident classification and resolution time may be included in a future version of the rulebook.
32 This excludes maintenance required for updates mandated by the digital euro scheme standards.
33 The definition of off-peak hours will be further detailed in a future version of the rulebook and take into account time zone differentiation.

TER.06 Send the response of the transaction request to the DESP. A payer PSP shall aim at a maximum latency for 99% of online digital euro payment transactions of below 300ms whereby this duration is measured as the elapsed time between the moment a payment request, sent by the DESP, is received by the payer PSP and the moment a response is sent back to the DESP, with the payer PSP conducting the following tasks in the meantime:

- Validation whether payment is a (Soft)POS payment
- Accept or reject payment
- Check end user balance and holding limit
- Reverse waterfall checks and blocking funds if required
- Decrease digital euro funds
- Send the response of the transaction request to the DESP

TER.07 A commercial bank money (CoBM) payer PSP shall aim at a maximum latency for 99% of online digital euro payment transactions of below 150ms whereby this duration is measured as the elapsed time between the moment a payment request, sent by the DESP, is received by the payer PSP and the moment a response is sent back to the DESP, with the payer CoBM PSP conducting the following tasks in the meantime:

- Check if linked non-digital euro payment account is activated and has sufficient balance
- Block funds on linked non-digital euro payment account
- Sending the response of the transaction processing request to the DESP

TER.08 A CoBM payee PSP shall aim at a maximum latency for 99% of online digital euro payment transactions of below 150ms whereby this duration is measured as the elapsed time between the moment a transaction request, sent by the DESP, is received by the payee's PSP and the moment a response is sent back to the DESP, with the payee CoBM PSP conducting the following tasks in the meantime:

- Check if linked non-digital euro payment account is activated
- Sending the response of the transaction processing request to the DESP

4.4 Distributing PSP technical implementation requirements

This subsection introduces the implementation specifications distributing PSPs serving individual digital euro users should implement. The implementation specifications are further detailed in Annex D1 (Front-end implementation specifications) and Annex D2 (Back-end implementation specifications).

The front-end implementation specifications prescribe the requirements for individual users' payment instruments, and the services in the distributing PSP domain as depicted in

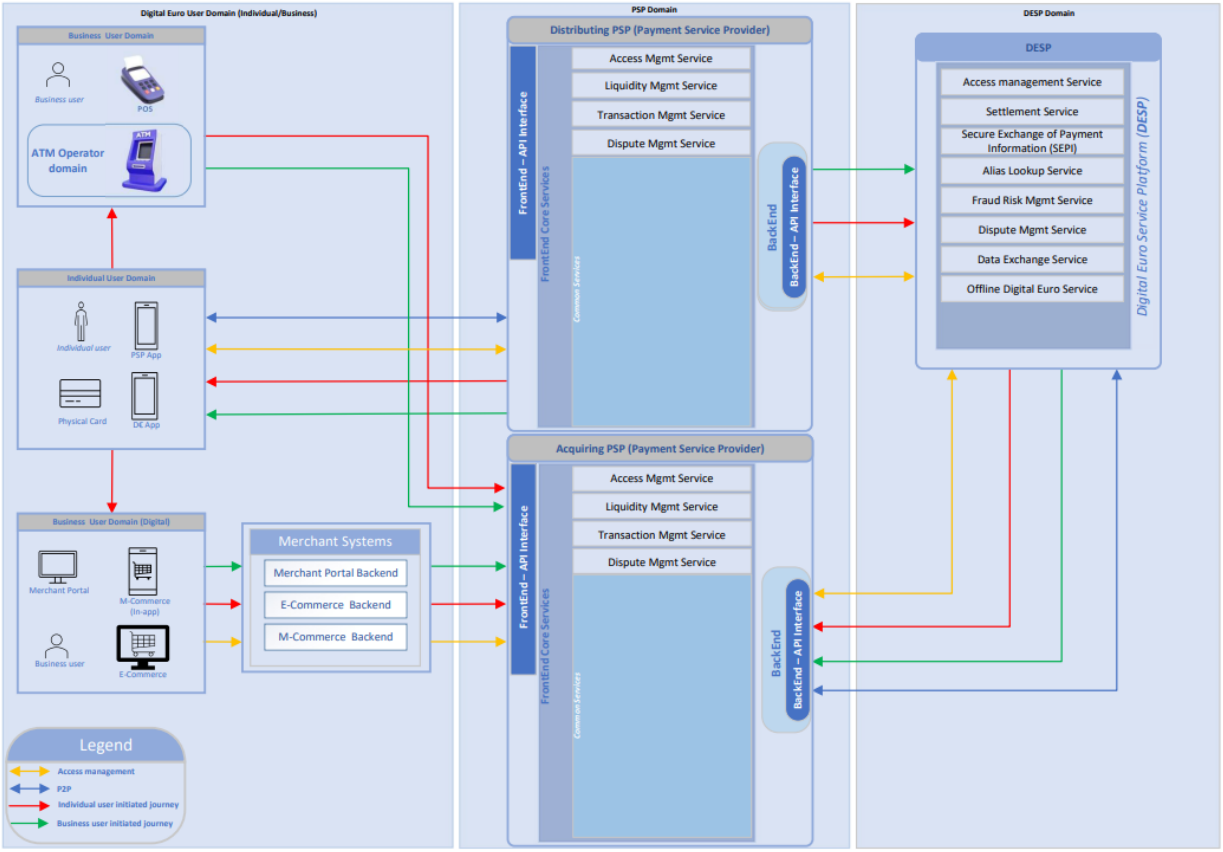

Figure 4-1. Front-end implementation specifications for distributing PSPs are documented in specification #1 (Individual user PSP requirements), specification #3 (Payment instrument requirements), and specification #5 (Common services). The back-end implementation specifications in Annex D2 prescribe how distributing PSPs can invoke services in the DESP domain as also depicted in

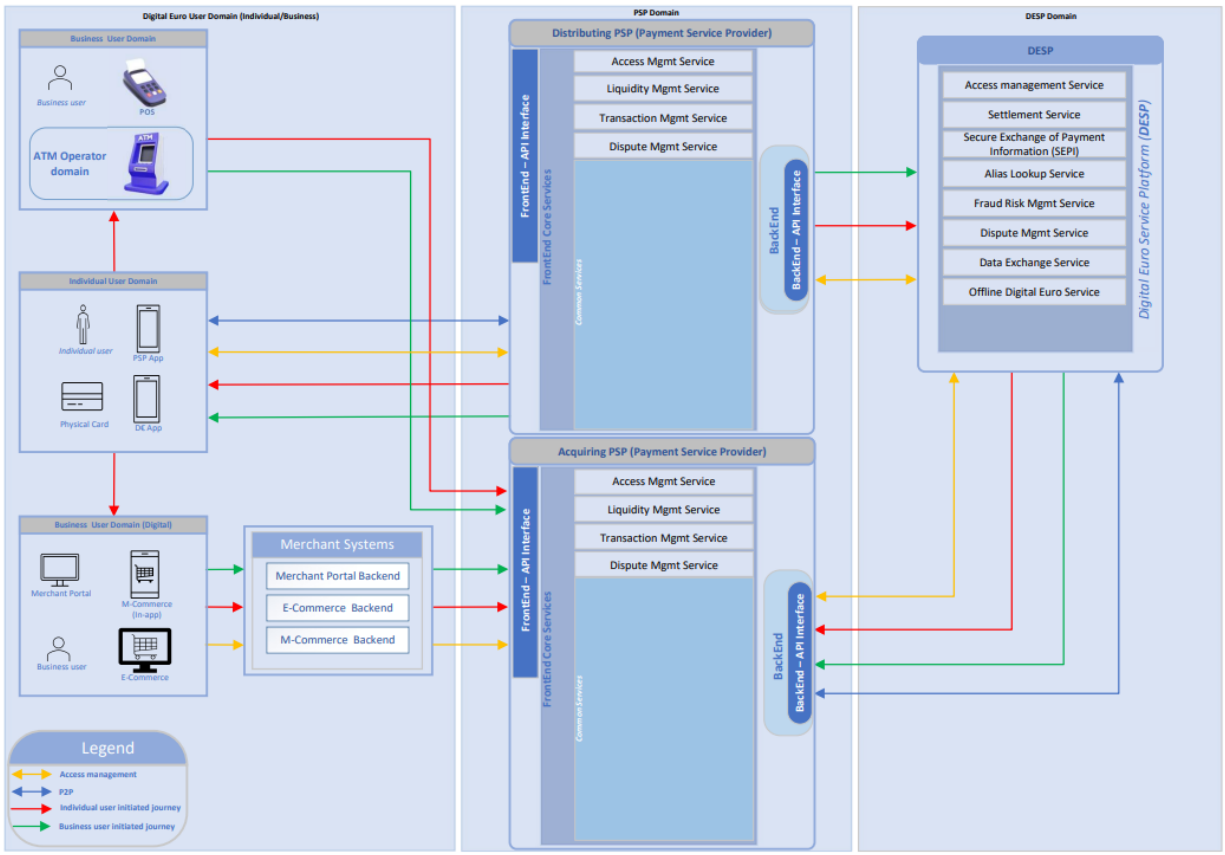

Figure 4-1.

TER.09 Distributing PSPs shall implement the specifications in Annex D1. relevant to the digital euro payment services they offer.

TER.10 Distributing PSPs shall implement the specifications in Annex D2 relevant to the digital euro payment services they offer.

A future version of the rulebook will include implementation specifications for the offline wallet SDK, offline distribution service, and integration with the DESP offline issuance component[34].

4.4.1 Distributing PSP – Individual user domain requirements

The following tables list the services for payment instruments through which individual users can consume digital euro payment services as depicted in

[34] Implementation specifications for the offline functionalities of the digital euro will be further detailed when a vendor for the offline solution is selected.

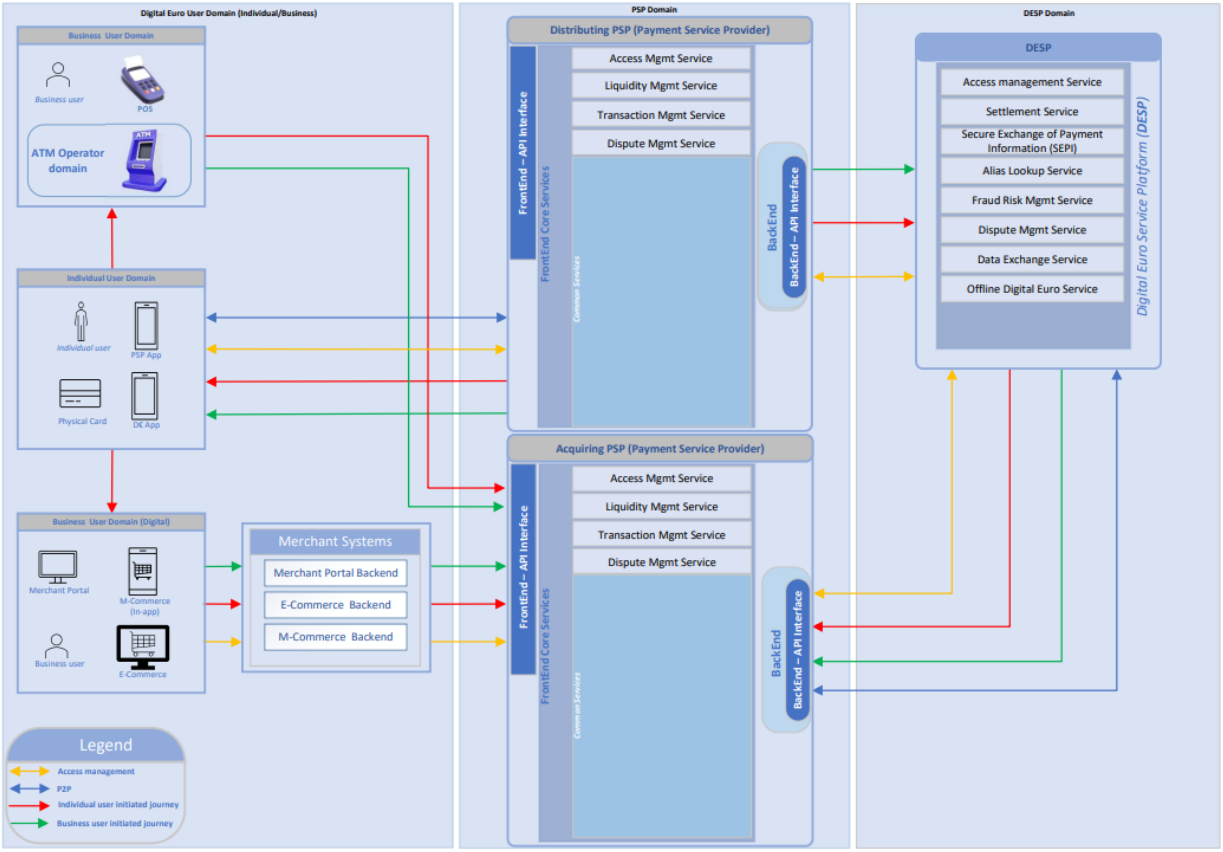

Figure 4-1. The tables refer to the relevant implementation specifications and chapters in Annex D1 which are further detailed in specification #3. The current version of the rulebook prescribes implementation specifications for proprietary PSP applications and PSP web pages.

A future version of the rulebook will include specifications for the physical card and the digital euro app[35]. Moreover, some specifications in this overview may still have placeholders.

PSP app		
Core service	**Service**	**Specification**
General requirements	Functional requirements[36]	• Specification #3 – 4.1.1

[35] Future requirements for the digital euro app will be detailed further in a future version of the rulebook .

[36] Including requirements on, supported payment instruments, user experience, accessibility, personalised settings, QR code service, NFC communication, user authentication, user activation, user alerts, and visual consistency and branding. Some specifications have placeholders for a future version of the rulebook.

	Non-functional requirements[37]	• Specification #3 – 4.1.2
Access management[38]	Onboarding of a digital euro user	• Specification #3 – 4.2.1
	Offboarding of a digital euro user	• Specification #3 – 4.2.2
	User lifecycle management	• Specification #3 – 4.2.3
Liquidity management[39]	Manual funding of online holdings	• Specification #3 – 4.3.2
	Manual defunding of online holdings	• Specification #3 – 4.3.3
Transaction management	P2P	• Specification #3 – 4.4.1.2 (QR-code) • Specification #3 – 4.4.1.3 (NFC) • Specification #3 – 4.4.1.4 (Alias) • Specification #3 – 4.4.1.5 (DEAN) • Specification #3 – 4.4.1.6 (Standing order)
	POS	• Specification #3 – 4.4.2
	Balance inquiry and transaction management[40]	• Specification #3 – 4.4.3

[37] Including requirements on, download rules, supported operating systems, security, deployment, performance, compliance, availability, data integrity, disaster recovery. Some specifications have placeholders for a future version of the rulebook.
[38] Access management specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the access management specifications with the E2E flows will be included in a future version of the rulebook.
[39] Liquidity management specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the liquidity management specifications with the E2E flows will be included in a future version of the rulebook.
[40] Transaction history will only be available for online digital euro payments.

	Dispute management[41]	• Updated dispute management specifications will be included in a future version of the rulebook

Online Banking (PSP)		
Core service	**Service**	**Specification**
General requirements	Functional requirements[42]	• Specification #3 – 5.1.1
	Non-functional requirements[43]	• Specification #3 – 5.1.2
Access management[44]	Onboarding of a digital euro user (individual user)	• Specification #3 – 5.2.1.1
	Offboarding of a digital euro user (individual user)	• Specification #3 – 5.2.1.2
	User lifecycle management (individual user)	• Specification #3 – 5.2.1.3
	Switching (individual user)	• Specification #3 – 5.2.2.2
Liquidity management[45]	Manual funding online holdings	• Specification #3 – 5.3.2
	Manual defunding online holdings	• Specification #3 – 5.3.3

[41] Dispute specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the dispute specifications with the E2E flows will be included in a future version of the rulebook.
[42] Including requirements on, seamless navigation, responsive design, visual consistency and branding, smooth performance, accessibility, personalised settings, user experience. Some specifications have placeholders for a future version of the rulebook.
[43] Including requirements on, supported operating systems, security, deployment, performance, compliance, availability, data integrity, disaster recovery. Some specifications have placeholders for a future version of the rulebook.
[44] Access management specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the access management specifications with the E2E flows will be included in a future version of the rulebook.
[45] Liquidity management specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the liquidity management specifications with the E2E flows will be included in a future version of the rulebook.

Transaction management	P2P	• Specification #3 – 5.4.1.2 (Alias) • Specification #3 – 5.4.1.3 (DEAN) • Specification #3 – 5.4.1.4.1 (Standing order set-up) • Specification #3 – 5.4.1.4.2 (Standing order management)
	Balance inquiry and transaction management[46]	• Specification #3 – 5.4.2
	Dispute management[47]	• Updated dispute management specifications will be included a future version of the rulebook

4.4.2 Distributing PSP - Front-end requirements

The following table lists services to be integrated in the distributing PSP service domain as depicted in Figure 4-1. These are further detailed in specification #1 and specification #5.

