EUROPEAN CENTRAL BANK

EUROSYSTEM

Digital Euro Scheme Rulebook

Version:	0.9
Status:	DRAFT
Date:	30/06/2025

DISCLAIMERS FOR DRAFT RULEBOOK v0.9

Preliminary and non-binding nature of version 0.9

This document represents a preliminary draft version (version 0.9) 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 0.9, which was shared with the RDG members on 30 June 2025, 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.

Rulebook development process

The content of version 0.9 is subject to further adjustments and refinements as part of the development process in the context of the digital euro project's preparation phase, as well as necessary adjustments arising from legislative discussions.

This document has not been approved by the ECB's decision-making bodies. It is a working document meant to involve stakeholders and foster transparency and collaboration in the rulebook development process. As a result, version 0.9 incorporates input from various stakeholders, including members of the RDG, who in turn represent diverse perspectives from both the public and private sectors. While care has been taken to represent accurately all views and forge consensus where possible, the combined content of version 0.9 need not fully reflect the views of individual RDG members, their organisations, or the broader constituencies they represent.

A final draft of the preliminary rulebook will incorporate any future amendments stemming from legislative discussions among co-legislators on the European Commission's proposed regulation on the establishment of the digital euro[2] and be subject to public consultation.

Informational purpose only

The publication of this draft is for informational purposes only and does not constitute or imply any commitment, guarantee or precise assurance regarding the final content, standards and scope of the digital euro rulebook. The publication of this draft is not meant to create expectations of the ECB endorsement or finality of any specific policy, framework, legal or operational approach related to the digital euro. The document should be considered as a reflection of a work-in-progress, open to ongoing input and discussion.

[1] https://www.ecb.europa.eu/euro/digital_euro/timeline/rulebook/html/index.en.html
[2] COM(2023) 369 final, 28.6.2023, available at: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:52023PC0369

No reliance for implementation

Due to its preliminary nature, the draft rulebook version 0.9 is not intended for use as a basis for implementing any systems, processes, or policies related to the digital euro. Any such actions, prior to the publication of the officially approved rulebook, are under actors' own responsibility.

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 has been further developed compared to the last version 0.8 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 is generally based on the 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). Both proposals are currently subject to the legislative process, in which the EU co-legislators can decide to amend the proposals. Therefore, the current draft rulebook remains sufficiently flexible to cater for potential adjustments and can only be finalised after the adoption of both regulations. Furthermore, other areas of the rulebook will be further developed in line with ongoing elaborations on complex subject matters and decisions by the Governing Council of the ECB or are dependent on the selection 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.

The purpose of the current draft is to inform the RDG and its constituencies, and to invite them for further comments in order to further advance the rulebook drafting.

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]	2023/0212/COD	Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro
[2]	2023/0211/COD	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	European Accessibility Act (EAA).

Table 0-1 - Documents referenced

0.2 List of annexes

- A1: Certification, testing and onboarding
- B1: Illustrative User Journeys
- B2: End-to-end flows
- C1: Reporting requirements
- D1.1 Front-end implementation specifications
- D1.2 Core data requirements
- D2. Back-end implementation specifications
- E1: Risk management requirements - CONFIDENTIAL
- F1: Minimum UX requirements
- G1: Rulebook change request form

0.3 Change history

The change history has the following logic. 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.

New versions 0.9x will be 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 issuance of the draft regulation [1]. The public consultation will be on this first version of the first draft after its alignment with the EU Regulation.

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 10).

Issue number	Dated	Reason for revision
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	6th 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	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.

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 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. This rule numbering convention is specific for the rulebook and does not cover the current numbering convention used for the business rules outlined in section 3, dispute management requirements in section 5 and related annexes.

Rulebook section	Rulebook #
Document information	DOI.XX
Scheme rulebook Scope	SRS.XX
Participation and adherence requirements	PAR.XX
Functional requirements	FUR.XX
Technical requirements	TER.XX
Risk management requirements	RMR.XX
Dispute management requirements	DMR.XX
User experience requirements	UXR.XX
Brand rules	BRR.XX
Digital euro fees, limits and tresholds 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 payments 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 PSP 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 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 or visitors. Additionally, subject to agreements or arrangement between the European Central Bank and respective central banks, services may be provided to national and legal persons residing or established in EU member states outside the euro area[1] or other third-countries[2].The geographical scope allows for the provision of both domestic and cross-border digital euro payment transactions.

[1] Subject to article 18 of Procedure 2023/0212/COD - proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro and Procedure 2023/0211/COD - 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

[2] Subject to article 19 and 20 of Procedure 2023/0212/COD - proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro

1.4 Participants' scope

1.4.1 Actors involved

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):

- **Payer,** which can be *''anyone who has a digital euro payment account and allows a payment order from that digital euro payment account''*[3]. A payer can either be a natural or a legal person. The rulebook and its annexes occasionally refers to the Payer as the "consumer" or "digital euro individual user," depending on context.
- **Payee,** which can be *''anyone who is the intended recipient of funds which have been the subject of a digital euro payment transaction''*[4]. A payee can either be a natural or a legal person. The rulebook and its annexes occasionally refers to the Payee as the ''merchant'' or ''digital euro business user'', depending on context.
- **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[5]. The rulebook and its annexes occasionally refers 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 is referred to as the **acquiring PSP**. The rulebook and its annexes also occasionally refers to the Payee PSP as the ''payee distributing PSP'' or the ''business user PSP'', depending on context; or;
    - **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 entity 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 can not be the same entity as the payee PSP / the acquiring PSP.

---

3 As defined in the proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro (COM/2023/369 final) (and amended over time)

4 As defined in the proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro (COM/2023/369 final) (and amended over time)

5 As defined in section 1.5 Services in scope of this rulebook

- **(Potential) third-party services providers** 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**
- **Provider(s) of the digital euro service platform (DESP)**
- **Providers of TARGET services** relevant to the provision of the digital euro payment 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 accounts. These PSPs are, therefore, participants in the digital euro scheme, acting at a minimum as ‘’commercial bank money PSPs’’.

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 ‘’distributing PSPs’’.

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, acquiring PSPs, the payer’s commercial bank money PSP and the payee’s commercial bank money PSP are all 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 before and involved in digital euro payment services and their relationships, categorised into six types.

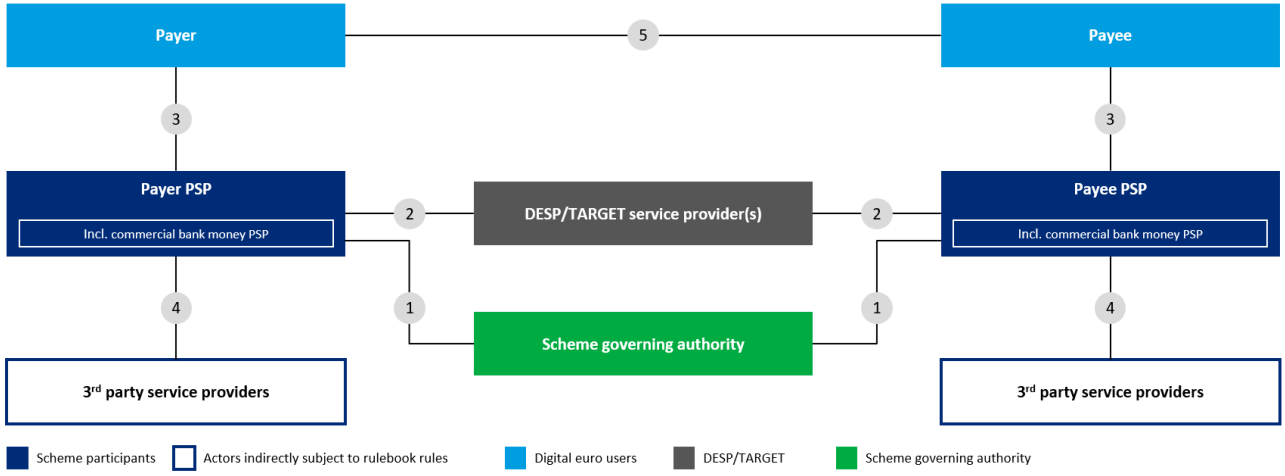

Figure 1-1 Scheme actors model

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

(2) The relationship between a participating PSP and the providers 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. The provision of DESP DCAs to PSPs will be governed by the TARGET Guideline.

(3) The relationship between the digital euro user (payer, payee) and their PSP for digital euro payment services are 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 to ensure harmonised provision of basic digital euro payment services.

(4) The relationship between a participating PSP and its third-party service provider are 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 DESP/TARGET service provider(s) and the Scheme Governing authority 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]. Namely, Annex I lists the following services (to be amended over time) 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:
    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][6] 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.

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

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

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

1.6 Payment instruments, acceptance solutions and communication technologies in scope

1.6.1 Payment instruments in scope

The set of rules, standards, and procedures included in the rulebook for the provision of digital euro payments services covers the following electronic payments instruments and user to application interfaces:

- Mobile applications - for online and offline digital euro
- Websites - for online digital euro
- Physical card (including battery powered cards) - for online and offline digital euro

[6] Payment service providers providing account servicing payment services within the meaning of Directive 2015/2366 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 app[7] - for online and offline digital euro

1.6.2 Acceptance solutions in scope

For the provision and acceptance of digital euro payments services the rulebook covers the following acceptance solutions:

- Point-of-sale terminals and devices – for online and offline digital euro
- E-Commerce checkout webpages – for online digital euro
- M-commerce checkout applications – for online digital euro
- ATMs – for online and offline digital euro
- Apps and digital euro app – for online and offline digital euro
- Battery-powered cards – for offline digital euro

1.6.3 Communication technologies in scope

The rulebook covers the following communication technologies enabling the transmission of data between two devices:

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

1.7 DESP and TARGET

The Eurosystem's provision of DESP services (incl. 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.

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

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 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 participant's non-adherence with the rulebook requirements, while also addressing potential exemptions and scheme governing authority rights. Finally, it describes the procedure for a participant's withdrawal from the scheme, ensuring participants understand their obligations and rights.

2.2 Scheme participation

Further details on the onboarding process will be provided in a dedicated scheme and DESP onboarding guides. For the offline digital euro, the XXX 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, an entity shall fullfil the following eligibility criteria and demonstrate them when requesting participation and during their onboarding process to the scheme:

(1) the entity 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 [1].

(2) the entity needs to have a signed and valid servicing contract with the operator of the digital euro service platform (DESP);

(3) the entity needs to have access to a DESP DCA, i.e. being able to be debited/credited in a DESP DCA as part of a funding/defunding operation, but not necessarily owning or being able to directly instruct a DESP DCA; and

(4) the entity shall meet the rules set by the digital euro scheme rulebook.

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 scheme governing authority of any matter that does or could change or materially affect its eligibility to participate without undue delay.

PAR.04 In the event the scheme participant does not fulfill eligibility criteria PAR.01(1) any longer, the scheme governing authority will terminate the participation in the scheme.

PAR.05 In the event a scheme participant does not fulfill eligibility criteria PAR.01(2) or PAR.01(3), the scheme governing authority may terminate the participation in the scheme (see PAR.61).

PAR.06 In the event a scheme participant does not fulfill the eligibility criteria PAR.01(4), the scheme governing authority will start the process described in the rulebook for not adhering to scheme rules (see section 2.5).

PAR.07 The scheme governing authority must take reasonable measures to inform the scheme participant of matters affecting a scheme participant's participation status. The scheme governing authority may take measures to inform other scheme participants or digital euro users of a loss of eligibility.

2.2.2 Becoming a participant

PAR.08 To become a scheme participant an applicant shall undergo the onboarding process to the scheme, including the necessary processes required to meet eligility 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 scheme governing authority and follow the process described in the below sections 2.2.2.1 to 2.2.2.6.

PAR.09 The application may be iniated by the scheme governing authority for PSPs subjected to mandatory provision of digital euro services.

Figure 2-1 - PSP onboarding process overview

2.2.2.1 PSP initiation of scheme participation

PAR.10 To initiate the application process, the applicant shall contact the scheme governing authority to request the necessary registration documentation required to start the participation request process. The scheme governing authority may proactively share the relevant documentation with PSPs subjected to mandatory provision of digital euro services..

PAR.11 The applicant shall submit a completed and signed participation request form along with all necessary documentation to the scheme governing authority.

PAR.12 In any step of the process, the applicant shall reply to any request of the scheme governing authority for additional information and documentation without undue delay.

2.2.2.2 Validation of the PSP request to scheme participation

PAR.13 The scheme governing authority validates the participation request and the comprehensiveness of the necessary documentation for the PSP application against the eligibility criteria set in section 2.2.1.

PAR.14 The applicant shall follow the onboarding guide provided by the scheme governing authority via an online portal.

PAR.15 In case of mandatory provision of digital euro services, the scheme governing authority validates the PSP request to scheme participation immediately, trigering the submission of application to participate by the PSP (see section 2.2.2.3).

2.2.2.3 Submission of application to participate by the PSP

PAR.16 Once the PSP's application is validated, the official registration of the PSP's application for scheme participation is finalised and communicated to the applicant.

2.2.2.4 PSP solution(s)[8] certification

PAR.17 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.18 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 D1.1 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 and Certification. The processes for (ii) back-end testing and certification are defined in the [DESP onboarding guide for PSP].

2.2.2.5 PSP solution(s) approval

PAR.19 The [Certification Entity] of the scheme governing authority 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 scheme governing authority, 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.20 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 scheme governing authority. 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 basic services as required bythe draft regulation [1].

The details for PSP solution(s) approval are described in annex A1 Testing and Certification.

2.2.2.6 PSP operationally ready to offer digital euro payment services

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

PAR.21 An applicant becomes a scheme participant once it has been confirmed by the scheme governing authority that it successfully meets all eligibility criteria and has successfully undergone the onboarding process, including the certification and approval for its solutions by the scheme governing authority.

PAR.22 The scheme governing authority shall communicate the PSP's participation by updating the list of digital euro scheme participants available on the ECB website.

2.2.3 Register of digital euro scheme participants

PAR.23 The scheme governing authority maintains and regularly updates the list of digital euro scheme participants, accessible via the ECB website. The list 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 (BIC); (iii) type of entity/license owned, (iv) the certified and approved digital euro solutions it provides, and (v) the date on which each entity acquired Participant status.

PAR.24 By submitting an application to become a voluntary participant, an entity consents to the publication of the details outlined in this section.

PAR.25 In the event of changes to an applicant's / scheme participant's information, resulting in inaccuracies in the list of scheme participants, the participant shall inform the scheme governing authority at the earliest reasonable opportunity.

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

2.4 Adherence to the rulebook

PAR.26 A scheme participant shall adhere to (or comply with) the digital euro scheme rulebook from the moment it joins the scheme, ensuring full adherence with all rulebook provisions throughout its participation. This obligation also applies in case of outsourcing and use of third-party service providers.

PAR.27 Furthermore, scheme participants shall ensure that the requirements eventually applicable to merchants and customers are complied with, by the latter.

PAR.28 A scheme participant shall conduct self-assessments of adherence with rulebook requirements initially, at the point of onboarding in line with section 2.2.2., and continuously afterwards, on an annual basis. A scheme participant shall communicate the outcome of of the self-assessments to the scheme governing authority. For the purpose of conducting self-assessments, an assessment methodology and templates will be provided by the scheme governing authority to scheme participants.

PAR.29 A scheme participant must promptly, upon identification, report a breach with a rulebook rule to the governing authority. In case a scheme participant has identified a breach with a rule of the rulebook, the scheme participant may request a temporary exemption because of specific circumstances from the governing authority in line with the exemption requirements outlined in section 2.6.

PAR.30 The governing authority will also assess a scheme participant's adherence to the rulebook. Other stakeholders may inform the governing authority of potential non-adherence of a scheme participant, including, through reports or feedback from digital euro users via established complaint mechanisms.

PAR.31 In case the governing authority has confirmed the non-adherence, the scheme participant will be informed and requested to refrain from the actions resulting in non-adherence and/or take any appropriate remedial action.