Distributing PSP services		
Core service	**Service and description**	**Specification**
Access management	**Balance and holding limit:** Management of rules to validate that the conditions are met at the digital euro payment	Specification #1 – 6.4 Specification #5 – 7.2: Notification service[48]

[46] Transaction history will only be available for online digital euro payments.
[47] Dispute specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the dispute specifications with the E2E flows will be included in a future version of the rulebook.
[48] Reason codes for this service are captured in the notification service in specification #5.

	account for a proper digital euro transaction execution.	
	Non-digital euro payment account: Non-digital euro payment account status checks and account balance checks to validate if the account is active, live, ready for transactions, and (reverse) waterfall is needed.	Specification #5 – 4.7: Commercial bank money account service
Liquidity management	**Funds management**: management of the rules to manage funds non-digital euro payment account (debit, credit, block, release).	• Specification #5 – 5.2: Non-digital euro payment account funds management service
Transaction management	**Payment initiation**: Management of payment requests initiated by a digital euro user (covering all payment instruments).	• Specification #1 – 8.1 ▪ Specification #5 – 7.2: Notification service[49] • Specification #5 – 4.2: Alias look-up dispatch service • Specification #5 – 4.3: PSP identifier look-up dispatch service • Specification #5 – 4.6: Link creation service • Specification #5 – 6.5: Tokenisation service
	Recurring payment: Management of rules to collect the user details data and store them.	• Specification #1 – 8.2

[49] Reason codes for this service are captured in the notification service in specification #5.

	Standing order: management of parameters defined by the user to request a standing order set-up.	• Specification #1 – 8.3
	Payment processing: Invoked during a payment transaction process after payment initiation in relation to the DESP	• Specification #5 – 6.2 Payment processing service
	Fraud and risk: Management of central score and local fraud and sanction controls to block litigious or suspicious transactions according to the current regulation	• Specification #5 – 6.6 Fraud and risk service
Dispute management	Updated Dispute management implementation specifications will be included in a future rulebook version	
Offline Distribution service	Message transmission for (de)funding transactions. Connected on one side with digital euro user wallets and on the other side, with the PSP's back-end system and the DESP to perform funding and defunding operations and online integrity checks.	

Specification #5 describes common services relevant for both distributing PSPs and acquiring PSPs. Additional services in specification #5 not mapped to one of the core services in the table above are, authentication services[50]. Specifications for authentication services will be included in a future version of the rulebook.

Specification #6 (Technical standard)[51] and #7 (Data management) of Annex D1 (Front-end specifications) respectively describe security standards and the data model to which distributing PSPs should adhere to.

[50] Authentication services are relevant to all core services (i.e., Access management, liquidity management, transaction management).
[51] Specification #6 will be included in a future version of the rulebook

4.4.3 Distributing PSP – DESP interface requirements

The following table lists the DESP services which distributing PSPs can invoke, these are further described in Annex D2 (Back-end implementation specifications).

Distributing PSP DESP interfaces		
Service	**Function**	**Description**
Access management service (AM)	User registration and management	Individual user registration and lifecycle management.
	DEAN creation and management	Creation of an individual user Digital Euro Account Number for digital euro settlement purposes.
	Alias registration and management	Option to register an alias which can be used for digital euro payments.
	Switching	Function supporting account switching process between PSPs, while retaining access to digital euro holdings and the same Digital Euro Account Number.
Alias Lookup Service (AL)	Payment with alias	Individual user payment instructions using the alias of the payee.
	Payment request with alias	Individual user requests for a payment using the alias of the payer.

Secure Exchange of Payment Information (SEPI) Service	Payment with a QR-token	Individual user payment requests involving a QR-token creation or decoding.
	Payment with Pay-by-link (PBL)	Individual user payment requests involving a PBL token creation or decoding.
	Payment with NFC	Contactless (NFC) surrogate value generation, provision and decoding.
Fraud Risk Management Service (FR)	Fraud risk score request	Distributing PSP requests for a fraud risk score from DESP.
	Feedback loop	Distributing PSP submission of fraudulent transactions related relevant data or transactions that were reassessed as non-fraudulent to DESP.
Dispute Management Service (DM)	Pre-dispute	Distributing PSP pre-dispute creation and status updates.
	Dispute	Distributing PSP dispute creation and status updates.
Data Exchange Service (DE)	Import data from DESP	PSP request to retrieve machine-readable data from DESP such as specific pre-defined reports or queries, e.g. for reconciliation or parameter data updates.
	Export data to DESP	PSPs submission of data, e.g. reports and statistics.

Settlement Service (SE)	Funding and Defunding Transaction	PSP funding request that allows a digital euro user to acquire digital euros, in exchange for either cash or commercial bank money, creating a direct liability of the Eurosystem towards that digital euro user. PSP defunding request that allows a digital euro user to exchange digital euro with cash or commercial bank money.
	Payment Transaction	A digital euro transaction, initiated by either payer or payee PSP, and confirmed by the corresponding PSP.
	Combined Transaction	Combined transaction is a digital euro transaction involving payment with funding (reverse waterfall) or payment with defunding (waterfall).
	Reservation Transaction	Validation of digital euro transaction subject to pre-authorisation from an individual digital euro user.
	Refund Transaction	Validation of digital euro payment transaction that involves refund from the payee to the payer.
Offline Issuance component	Funding and Defunding transaction	Funding offline digital euro holdings with commercial bank

		money or online digital euro; defunding offline digital euro holdings to a non-digital euro payment account or online digital euro.

Implemented interfaces are subject to certification procedures as described in Annex A1 (Testing, certification and approval

4.5 Acquiring PSP technical implementation requirements

This subsection introduces the implementation specifications for acquiring PSPs serving digital euro business users, government users, and other public entity users. Like for distributing PSPs the implementation specifications are further detailed in Annex D1 (Front-end implementation specifications) and Annex D2 (Back-end implementation specifications)

Front-end requirements for acquiring PSPs are documented in specification #2 (Business user PSP requirements), specification #4 (Acceptance solution requirements), and specification #5 (Common services). The back-end implementation specifications in Annex D2 prescribe how acquiring PSPs can invoke services in the DESP domain. The specifications span across the domains depicted in

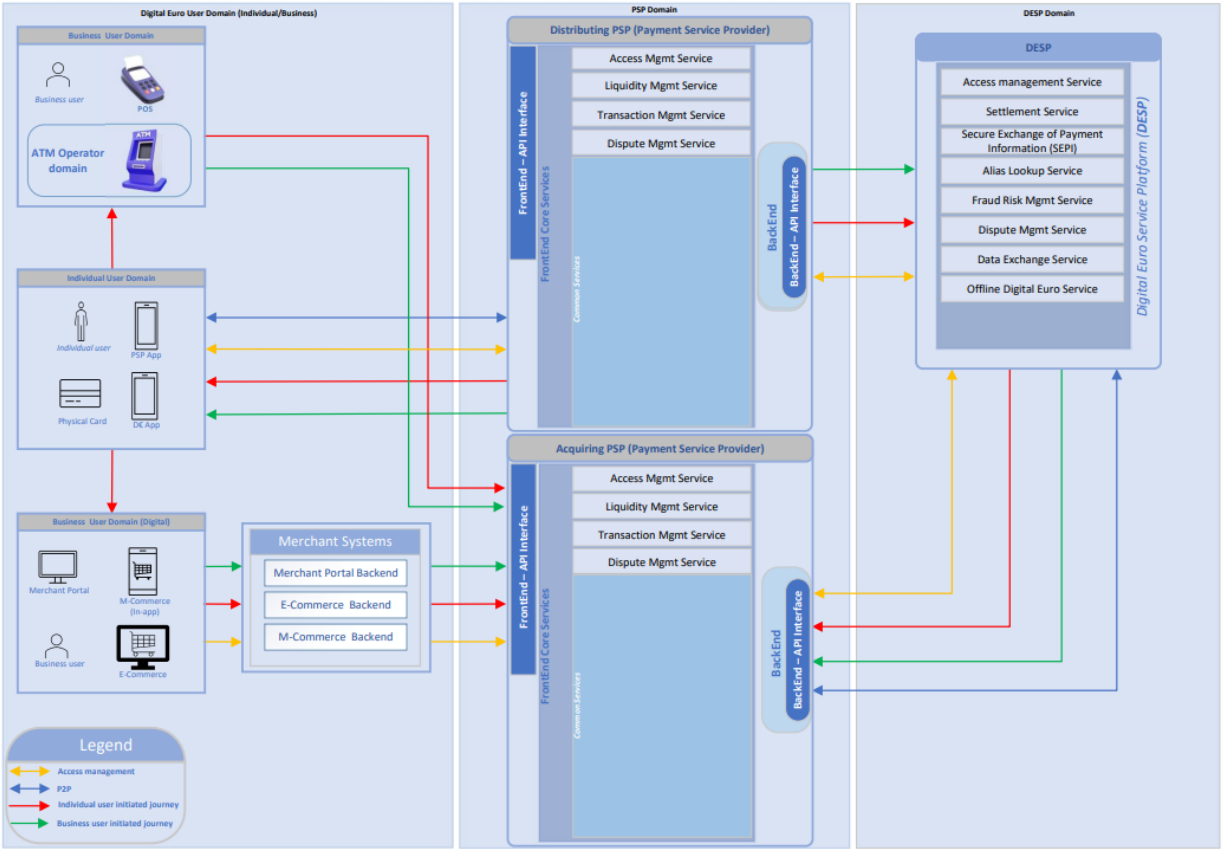

Figure 4-1.

TER.11 Acquiring PSPs shall implement the specifications in Annex D1 relevant to the digital euro payment services they offer.

TER.12 Acquiring PSPs shall implement the specifications in Annex D2 relevant to the digital euro payment services they offer.

A future version of the rulebook will include implementation specifications for the offline wallet SDK, offline payment instruments, and integration with the DESP offline issuance component[52].

4.5.1 Acquiring PSP – Business user PSP requirements

The following tables lists the services per acceptance solution made accessible by acquiring PSPs through which digital euro payment services are executed as depicted in

[52] Implementation specifications for the offline functionalities of the digital euro will be further detailed when a vendor for the offline solution is selected.

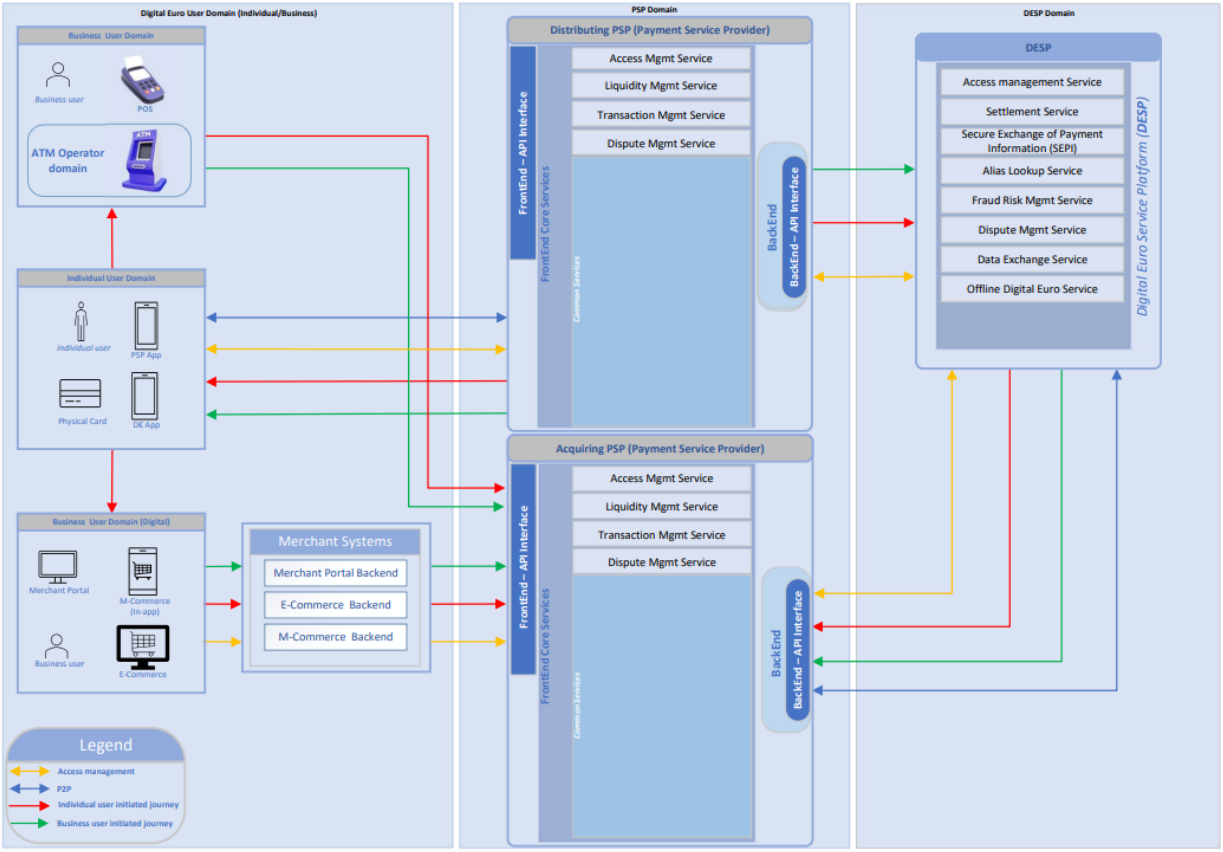

Figure 4-1. The tables refer to the relevant implementation specifications and chapters in Annex D1, which are further detailed in specification #4. The current version of the rulebook prescribes implementation specifications for e-commerce, m-commerce transactions and a limited set of specifications for ATM services. A future version of the rulebook will include specifications for POS terminals. Moreover, some specifications in this overview may still have placeholders.

Acquiring PSP acceptance solutions		
Acceptance solutions	**Service**	**Specification**
E-commerce	General requirements	▪ Specification #4 – 4.1.1 (Functional requirements[53])

[53] Including, digital euro payment method, visual consistency and branding, user experience, online notifications to the user

		▪ Specification #4 – 4.1.2 (Non-functional requirements[54]
	E-commerce payment	• Specification #4 – 4.2.2 (QR-code) • Specification #4 – 4.2.3 (Alias) • Specification #4 – 4.2.4 (DEAN) • Specification #4 – 4.2.5 (Pay-by-link)
	Recurring payment on e-commerce	• Specification #4 – 4.3.2 (QR-code) • Specification #4 – 4.3.3 (Alias) • Specification #4 – 4.3.4 (Pay-by-link) • Specification #4 – 4.3.5 (Recurring payment management)
	Pre-authorisation on e-commerce	• Specification #4 – 4.4.2 (QR-code) • Specification #4 – 4.4.3 (Alias) • Specification #4 – 4.4.4 (Pay-by-link) • Specification #4 – 4.4.5 (pre-authorisation management)
	Refund on e-commerce	• Specification #4 – 4.5

[54] Including, supported operating systems

M-Commerce	General requirements	▪ Specification #4 – 5.1.1 (Functional requirements[55]) ▪ Specification #4 – 5.1.1 (Non-functional requirements[56]
	M-commerce payments via PSP or Digital Euro App	• Specification #4 – 5.2
	Recurring payment on m-commerce	• Specification #4 – 5.3
	Pre-authorisation on m-commerce	• Specification #4 – 5.4
POS	General requirements	▪ Specification #4 – 6.1.1 (Functional requirements)
ATM[57]	Manual funding	• Specification #4 – 7.1.2 (Card) • Specification #4 – 7.1.3 (QR code)
	Manual defunding	• Specification #4 – 7.2.2 (Card) • Specification #4 – 7.2.3 (QR code)
	Account balance inquiry and transaction management transaction history[58]	• Specification #4 – 7.3

[55] Including, digital euro payment method, visual consistency and branding, user experience, online notifications to the user
[56] Including, supported operating systems
[57] ATM specifications have not been aligned with the latest version of the E2E flows (Annex B2), a consistent version of the ATM specifications with the E2E flows will be included in a future version of the rulebook.
[58] Transaction history will only be available for online digital euro payments.

4.5.2 Acquiring PSP front-end requirements

The following table lists services to be integrated in the acquiring PSP service domain as depicted in Figure 4-1. These are further detailed in specification #2 and specification #5.

Acquiring PSP services		
Core service	**Service and description**	**Specification**
Access management	**Account management:** Management of accounts for business users such as checking the validity of the link to the non-digital euro payment account	• Specification #2 – 6.1 ▪ Specification #5 – 7.2: Notification service[59]
	non-digital euro payment account status checks and account balance checks to validate if the account is active, live, ready for transactions, and (reverse) waterfall is needed.	• Specification #5 – 4.7: non-digital euro payment account service
Liquidity management	**Fund management:** Management of rules to manage funds in non-digital euro payment account (debit, credit, block, release)	• Specification #5 – 5.2: Funds management service
Transaction management	**Payment initiation:** Management of payment requests: initiated by a digital euro user (covering all payment instruments)	• Specification #2 – 8.1 • Specification #5 – 4.2: Alias look-up dispatch service • Specification #4.3 – PSP identifier look-up dispatch service

[59] Reason codes for this service are captured in the notification service in specification #5.

		• Specification #5 – 6.5: Tokenisation service • Specification #5 – 4.6: Link creation service ▪ Specification #5 – 7.2: Notification service[60]
	Recurring payment: Management of recurring payment (set-up, modification, termination, recurring payment transaction)	• Specification #2 – 8.2 ▪ Specification #5 – 7.2: Notification service[61]
	Payment processing: Invoked during a payment transaction process after payment initiation in relation to the DESP	• Specification #5 – 6.2 Payment processing service
	Fraud and risk: Management of central score and local fraud and sanction controls to block litigious or suspicious transactions according to the current regulation	• Specification #5 – 6.6 Fraud and risk service
Dispute management	Updated Dispute management specifications will be included in a future rulebook version	
Offline Distribution service	Message transmission for (de)funding transactions. Connected on one side with digital euro user wallets and on the other side, with the PSP's back-end system and the DESP to perform funding and defunding operations and online integrity checks.	