PAR.32 The response of the governing authority to non-adherence is commensurate with the severity and impact of the breach, ensuring a balanced, fair and effective approach to scheme participants' non-adherence. The measures outlined in the paragraphs [PAR.33] – [PAR.47] are neither cumulative nor sequential. Any timeframes for the measures are indicative and dependent on the application of the principle of proportionality.

PAR.33 Upon verification of non-adherence by the governing authority, the governing authority will issue an initial notice of non-adherence to the scheme participant. The adherence notice will be addressed to the management body of the scheme participant.

PAR.34 The written non-adherence notice from the governing authority will:

1. Specify the exact rulebook terms or provisions that are not met.

2. Assign a severity level (high, medium, low)[9] to the non-adherence, based on the type of rulebook requirement that was breached, the materiality of the breach, the existence of persistent or cumulative cases of non-adherence.

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

4. Provide a deadline for full rectification of adherence (60 days), which may be adjusted based on the level of severity of the non-adherence.

5. Require reporting back to the governing authority upon rectification of the remediation measures put in place by the scheme participant.

6. Inform the scheme participant about their right to object the notice if they believe it is incorrect. The scheme participant needs to provide adequate reasons for their objection to the governing authority in writing (20 days). The governing authority will then assess the objection and in the case that it is rejected, provide a written statement with a justification to the scheme participant. In this case, the governing authority will also inform the scheme participant of the points (3)-(5).

PAR.35 A scheme participant must submit a remediation plan to the governing authority in writing within the deadline specified in the adherence notice. The plan should detail corrective actions, timelines for their adoption, and anticipated outcomes, demonstrating the scheme participant's commitment to resolving the non-adherence.

[9] 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.

PAR.36 Alternatively, in cases of low severity, a scheme participant may respond to the initial notice of non-adherence with a request for a temporary exemption based on unique or extenuating circumstances. This shall be in line with the exemption requirements outlined in section 2.6.

PAR.37 In cases of high severity, the scheme participant may be required to take immediate action to resolve the non-adherence, rather than providing a remediation plan.

PAR.38 If a scheme participant fails to meet the deadlines set in the initial adherence notice or the submitted remediation plan, the governing authority will issue second non-adherence notice. The governing authority may extend the remediation deadline, contingent on:

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

PAR.39 If the remediation plan is not considered adequate by the governing authority, another written notice with a request to amend the plan may be notified to the scheme participant.

2.4.1 Penalty mechanism

PAR.40 Failure to act in line with the adherence notice within the imposed deadlines or in line with the remediation plan may result in further actions being taken by the governing authority against the scheme participant in the form of pecuniary fines or contractual penalties. The governing authority 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 participant's planned or existing remediation measures or with a request for further time in order to address the non-adherence.

PAR.41 In cases of continued non-adherence, the governing authority may impose effective, proportionate and dissuasive penalties or fines, taking into account the scheme participant's size, activity and non-adherence's impact.

PAR.42 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.43 In cases of low severity non-adherence, in order to apply the principle of proportionality, the governing authority may provide guidance rather than impose fines, focusing on corrective actions.

2.4.2 Suspension

PAR.44 The governing authority 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 governing authority must notify the management body of the scheme participant in writing, indicating the grounds and the time period 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 portability and minimising disruption.

2.4.3 Termination

PAR.45 The governing authority 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 governing authority of the termination, the scheme participant will also have the opportunity to contest the termination, prior to it taking effect, providing adequate grounds to the governing authority in case of objection.

PAR.46 In clearly and narrowly defined exceptional circumstances, immediate exclusion of a scheme participant from the digital euro scheme by the governing authority 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 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 governing authority, and will take into account, amongst others, the remaining operational capabilities of the scheme participant.

PAR.47 Upon the termination of a scheme participant's participation in the scheme, the governing authority must publicly communicate its termination, having already ensured prior to facilitate a smooth transition of services for digital euro users. 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.48 A scheme participant that is not subject to the obligation of mandatory provision of the digital euro services under the draft regulation [1] 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 scheme governing authority. The scheme participant would need to inform its digital euro users of the withdrawal and about the process of digital euro account switching.

PAR.49 In all cases where a scheme participant withdraws its participation, they must ensure continued access for users to the digital euro scheme until the end of the scheme participant's participation.

PAR.50 The scheme participant needs to ensure adherence with all rulebook requirements and remains responsible until the end of participation.

PAR.51 The scheme participant shall support potential dispute cases, ensure data storage and availability as well as fee settlement beyond the termination of its participation in the digital euro scheme.

PAR.52 The scheme participant shall facilitate, in advance of the technical offboarding from the DESP, the switching of digital euro accounts of digital euro users to other scheme participants.

PAR.53 The withdrawal of a scheme participant's participation in the scheme should also be publicly communicated, including the last day of the scheme participant's operations, 30 days before the day of which the withdrawal enters into effect by the governing authority.

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 supported by end-to-end (E2E) process flows. Summarised process flows are included in this section while detailed process flows are included in Annex B2 – E2E flows. The process flows were designed on the basis of illustrative user journeys, available in Annex B1– Illustrative user journeys.

3.2 Illustrative user journeys

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

FUR.01 The user journeys are illustrative of the intended outcomes and are not directly binding for scheme participants.

FUR.02 Scheme participants may offer additional use cases not included in the illustrative user journeys

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

3.3 Identification of digital euro users

3.3.1 Digital Euro Account Number

FUR.03 When requesting a Digital Euro Account Number (DEAN) from the Digital Euro Service Platform (DESP) to create a new digital euro account, scheme participants shall provide a pseudonymised digital euro user unique identifier mirroring the attributes of Personal Identification (PID) foreseen by the eIDAS2 Regulation.

FUR.04 A DEAN is requested by a scheme participant from the DESP. The DESP generates the DEAN and then provides it to the requesting PSP. The PSP then assigns the DEAN to the digital euro user that wishes to open digital euro services.

FUR.05 The DEAN is independent of the requiring PSP and does not rely on country identification.

FUR.06 Even though, the DEAN is PSP and country agnostic, scheme participants can request PSP and country identification to DESP: a mapping table linking each DEAN with its PSP identifier will be requestable by the scheme participant. This table will make it possible to identify the scheme participants responsible for an account and the country associated to this scheme participant.

FUR.07 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.
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).

3.3.2 Alias

The DEAN is the basic identifier requested in the digital euro legal act, 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 user in the payment process as long as the alias is registered.

FUR.08 The provision of an alias by the user is voluntary.

FUR.09 Scheme participants shall support the alias registration.

FUR.10 Consumers can use an alias, mapped to the corresponding DEAN, for identifying themselves and using digital euro services.

FUR.11 An alias shall only be a phone number that is linked to the digital euro individual user.

FUR.12 There is only a one-to-one relationship between the alias (phone number) and DEAN.

FUR.13 Scheme participants shall perform an alias verification when registering 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).

FUR.14 In case an individual user's mobile 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 alias. His/her PSP should then take the request further to the DESP component – following the alias verification as outlined above. It is also recommended that PSPs put in place a periodic (e.g. annual) reconfirmation requirement to ensure that their customers' alias is still up to date.

FUR.15 Business users are not able to use an alias as an identification method.

FUR.16 When using a physical card as a form factor, the DEAN shall be printed on the card to identify users

3.3.3 Identification and authentication of components

FUR.17 Only those components provided by a scheme participant or any other third party registered within the scheme shall be authorised to operate within the digital euro transaction flows.

Digital euro components refer to the various technological and infrastructural elements that collectively enable digital euro transactions between parties. The components include ATMs, physical POS or virtual POI, merchant devices, APIs, applications or chipcards. To ensure the security, integrity and efficiency in this ecosystem, the identification and authentication of these different components are essential.

The interactions, communication, and identification protocols for these components will be elaborated in the rulebook section dedicated to their respective use cases.

Every specific interaction point will be detailed once the respective specification work concludes e.g. the card to terminal specifications will likely be driven by the standard selected for the respective transaction lag. The standard will define in which way the card/phone identifies itself towards the terminal. The same will need to be defined also for all the different other use cases.