Specification #5 describes common services relevant for both distributing PSPs and acquiring PSPs. Additional services in specification #5 not mapped to one of the core services in the table above are,

[60] Reason codes for this service are captured in the notification service in specification #5.
[61] Reason codes for this service are captured in the notification service in specification #5.

authentication services[62]. Specifications for authentication services will be included in a future version of the rulebook.

Specification #6 (Technical standard)[63] and #7 (Data management) of Annex D1 (Front-end specifications) respectively describe security standards and the data model to which acquiring PSPs should adhere to.

4.5.3 Acquiring PSP – DESP interface requirements

The following table lists the DESP services which acquiring PSPs can invoke. These are further described in Annex D2 (Back-end implementation specifications).

Acquiring PSP DESP interfaces		
Service	**Function**	**Description**
Access management service (AM)	User registration and management	Business user registration and lifecycle management.
	DEAN creation and management	Creation of business user Digital Euro Account Number for digital euro settlement purposes.
Alias Lookup Service (AL)	Payment request with alias	Business user request of a payment using the alias of the payer.
Secure Exchange of Payment Information (SEPI) Service	QR-token creation	Business user request involving a QR-token creation from DESP via their PSP.
	Pay-by-link token creation	Business user request involving a PBL token creation for sales transaction in remote environment/e-commerce.
Dispute Management Service (DM)	Pre-dispute	Acquiring PSP pre-dispute status updates.

[62] Authentication services are relevant to all core services (i.e., Access management, liquidity management, transaction management).
[63] Specification #6 will be included in a future version of the rulebook

	Dispute	Acquiring PSP dispute status updates.
Data Exchange Service (DE)	Import data from DESP	PSP request to retrieve machine-readable data from DESP such as a specific pre-defined reports or queries, e.g. for reconciliation or parameter data updates.
	Export data to DESP	PSPs submission of data, e.g. reports and statistics.
Settlement Service (SE)	Funding and Defunding Transaction	Funding is a process whereby a digital euro user acquires digital euros, in exchange for either cash or non-digital euro payment account. Defunding is a process whereby a digital euro user exchanges digital euro with cash or commercial bank money.
	Payment Transaction[64]	A digital euro transaction, initiated by either payer or payee PSP, and confirmed by the corresponding PSP.
	Combined Transaction	A digital euro transaction involving payment with funding (reverse waterfall) or payment with defunding (waterfall).
	Reservation Transaction	A digital euro transaction subject to pre-authorisation

[64] In line with the mandatory activation of (reverse) waterfall for business users, the acquiring PSP will only initiate combined transactions.

		between a business user and an individual user.
	Refund Transaction	A digital euro payment transaction that involves refund from the payee to the payer.
Offline Issuance component	Funding and Defunding transaction	Funding offline digital euro holdings with commercial bank money or online digital euro; defunding offline digital euro holdings to a non-digital euro payment account or online digital euro.

Implemented interfaces are subject to certification procedures as described in Annex A1 (Testing, certification and approval).

5 Risk Management Requirements

5.1 Section overview

This section sets out the general risk management principles and rules for digital euro scheme participants. While this section focuses on fraud risk and operational risk, payment risks are covered in Annex E1. Additional risk domains are expected to be incorporated either in this section or in Annex E1 after the completion of the ongoing risk analysis and review. Potential domains for investigation are financial crime risk (including anti-money laundering, counter-terrorism financing and sanction evasion), privacy risk and legal risk.

In line with the scheme's responsibility to manage risks across the digital euro, additional risks and corresponding mitigations may be incorporated as new risk scenarios are identified and assessed through ongoing analysis, review and scheme participants' feedback.[65] The purpose of these rules is to manage risks, safeguard the integrity of the digital euro scheme, supporting end-users' trust and safety.

5.2 Fraud risk

5.2.1 Fraud risk overview

Definition

Fraud in the context of the scheme refers to both (i) "*Unauthorised payment transactions made, including as a result of the loss, theft or misappropriation of sensitive payment data or a payment instrument, whether detectable or not to the payer prior to a payment and whether or not caused by gross negligence of the payer or executed in the absence of consent by the payer ('unauthorised payment transactions'[66])*" and (ii) *"Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to give the instruction to do so to the payment service provider, in good-faith, to a payment account it believes belongs to a legitimate payee ('manipulation of the payer')[67]*".

Fraud rules mitigate the risks of unauthorised transactions and manipulation of the payer for digital euro payment transactions. These rules include controls to prevent unauthorised transactions, and manipulation of payers through scams and impersonation, rules pertaining to payment authorisation to reduce risks of fraud by social engineering, phishing, or unauthorised access to payers' payment initiation functions, rules for interacting with the digital euro Risk and Fraud Management (RFM) component in the Digital Euro

[65] This analysis also includes payment instrument risk rules, a former chapter of Annex E1.
[66] EBA/GL/2018/05 Part 3.1 Guidelines on fraud data reporting applicable to Payment Service Providers, Guideline 1: Payment transactions and fraudulent payment transactions - Paragraph 1.1.a.
[67] EBA/GL/2018/05 Part 3.1 Guidelines on fraud data reporting applicable to Payment Service Providers, Guideline 1: Payment transactions and fraudulent payment transactions - Paragraph 1.1.b.

Service Platform (DESP), which provides transaction-level risk scoring to help scheme participants in identifying fraudulent transactions, rules establishing the role of the Scheme governing authority in fraud intelligence and awareness, and rules to facilitate cooperation between scheme participants during fraud investigations.

5.2.2 Fraud and dispute management

End-users should file disputes when they believe they have been victims of fraud and wish to challenge a payment; however, it is to be noted that fraud is characterised by an intent to deceive, which cannot always be realistically assessed by the end-user. In practice, to align with end-user experience, the valid reasons for disputes are based on factual outcomes rather than assumptions of intent. For example, an end-user may report a dispute because they notice that a digital euro transaction was processed several times or a product was never delivered without requiring the end-user or scheme participants to assess upfront whether these disputes are linked to a deceptive intent constituting fraud or not. The list of valid reasons to dispute are detailed in Section 6 on dispute management.

5.2.3 Onboarding and established business relationship with end-users

RMR.01 Scheme participants shall, when onboarding natural persons and legal entities for digital euro payment services, comply with all obligations arising under the European Union anti-money laundering and counter-terrorist financing framework, including any amendment thereof, as well as all applicable European Union targeted financial restrictive measures.

RMR.02 When onboarding a business user, a scheme participant shall assign the business user one or more Merchant Category Codes (MCCs) representing the business user's activity in line with ISO 18245 standard.

RMR.03 When onboarding a business user, an acquiring PSP shall verify that the business user's commercial and legal names do not attempt to illicitly impersonate other businesses or reuse, imitate, or incorporate a well-known name, such as that of registered corporations, financial institutions, or governmental entities in a manner likely to deceive payers.

5.2.4 Verification of payees

RMR.04 A payer's PSP shall offer the payer verification of payee services, in compliance with the relevant provisions in the Digital Euro Regulation, including any amendments thereof.

5.3 Interaction with the Risk and Fraud Management (RFM) component

5.3.1 Usage of the RFM component[68]

Effective fraud detection and prevention are essential components of the safety and soundness of the digital euro. The DESP operator manages the RFM component, which aids scheme participants in identifying fraudulent transactions that may not be detected through their own tools alone and provides standardised situation awareness and threat intelligence reports as well as real-time fraud scores, which are available to the scheme participants. The RFM component serves as a tool assisting scheme participants to comply with their legislative and regulatory requirements on fraud and to mitigate fraud risk in the digital euro. A scheme participant is encouraged but not required to include the RFM risk score as an additional parameter in their fraud prevention system.

RMR.05 A scheme participant shall interact with the RFM component as required in this subsection when processing online transactions. The requirements under this section are not applicable to offline digital euro transactions.

RMR.06 A scheme participant shall always take the final decision for either rejecting, holding, stopping, or releasing transactions with the objective of ensuring the security, integrity, and reliability of payment services for payment service end-users.

RMR.07 A scheme participant shall send a risk score request for each online transaction related to P2P, e-commerce and POS use cases to the RFM component during the pre-settlement process in accordance with requirements laid down in Annex X on interaction with the RFM component (the annex will be developed in collaboration with the RFM component service provider). The RFM component will provide a response, including a risk score and reasoning.

RMR.08 A scheme participant is encouraged, but not required, to make use of the provided risk score.

RMR.09 A scheme participant shall decide to reject, hold, stop, or release transactions, when required or allowed under applicable EU or national law, including for reasons related to the prevention of fraud, with the objective of ensuring the security, integrity, and reliability of payment services for payment service end-users.

[68] Interactions with the RFM component for transactions involving different intermediaries (e.g. when the digital euro intermediary and the commercial money intermediary are two different scheme participants) will be addressed in a future version of the rulebook if needed.

RMR.10 For digital euro transactions, a scheme participant shall not send the settlement message before it has received the RFM risk score for the transaction, except where the RFM response exceeds the specified maximum time limit. *This will be determined at a later stage to address potential incident of the RFM component*

RMR.11 Only for POS transactions, a scheme participant may initiate the settlement process before receiving the RFM risk score for the transaction.

5.3.2 Feedback loop

RMR.12 A scheme participant shall report to the RFM component both i) newly confirmed fraud cases, and ii) previously reported transactions that were subsequently re-assessed as non-fraudulent in accordance with requirements in the Annex X on interaction with the RFM component the annex will be developed in collaboration with the RFM component service provider

5.3.3 Fraud intelligence and situational awareness

The Scheme governing authority facilitates fraud intelligence for the digital euro across scheme participants. This includes setting up fraud reporting requirements, information sharing (e.g. about known and emerging practices of fraudsters, fraud trends), and thus supporting PSPs to learn from the expertise and experience to further improve fraud prevention across the digital euro scheme.

RMR.13 Scheme participants shall comply with the fraud intelligence and escalation program implemented by the Scheme governing authority in order to reduce frauds in the digital euro (the program will be defined at a later stage).

5.3.4 Payment initiation, review, consent, authentication and confirmation

RMR.14 A scheme participant shall comply with strong customer authentication requirements in line with the requirements arising under the European Union payment service regulatory framework, including any amendment thereof.

RMR.15 For e-commerce, m-commerce, P2P, and QR-code payee-initiated transactions, the payer's PSP shall, before and after each transaction, provide a payer with information about the amount, transaction type and end-user name of the payee, to assist the payer in identifying unauthorised or incorrect transactions.

RMR.16 For POS transactions, excluding QR-code transactions the payer's PSP shall, before and after each transaction, provide the payer with information about the amount to assist the payer in identifying unauthorised or incorrect transactions.

RMR.17 An acquiring PSP shall enable business users to use their registered or commercial name in their payment message. It is recommended that the choice of name aligns with the name most likely recognised by the payee's customers, thereby reducing the risk of misunderstanding or disputes and ensuring clear identification of the payee.

RMR.18 The payer's PSP shall send a confirmation of transaction success or failure to the payer. The payee's PSP shall send a confirmation of transaction success to the payee. The confirmation shall include the amount, date, time, end-user name of the counterpart, and location to provide immediate feedback, help verify authenticity, and reduce false non-payment claims.

5.3.5 Investigation assistance between scheme participants

RMR.19 A scheme participant shall provide investigation assistance to the Scheme governing authority or to other scheme participants in the course of investigation of potentially fraudulent activities such as liaising with relevant stakeholders (such as their individual users, business users and third-party service providers).

RMR.20 A scheme participant shall respond to a request from the Scheme governing authority or from another scheme participant in a timely manner, at the latest within five business days.

5.4 Operational risks

Operational risk is defined as the risk of negative financial, business and/or reputational impacts on digital euro payment services (Section 1.5.) resulting from inadequate or failed internal governance and business processes, people, systems, or from external events. Payment service providers participating in the digital euro scheme shall implement appropriate technical and organisational measures, including state-of-the-art best practices for operational and security risk management, ensure a high level of operational resilience and contribute to a high operational resilience of the digital euro scheme.

RMR.21 In order to achieve a harmonised and high level of digital operational resilience, scheme participants shall meet the requirements laid down by the Regulation (EU) 2022/2554 (DORA) and the associated regulatory technical standards and implementing technical standards,

including any amendments thereof, for the provision of digital euro payment services. In this regard, scheme participants shall consider the provision of digital euro payment services as a critical or important function, as defined in DORA. Taking into account that certain PSPs are excluded from the scope of DORA (such as post office giro institutions or credit unions), a proportionality approach shall apply when evaluating the compliance with the requirements under this section.

RMR.22 Scheme participants shall ensure adherence to EU data protection rules, specifically meeting the requirements of Regulation (EU) 2016/679 (GDPR), including any amendment thereof, ensuring the security of personal data, and meeting digital euro data privacy requirements at all times.

5.4.1 Business continuity requirements

Business continuity is defined as the capability of a scheme participant to continue the delivery of digital euro payment services within predefined time frames at predefined capacity during a disruption.

RMR.23 Scheme participants shall implement and test a comprehensive business continuity policy to ensure the continuity of the provision of digital euro payment services, in line with the ICT business continuity policy as defined in DORA, and meeting the Reliability and performance requirements of the digital euro rulebook (Section 4.3).

RMR.24 In exceptional circumstances, including repeated or major incidents or the existence of a significant threat that may compromise the continuity of digital euro services, the Scheme governing authority may request that the scheme participant shares its business continuity policy, as defined in DORA, for the provision of digital euro payment services, or parts thereof.

RMR.25 Scheme participants shall report major incidents to the Scheme governing authority when the incident affects the provision of the digital euro payment services. *(Incident classification and reporting requirements will be determined in a later stage in Annex C1*).

RMR.26 Scheme participants shall ensure adherence to the requirements on payment service user relationship management as defined in EBA/GL/2019/04 Section 3.8 for the provision of digital euro payment services. Scheme participants shall notify end-users in the event of major incidents or significant threats that affect or could affect digital euro payment services.

RMR.27 Scheme participants shall designate and provide to the Scheme governing authority the contact information of one business continuity representative and one alternate for the provision of digital euro payment services. Scheme participants shall submit this information without undue delay, during the scheme onboarding process and whenever there is a change in the designated contact persons.

RMR.28 The Scheme governing authority organises logistic exercises with an annual frequency to test communication tools and the reachability of the business continuity contacts. Scheme participants shall participate upon the Scheme governing authority's invitation.

RMR.29 The Scheme governing authority may organise regular business continuity and crisis management exercises to test the continuity of the provision of digital euro payment services under exceptional but plausible scenarios. Scheme participants are encouraged to participate upon the Scheme governing authority's invitation.

5.4.2 Cyber and ICT risk requirements

For the purpose of this chapter, cyber risk shall be considered in line with ICT risk definition and requirements set out in DORA. Therefore, in the context of digital euro, it means any reasonably identifiable circumstance in relation to the use of network and information systems which, if materialised, may compromise the security of the network and information systems[69], of any technology dependent tool or process, of operations and processes, or of the provision of services by producing adverse effects on the provision of digital euro payment services.

RMR.30 Scheme participants shall implement and test a sound, comprehensive and well-documented ICT risk management framework as part of their overall risk management system, which enables them to address ICT risk, quickly, efficiently and comprehensively and to ensure that the requirements in the Reliability and performance requirements section (Section 4.3) of this rulebook are met.

RMR.31 In exceptional circumstances, including repeated or major incidents or the existence of a significant threat that may compromise the continuity of digital euro services, the Scheme governing authority may request that the scheme participant shares its ICT risk management

[69] As defined in Directive (EU) 2022/2555 'security of network and information systems' means the ability of network and information systems to resist, at a given level of confidence, any event that may compromise the availability, authenticity, integrity or confidentiality of stored, transmitted or processed data or of the services offered by, or accessible via, those network and information systems.

framework, as defined in DORA, supporting the provision of digital euro payment services, or parts thereof.

RMR.32 Taking into account the digital euro real-time environment, scheme participants shall adequately maintain redundant ICT assets and capacities, including when the services are provided by third parties, to promptly switchover from a primary to a redundant ICT asset and capacity ensuring the continuity of the provision of digital euro payment services.

RMR.33 Scheme participants are recommended to exchange amongst themselves and with the Scheme governing authority cyber threat information and intelligence, within trusted communities, as defined in DORA, raising awareness in relation to cyber threats that may affect digital euro payment services.

RMR.34 Scheme participants shall notify significant cyber threats, as defined in DORA, to the Scheme governing authority when they deem the threat to be of relevance for the digital euro scheme. The Scheme governing authority may provide alerts to relevant stakeholders.

5.4.3 Third-party risk requirements

Third-party risk is defined as the risk of financial or operational impact from scheme participants relying on outside parties (or subcontractors of the latter) to provide digital euro payment services that fail to provide services or perform activities on their behalf.

RMR.35 Scheme participants shall manage third-party risk in line with DORA requirements on ICT third-party risk management.

RMR.36 Scheme participants that have in place contractual arrangements for the use of third-party services and potential sub-contractors for the provision of digital euro payment services shall, at all times, remain fully responsible for compliance with, and the discharge of, all obligations under the rulebook.

RMR.37 Scheme participants shall ensure that contractual arrangements with third-party service providers (including their potential subcontractors) for the provision of digital euro payment services are in line with the Reliability and performance requirements section of this rulebook (Section 4.3).

RMR.38 Scheme participants shall make available to the Scheme governing authority, upon its request, the register of third-party service providers supporting scheme participant's digital euro payment services as defined in DORA, along with any information deemed necessary to the provision of such services. Scheme participants shall ensure that their contracts with third-party service providers enable them to share such information with the Scheme governing authority.