3.4 Authentication of digital euro users

3.4.1 Users onboarded on the digital euro app

FUR.18 Scheme participants shall implement and make available seamless authentication for online digital euro transactions and online access to digital euro 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.19 Scheme participants shall enroll 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.20 For e-commerce transactions, decoupled authentication using biometrics or a PIN via a notification in the user's digital euro or PSP app is the primary authentication method.

3.4.2 Users relying on PSPs' digital interfaces

FUR.21 Scheme participants are free to implement their preferred strong customer authentication method when users rely on their digital interfaces. The authentication method shall comply with all applicable regulatory frameworks and associated security requirements.

FUR.22 Scheme participants must abide by the minimum user experience standards set in section 8.

3.4.3 Authentication for offline digital euro

FUR.23 Authentication for offline payment transactions (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 Authentication with no smartphone (inclusion use cases)

FUR.24 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 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.25 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 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 of most relevance to digital euro users.

- **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 a digital euro**: details funding/defunding of the user’s digital euro account from and to a non-digital euro payment account to be available 24 hours a day during all calendar days of the year 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 and 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.

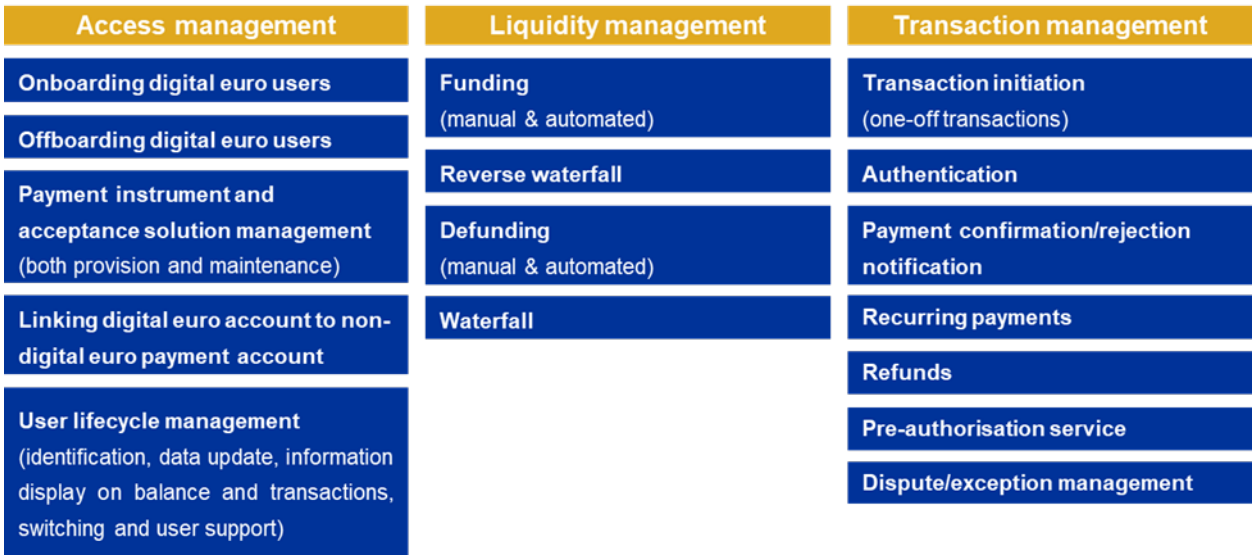

Figure 3-1 Overview of digital euro services

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

FUR.27 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.

<u>High-level overview</u>

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[10]. 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 Euro 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.

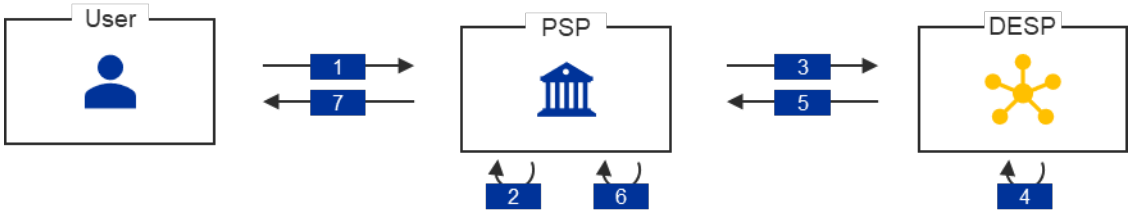

Figure 3-2 High level flow for the onboarding of a digital euro user

Description of steps:

1. The user requests its PSP to provide access to digital euro services
2. The PSP onboards (only if unknown) and/or authenticates the user according to its processes and applicable regulations
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
5. The DESP returns the generated DEAN and confirms to the PSP the updated mapping
6. 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)
7. The PSP informs the user about successful onboarding and shares the DEAN associated with the digital euro account.

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

[10] 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.

Applicable business rules and end-to-end flows

Business rules	
Individual user business rules:	
AM-011-001	An individual user can have only one digital euro 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 account.
AM-011-004	If an individual user already holds a digital euro account, the PSP should offer the user to switch the existing account instead (see section 3.5.2.2).
AM-011-005	When opening a new digital euro 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 accounts.
AM-012-002	A business user can have an unlimited number of offline digital euro devices.
AM-012-003	When opening (a) new account(s) upon an onboarding request from a business user, the PSP must request one or multiple DEAN(s) 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	
AM-1.1	Onboarding of an individual user part I (online and offline)
AM-1.2	Onboarding of a business user (online and offline)
AM-1.3	Digital euro app configuration and onboarding of an individual user

3.5.2.2 Switching

FUR.28 Scheme participants are responsible for the switching function enabling individual users to seamlessly transfer digital euro holdings as well as all or some digital euro payment services across PSPs, while maintaining the same DEAN.

FUR.29 Scheme participants shall ensure a seamless transition of digital euro 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, mobile applications, and in-person customer service.

FUR.30 Upon receiving a switching request, the new PSP shall gather the necessary data and conduct 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.31 Individual users shall not be charged fees for switching including transferring transaction history, and/or standing orders and recurring payments, and a remediation period of at least 90 days shall be granted to resolve any issues arising from the switch.

FUR.32 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 accounts 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.33 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.34 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, cannot be recovered. Therefore, the new PSPs should clearly communicate this limitation to the user, confirm the completion of the process, and provide any necessary follow-up information.

High-level switching overview

Scheme participants shall enable 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 were to 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 her digital euro holdings. Such a procedure will allow digital euro users to switch to another scheme participant even without the support of the previous 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 previos PSP's data in the emergency case.

Account switching does not cover the switching of individual user's offline digital euro holdings. Since they are locally stored on the offline device, prior to deactivating the offline device for the switching any offline digital euro holdings can be defunded to either online digital euro holdings, private money or cash, or 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
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 3.5.4.5); • 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 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 3.5.4.4, after obtaining one single explicit consent to seamlessly continue all such arrangements without requiring the user to re-authorise each one individually.
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 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 device 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 account(s) nor their offline devices and holdings.
End-to-end flows	
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.35 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.36 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.

High-level lifecycle managment overview

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

- Manage digital euro 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 account(s)	
Individual user business rules:	
AM-021-001	The PSP must give individual users the possibility to block and unblock their digital euro 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 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 (a) new digital euro account(s) (see section 3.5.2.1 or close (an) existing digital euro account(s).

AM-022-002	If the digital euro account to be closed happens to be the last digital euro account of that business user with the PSP, the PSP must initiate the offboarding on behalf of the business user (see section 3.5.2.4).
AM-022-003	The PSP must ensure that a digital euro account of a business user is maintained for the period of [to be defined] after closure for refunds and claims (see section 3.5.4.6).
Business rules - Viewing, registering or edititing profile settings such as alias(-es)	
Individual user business rules:	
AM-021-002	The PSP is only allowed to register aliases for users to which it provides digital euro services.
AM-021-003	The PSP is only allowed to register aliases for individual users.
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 user.
AM-021-006	Only one alias can be registered per digital euro account.
AM-021-007	The PSP must verify that the alias provided is available to the user.
AM-021-008	The PSP must manage its user's aliases by promptly updating, amending and deactivating them as soon as a change is required by the users.
AM-021-009	The PSP is responsible for the correctness of the association between the alias and the user's DEAN and shall be liable for any damage caused by an incorrect association.
AM-021-010	The PSP is not permitted to use the registered alias(es) received as part of a digital euro payment instruction/request for any other purpose than the initiation of a digital euro payment transaction.
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 at least the following notifications: • a credit to their digital euro account • a debit to their digital euro 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
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 at least the following notifications: • a credit to their digital euro account • a debit to their digital euro account • execution of a waterfall transaction

	• execution of a reverse waterfall transaction • execution of an offline funding transaction • execution of an offline defunding transaction • 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.
Businss 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 account can be any payment account held by the user at either the same PSP which services the user's digital euro 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 account for funding and defunding purposes including waterfall and reverse waterfall (see section 3.5.3), either during onboarding or at any later point in time.
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 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 account(s) and must allow to change the link to a payment account(s), while ensuring that a business user's digital euro 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 3.5.3.2).
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 about the current online digital euro balance and transaction history at the user's request. For offline digital euro holdings, the PSP must inform the user of the current offline balance stored locally on the user's offline device.
Business rules - Blocking and unblocking digital euro payment instrument(s) or acceptance solution(s)	

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, app, offline 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 digital euro 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 is reported found or recovered by the authorised individual user.
AM-021-021	When an offline device connects online, the PSP must check whether the offline device has been reported lost or stolen and if so the status of the offline device shall be set as disabled.
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, payment gateway, 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).
End-to-end flows	
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 notification preferences)
AM-4.1.4	End user (individual) amendments (offline notification preferences)
AM-4.1.5	End user (individual) amendments (un-blocking digital euro form factor(s))
AM-4.1.6	End user (individual) amendments (un-blocking digital euro account)
AM-4.1.7	End user (individual) amendments (de-activate form factors)
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.37 As scheme participants, PSPs are responsible for the offboarding of digital euro users.

FUR.38 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 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.

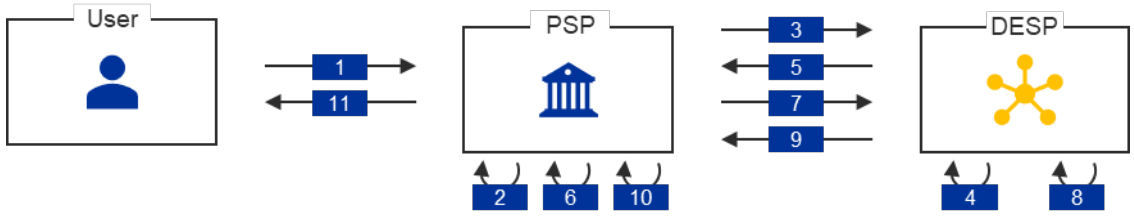

Figure 3-3 - High level flow for the offboarding of a digital euro user

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 account and payment instrument(s) or acceptance solution(s)
3. If the user's digital euro 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 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 account and deactivate user registration
8. The DESP deactivates the user registration and closes the user's digital euro account
9. The DESP confirms the deactivation of user registration and closing of the user's digital euro account to the PSP
10. The PSP disables 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	
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 3.5.4.5); • 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 account(s) is (are) blocked by the PSP for e.g. compliance or fraud reasons.
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 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 payments 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 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	
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 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 requires linking an existing non-digital euro payment account with the online digital euro account.

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

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

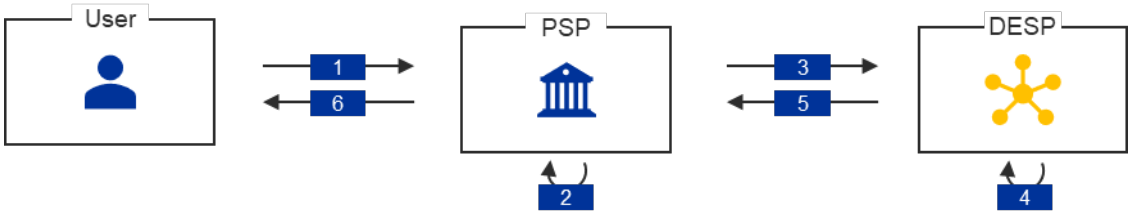

Figure 3-4 High level flow for a manual (de)funding operation[11]

Description of steps:

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

3.5.3.1 Funding

FUR.39 Scheme participants shall support the full range of funding functionalities for users to fund their digital euro holdings.

FUR.40 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 digital euro holdings online and offline. Funding can be done from a non-digital euro payment account held at the scheme participant of the user's choice or from cash. Funding functionalities from non-digital euro payment accounts shall be available 24 hours a day and on all calendar days of the year. Funding from cash via ATM or PSP's branch(es) of

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

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 manual funding from a non-digital euro payment account or cash;
- Online automated funding from a non-digital euro payment account.

Offline digital euro funding

- Offline manual funding from a non-digital euro payment account or cash;
- Offline manual funding from online digital euro holdings;
- Offline 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 payment account held by the user at either the same scheme participant which services the user's digital euro 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 functionalities can be activated at the individual user's choice from a non-digital euro payment account (e.g. the linked payment account).[12] Additionally, in case of offline, automated funding functionalities can be activated from the online digital euro holdings. 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 an outgoing transaction.[13]

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

Applicable business rules and end-to-end flows

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

Business rules	
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 on 24 hours a day and on all calendar days of the year. The non-digital euro payment account can be any payment account held by the user at either the same PSP which services the user's digital euro account or at another PSP that is a scheme participant.
LM-020-002	The PSP must ensure that the manual funding functionalities from cash are available to digital euro users who have an existing relationship with the PSP, with these functionalities accessible trough ATM and/or PSP's branch according to their respective service hours if provided by the PSP.
Individual user business rules:	
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 3.5.3.2), 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 start date, funding frequency, and funding amount, 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 an outgoing transaction.
LM-021-004	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-021-005	The PSP must allow individual users to specify that the automated funding can only be applied if the non-digital euro payment account holds sufficient balance, only within the financial agreement specified between the user and the PSP providing the non-digital euro payment account.
LM-021-006	If the individual user has linked a non-digital euro payment account to the digital euro account, this linked 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 payment account.
LM-021-007	After having made any debit to the individual user's digital euro account (see section 3.5.4), the PSP must check if the available balance on the online digital euro 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	
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 PSP (triggered by digital euro PSP)

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 PSP (triggered by digital euro PSP)
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
Ofline end-to-end flows:	
LM-1.8	Offline manual funding from non-digital euro payment account via app
LM-1.9	Offline manual funding from online digital euro holdings via app
LM-1.10	Offline digital euro manual funding of offline card from online digital euro holdings via app & NFC device
LM-1.11	Offline digital euro manual funding from cash deposit at ATM with card (contact and contactless) or smartphone
LM-1.12	Offline scheduled/automated funding from non-digital euro payment account via app
LM-1.13	Offline scheduled/automated funding from online digital euro holdings via app

3.5.3.2 Defunding

FUR.41 Scheme participants shall support the full range of methods for user's to defund their digital euro holdings.

FUR.42 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 digital euro holdings online and offline. Defunding can be done to a non-digital euro payment account at the scheme articipant of the user's choice or to cash. Defunding functionalities to a non-digital euro payment account shall be available 24 hours a day and on all calendar days of the year. 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 manual defunding to a non-digital euro payment account or cash;

- Online automated defunding to a non-digital euro payment account.

Offline digital euro defunding

- Offline manual defunding to a non-digital euro payment account or cash;
- Offline manual defunding to online digital euro holdings;
- Offline 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 payment account held by the user at either the same PSP which services the user's digital euro 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 (e.g. the linked payment account).[14] Aditionally, in case of offline, automated defunding functionalities can be activated to the 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 treshold (within the holding limit), which is automatically maintained by defunding the surplus amount if the set maximum treshold is breached after an incoming 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	
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 on 24 hours a day and on all calendar days of the year. The non-digital euro payment account can be any payment account held by the user at either the same PSP which services the user's digital euro account or at another PSP that is a scheme participant.