RMR.39 The scheme participant's contractual arrangements on the use of third-party services for the provision of digital euro payment services shall include:

- The obligation of the third-party service provider to fully cooperate with the Scheme governing authority; and

- In exceptional circumstances, including in light of repeated or major incidents or the existence of a significant threat, the right of unrestricted access, inspection and audit by the scheme participants and their auditors, and the right to have effective access to data and premises relating to the use of services supporting the provision of digital euro payment services

5.5 Potential other risks

Placeholder.

Potential domains for investigation are: financial crime risk (including anti-money laundering, counter-terrorism financing and sanction evasions), privacy risk and legal risk.

6 Dispute management requirements

As the draft section on dispute management requirements is currently undergoing a wider review to further detail the underlying framework, no immediate changes to the draft rulebook were incorporated in comparison to the previous draft rulebook version 0.9. The input received during the consultation on draft rulebook version 0.9 will directly contribute to the ongoing work, which will be reflected into a subsequent version of the draft rulebook.

6.1 Section overview

This section defines the requirements of the dispute management services for the digital euro scheme. These requirements are outlined through functional rules, dispute reasons and scenarios, and summarised process flows. Detailed process flows are included in Annex B2 End-to-end flows, along with all other digital euro end-to-end flows.

6.2 Dispute management overview

A dispute management process allows a digital euro payer to challenge an eligible consumer-to-business or an eligible peer-to-peer transaction charged to their digital euro payment account.

Eligible transactions cover consumer-to-business and peer-to-peer transactions, the actors involved in the dispute management process are: the payer, the payee, the payer's PSP, the payee's PSP, and the DESP operator. A payer's PSP is a distributing PSP. A Payee's PSP is a distributing PSP when servicing natural person and an acquiring PSP when servicing a business user.

DMR.01 If the payer has had more than one PSP, the PSP servicing the digital euro payment account from which the disputed transaction was debited shall be considered as payer's PSP.

DMR.02 If the payee has more than one PSP, the PSP servicing the digital euro payment account to which the disputed transaction was credited shall be considered the payee's PSP.

DMR.03 Each dispute management process arising in the context of the digital euro scheme shall be associated with a specific digital euro transaction. The dispute management process[70] consists of:

[70] A possible arbitration phase, which can follow the dispute phase, is not governed by this rulebook.

(1) **A pre-dispute phase**, allowing the payer to seek resolution with the payee with the intermediation of their respective PSPs and, if no agreement is reached

(2) **A dispute phase**, for PSPs to agree on a decision on the dispute

DMR.04 A payer disputes a digital euro transaction by providing information and supporting documentation to explain the reason for the dispute. Based on the information received, the payer's PSP classifies the dispute under a specific 'dispute reason' and sets a 'dispute amount', which may differ from the original transaction amount.

DMR.05 The DESP Dispute component is the infrastructure that enables the exchange of messages, notifications, and supporting documentation between PSPs in the context of a dispute management process.

6.2.1 Dispute eligibility requirements

DMR.06 Scheme participants shall comply with the requirements governing the eligibility of a digital euro payment transaction for dispute.

Dispute Eligibility Requirements	
General requirements:	
DM-020-001	A scheme participant shall only accept dispute initiation requests submitted by the digital euro payer directly.
DM-020-002	A scheme participant shall ensure that every dispute management process is associated with a unique digital euro payment transaction identifier.
DM-020-003	A scheme participant shall verify that the disputed transaction falls under the category of online digital euro payment transactions before proceeding with the dispute process.
DM-020-004	A scheme participant shall ensure that no prior or active dispute management process exists for the same transaction and reason before accepting a new dispute.
End-to-end flows – Dispute Management	
TM-6.1	Pre-dispute
TM-6.2	Dispute
The end-to-end flows are detailed in Annex B2 End-to-end flows of this rulebook.	

6.2.2 Supporting documentation requirements

DMR.07 The scheme participant and digital euro user shall provide documentation to support their respective claims.

Supporting documentation	
General requirements:	
DM-020-005	PSPs shall assign a hashed value to each piece of supporting documentation provided during a dispute management process, regardless of whether the piece of documentation was provided by the PSP itself or by the respective digital euro user.
DM-020-006	The DESP – Dispute component shall validate the correctness of the hashed value of each piece of documentation, without being able to access its content
DM-020-007	The DESP – Dispute component shall not be able to see data related to payer and payee, the supporting documentation and their content as well as business reasoning – this will be encrypted and only visible to the PSPs participating in the process.
DM-020-008	The DESP – Dispute component shall only store the inbound and outbound hashed values of the encrypted pieces of documentation for consistency reasons
DM-020-009	The DESP – Dispute component shall store all statuses and make it accessible to PSPs for future reference.
DM-020-010	The aggregate supporting documentation shall not exceed 50 megabytes per dispute management process, per digital euro user involved.
DM-020-011	Each piece of supporting text documentation shall not exceed two (2) megabytes per file.
DM-020-012	Each piece of supporting image or photo documentation shall not exceed ten (10) megabytes per file.
DM-020-013	Each piece of supporting spreadsheet documentation shall not exceed five (5) megabytes per file.

DMR.08 Scheme participants shall provide supporting documentation in any of the formats listed in the table below within the indicated maximum data size.

Supported formats		
Text documents (up to 2 megabytes per file)	8-Bit UCS Transformation Format	UTF
	Open Document Text	.odt
	Microsoft Word	.docx, .doc
	Portable Document Format	.pdf
Images or photos (up to 10 megabytes per file)	Portable Network Graphic	.png

	Tagged Image File Format	TIFF
	JPEG File Information Format	JFIF
	Joint Photographic Experts Group	.jpeg, .jpg
	Rich text format	.rtf
	Text document	.txt
	Portable Document Format	.pdf
	OpenDocument Graphics	.odg
Spreadsheets (up to 5 megabytes per file)	Comma separated values	CSV
	Open Document Spreadsheet	.ods
	Microsoft Excel	.xsl .xlsx

6.2.3 Dispute status

The dispute management status describes the state of advancement of a dispute management process.

DMR.09 The status shall be updated by either (1) the DESP - Dispute component, (2) the payer's PSP or the payee's PSP. Depending on the status, other parties involved in the dispute management process shall be notified.

Statuses for a digital euro dispute management process with respective roles of involved parties are listed in the table below.

Possible statuses						
Status	Status trigger	Payer	Payer's PSP[71]	DESP	Payee's PSP[72]	Payee
Pre-dispute request accepted	The DESP has accepted the received pre-dispute request		Status notified	Updates status	Status notified	Status notified

[71] Payer's distributing PSP
[72] Payee's distributing PSP (in case of peer-to-peer transaction disputes) or payee's acquiring PSP (in case of consumer-to-business transaction disputes)

Pre-dispute request rejected	The DESP has rejected the pre-dispute request	Status notified	Status notified	Updates status		
Pre-dispute response accepted	The DESP has accepted the pre-dispute response	Status notified	Status notified	Updates status	Status notified	
Pre-dispute response rejected	The DESP has rejected the pre-dispute response			Updates status	Status notified	Status notified
Pre-dispute positive	The payer's PSP has accepted the pre-dispute response	Status notified	Updates status	Status notified	Status notified	Status notified
Pre-dispute negative	The payer's PSP has rejected the pre-dispute response on behalf of the payer	Status notified	Updates status	Status notified	Status notified	Status notified
Pre-dispute closed	Either: • The payer has accepted the pre-dispute response, and the remediating action has been carried out • The payer has rejected the pre-dispute response • The pre-dispute has escalated to the dispute phase	Status notified	Status notified	Updates	Status notified	Status notified
Dispute requested	The payer's PSP has sent a dispute request message to the DESP		Status notified	Updates status		
Dispute request accepted	The DESP has accepted the Dispute request		Status notified	Updates status	Status notified	Status notified
Dispute request rejected	The DESP has rejected the Dispute request	Status notified	Status notified	Updates status		
Dispute response accepted	The DESP has accepted the Dispute response	Status notified	Status notified	Updates	Status notified	
Dispute response rejected	The DESP has rejected the Dispute response			Updates	Status notified	Status notified
Dispute positive	The payer's PSP has accepted the Dispute response	Status notified	Updates	Status notified	Status notified	Status notified
Dispute negative	The payer's PSP has rejected the Dispute response	Status notified	Updates	Status notified	Status notified	Status notified
Dispute closed	Either: • The payer's PSP has accepted the dispute response, and the	Status notified	Status notified	Updates	Status notified	Status notified

	remediating action has been carried out • The payer's PSP has rejected the dispute response • The dispute has escalated to an arbitration case					
Dispute arbitration successful	The payer has won the arbitration case	Status notified	Updates	Status notified	Status notified	Status notified
Dispute arbitration unsuccessful	The payee has won the arbitration case	Status notified	Updates	Status notified	Status notified	Status notified

6.3 Dispute management process

This section provides high-level dispute management functional rules and a high-level process description, including applicable timeframes. A detailed process and end-to-end flow description is provided in Annex B2 End-to-end flows of this rulebook.

6.3.1 Dispute process requirements

Requirements governing the dispute management process, including timeframes, pre-dispute phase and dispute phase functional rules are provided in the table below.

Functional requirements	
General functional requirements:	
DM-030-001	Disputes shall be initiated within 90-180 business days since the disputed transaction settlement date[73], if the dispute transaction has settled.
DM-030-002	Disputes shall be initiated within 90-180 business days since the disputed transaction reservation authorisation date, if the disputed transaction has not settled.
PSP functional rules:	
DM-030-003	The payer's PSP shall classify the dispute under a 'dispute reason' (and reason code) and set a 'dispute amount' based on the available information and documentation.
DM-030-004	The payee's PSP shall send a pre-dispute response to the DESP – Dispute component within 10 business days of receiving a Notification of accepted pre-dispute.
DM-030-005	The payer's PSP shall send a dispute request to the DESP – Dispute component within 5 business days of the pre-dispute phase closing.
DM-030-006	The payer's PSP shall accept or reject a dispute response to the DESP – Dispute component within 10 business days after the dispute response received.

[73] Without prejudice to the right of the payer to initiate a legal proceeding in accordance with the national legal framework

DM-030-007	The payee's PSP shall send a dispute response to the DESP – Dispute component within 10 business days of receiving a Notification of accepted dispute.
DM-030-008	Business days are defined consistently with the definition provided by TARGET Services T2 and TARGET2-Securities, running from Monday to Friday, with the exception of public holidays in Germany.

6.3.2 Dispute management process

The dispute management process consists of (a) a mandatory pre-dispute phase, and – if no agreement is reached during the pre-dispute phase - (b) a dispute phase. A dispute management process escalates from pre-dispute to dispute phase if neither party have accepted the other party's response within the applicable timeframe.

a) Pre-dispute phase

The pre-dispute phase is a mandatory step for a digital euro payer to initiate a dispute management process and is intended for PSPs to facilitate the exchange of information between payer and payee via a front-end service provided by the respective PSPs. PSPs can also provide additional information, to their respective payer and payee as well as to the counterparty PSP to facilitate the resolution of a pre-dispute before it escalates to the dispute phase.

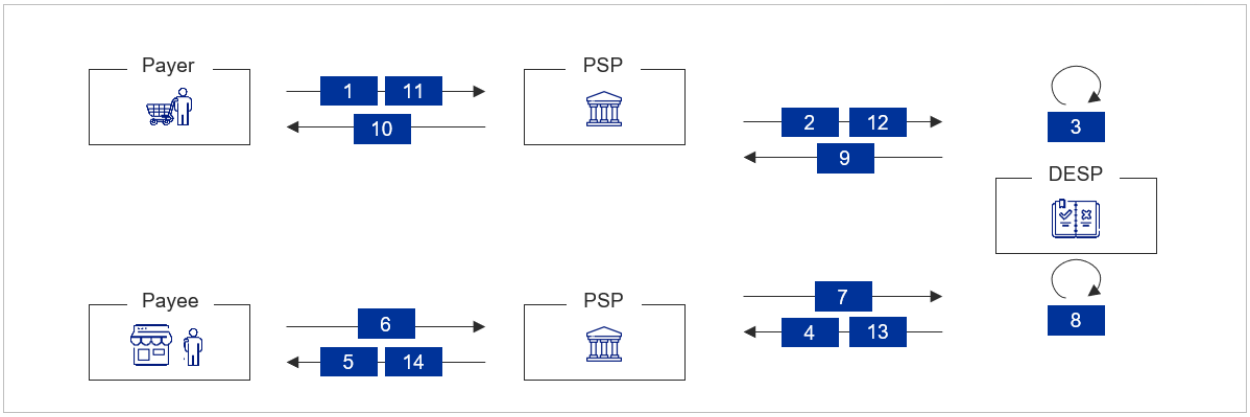

Figure 6-1 - High-level process flow for the pre-dispute phase.

Description of steps:

A digital euro payer initiates a pre-dispute with its PSP via a dedicated dispute management feature in the digital euro front-end services.

1. The payer's PSP reviews the information and documentation received, and sends a pre-dispute request to the DESP – Dispute component[74].

2. The DESP - Dispute component runs a pre-dispute request validation, based on dispute eligibility requirements (Section 6.2.1.), supporting documentation rules (Section 6.2.2), dispute process requirements (Section 6.3.1.) and back-end implementation specifications (Annex D2).

3. If the pre-dispute request is valid, the DESP – Dispute component registers a pre-dispute request acceptance, sends a notification of accepted pre-dispute request to the payee's PSP (if not valid, the DESP – Dispute component registers a pre-dispute request rejection); the status updates to "Pre-dispute request accepted" (if not valid, it updates to "Pre-dispute request rejected").

4. The payee's PSP receives and forwards the pre-dispute request to the payee.

5. The payee reviews and either accepts or rejects the pre-dispute request.

6. The payee's PSP reviews the payee's response and sends a pre-dispute response to the DESP - Dispute[75] within 10 business days of receiving the pre-dispute request.

7. The DESP - Dispute component runs a pre-dispute response validation, based on supporting documentation requirements (Section 6.2.2), dispute process requirements (Section 6.3.1.) and back-end implementation specifications (Annex D2).

8. If valid, the DESP – Dispute component registers a pre-dispute response acceptance, and forwards the pre-dispute response to the payer's PSP (if not valid, the DESP – Dispute component registers a pre-dispute response rejection); the status updates to "Pre-dispute response accepted" (if not valid, it updates to "Pre-dispute response rejected").

9. The payer's PSP receives and forwards the pre-dispute response to the payer.

10. The payer reviews and either accepts or rejects the pre-dispute response.

---

[74] The payer's distributing PSP may return to the payer to collect additional information and/or documentation
[75] The payee's distributing PSP may return to the payee to collect additional information and/or documentation

11. The payer's PSP forwards the payer's decision to the DESP – Dispute component; the status updates to "Pre-dispute positive" or "Pre-dispute negative").

12. The DESP – Dispute component forwards the decision to the payee's PSP.

13. The payee's PSP notifies the payee.

If neither the payer nor the payee have accepted the counterparty's decision, and if the payer wants to, the pre-dispute escalates to the dispute phase; the status updates to "Pre-dispute closed".

b) Dispute phase

The dispute phase is a possible subsequent phase that occurs only if the payer and the payee fail to reach an agreement during the pre-dispute phase and is intended for the payer's PSP and payee's PSP to find an agreement on the dispute. In the dispute phase, PSPs take on an active role aimed at resolving the dispute, providing additional information and documentation if applicable.

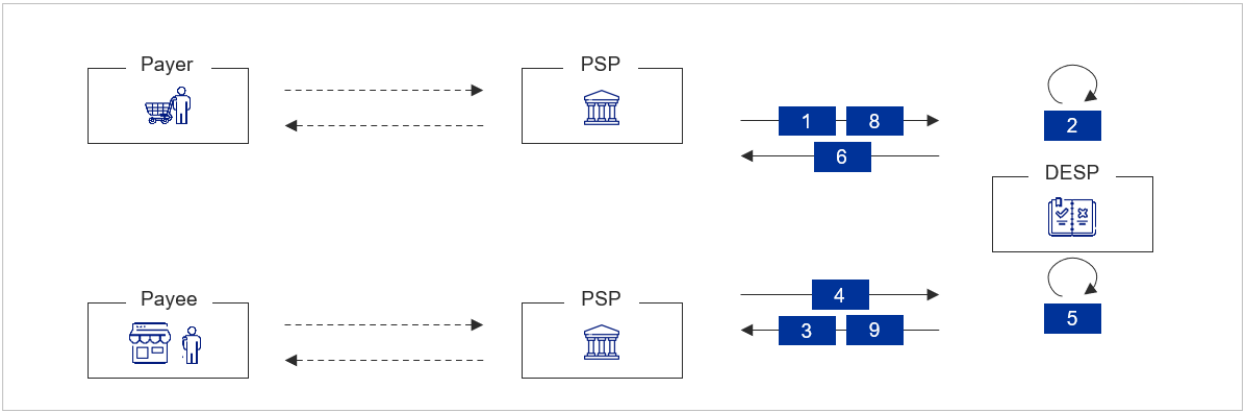

Figure 6-2 - High-level process flow for the dispute phase.

Description of steps:

1. Consistently with the functional rules governing the dispute management process, the payer's PSP sends a dispute request to the DESP – Dispute component[76] within 5 business days of the pre-dispute closing; the status updates to "Dispute requested".