[14] The non-digital euro payment account can be any payment account held by the user either at the same PSP which services the user's digital euro account or at another PSP that is a scheme participant.
[15] 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.

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.
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 start date, defunding frequency, and defunding amount, 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 user has set up automated defunding and the defunding amount is not available on the digital euro account, the defunding process must be aborted and the PSP must inform the user.
LM-041-004	If the user has linked a non-digital euro payment account to the digital euro account, this linked 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 select another non-digital euro payment account instead of the linked payment account.
LM-041-005	When processing an incoming transaction to the user's digital euro account (see section 3.5.4), the PSP shall check if the incoming transaction would breach the maximum threshold specified by the user on the online digital euro 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	
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 PSP (triggered by digital euro PSP)
LM-2.3	Online automated/scheduled defunding to non-digital euro payment account same PSP
LM-2.4	Online automated/scheduled defunding to non-digital euro payment account different PSP (triggered by digital euro PSP)
LM-2.5	Online manual defunding with cash withdrawal at PSP branch
LM-2.6	Online manual defunding with cash withdrawal at ATM though 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 (PwCB) with NFC through card (contact and contactless) or smartphone
LM-2.8.2	Online purchase with Cash Back (PwCB) with QR code

Offline end-to-end flows:	
LM-2.10	Offline manual defunding to non-digital euro payment account via app
LM-2.11	Offline digital euro manual defunding to online digital euro holdings via app
LM-2.12	Offline digital euro manual defunding to online digital euro holdings via app & 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
LM-2.15	Offline scheduled or automated defunding to online digital euro holdings via app

3.5.3.3 Reverse waterfall

FUR.43 An individual user may allow automatic transfers of money via a reverse waterfall functionality from the linked non-digital euro payment account if digital euro holdings are not sufficient to complete a digital euro payment transaction.

FUR.44 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 money 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 to enforce business user's online holding limit while ensuring an adequate user experience when paying a business in digital euro (see section 3.5.3.5).

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

Busines rules	
General business rules:	
LM-030-001	The PSP must ensure that the reverse waterfall functionality is available to digital euro users on 24 hours a day and on all calendar days of the year.
LM-030-002	If reverse waterfall is 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 that the reverse waterfall can only be applied if the linked 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.
Business user business rules:	
LM-032-001	The PSP must ensure that a business user has activated the reverse waterfall option at all times.
End-to-end flows	
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.45 An individual user may allow automatic transfers of money to the linked non-digital euro payment account via a waterfall functionality if the online digital euro holding limit is reached.

FUR.46 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 money 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 payment.

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 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

In exceptional circumstances an additional waterfall may be necessary after 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
General business rules:

LM-050-001	The PSP must ensure that the waterfall functionality is available to digital euro users on 24 hours a day and on all calendar days of the year.
LM-050-002	If waterfall is required, 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	
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
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.47 Scheme participants shall comply with the business rules applicable to enforcing the digital euro holding limits for user's digital euro accounts as defined in this subsection.

Business rules	
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 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 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 3.5.3.2).

3.5.4 Transaction management

FUR.48 Scheme participants shall be responsible for the transaction management outlining the ways of digital euro users paying and receiving payments at any time (24 hours a day and on all calendar days of the year) and everywhere.

FUR.49 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 at any time (24 hours a day and on all calendar days of the year) and everywhere. This involves providing a variety of payment instruments and acceptance solutions, such as cards and payment apps for individual users, and physical or virtual points of interaction for business users, like POS or e/m-commerce systems. These instruments and solutions are supported by different communication technologies (e.g. chip contact, NFC, QR code and possibly an alias). 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[16] (see section 3.5.4.2), and
- (online and offline) POS payment transactions[17] (see section 3.5.4.3).

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

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).

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 accaptance 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):

- a digital euro payment transaction initiated by the payer and submitted to DESP by the payer's PSP (payer-initiated transaction), and
- a digital euro payment transaction initiated by the payee and submitted to DESP by the payee's PSP (payee-initiated transaction).

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.

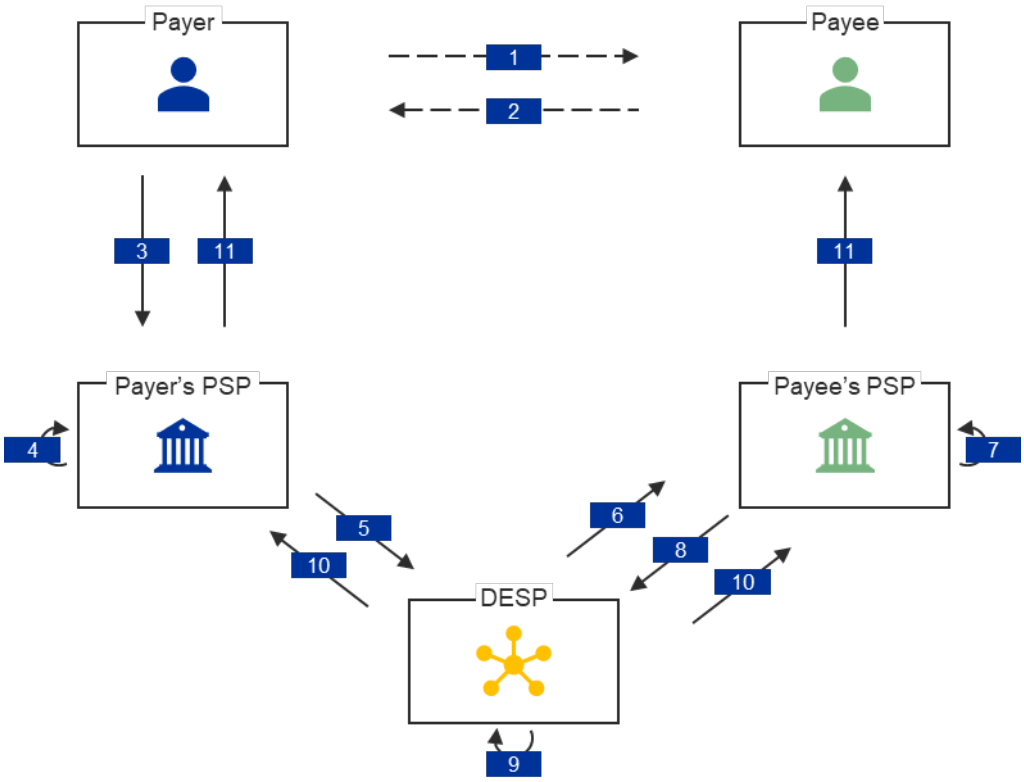

Figure 3-5 High level flow of a payer-initiated online transaction - P2P payment[18]

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

[18] 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 account(s) and the PSP(s) providing the non-digital euro payment account(s) are not the same.

9. The DESP initiates the settlement instruction, 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.

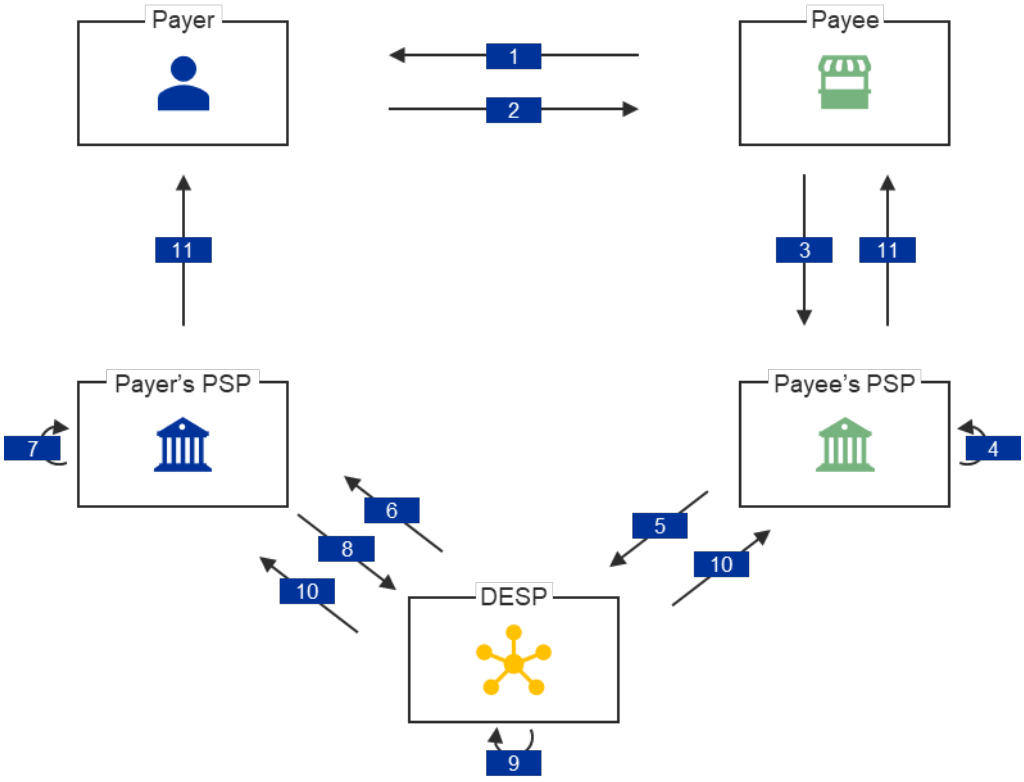

Figure 3-6 High level flow of a payee-initiated online transaction - POS payment[19]

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

[19] 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 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 transaction including consent details with its PSP
4. The payee's PSP validates the digital euro payment transaction
5. The payee's PSP submits the digital euro payment transaction to the DESP
6. The DESP forwards the digital euro payment transaction to the payer's PSP for validation
7. The payer's PSP validates the digital euro payment transaction
8. The payer's PSP sends the validation response to the DESP
9. The DESP initiates the settlement instruction, 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

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

Business rules	
General business rules:	
TM-000-001	The PSP shall ensure that paying and receiving payments in digital euro is possible for digital euro users on 24 hours a day and on all calendar days of the year.
TM-000-002	The PSP shall perform validations of digital euro payment transactions (including funding/defunding) as per the implementation specifications.
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 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 3.5.2.3).
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 which holds sufficient balance to compensate for the insufficient digital euro holdings, within the financial agreement specified between the user and the PSP providing the non-digital euro payment account, and has activated the reverse waterfall option (see section 3.5.3.3).
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 closed, invalid or being monitored for suspected fraudulent or other illegal activity.
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 closed, invalid or being monitored for suspected fraudulent or other illegal activity.
TM-000-012	The PSP must make the status/result of a digital euro payment transaction known to it's digital euro user immediately.
TM-000-014	When processing digital euro payment transactions, PSPs shall interact with the DESP Risk and Fraud Management (RFM) component as required in section 5.
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 mechanism, 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 reject any further incoming digital euro payment transaction while an incoming transaction is still being processed.
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.50 Individual users may use the digital euro for initiating one-off P2P digital euro payment transactions.

FUR.51 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	
Online end-to-end flows (payer-initiated):	
TM-3.1	P2P payment with QR code in-app (payee-initiated)

TM-3.2	P2P payment with NFC (online), payer-initiated
TM-3.5	P2P payment with alias (payer-initiated)
TM-3.7	P2P payment with payment request by link
TM-3.10	P2P Account to account payment with DEAN (payer-initiated) – same PSP
TM-3.11	P2P Account to account payment with DEAN (payer-initiated) – different PSPs
Online end-to-end flows (payee-initiated):	
TM-3.3	P2P payment with NFC (online), payee-initiated
TM-3.6	P2P payment with alias (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 payment

FUR.52 Individual and business users may use the digital euro for initiating one-off e-commerce digital euro payment transactions.

FUR.53 Scheme participants shall comply with the end-to-end process flows for e-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	
Online end-to-end flows (payer-initiated):	
TM-2.1	E-commerce (incl. C2G) payment with QR code
TM-2.3	E-commerce (incl. C2G) payment with pay by link
TM-2.4	M-Commerce payment (in-app)
Online end-to-end flows (payee-initiated):	
TM-2.2	E-commerce (incl. C2G) payment with alias or DEAN

3.5.4.3 Point-of-sale payment

FUR.54 Individual and business users may use the digital euro for initiating one-off POS digital euro payment transactions.

FUR.55 Scheme participants shall comply with the end-to-end process flows for 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	
Online end-to-end flows (payer-initiated):	
TM-1.1	POS payment with payee-generated QR code (dynamic)
Online end-to-end flows (payee-initiated):	
TM-1.2	Online contact and contactless POS payment with mobile device, card or wearable
TM-1.3	Online contact and contactless POS payment with mobile device, card or wearable – different PSPs
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.56 Individual users may set standing orders for automatically initiating digital euro payment transactions.

FUR.57 Business users may set up recurring payments to be accepted and authorised by the individual user for automatically initiating digital euro payment transactions.

FUR.58 Scheme participants shall comply with the business rules and end-to-end process flows for standing orders and recurring digital euro payment transactions as stated in this subsection.

High-level overview

Individual users may set standing orders for automatically initiating digital euro payment transactions to other 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 indivudal 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	
Individual user business rules:	
TM-041-001	When receiving a recurring payment and/or and standing order setup or modification, the payer's PSP must store the recurring payment and/or and standing order parameters autorised 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 it's individual users, the payer's PSP must validate the recurring payment against the recurring payment parameters autorised 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 PSP shall allow an individual user to terminate a standing order.
TM-041-004	The PSP shall allow an individual user to modify a standing order and shall store the modifications autorised 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 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	
Online end-to-end flows (payer-initiated):	
TM-4.3	Standing order
Online end-to-end flows (payee-initiated):	
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
TM-4.2	Recurring m-commerce payment (in-app)
Online end-to-end flows (other):	
TM-4.4	Recurring payment management by individual user (RTP type)
TM-4.5	Recurring payment management by merchant
TM-4.6	Standing order management by individual user

3.5.4.5 Pre-authorisation service

FUR.59 Individual and business users may use the digital euro in services requiring a payment pre-authorisation[20] where the payable amount and payment time are not known at the checkout.

FUR.60 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

[20] A payment "pre-authorisation" in the front-end solution equals to "reservation" of digital euro holdings in the DESP.

user to ensure that the individual user pays for consumed goods or services. Since the individual user can only be charged the pre-authorised amount at most,[21] the service ensures a good user experience.

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	
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 account.
TM-050-003	The amount of digital euro holdings reserved by pre-authorisation(s) on the individual user's digital euro 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 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 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 reservation from the moment of the confirmation that the digital euro holdings have been blocked throughout the entire duration of the reservation.

[21] 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.

End-to-end flows	
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
TM-5.3	Pre-authorisation service on m-commerce (lower or equal final amount)
Online end-to-end flows (other):	
TM-5.4	Modification of a reservation/pre-authorisation

3.5.4.6 Refund

FUR.61 Business users may use the digital euro for initiating digital euro payment refunds.

FUR.62 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 individual user request 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	
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.
End-to-end flows	
Online end-to-end flows (payee-initiated):	
TM-7.1	Refund (POS)
TM-7.2	Refund (e-commerce)
Offline end-to-end flows:	
TM-7.3	Refund for purchase in offline digital euro via 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 availale in (annex D).

The implementation specifications outlined in section 4.4 and section 4.5 are systematically organized into the three key domains of the digital euro functional architecture, as depicted in Figure 4-1 below[22]:

- **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.

[22] 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.