[76] The payer's distributing PSP may ask the payer for additional information and/or documentation

2. The DESP - Dispute component runs a dispute request validation, based on dispute eligibility requirements (Section 6.2.1.), supporting documentation requirements (Section 6.2.2.), dispute process requirements (Section 6.3.1.) and back-end implementation specifications (Annex D2).

3. If valid, the DESP – Dispute component registers a dispute request acceptance, sends a notification of accepted dispute, and forwards the dispute request to the payee's PSP (if not valid, the DESP – Dispute component registers a dispute request rejection); the status updates to "Dispute request accepted" (if not valid, it updates to "Dispute request rejected").

4. The payee's PSP reviews, either accepts or rejects the dispute request[77], and – within 10 business days of receiving the dispute request - sends a dispute response to the DESP – Dispute component.

5. The DESP - Dispute component runs a dispute response validation, based on supporting documentation requirements (Section 6.2.2.), dispute process requirements (Section 6.3.1.) and back-end implementation specifications (Annex D2); the status updates to "Dispute response accepted" (if not valid, it updates to "Dispute response rejected").

6. If valid, the DESP – Dispute component registers a dispute response acceptance and forwards the dispute response to the payer's PSP (if not valid, the DESP – Dispute component registers a dispute response rejection).

7. The payer's PSP reviews and either accepts or rejects the dispute response, notifies the payer, and – within 10 business days of receiving the dispute response – forwards the decision to the DESP – Dispute component; the status updates to "Dispute positive" or "Dispute negative" and "Dispute closed" (if not valid, it updates to "Dispute request rejected").

8. The DESP – Dispute component forwards the decision to the payee's PSP.

9. The payee's PSP notifies the payee.

6.3.3 Dispute management process for funding, defunding transaction disputes

This is a placeholder for dispute management process for funding, defunding transactions

[77] The payee's distributing PSP may ask the payee for additional information and/or documentation

6.4 Dispute reasons

6.4.1 Reason coding conventions

Dispute reason codes identify unique dispute reasons. The code is composed of three strings, separated by a dash:

- The first three-letter string “DIS” is the same across reasons and identifies dispute management services
- The second three-letter string identifies the type of payment transaction under dispute, “TXM” for consumer-to-business and peer-to-peer transaction dispute, and “LQM” for funding, defunding transaction disputes
- The third three-digit string numbers the reasons progressively

6.4.2 Dispute reasons in consumer-to-business and peer-to-peer transaction disputes

This section provides dispute management rules and processes for the following use cases:

- E-commerce payment transactions
- M-commerce payment transactions
- POS payment transactions
- Peer-to-peer payment transactions

Valid reasons for disputing a digital euro payment transaction consist of technical and fraud reasons. The full list of valid dispute reasons is provided in the table below, including the applicability to different use cases.

Dispute reasons, reason codes, use case applicability					
Reason code	Reason	E-com	M-com	POS	Peer-to-peer
DIS-TXM-001	Single transaction not authorised by the payer	Yes	Yes	Yes	Yes
DIS-TXM-002	Single transaction with cancelled authorisation or consent debited	Yes	Yes	Yes	Yes
DIS-TXM-003	Duplicated transaction with identical transaction properties	Yes	Yes	Yes	Yes
DIS-TXM-004	Duplicated transaction with different transaction properties	Yes	Yes	Yes	Yes
DIS-TXM-005	Duplicated transaction initiated by the payee	Yes	Yes	Yes	Yes

DIS-TXM-006	Incorrect transaction amount	Yes	Yes	Yes	Yes
DIS-TXM-007	Incorrect transaction data	Yes	Yes	Yes	Yes
DIS-TXM-008	Transaction sent to incorrect payee	Yes	Yes	Yes	Yes
DIS-TXM-009	Recurring transaction not authorised by the payer	Yes	Yes	Yes	Yes
DIS-TXM-010	Misrepresentation of goods or services	Yes	Yes	Yes	No
DIS-TXM-011	Lost or stolen payment instrument	Yes	Yes	Yes	Yes
DIS-TXM-012	Payment instrument not received	Yes	Yes	Yes	Yes
DIS-TXM-013	Counterfeit payment instrument	Yes	Yes	Yes	Yes
DIS-TXM-014	Account take-over	Yes	Yes	Yes	Yes
DIS-TXM-015	PSP, payee or other entity impersonation	Yes	Yes	Yes	Yes
DIS-TXM-016	Goods or services not delivered	Yes	Yes	Yes	No
DIS-TXM-017	Counterfeit or pirated goods	Yes	Yes	Yes	No

For each dispute reason, the respective scenarios covered, conditions for initiating a dispute and supporting documentation are provided.

a. [DIS-TXM-001] Single transaction not authorised by the payer

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A single digital euro payment transaction was processed and debited from the payer's digital euro payment account without their authorisation or consent • A digital euro payment transaction was processed after the payer had declined the same digital euro payment transaction • A digital euro payment transaction was processed after the digital euro payment transaction was declined due to technical issues
Conditions for initiating a dispute	The disputed transaction is either consumer-to-business or peer-to-peer • The digital euro payment transaction was declined or not authorised by the payer • The digital euro payment transaction was processed, settled, and recorded in the payer's digital euro payment account, despite being declined or not authorised by the payer • The digital euro payment transaction was processed, settled, and recorded in the payer's digital euro payment account, despite being declined due to technical issues
Supporting documentation	To be provided by the payer and payer's PSP: • Documentation proving that the payer did not authorise the transaction • Documentation proving that the payer had declined the disputed digital euro payment transaction

	To be provided by the payee and payee's PSP: • Documentation proving that the payer had authorised the disputed digital euro payment transaction

b. [DIS-TXM-002] Single transaction with cancelled authorisation or consent debited

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A single digital euro payment transaction was initially authorised by the payer, but the authorisation or consent was subsequently cancelled by the payer; despite the cancellation, the transaction was processed and debited from the payer's digital euro payment account
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The digital euro payment transaction was cancelled by the payer • The digital euro transaction was processed, settled, and recorded in the payer's digital euro payment account, despite the cancellation of the authorisation or consent by the payer
Supporting documentation	To be provided by the payer and payer's PSP: • Documentation proving that the payer cancelled the authorisation or consent of the transaction

c. [DIS-TXM-003] Duplicated transaction with identical transaction properties

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro payment transaction was authorised once by the payer but was recorded and debited more than once with the same authorisation identifier[78] and timestamp[79]
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The payer authorised the transaction only once • The digital euro transactions were processed, settled, and recorded in the payer's digital euro payment account • The payer authorised the transaction only once
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro payment account statement clearly showing the duplicated charges for the same transaction To be provided by the payee and payee's PSP: • If applicable, transaction processing logs to support technical investigation • If applicable, purchase order, invoice, or receipt

d. [DIS-TXM-004] Duplicated transaction with different transaction properties

Scenarios covered, conditions for initiating a dispute, supporting documentation

[78] Based on data element AuthorisationCode [Au1]
[79] Based on data element CreationDateTime [Tm1]

Scenarios covered	• A digital euro payment transaction was authorised once by the payer but was recorded and debited more than once with different authorisation identifier and timestamp
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The payer authorised the transaction only once • The respective digital euro transactions were processed, settled, and recorded in the payer's digital euro payment account
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro payment account statement clearly showing the duplicated charges for the same purpose To be provided by the payee and payee's PSP: • If applicable, transaction processing logs to support technical investigation • Purchase order, invoice, or receipt for each transaction

e. [DIS-TXM-005] Duplicated transaction initiated by the payee

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro payment transaction was initiated by the payee multiple times beyond the single authorisation or consent provided by the payer
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The payer authorised the transaction only once • The respective digital euro transactions were processed, settled, and recorded in the payer's digital euro payment account
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro payment account statement clearly showing the duplicated charges for the same purpose To be provided by the payee and payee's PSP: • purchase order, invoice, or receipt for each transaction • Documentation proving that the recorded transactions were authorised by the payer

f. [DIS-TXM-006] Incorrect transaction amount

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro payment transaction was authorised by the payer for a specific amount[80], but a different amount was recorded and debited from the payer's digital euro payment account • The payee entered a different amount than what was authorised by the payer
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The payer recognises the payee, and the payer authorised the transaction but for a different amount which was recorded or debited from the payer's digital euro payment account

[80] Based on data element Amount [Tr2])

Supporting documentation	To be provided by the payer and payer's PSP: • Link[81] or QR code[82] used by the payer to authorise the payment transaction • For consumer-to-business digital euro transactions: Purchase order, receipt, invoice or other documentation proving that the authorised amount differs from the debited amount • For peer-to-peer digital euro payment transactions: transaction confirmation or receipt with details of the intended amount To be provided by the payee and payee's PSP: • Purchase order, receipt, invoice, transaction record or other documentation showing that amount debited matches the amount originally authorised by the payer

g. [DIS-TXM-007] Incorrect transaction data

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro payment transaction was recorded with invalid or incorrect data, including transaction date or time, payee[83], country, remittance information or scheduled execution date
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The digital euro payment transaction is not a recurring payment transaction or pre-authorised recurring transaction • One or more data points recorded in the payer's digital euro payment account do not match the data points originally authorised by the payer (e.g., authorisation code, transaction date or time, payee name, or country)
Supporting documentation	To be provided by the payer and payer's PSP: • Purchase order, receipt, invoice, authorisation record, or confirmation screen showing that the original transaction details differ from those recorded in the payer's transaction history To be provided by the payee and payee's PSP: • Purchase order, receipt, invoice, transaction processing log or other documentation proving that that the recorded transaction details are consistent with the original transaction authorisation or consent provided by the payer

h. [DIS-TXM-008] Transaction sent to incorrect payee

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro transaction was credited to a different payee than the one intended by the payer
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The incorrect crediting of the digital euro transaction was due to: ○ A mistake in the payee information input (e.g., incorrect payee ID, QR code, or link used)

[81] Based on data element Return URL [Tr46]
[82] Based on data element Transaction Token [Tr58]
[83] Based on data element CreditorAccountName [Ac14]

	○ A technical issue or mismatch between the intended payee's details and those stored or processed by the payer's PSP
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP indicating that the transaction was intended for a different recipient • Proof of intended payee details (e.g., screenshot, invoice, QR code, or link originally provided by the legitimate intended recipient) • Evidence of mismatch between the intended recipient and the actual credited payee (e.g., discrepancy in account details, or confirmation message) • Transaction processing log showing the disputed payment To be provided by the payee and payee's PSP: • Transaction processing logs confirming the receipt of the digital euro payment, including timestamp, payee details, and method of payment • Confirmation whether the received amount have been accessed, used, or returned • Cooperation documentation (if any) showing whether the payee agreed to return the funds after being notified

i. [DIS-TXM-009] Recurring transaction not authorised by the payer

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A recurring digital euro payment transaction was never authorised by the payer • A recurring digital euro payment transaction was debited from the payer's digital euro payment account, which does not comply with the authorised amount, frequency, duration or designated payee • A recurring transaction was debited from the payer's digital euro payment account instead of a one-off digital euro payment transaction, contrary to what the payer authorised • A recurring digital euro transaction was debited from the payer's digital euro payment account after the payer had withdrawn authorisation or consent for it
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The recurring digital euro payment transaction does not comply with the pre-authorised terms agreed to by the payer, i.e., maximum transaction amount, payment frequency, duration of authorisation or consent or designated payee, either due to a failure in the payer's PSP's internal systems or processes or due to delayed or missing updates to the recurring payment status after cancellation or modification by the payer
Supporting documentation	To be provided by the payer and payer's PSP: • Purchase order, receipt, invoice, or other documentation showing the agreement of the original authorisation or consent details of the recurring digital euro payment transaction authorised (e.g., amount, frequency, payee) • Documentation showing that the disputed transaction exceeds or differs from the authorised terms To be provided by the payee and payee's PSP: • Purchase order, receipt, invoice, or other transaction documentation proving that the disputed transaction complies with the recurring digital euro payment transaction's parameters authorised by the payer

j. [DIS-TXM-010] Misrepresentation of goods or services

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• The characteristics of the goods or services were intentionally misrepresented by the payee in the agreement with the payer or advertisement
Conditions for initiating a dispute	• The disputed transaction is consumer-to-business • The payer received the goods or services • The payer has reached out to the payee and not received sufficient support or explanation by the payee • The goods or services were intentionally and objectively misrepresented by the payee

Supporting documentation	To be provided by the payer and payer's PSP:
	• Documentation from the payer to the PSP, showing the details of:
	  ○ How the goods or services were advertised, promoted or agreed upon with the payee
	  ○ How the goods or services received deviate from the agreed terms or do not meet the expectations set by the initial description or agreement
	To be provided by the payee and payee's PSP:
	• Documentation showing that the payer and payee reached an agreement regarding the dissatisfaction over the goods or services and that a corrective action has been issued
	• Documentation showing that the payer received the goods or services conformed to the original advertisement or agreement and met the promised description

k. [DIS-TXM-011] Lost or stolen payment instrument

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• The payer claims not to recognise a digital euro payment transaction that was processed after the payment instrument was reported as lost or stolen to the payer's PSP; the payer no longer possesses the payment instrument

Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer
	• The payer has reported the payment instrument as lost or stolen to their PSP
	• One of the following conditions must be met:
	  ○ The disputed transaction was carried out using contactless payment methods, but the payment instrument was configured to require PIN authentication, and the terminal was not capable of verifying the PIN, either due to a hardware issue or lack of a PIN pad
	  ○ The transaction was performed using contactless payment methods without PIN verification or on-device payer verification (e.g., biometrics, etc.)
	  ○ The transaction was processed after the payment instrument was officially reported as lost or stolen

Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP, confirming they did not possess the payment instrument when the transaction took place, and therefore, they did not authorise, initiate or participate in the disputed transaction

	• Law enforcement or police report (e.g., case number or copy of the complaint) documenting the loss or theft of the payment instrument To be provided by the payee and payee's PSP: • Documentation showing the transactions details (e.g., time, place of purchase), such as timestamped transaction processing logs, receipts, invoices or transaction statements

l. [DIS-TXM-012] Payment instrument not received

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• A digital euro payment transaction was initiated using a payment instrument that was never received or possessed by the payer
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The payer did not authorise the transaction • No strong customer authentication methods were performed by the payer • The PSP has provided the payer the delivery details of the payment instrument • The PSP has informed the payer of the timeframe for reporting issues related to the delivery or activation of the payment instrument, as well as the consequences of not reporting within the given timeframe
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP, confirming that they never received or possessed the payment instrument and therefore they did not authorise, initiate or participate in the disputed transaction • If a dispute is raised after the specified timeframe provided by the PSP, the payer must provide evidence that they received the original delivery and timeline instructions from the PSP • For transactions made using contactless methods despite the payment instrument being configured to require PIN authentication, the payer's PSP shall provide documentation confirming the payment instrument configuration at the time of the transaction To be provided by the payee and payee's PSP: • Documentation showing the transactions details (e.g., time, place of purchase), such as timestamped transaction processing logs, receipts, invoices or transaction statements

m. [DIS-TXM-013] Counterfeit payment instrument

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• One or more digital euro payment transactions were authorised using a counterfeit or mimicked version of the payer's payment instrument, despite the payer still having physical possession of the original payment instrument
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer

	• The payer did not authorise the transaction through SCA methods and there is no indication that the SCA process was bypassed with the payer's involvement
	• One of the following conditions must be met:
	  ○ A counterfeit payment instrument was used at a POS terminal, and the digital euro transaction was not processed as secure element-protected due to the terminal's inability to support secure elements, and yet, the transaction was still authorised
	  ○ The digital euro transaction was processed using the secure element for validation, but the authorisation or consent data were not fully transmitted during the transaction processing by the payer's PSP or the POS terminal, leading to a flawed authorisation

Supporting documentation	To be provided by the payer and payer's PSP:
	• Written declaration from the payer to the PSP, confirming that they did not authorise, initiate or participate, in the disputed transaction
	• Details on the configuration of the payment instrument, including:
	  ○ Whether the payment method defaults to PIN or contactless
	  ○ Contactless transaction limits and any authentication thresholds applied.
	To be provided by the payee and payee's PSP:
	• Documentation proving that the disputed digital euro transaction was authorised by the payer utilising secure element-protected SCA
	• Evidence confirming that SCA was performed, even though the payment instrument's settings did not default to SCA
	• Records showing whether the contactless authentication limits were exceeded and if SCA was triggered or bypassed.
	• Documentation showing the transactions details (e.g., time, place of purchase), such as timestamped transaction processing logs, receipts, invoices or transaction statements

n. [DIS-TXM-014] Account take-over

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• One or more digital euro payment transactions were executed without the payer's authorisation or consent by a fraudulent party who gained control over the payer's digital euro payment account. The payer states that they retain possession of their payment instruments (e.g., card, digital euro app, wearables), indicating that the unauthorised activity arised from an account-level breach rather than the loss or theft of a payment instrument
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The digital euro payment transaction details show inconsistencies in the application of authentication factors used for SCA • One of the following conditions must be met:

	○ The device used to perform SCA does not match the one agreed upon and registered with the PSP (e.g. hacked digital euro app session on another device, use of a hacked wearable device, use of a device not associated with the payer) ○ The knowledge-based authentication factor (e.g., password, PIN) does not align with the recorded method or was used in an inconsistent context (e.g., password validated in a PIN-authenticated transaction) ○ The biometric authentication factor recorded (e.g., face or fingerprint recognition) does not match the method agreed upon with the PSP or was technically implausible (e.g., face recognition validated on a 2D camera where it should not be possible) ○ The transaction was performed using only one authentication factor, instead of the minimum SCA requirement of two distinct authentication factors
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP, alleging that they did not participate in, authorise, or initiate the disputed transaction and remain in possession of the registered payment instrument • Law enforcement or police report (e.g., case number or copy of the complaint) documenting the account take-over incident To be provided by the payee and payee's PSP: • The payee and payee's PSP are not required to submit documentation supporting the dispute. The payee and their PSP are not considered responsible for unauthorised transactions resulting from authentication failure on the side of the PSP

o. [DIS-TXM-015] PSP, payee or other entity impersonation

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• The payer claims to have been deceived into authorising a digital euro payment transaction by a fraudster falsely claiming to be a representative of the PSP, a legitimate payee or other trusted entity
Conditions for initiating a dispute	• The disputed transaction is either consumer-to-business or peer-to-peer • The digital euro payment transaction was authorised by the payer • After the incident, the payer contacted their PSP, and the payer's PSP confirmed that they had not initiated any contact with the payer to request personal details or authorise the transaction • The payer claims to have been deceived into authorising a digital euro payment transaction by a fraudulent merchant posing as a legitimate merchant and no goods or services were received • The payer claims to have been deceived into authorising a digital euro payment transaction by responding to a fraudulent invoice, email or any other type of communication from an individual impersonating a trusted brand, payee, platform, organisation or institution
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP, alleging that the payer was misled by a fraudster impersonating a PSP representative, a trusted brand,

	platform, organisation or institution. The declaration shall include a description of the manipulation tactics used • Documentation proving that the fraudster unlawfully used the name, branding, contact details or other identifiers of the PSP, trusted brand, payee, platform, organisation or institution. This can include screenshots of phone calls, messages or emails, images of letters, or other materials that could be reasonably mistaken as legitimate communication from the PSP, trusted brand, platform, organisation or institution To be provided by the payee and payee's PSP: • Documentation demonstrating that the payee and the payee's PSP were not involved in the fraudulent activity

p. [DIS-TXM-016] Goods or services not delivered

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• The payer authorised a digital euro payment transaction, but the payee intentionally did not deliver the agreed goods or services in exchange for the digital euro payment
Conditions for initiating a dispute	• The disputed transaction is consumer-to-business • The payee's advertisement or agreement with the payer concerning the good or services objectively provided for the delivery of goods or services to be included in the obligation by the payee to the payer • The payer did not receive a transaction order confirmation from the payee • No tracking number or other verifiable proof of delivery was provided to the payer • The payer has reached out to the payee and not received sufficient support or explanation by the payee
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP confirming that a digital euro payment transaction was conducted in exchange of goods or services, which were not delivered • Documentation showing the payer's unsuccessful attempts to contact the payee to resolve the issue To be provided by the payee and payee's PSP: • Documentation showing that the goods or services related to the disputed digital euro payment transaction were delivered to the payer • Documentation showing that the reception of goods or services related to the disputed digital euro payment transaction were signed by the payer

q. [DIS-TXM-017] Counterfeit or pirated goods

Scenarios covered, conditions for initiating a dispute, supporting documentation	
Scenarios covered	• The payer claims to have purchased goods that were delivered as counterfeit or pirated

Conditions for initiating a dispute	• The disputed transaction is consumer-to-business • "Counterfeit" refers to an unauthorised imitation of a branded product, thereby infringing licensing permissions, intellectual property rights, or copyrights • "Piracy" refers to an unauthorised reproduction of a good protected by intellectual property rights, constituting an exact copy rather than a mere imitation • The payer authorised the payment transaction with the intention of purchasing a genuine good • The disputed good is confirmed to be counterfeit/pirated
Supporting documentation	To be provided by the payer and payer's PSP: • Written declaration from the payer to the PSP confirming that a digital euro payment transaction was made for goods they claim to be counterfeit/pirated or lacking genuine product attributes • Documentation from the payer regarding the payment transaction, such as a purchase receipt or similar proof, including payment amount, date and time, payer information, description of the disputed goods and an explanation supporting the counterfeit/piracy claim • Documentation from the payer that specify the location of the item, including but not limited to: ○ The good is in possession of the payer ○ The good is in possession of a governmental authority ○ The good is in possession of the customs agency ○ The good is not in possession of the payer, but the payer can provide documentation of the delivery and product properties ○ The good was returned to the payee • Documentation presented by the payer supporting the counterfeit/piracy claim, such as a confirmation from the intellectual property rights holder, a customs declaration, a law enforcement report, or an expert assessment report To be provided by the payee and payee's PSP: • Documentation showing that the payee holds the appropriate license, intellectual property rights, or is an authorised manufacturer or retailer of the disputed goods. Verification may be based on the identification of the payee as a source of counterfeit/pirated goods, or on the confirmation that goods themselves are non-compliant with applicable certifications. Such verifications must come from an authorised entity, including but not limited to: ○ The intellectual property owner or an authorised representative ○ A customs agency ○ A law enforcement agency or other governmental authority ○ A qualified third-party expert or accredited organisation providing a formal expert assessment • Documentation showing how the delivered goods meet the characteristics of a genuine product and how it differs from a counterfeit/pirated good, as per the payer's claim

ii. Dispute reasons for funding, defunding transaction disputes

a. [DIS-LQM-001] xxx

This is a placeholder for dispute reasons for funding, defunding transactions

6.5 Dispute prevention and optimisation

DMR.10 Scheme participants shall facilitate the payer's ability to review and recognise digital euro payment transaction data, as a way to reduce the likelihood of a dispute to arise. The functional rules governing the eligibility of a digital euro payment transaction for dispute are provided in the table below.

Functional requirements	
PSP functional requirements:	
DM-060-001	Scheme participants shall adopt solutions aimed at preventing disputes from arising
DM-060-002	Scheme participants shall adopt solutions aimed at facilitating the dispute resolution
DM-060-003	Payers' PSPs shall facilitate the initiation of disputes by showing – to a minimum – digital euro payment transaction timestamp[84], amount[85], currency[86], payee name[87]
DM-060-004	Scheme participants shall notify digital euro users on the progress of their disputes management processes.
DM-060-005	Scheme participants shall suggest relevant types of documentation that digital euro users may provide to support their disputes

[84] Based on data element CreationDateTime [Tm1]
[85] Based on data element Amount [Tr2]
[86] Based on data element Currency [Tr16]
[87] Based on data element CreditorAccountName [Ac14]

7 Brand rules

7.1 Section overview

The objective of this section is to describe digital euro brand rules for scheme participants and other actors to adhere to when implementing and using the digital euro logo and other branding elements in various contexts.

This section provides the rules for the use of the digital euro brand, ensuring that its application facilitates a harmonised and consistent user experience regardless of the payment service providers involved and the front-end services used.

These brand rules will apply to all relevant use cases and channels where the digital euro brand is used and are mandatory unless indicated otherwise.

To accommodate for the various brand implementation scenarios that apply for payment service providers and future applications, the brand rules are complemented with a style guide:

- Brand rules – applicable across all channels and uses of digital euro brand, both physical and digital, to ensure consistent display and clarity
- Style guide – source of branding assets and visual references linked to brand rules to support consistent digital euro branding implementation in various environments. [PLACEHOLDER: add link to the style guide]

Note: For guidelines on branding placement for touchpoints that are not included in these brand rules, refer to the relevant specifications included in the style guide. [PLACEHOLDER: add link to the style guide]**.**

Note: For guidelines on co-branding and communication to end users, refer to the Brand guidelines. [PLACEHOLDER: add link to the Brand guidelines]**.**

7.2 Brand elements

7.2.1 Logo requirements

BRR.01 The full brand logo consists of a combination of textual and graphical elements and shall be used in accordance with the style guide.

BRR.02 The full brand logo shall be used whenever possible in full colour and following the size, spacing and background specifications provided in the style guide. If the use of the full digital euro logo, full colours or size is not possible, alternatives are made available in Section 7.2.6.

BRR.03 In all use cases, the digital euro branding shall only use the approved and unaltered versions of the digital euro logo and branding assets (e.g., banners, brand mark, icons). All approved branding assets can be found in the style guide.

Downloadable assets for the logo and other branding can be found in the style guide. [PLACEHOLDER: add link to the style guide].

7.2.1.1 Logo placement

BRR.04 The logo and other branding elements shall be displayed in relevant scenarios and screens. By default, the logo shall be used in the following scenarios:

- Signalling availability of digital euro services and at all points of interaction (POI) relating to digital euro PSP and third-party environments (websites, in PSP-app integrations, third-party apps and wallets)
- Signalling acceptance at merchant locations (physical, websites and apps) and PSP in-branch locations
- In specific screens following the indications provided in the illustrative user journeys and the style guide

7.2.1.2 Minimum size

BRR.05 The logo shall be displayed in a minimum size that ensures clear legibility and compliance with the indications found in the style guide.

Specific print & digital requirements can be found in the style guide: [PLACEHOLDER: add link to the style guide]

7.2.1.3 Spacing

BRR.06 Minimum free space around the logo shall be included to ensure recognition and unobstructed view following the specifications in the style guide.

Specific print & digital requirements can be found in the style guide: [PLACEHOLDER: add link to the style guide].

7.2.1.4 Colour

BRR.07 The full colour logo shall be used whenever possible in colours specified in the style guide. The use of colours outside the defined colour palette is not permitted.

BRR.08 Grayscale version of the logo and other assets shall be used only when the print or display do not support full colour. If displayed with other brands the grayscale digital euro logo shall maintain equal prominence to other logos, as explained in **Section 7.2.2.2 Equal prominence in colour**.

BRR.09 When using grayscale alternatives, other requirements regarding placement, minimum size, sufficient contrast with the background and spacing remain applicable.

Downloadable full colour logo assets and grayscale alternatives can be found in the style guide. [PLACEHOLDER: add link to the style guide]

7.2.1.5 Background

BRR.10 The logo shall be placed on a simple or solid colour background providing sufficient contrast and legibility. The logo shall not be placed on busy imagery or patterned or gradient background that could obscure its legibility.

BRR.11 The background should be used in accordance with guidance and examples provided in the style guide. [PLACEHOLDER: add link to the style guide].

7.2.2 Equal prominence in display with other brands

When digital euro branding is represented alongside other payment brands, the following requirements are applicable:

BRR.12 For layout and prominence decisions, the digital euro acceptance marks and logo shall be treated as a core payment scheme, on par with other payment schemes. As such the digital euro logo shall be displayed on the same screen, panel or physical surface as other core payment schemes when they signal acceptance. It must not be moved to a different or less visible area (e.g., footer, second page) while core payment schemes remain in the primary view.

BRR.13 The digital euro brand logo and/or its provided alternatives shall maintain equal prominence to other payment brands, meaning that the size, colour treatment, frequency and placement of digital euro branding shall match that of core payment schemes and payment brands in all digital and physical channels.

7.2.2.1 Equal prominence in size

BRR.14 In any logo group the height of the digital euro logo must be no less than 90% of the height of the largest payment brand logo, and no less than 100% of the smallest payment brand logo.

BRR.15 The digital euro logo shall be displayed at the official aspect ratio. It must not be compressed or expanded to make it visually smaller or less legible than other payment brand logos.

BRR.16 Where payment icons are presented on a grid, the digital euro icon shall occupy a grid cell of identical size to other payment brands.

7.2.2.2 Equal prominence in colour

BRR.17 If any other payment brand logo is displayed in full colour, the digital euro logo must also be displayed in full colour.

BRR.18 When grayscale alternatives of digital euro branding are used, other payment brands need to also be displayed in grayscale in the same view.

BRR.19 In monochrome or single-colour icon systems, the digital euro icon may match the house colour, but must maintain equal stroke weight, line style and visual density as other payment brand icons.

7.2.3 Sensory check-out branding

Note: Sensory check-out branding is a form of animation, sounds and haptics serving to provide consumers with auditory, visual and haptic cues about digital euro transactions. Depending on the environment and technical capabilities, all three (animation, sound and haptics) can be used together or separately.

BRR.20 Animated check-out branding and check-out sound shall be used to indicate the status of the transaction (successful or failed with respective sounds) when technology or platform supports them, at physical point-of-sale (POS), in digital environments, mobile environments and voice environments.

BRR.21 For payments that do not include a screen, sound and/or haptic vibrations shall be used without the animation, if supported.

BRR.22 If there are any check-out animations, sounds and/or haptics associated with another payment brand at the POS or other POI, then the digital euro check-out animation and/or sound shall also be enabled and maintain equal prominence to other brand animations including frequency, volume and intensity.

BRR.23 Check-out animations, sounds and haptics shall follow the guidance and use the assets provided in the style guide. [PLACEHOLDER: add link to the style guide].

7.2.3.1 Animations

BRR.24 Check-out animations shall be displayed with the check-out sound and haptics (if used) and shall be separate from any other pre-existing animations, sounds or haptics of the point-of-interaction (POI).

BRR.25 Check-out animation shall be displayed in full colour and at the highest possible resolution supported by the POS or POI.

BRR.26 Animations shall be displayed at a minimum size ensuring legibility and without any alterations to colour treatment, proportions or speed following the indications in the style guide.

BRR.27 If due to restrictions animations cannot be displayed, static branding elements shall be used.

7.2.3.2 Sounds and haptics

BRR.28 Check-out sound shall be played with the highest fidelity supported by the POS or POI device.

BRR.29 If the device does not support polyphonic sound, check-out sound shall not be implemented.

BRR.30 Haptic vibrations shall be used in conjunction with the check-out animations and sound when displaying an outcome of digital euro transaction where relevant and supported by the technology or platform.

BRR.31 In primarily voice environments that use spoken confirmation, check-out sound shall be played alongside a verbal confirmation.

7.2.4 Brand integrity

BRR.32 It is not permitted to alter the logo design and other brand elements, place any additional text within the logo, change the proportions, rotation, aspect ratio, resolution, include 3D elements or add any other visual alterations or filters to the logo and other branding elements.

BRR.33 The logo must not be used in text as a part of the sentence and shall instead include the brand name in text format following the capitalisation and relevant localised name adaptations as indicated in the style guide.

BRR.34 Digital euro branding shall not be used in any way that could negatively impact the public perception, reputation, or value of the brand, brand products or services, scheme participants, or merchants.

BRR.35 Participants shall not use any branding in a way that could mislead consumers, merchants, or other participants about the scheme, products, services, or their source, affiliations, sponsorships, or associations.

Note: For visual references on correct usage of the logo design and practical do's and dont's, see the style guide **[PLACEHOLDER: add link to the style guide]**.

7.2.5 Adaptation in local use

BRR.36 When using digital euro branding (e.g., full logo including brand name or brand name in text), scheme participants shall consider localisation needs in the area where the digital euro brand is used and shall ensure that all branding elements are aligned with the localisation guidance found in the digital euro style guide. **[PLACEHOLDER: add link to the style guide]**

7.2.6 Small and limited displays

For small display devices that do not allow for full logo display, or displays with limited capabilities, alternatives for the logo are provided as follows:

BRR.37 If the minimum size logo is too large to be legibly displayed, the brand approved mark and/or full name in text shall be used with specified capitalisation as outlined in the style guide.

BRR.38 If the display does not support graphics, the full name in text shall be used with specified capitalisation as outlined in the style guide.

BRR.39 If using the full name in text is not possible, the shortened version of the brand name shall be used with specified capitalisation as outlined in the style guide.

BRR.40 If other payment brand logos are displayed on a small screen (e.g., POS) the digital euro shall appear alongside other core payment schemes. If it cannot appear in the same view as core payment schemes due to format limits, no other specific payment brand logo shall be shown, and a generic or category-based symbol shall be used instead. In this case the digital euro logo should appear in its own category.

Downloadable scalable logo, brand mark and digital euro name in text specifications can be found in the style guide. [PLACEHOLDER: add link to the style guide]

7.3 Brand visibility at physical touchpoints

BRR.41 Brand acceptance signage shall be prominently displayed at point-of-interaction (POI) including but not limited to point-of-sale (POS), terminals, cash registers, self-checkout and ATMs. Acceptance signage should be placed on digital screens using brand approved acceptance assets, or, if digital on-screen acceptance signalling is not possible, ready-made sticker designs or stand-up displays shall be used.

BRR.42 The digital euro acceptance sticker shall be displayed on a main entry door and/or window near the customer facing property entrance (such as merchant or in-branch physical locations offering support with digital euro payment accounts or services) with following specifications:

a) The acceptance sticker shall be placed at eye level, ensuring it will be easily visible from the outside.

b) If it is not possible to display acceptance signage on doors or windows (e.g., due to property restrictions) and no other brand acceptance signage is displayed on the doors and/or windows, then it must be ensured that digital euro acceptance signage (digital or sticker) is at the very least clearly visible to consumers at point-of-interaction (POI) including but not limited to point-of-sale (POS), terminals, cash registers, self-checkout and ATMs.

BRR.43 Digital euro acceptance signage and stickers shall be displayed with equal prominence in relation to core scheme payment brands, ensuring that it is prominently placed in the same visual field as other payment acceptance signage and easily recognisable as a supported payment means for the consumers.

BRR.44 If the acceptance signage of other brands is displayed in an acceptance panel, the digital euro acceptance signage shall be integrated into the same acceptance panel as a clearly separate means of payment and must not be relegated to a less visible area.

BRR.45 Only unaltered acceptance signage provided in the style guide shall be used to signal digital euro acceptance.

Downloadable acceptance signage assets can be found in the style guide. [PLACEHOLDER: add link to the style guide]

7.4 Brand visibility in e-commerce/m-commerce

The brand shall be displayed at least in the specific scenarios. By default, the digital euro branding shall be represented in following scenarios:

- When signalling acceptance of available payment methods – using the digital acceptance signage
- When representing digital euro payment account-related information (e.g., stored DEAN, alias)
- Pre-purchase:
    - In payment method selection screen
    - At check out, within immediate proximity of the payment trigger
    - During consent & authentication
- Post-purchase – for any payments made with digital euro:
    - On the payment result / confirmation page
    - In transaction history; In receipts (including, but not limited to, push notifications, email, [digital] receipts)

- Other screens as indicated in the illustrative user journeys.

BRR.46 If the display of the full-sized logo is not possible, it is permitted to use a brand approved brand mark and/or full brand name or shortened brand name in text with specified capitalisation, as outlined in the style guide.

BRR.47 The digital euro branding shall be clearly identifiable as a separate means of payment, with its own logo and name while being displayed with other payment brands in a separate visual group or screen. The digital euro branding shall be placed in a way that makes it easily noticeable for consumers where possible at first glance. At the very least it must not be relegated to a secondary row or 'other payments' category (or its equivalents) when other core payment schemes appear in the primary row unless all other core payment schemes follow the same other ordering principles (e.g., alphabetical, domestic preference).

BRR.48 In payment method selection screen where payment brands are not listed individually but organised into generic or category-based groups, the digital euro shall be categorised in a group clearly identifying it as central bank money.

BRR.49 If payment brands are presented in a carousel, the digital euro shall receive exposure that is equivalent in frequency, duration and visibility equal to other core payment schemes. The digital euro shall be visible in the first full rotation or at least within the first swipe or scroll of the carousel together with other core payment schemes following the same ordering principles (e.g., alphabetical, domestic preference). It must not be positioned so far in the sequence that a typical user is unlikely to encounter it.

7.4.1 Express check-out buttons

BRR.50 Whenever branded express check-out buttons are presented:

- Digital euro express check-out buttons shall be displayed with equal prominence to the direct check-out buttons of other payment means, specifically the digital euro branding shall maintain equal size, visibility and proximity to order details as any other branded express check-out button in the same view.

- The position of express check-out buttons of digital euro shall follow the same neutral ordering principles (e.g., alphabetical, domestic preference) and must not be consistently placed last without justification.

Downloadable icons, express check-out buttons and other digital branding assets can be found in the style guide**. [PLACEHOLDER: add link to style guide]**

7.5 Physical and digital receipts

BRR.51 Receipts of digital euro transactions shall include the full brand name in text with specified capitalisation as outlined in the style guide **[PLACEHOLDER – add link to the style guide].**

BRR.52 In channels or formats where the full brand name in text cannot be used — due to character limits (e.g. transaction history and other post-purchase notifications where the logo cannot be displayed) - the shortened digital euro brand name in text shall be used with the specified capitalisation as outlined in the style guide. **[PLACEHOLDER – add a link to the style guide].**

7.6 Card design

7.6.1 Physical card design

BRR.53 Digital euro branding is required on all cards supporting digital euro services.

BRR.54 Digital euro branding shall always be prominently positioned on the front of the card while ensuring that the name and other text elements on the card are clearly legible and not obscured by the branding elements.

BRR.55 To further facilitate accessible card usage for visually impaired users, cards are recommended to include embossed print, braille markings for the brand and name on the card, and tactile notches on a single standardised location to indicate the type of the card and correct orientation for inserting it. (optional)

On cards where another payment scheme already requires or recommends tactile elements, a notch or a cut, these features shall be accepted as the primary tactile accessibility features for the card. Additional or separate notches are not required.

BRR.56 The placement of the branding elements on the card shall follow the specifications in the digital euro style guide. **[PLACEHOLDER: add link to the style guide].**

7.6.2 Digital card representation

BRR.57 Digital card representation shall follow the physical card design, including name and other text elements. It must not show the chip or add any additional shading or 3D elements.

BRR.58 When the digital euro card is represented alongside other digital cards, it shall maintain equal legibility and prominence to other cards represented in the same view.

7.6.3 Co-badging representation

BRR.59 In the case of co-badging or triple-badging, the digital euro logo shall be prominently placed on the front of the card, following the same specifications as other digital euro physical cards.

BRR.60 In cases where the card design places all brand logos on the back it is allowed to position the digital euro logo on the back of the card as long as all other payment scheme and brand logos are also positioned on the back. Digital euro logo must maintain equal prominence in terms of size and visibility with other payment scheme and/or brand logos featured on the card. The digital euro logo must not be placed on the back of the card if any other payment scheme and/or brand logos are placed on the front of the card.

7.7 QR codes

BRR.61 QR codes for digital euro payments shall be made recognisable as such by including the digital euro logo within close proximity to the QR code and other required branding elements as prescribed by the style guide. The logo shall be placed within a protected area either at the top or the bottom of the QR code.

BRR.62 The branding of the QR codes shall follow any additional specifications included in the digital euro style guide. **[PLACEHOLDER: add link to the style guide].**

7.8 In PSP-app/portal/wallet integrations

BRR.63 When digital euro services are integrated in an app, a portal or a wallet, it is recommended to feature a dedicated section containing all integrated digital euro services and display them with digital euro branding as indicated in the style guide. (optional)

BRR.64 Digital euro branding shall be displayed in PSP environments including, but not limited to the following scenarios:

- Signalling the availability of onboarding to the digital euro
- Signalling the availability of adding existing digital euro credentials; Option for funding and defunding of digital euro payment accounts
- Representing available digital euro-based payment options and features
- When representing digital euro payment account related information (e.g., DEAN, alias, balance)
- During consent & authentication
- In transaction history
- In receipts (e.g., push notifications, email, digital receipts)

BRR.65 The digital euro branding, such as logo, icon or name, shall be included in a protected area, either in the header, the footer of the screen or in specific areas (e.g., next to digital euro payment account balance), at least in selected screens of digital euro services indicated in the illustrative user journeys (such as, but not limited to: payment set-up screen, sending/requesting digital euro screen, etc.).

BRR.66 If an app, portal or wallet displays supported payment methods as tiles or rows on the home screen, digital euro branding shall be integrated on par with other brands and represented at the same visual level as other payment brands supported in the app, portal or wallet.

BRR.67 When proprietary PSP payment and other partner payment scheme options are presented, the digital euro options shall be included in the same option group with equal icon size and label styling. It shall not be relegated to secondary menus if proprietary or partner brands are shown in primary views.

BRR.68 PSP brand can remain primary at the app level (header, splash screen, sensory branding), but within the digital euro-related account or service interfaces, the digital euro must have equal visual weight to other payment brands featured in the app in terms of size, frequency and visibility of the branding.

BRR.69 In confirmation screens and receipts, the digital euro logo shall appear where other brand's logos are used to indicate which payment method was used. If other brands are indicated with a name instead of a logo, the digital euro name shall be used following capitalisation and regional adaptation specifications provided in the style guide.

BRR.70 The implementation of digital euro branding assets in PSP-app/portal/wallet integrations shall follow specifications on logo use (e.g., minimum size, spacing, background use, etc.), as provided in the digital euro style guide. **[PLACEHOLDER: add link to the style guide].**

8 Digital euro fees, limits and threshold requirements

[Placeholder

9 Scheme rulebook management

[Placeholder]

10 Glossary

Please note that the terms and definitions in this glossary are not final and are subject to change.

Term	Definition
Acceptance solution	A combination of a digital euro user device, a user interface, and a communication technology, used by the payee which enables the acceptance of digital euro payment transactions.
Acquiring of payment transactions	A payment service provided by a payment service provider contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee.[88]
Acquiring payment service provider	A payment service provider (PSP) that contracts with a business digital euro user to provide digital euro services.
Additional digital euro services	Services that go beyond the basic digital euro payment services.
Alias lookup service	A service that maps an identifier (user alias) linked to a digital euro user—such as an (optional) mobile phone number and/or digital euro payment account number (DEAN)—to the corresponding payment service provider (PSP).
Assisted use	A situation in which a digital euro user accesses digital euro payment services with support. This support may include, inter alia, direct interaction with the payment service provider's staff (e.g. in a branch or via telephone services), as well as the use of systems mimic human interaction.
Automated defunding	A functionality that allows a digital euro user to decrease the digital euro balance on his/her own digital euro payment account to be triggered based on a pre-defined threshold amount rule and/or date rule set by the digital euro user.
Automated funding	A functionality that allows a digital euro user to increase the digital euro balance on his/her own digital euro payment account to be triggered based on a pre-defined threshold amount rule and/or date rule set by the digital euro user.

[88] Article 4(44) of Title 1 of Directive [4]

Back-end infrastructure	All hardware and software components comprising the Digital Euro Service Platform, e.g. necessary for recording of digital euro holdings in the Eurosystem ledger and processing of digital euro payment transactions.
Business continuity	The capability of an entity to continue the delivery of digital euro payment services within predefined time frames at predefined capacity during a disruption.
Business digital euro user	A natural or legal person, who is acting for purposes of his or her trade, business, craft or profession and is allowed to open a digital euro payment account.
Business-to-business (B2B) digital euro payment transactions	A digital euro payment transaction made by one business digital euro user to another.
Business-to-person (B2P) digital euro payment transactions	A digital euro payment transaction from a business digital euro user to an individual digital euro user.
Central bank money (CeBM)	Liabilities of a central bank which can be used for settlement purposes.[89]
Commercial bank money (CoBM)	Commercial bank liabilities that take the form of deposits held at the commercial bank which can be used for settlement purposes.[90]
Commercial bank money payment service provider (CoBM PSP)	A payment service provider (PSP) that provides non-digital euro payment accounts.
Communication technology	Technology used for the transmission of data between two devices. This includes proximity (e.g. NFC) and remote methods (e.g. internet).
Comparable digital means of payment	Digital means payment, including debit card payment and instant payment at the point of interaction but excluding credit transfer and direct debit that are not initiated at the point of interaction.[91]

[89] *ECB glossary*. Source: https://www.ecb.europa.eu/services/glossary/html/glossc.en.html
[90] *ECB glossary*. Source: https://www.ecb.europa.eu/services/glossary/html/glossc.en.html
[91] Article 2(25) of Chapter 1 of the draft Regulation [1]

Conditional digital euro payment transaction	A digital euro payment transaction which is instructed automatically upon fulfilment of pre-defined conditions agreed by the payer and by the payee.[92]
Countering the financing of terrorism (CFT) check	A check aimed at countering the solicitation, collection and provision of money that may be used to finance terrorist acts or organisations.
Credit institution	An undertaking the business of which is to take deposits or other repayable funds from the public and to grant credits for its own account.[93]
Cross-border digital euro payment transaction	A digital euro payment transaction in which the scheme participants providing digital euro payment services to the payer and the payee are located in different Euro area Member States.
Cryptography	A technique and algorithm for securing communications and information by converting data into a coded format that can only be accessed or deciphered by those authorised to do so. It ensures properties such as confidentiality, data integrity, secure authentication, and non-repudiation of messages
Defunding	The process whereby a digital euro user exchanges digital euro with cash or other funds.[94]
Device based remote authentication	A mechanism that requires a device or application to communicate with a remote server or service to verify a user's identity. This process typically involves transmitting credentials or authentication data over a network to validate access.
Digital euro	A digital form of the single currency available to natural and legal persons.[95]
Digital euro access management	The process of onboarding/offboarding and lifecycle management of digital euro user.
Digital euro account number (DEAN)	A unique identifier of a digital euro payment account. Digital euro account number (DEAN) is created by digital euro service platform (DESP) and provided to the digital euro user by the payment service provider (PSP).

[92] Article 2(17) of Chapter 1 of the draft Regulation [1]
[93] Article 4(1) of Part 1 of the Regulation [8]
[94] Article 2(12) of Chapter 1 of the draft Regulation [1]
[95] Article 2(1) of Chapter 1 of the draft Regulation [1]

Digital euro actor	A digital euro user, scheme participant, the European Central Bank (ECB) or the National Central Bank (NCB) acting as stakeholders in the digital euro environment using digital euro or providing digital euro payment services as applicable.
Digital euro app	A digital interface made available by the ECB and the national central banks (NCBs) to payment service providers (PSPs), through which digital euro users can access and use digital euro payment services provided by their respective PSPs.
Digital euro component	A part or element that contributes to the overall functionality of the digital euro service platform (DESP).
Digital euro entry	A record in the Eurosystem ledger in the back-end infrastructure of the digital euro holdings held by a digital euro user.
Digital euro environment	A combination of actors (including end users and payment service providers (PSP)) and the digital euro service platform (DESP) to deliver digital euro payment services.
Digital euro funding request	A request submitted by a payment service provider (PSP) to digital euro service platform (DESP) to start the digital euro settlement process of a funding transaction.
Digital euro legal tender status	Entails the mandatory acceptance of the digital euro, at full face value, with the power to discharge from a payment obligation.[96]
Digital euro liquidity management	The process to support funding and defunding of digital euro payment accounts necessary for the provision of digital euro payment service.
Digital euro payment account	An account held by one or more digital euro users with a payment service provider to access digital euro recorded in the digital euro settlement infrastructure or in an offline digital euro device and to initiate or receive digital euro payment transactions, whether offline or online, and irrespective of technology and data structure.[97]
Digital euro payment instruction	A request initiated by a payment service provider (PSP) to digital euro service platform (DESP) to start the digital euro settlement process of a payment transaction.

[96] Article 7(2) of Chapter 3 of the draft Regulation [1]
[97] Article 2(5) of Chapter 1 of the draft Regulation [1]

Digital euro payment services	Any of the business activities including enabling digital euro users to access and use the digital euro, enabling digital euro users to initiate and receive digital euro payment transactions and providing digital euro users with digital euro payment instruments, managing digital euro users' digital euro payment accounts, conducting funding and defunding operations and providing additional digital euro payment services on top of basic digital euro payment services.[98]
Digital euro payment transaction	An act, initiated by a payer or on his or her behalf, or by the payee, of placing, transferring or withdrawing digital euro, irrespective of any underlying obligations between the payer and the payee.[99]
Digital euro payment transaction identifier	A unique identifier for a digital euro payment transaction generated and issued by the payment service providers (PSPs).
Digital euro payment transaction management	The process of processing a digital euro transaction, including authentication, payment initiation services and payment confirmation and/or rejection.
Digital euro pre-authorisation	An approval of a transaction type for which a digital euro amount is initially blocked in the digital euro ledger and only transferred (in whole or in part) to the payee after the delivery of a product or service. A payment "pre-authorisation" in the front-end solution equals to "reservation" of digital euro holdings in the digital euro service platform (DESP).
Digital euro scheme applicant	A payment service provider that formally submits an application to participate in the digital euro payment scheme.
Digital euro scheme rulebook	A single set of rules, standards and procedures that supervised payment service provider (PSP) has to follow when distributing a digital euro.
Digital euro service platform (DESP)	The technical platform enabling the issuance and redemption of digital euro and providing functions (e.g. settlement) that cannot be accomplished by an individual payment service provider (PSP) on its own.
Digital euro service platform (DESP) operator	An entity responsible for managing one or more digital euro component(s) in the digital euro service platform (DESP).
Digital euro service platform dedicated	To be defined in the TARGET Guidelines.

[98] Article 2(8) of Chapter 1 of the draft Regulation [1]
[99] Article 2(3) of Chapter 1 of the draft Regulation [1]

cash account (DESP DCA)	
Digital euro service platform dedicated cash account (DESP DCA) holder	To be defined in the TARGET Guidelines.
Digital euro settlement infrastructure	The settlement infrastructure of the digital euro adopted by the Eurosystem.[100]
Digital euro settlement process	The sequence of technical and operational steps following the submission of a digital euro payment instruction and resulting in settlement and the discharge of the digital euro users' payment obligations hosted at digital euro service platform (DESP).
Digital euro solution	An acceptance solution or a distributing solution approved by the digital euro scheme.
Digital euro user	Anyone making use of a digital euro payment service in the capacity of payer, payee, or both.[101]
Digital euro offline wallet	An application (applet) running on the tamper resistant hardware of the digital euro offline device.
Digital operational resilience	The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions.[102]
Distributing payment service provider	A payment service provider (PSP) that provides the individual digital euro user with payment instrument(s) to initiate and process the individual digital euro user's payment transaction.

[100] Article 2(19) of Chapter 1 of the draft Regulation [1]
[101] Article 2(4) of Chapter 1 of the draft Regulation [1]
[102] Article 3(1) of Chapter 1 of Regulation [5]

Distributing solution	A combination of a digital euro user device, a digital euro user interface and a communication technology, used by payer which enables the initiation and authentication of digital euro payment transaction.
E-commerce digital euro payment transaction	A digital euro payment transaction in which a payer remotely purchases goods, services from a merchant using digital euro as the means of payment.
Electronic money institution (EMI)	A legal person that has been granted authorisation to issue electronic money.[103]
Emergency switching	In cases of prolonged service disruption or data loss by a payment service provider (PSP), the Eurosystem may declare an emergency situation allowing users to switch their accounts to a new PSP without requiring support from the previous PSP, ensuring continuous access to digital euro holdings.
European digital identity wallets	An electronic identification means which allows the user to securely store, manage and validate person identification data and electronic attestations of attributes for the purpose of providing them to relying parties and other users of European Digital Identity Wallets, and to sign by means of qualified electronic signatures or to seal by means of qualified electronic seals.[104]
European System of Central Banks (ESCB)	The central banking system of the European Union. It comprises the ECB and the national central banks of all EU Member States (but the national central banks of EU Member States whose currency is not the euro are not involved in the conduct of the Eurosystem's monetary policy for the euro area because they retain responsibility for monetary policy under national law).[105]
Fraud risk	This refers to both: (i) Unauthorised payment transactions made, including as a result of the loss, theft, or misappropriation of sensitive payment data or a payment instrument—whether detectable or not to the payer prior to the payment, and whether or not caused by gross negligence of the payer, or executed in the absence of the payer's consent ("unauthorised payment transactions") and (ii) Payment transactions made as a result of the payer being manipulated by the fraudster to issue a payment order, or to instruct

[103] Article 2(1) of Chapter 1 of Directive [9]
[104] Article 1(42) of Regulation (EU) 2024/1183
[105] ECB glossary. Source: https://www.ecb.europa.eu/services/glossary/html/glossc.en.html

	the payment service provider to do so in good faith, to a payment account they believe belongs to a legitimate payee ("manipulation of the payer").[106]
Front-end service	All components necessary to provide services to digital euro users that interact via defined interfaces with back-end solutions and other front-end services.[107]
Funding	The process whereby a digital euro user acquires digital euros, in exchange for either cash or other funds, creating a direct liability of the European Central Bank or a national central bank towards that digital euro user.[108]
Government or other public authorities	A government or other public authority that in the context of digital euro payment transaction is acting as business digital euro user.
Government-to-government (G2G) digital euro payment transactions	A digital euro payment transaction from a government or other public authorities to another.
Government-to-person or business (G2X) digital euro payment transaction	A digital euro payment transaction from a government or other public authorities to an individual digital euro user or business digital euro user.
Holding limit	A maximum amount of digital euro that can be held by a single individual digital euro user at any time.[109]
Identification	The process of determining a digital euro user's or component's identity.
Individual digital euro user	A natural person who is acting for purposes which are outside his or her trade, business, craft or profession and is allowed to open a digital euro payment account.
Instructed party	A party which is either a payment service provider (PSP) which acts on behalf of itself or another payment service provider (PSP) to receive

[106] Guidelines on fraud reporting under Article 96(6) [4] (EBA-GL-2018-05)
[107] Article 2(20) of Chapter 1 of the draft Regulation [1]
[108] Article 2(11) of Chapter 1 of the draft Regulation [1]
[109] Recital (39) of the draft Regulation [1]

	forwarded settlement requests by digital euro service platform (DESP) from an instructing party.
Instructing party	A party which is either a payment service provider (PSP) which acts on behalf of itself or another payment service provider (PSP) to instruct settlement requests to the digital euro service platform (DESP).
Intermediated access	A model in which the Eurosystem does not directly serve digital euro users but instead relies on a scheme participant to provide onboarding, authentication, distribution, and other digital euro payment services.
Interoperability	The use of common rules, standards and processes across different payment service providers (PSPs).
Inter-PSP fee	A fee paid for each digital euro payment transaction directly or indirectly between two scheme participants.
Issuance of digital euro	A process performed by the Eurosystem which results in the creation of digital euro on the Eurosystem's balance sheet and the redemption of central bank reserves.
Know-your-customer (KYC) check	A mandatory check by scheme participants aimed at identifying digital euro users and risks attached to providing digital euro payment services to them.
Liquidity transfer	The process to transfer reserves between a scheme participant's general central bank reserves and central bank reserves dedicated for use in the digital euro environment. It is performed by the Eurosystem, upon instruction of the scheme participant on request of digital euro users.
Local storage	The secure storage and computational capabilities of a digital euro user's physical devices, such as smart cards or mobile phones.
Machine-to-machine (M2M) payment	Individual payments initiated without human interaction as part of a transfer solution.
Manual defunding	A functionality that allows a digital euro user to manually decrease the digital euro balance on his/her own digital euro payment account.
Manual funding	A functionality that allows a digital euro user to manually increase the digital euro balance on his/her own digital euro payment account.
Merchant category code (MCC)	A four-digit number listed in ISO 18245 standard for retail financial services used to classify a business user by the types of goods or services it provides.

Merchant service charge (MSC)	A fee paid by the payee to a payment service provider when acquiring a digital euro payment transaction.[110]
Mobile device	A device that enables digital euro users to authorise digital euro payment transactions online or offline including, in particular, smartphones, tablets, smartwatches, and wearables of all kinds.[111]
National central bank (NCB)	A national central bank of an EU Member State.[112]
Near-field communication (NFC)-based payment transaction	A payment transaction conducted with near-field communication (NFC) (frequently referred to as contactless) technology that enables communication between devices when in proximity.
Network service provider (NSP)	A provider that offers the network infrastructure as well as other connectivity-related value-added services to facilitate secure transmission of data between entities participating in the digital euro.
Non-digital euro payment account	An account held in the name of one or more payment service user at a commercial bank money payment service provider (CoBM PSP) which holds funds not classified as digital euro.
Offboarding of a digital euro user	A set of activities conducted by a scheme participant, upon the request of the user, to revoke the possibility of a digital euro user to make use of digital euro payment services.
Offboarding of a payment service provider	A set of administrative and technical activities conducted by a back-end infrastructure operator to revoke a payment service provider (PSP) to participate in the digital euro payment scheme and accessing the digital euro service platform (DESP).
Offline digital euro device	A physical device equipped with tamper-resistant hardware (typically a secure element). It enables the secure storage of offline digital euro value/credentials and the secure execution of offline transactions without relying on an online connection, while protecting against tampering and unauthorised modification.
Offline digital euro payment transaction	A digital euro payment transaction made in physical proximity without internet connectivity, where authorisation and settlement take place in the

[110] Article 2(24) of Chapter 1 of the draft Regulation [1]
[111] Article 2(31) of Chapter 1 of the draft Regulation [1]
[112] *ECB glossary*. Source: https://www.ecb.europa.eu/services/glossary/html/glossc.en.html

	offline digital euro device of both payer and payee, without the intervention of a third party.
Offline distribution component	The component(s) of the offline solution that operate at a payment service provider (PSP) back-end system, interacting directly or indirectly with other components like the offline digital euro devices for funding and defunding operations and other components, or the Eurosystem backend.
Offline issuance component	The component(s) of the offline solution that are part of the digital euro service platform (DESP), responsible for the issuance and redemption of the offline digital euro.
On device authentication	A mechanism that allows a user to access a device or application locally, using data stored on the device itself, without the need to contact a remote server.
Onboarding of a digital euro user	A set of activities conducted by a scheme participant to enable a digital euro user to make use of digital euro payment services.
Onboarding of a payment service provider	A set of administrative and technical activities conducted by the Eurosystem to enable a payment service provider (PSP) to participate in the digital euro payment scheme and to access the digital euro service platform (DESP).
Online digital euro payment transaction	A digital euro payment transaction which requires that at least either the payer or the payee is connected to a network and in which the final settlement takes place in the digital euro settlement infrastructure.
Operational risk	The risk that deficiencies in information systems, internal processes, human errors, management failures, or disruptions from external events may lead to service deterioration, interruption, or financial losses.
Other means of payments	Payment instruments and services that are commonly available to end users in the payments market and are supported by the same front-end solution as the digital euro, such as credit transfers, direct debits, card payments, mobile payment solutions, e-money wallets, and open banking-based payments, while explicitly excluding cash and any payment instruments not integrated into the digital euro-supporting front-end solution.
Payee	Anyone who is the intended recipient of funds which have been the subject of a digital euro payment transaction.[113]

[113] Article 2(10) of Chapter 1 of the draft Regulation [1]

Payee payment service provider	A payment service provider which offers digital euro payments services to the payee.
Payee-initiated digital euro payment transaction	A digital euro payment transaction submitted to the digital euro service platform (DESP) by the acquiring payment service provider (PSP) following an instruction from the payee.
Payer	Anyone who has a digital euro payment account and allows a payment order from that digital euro payment account.[114]
Payer payment service provider	A payment service provider which offers digital euro payments services to the payer.
Payer-initiated digital euro payment transaction	A digital euro payment transaction submitted to the digital euro service platform (DESP) by the distributing payment service provider (PSP) following a request from the payer.
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions.[115]
Payment authorisation	The consent given by a payer, or a third party acting on behalf of the payer, to execute the digital euro payment transaction.
Payment initiation service	A service to initiate a payment order at the request of the payment service user with respect to a payment account held at another payment service provider.[116]
Payment institution	A legal person that has been granted authorisation to provide and execute payment services throughout the Union.[117]
Payment instrument	A personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider and used in order to initiate a payment order.[118]
Payment service provider (PSP)	A legal person providing services (e.g. issuing of payment instruments, acquiring, payment authorisation, digital euro user authentication, offering value added service) enabling payments between digital euro users.[119]

[114] Article 2(9) of Chapter 1 of the draft Regulation [1]
[115] Article 4(12) of Title 1 of Directive [4]
[116] Article 4(15) of Title 1 of Directive [4]
[117] Article 4(4) of Title 1 of Directive [4]
[118] Article 4(14) of Title 1 of Directive [4]
[119] Article 4(11) of Title 1 of Directive [4]

Payment service provider (PSP) app	Software application provided by a distributing or acquiring PSP that allows users to access and manage their financial services, including digital euro services, using a mobile device.
Payment service provider (PSP) identifier	A unique code or reference assigned to a payment service provider (PSP) that is used to identify a scheme participant in the digital euro service platform (DESP).
Payment service provider (PSP) mapping	A process of linking a digital euro user's digital euro account number (DEAN) to the corresponding payment service provider (PSP) identifier to enable the exchange of digital euro payment data between involved PSPs.
Payment service provider (PSP) reference data	A set of data of a scheme participant that are relevant to participate in the digital euro payment scheme, for connecting to the digital euro service platform and for the provision of digital euro payment services.
Payment transaction environment	A specific context or setting in which a digital euro payment transaction occurs, such as remote or proximity settings.
Peer-to-peer validated digital euro	A digital euro payment technical solution in which a digital euro payment transaction between a payer and payee does not require validation by a third party.
Person or business-to-government (X2G) digital euro payment transaction	A digital euro payment transaction from an individual digital euro user or a business digital euro user to a government or other public authorities (e.g. payments of taxes, duties and fines).
Personal data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.[120]
Person-to-business (P2B) digital euro payment transaction	A digital euro payment transaction from an individual digital euro user to a business digital euro user. Typical person-to-business (P2B) digital euro payment transactions include point-of-sale (POS) payment orders in shops and e-commerce payment orders over the internet.

[120] Article 4(1) of Chapter 1 of Regulation [7]

Person-to-person (P2P) digital euro payment transaction	A digital euro payment transaction from one individual digital euro user to another.
Point of interaction (POI)	The payee's physical or virtual environment where a payment transaction is initiated.
Point of sale (POS)	The location and system of the merchant's physical premises where a digital euro payment transaction occurs.
Provider of support services	One or more entities, appointed by the European Central Bank, which provide services to all payment service providers distributing the digital euro that are aimed at facilitating the smooth functioning of digital euro payment transactions.[121]
Provider(s) of the Digital Euro Service Platform (DESP)	Entities, Eurosystem and providers of support services, which operate the central infrastructure of the digital euro.
Proximity payment	A payment that is initiated in physical proximity between the payer and payee.
Pseudonymisation	The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.[122]
Quick response (QR) code-based digital euro payment transaction	A digital euro payment transaction initiated via the use of a two-dimensional matrix barcode in the form of a machine-readable optical label with digital information.
Recurring digital euro payment transaction	A repeated digital euro payment transaction for which the payee has previously stored the payer's information and for which the payer has given authorisation (e.g. fixed amount, frequency, end date).
Redemption of digital euro	A process performed by the Eurosystem which results in the redemption of digital euro holdings and of the corresponding liability on the Eurosystem balance sheet.

[121] Article 2(30) of Chapter 1 of draft Regulation [1]
[122] Article 4(5) of Chapter 1 of Regulation [7]

Refund	Reimbursement of the payment amount, in full or in part, to the original payer by the original payee.
Remote payment	A payment that is initiated in a remote environment.
Reservation	A temporary hold on a digital euro amount in the ledger that guarantees availability of funds and is settled at a later stage (e.g., after delivery of goods or services).
Request to pay	A request initiated by a payee to a payer, requesting the payer to pay a certain amount to the payee.
Residence	The place where a natural person is legally resident in the Union.[123]
Reverse waterfall	A functionality whereby commercial bank money (CeBM) from a linked non-digital payment euro account chosen by a digital euro user is automatically converted into digital euro when the digital euro user's digital euro holdings are not sufficient to execute a digital euro payment transaction.
Scheme Governing Authority (SGA)	The decision-making entity responsible for the governance of the digital euro scheme.
Scheme participant	A payment service provider (PSP) that participates in the digital euro scheme, meeting the rules and requirements as set by the digital euro scheme rulebook.
Seamless Embedded Authentication Redirect	Service allowing the payer to authorise a digital euro payment transaction embedded in the payee environment.
Secure element (SE)	A tamper-resistant hardware component that provides a secure execution environment for sensitive applications and data, including cryptographic keys and operations.
Secure Exchange of Payment Information (SEPI)	A component facilitates secure transaction data exchange for digital euro payments, ensuring securing data and fraud prevention through the usage of surrogate values.
Settlement	The completion of a digital euro payment transaction resulting in discharging digital euro users' payment obligations.
Settlement instruction	A request initiated by the Eurosystem access gateway to the digital euro service platform (DESP) settlement component, after all involved payment service provider (PSP) have confirmed and provided the settlement information, to instruct the settlement of a transaction.

[123] Article 2(16) of Chapter 1 of the draft regulation [1]

Settlement recording	Recording of a transaction by atomically reflecting the money transfer between the entry(-ies) to debit and the entry(-ies) to credit including a potential reservation within the settlement ledger.
Settlement verification	A set of processes to check the availability of the payer's balance and perform any other task that may be necessary for the verifying entity, or entities, to assess whether the digital euro payment transaction can be settled.
Standing order	A payment instruction that payers give to their payment service providers (PSPs) to make regular, fixed payments (fixed interval) to a specific payee. Standing orders are automatically executed by payment service providers (PSPs) without the need for intervention by the payer.
Strong customer authentication (SCA)	An authentication based on the use of two or more elements categorised as knowledge (something only the user knows), possession (something only the user possesses) and inherence (something the user is) that are independent, in that the breach of one does not compromise the reliability of the others, and is designed in such a way as to protect the confidentiality of the authentication data.[124]
Surrogate value	A coded value that represents and replaces (sensitive) information so information can be processed safely
Suspension	The process of suspending a PSP's participation in the scheme, including its ability to provide digital euro services, for a defined period of time.
Switching	Upon a digital euro user's request, transferring from one payment service provider to another either the information about all or some digital euro payment services, including recurring payments, executed on a digital euro payment account, or the digital euro holdings from one digital euro payment account to the other, or both, with or without closing the former digital euro payment account, while maintaining the same account identifier.[125]
TARGET services operator(s)	Legal and/or organisational entity/entities that operates/operate the TARGET Services.
Technical proof	The master key/seed phrase generated by the payment service provider (PSP) during the onboarding or switching. It is required in emergency

[124] Article 4(30) of Title 1 of Directive [4]
[125] Article 2(26) of Chapter 1of the daft Regulation [1]

	switching to prove ownership of digital euro holdings in the digital euro service platform (DESP).
Termination	The process of terminating a payment service provider's (PSP's) participation in the scheme, including its ability to provide digital euro services, for an indefinite period of time.
Third country	A country that is not a member state of the European Union.
Third-party service provider (TPSP)	Parties contracted by one or several payment service providers (PSPs) to support their provision of digital euro payments services. Third-party service providers are not bound to a specific service and may support PSPs on services related to the digital euro based on a contractual agreement.
User Alias	A unique pseudonymous identifier used to protect user's identity when processing digital euro payments that can only be attributable to an identifiable natural or legal person by the payment service provider distributing the digital euro or by the digital euro user.[126]
User authentication	A unique piece of information created by the payment service provider distributing the digital euro that together with the user identifier allows a digital euro user to prove ownership of the online digital euro holdings recorded in the digital euro settlement infrastructure.[127]
User experience (UX)	The overall experience a digital euro user has when interacting with digital euro services.
User identifier	A unique identifier created by a payment service provider distributing the digital euro that unambiguously differentiates, for online digital euro purposes, digital euro users but that is not attributable to an identifiable natural or legal person by the European Central Bank and the national central banks.[128]
User journey	A scenario-based sequence of steps that a digital euro user takes to accomplish a specific goal within digital euro services.
Visitor	A natural person who does not have its domicile or residence in a Member State whose currency is the euro, and who is travelling to and staying in one of those Member States, including for tourism, business or education and training purposes.[129]

[126] Article 2(28) of Chapter 1 of the draft Regulation [1]
[127] Article 2(29) of Chapter 1 of the draft Regulation [1]
[128] Article 2(27) of Chapter 2 of the draft Regulation [1]
[129] Article 2(22) of Chapter 1 of the draft Regulation [1].

Waterfall	A functionality for facilitating the settlement of digital euro payment transactions by automatically converting the amount of digital euro that exceeds a defined holding limit into commercial bank money on a linked non-digital euro payment account, indicated by the digital euro user.
Wearable	A broad category of worn or carried physical devices which include a variety of options from less complex devices (e.g. tags) to smartwatches.
Wireframe	A simplified visual outline of the layout and structure of a digital euro service, showing key elements and user interface components.

11 Annexes

A1: Testing, certification and approval

B1: Illustrative user journeys and minimum UX requirements

B2: End-to-end process flows

C1: Reporting requirements

[Placeholder]

D1. Front-end implementation specifications

D2. Back-end implementation specifications

E1: Risk management requirements – CONFIDENTIAL

G1: Rulebook change request form

[Placeholder]