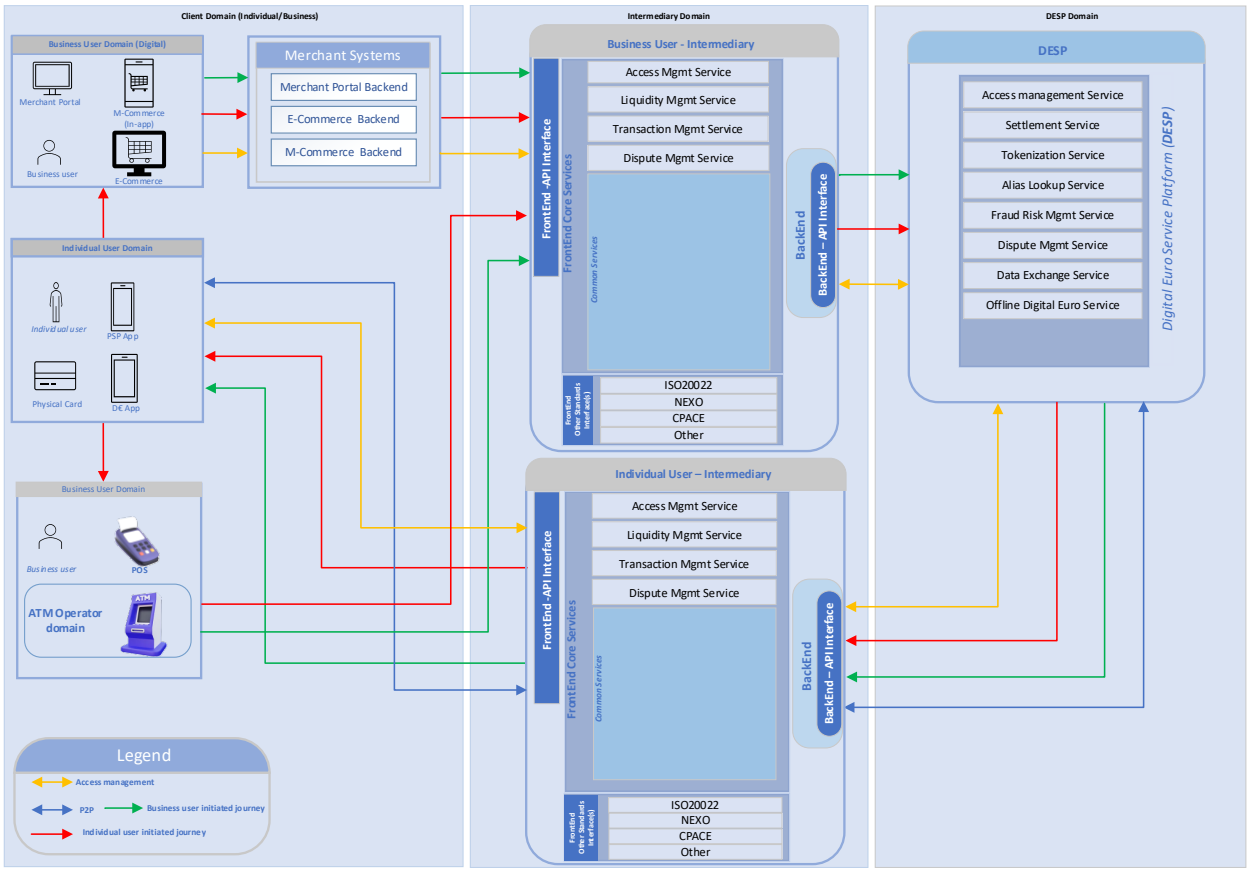

Figure 4-1 The digital euro functional architecture

4.2 Applicable standards

In order to foster a harmonized 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 the 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). 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.
- 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 and limited to the payment interfaces. These standards are preliminary candidates (not yet approved) and may be subject to change.

Solution type	User domain	Payment interface	Communication Technology	Standard
Online solution	Business user domain	E-commerce[23]	QR code	EPC QR[24]
		M-commerce[25]	Digital euro specific standard	
		POS[26]	QR code	EPC QR
			NFC and contact	CPACE
		ATM	NFC and contact	CPACE
	Individual user domain	Physical card	NFC and contact	CPACE
		PSP mobile application (including the P2P payment)	QR code	EPC QR
			NFC	CPACE

[23] The payment interface is, in this case, the merchant application running on a computer
[24] 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.
[25] The payment interface is, in this case, the merchant application running on a smartphone
[26] A POS can be a classic payment terminal or a SoftPOS (Point of sale with a payment application on a smartphone)

Offline solution	Offline solution is currently under definition

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 recommended 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	Payment interface	Technology	Standard
Online solution	E-commerce	Alias	**Nexo**
		Pay by link	**Digital euro specific standard**
	M-commerce	**Digital euro specific standard**	
	POS	**Nexo**	
	ATM	**Nexo**	
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 Non-functional requirements and reporting

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 resilience, efficiency and usability. The following categories of NFRs are established:

- **Reliability:** Service availability (planned or unplanned downtime) and recoverability capabilities.
- **Performance:** Transaction processing latency.

Where relevant and applicable, a future version of the rulebook will include requirement specific KPIs. In case such KPI will be included at a later stage this is indicated by eiter '' X_{Abc}'' or '' [X]''.

4.3.1 Reliability

TER.02 A scheme participant shall ensure a $X_{Availability}$% availability of all digital euro transaction, liquidity and access management services that are not dependent on (branch) service hours [27] 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[28]. 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 ensure a recovery time objective (RTO) of X_{RTO} 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[29].

TER.04 A scheme participant shall ensure that planned maintenance and scheduled downtime is communicated *[x]* days in advance, performed during off-peak hours[30], and does not exceed a cumulative maximum of $X_{\text{planned mainternance}}$ hours per calendar month.

[27] Including physical onboarding or offboarding (e.g.in-person identity verification or assisted access for vulnerable users).
[28] Unavailability of services is caused by a DESP failure or outage is not considered as non-compliance. A future version of the rulebook will include a more detailed definition of availability.
[29] More granular incident classification and resolution time may be included in a future version of the rulebook.
[30] The definition of off-peak hours will be further detailed in a future version of the rulebook and take into account time zone differentiation.

4.3.2 Performance

TER.05 A payee PSP shall ensure that maximum processing latency for 99% of online digital euro payment transactions is below $X_{\text{Payee PSP Latency}}$ whereby this duration is measured as the elapsed time between the moment a transaction processing 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 client balance.
- Waterfall checks - latency for the defunding of the digital euro online account shall be excluded from the computation.
- Sending the settlement message.

TER.06 A payer PSP shall ensure that the maximum processing latency for 99% of online digital euro payment transactions is below $X_{\text{Payer PSP Latency}} + \Delta_{E\text{-}Com,P2P}$ whereby this duration is measured as the elapsed time between the moment a payment processing 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:

- Check client balance and holding limit.
- Waterfall checks – excluding latency for the funding of the digital euro online account
- For E-Com and P2P only: receive the fraud score of the risk fraud management component of the DESP[31]. The latency of this task is referred to as $\Delta_{E\text{-}Com,P2P}$
- Perform fraud checks
- Sending the settlement confirmation message.

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 D1.1 (Front-end implementation specifications) and Annex D2 (Back-end implementation specifications). The front-end implementation specifications are complemented with which presents the core data requirements for digital euro services[32].

The front-end implementation specifications prescribe the requirements for individual users' payment instruments, user to application interfaces used in the individual user domain, and the services in the

[31] The fraud score of the risk fraud management component of the DESP must be read for e-commerce and P2P transactions. In case of POS transactions PSPs can optionally wait for the fraud score. Once the DESP's fraud score transmission time is established, this delta will be accumulated to the latency target for payer PSP processing of P2P and E-commerce transactions.

[32] The core data requirements are limited to the minimum requirements to initiate a digital euro payment transaction, the exhaustive list of all front-end data requirements is captured in specification #7 (Data management) of Annex D1.1 (Front-end implementation specifications).

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 dipicted in Figure 4-1.

TER.07 Distributing PSPs shall implement the specifications in annex D1.1. relevant to the digital euro payment servcies they offer

TER.08 Distritbuting PSPs shall use the the core data requirements in annex D1.2 relevant to the digital euro payment servcies they offer.

TER.09 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[33].

4.4.1 Distributing PSP – Individual user domain requirements

The following tables lists the services for payment instruments and user to application interfaces through which individual users can consume digital euro payemt services as depcited in Figure 4-1. The tables refer to the relevant implement specifications and chapters in annex D1.1 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[34]. Moreover, some specifications in this overview may still have placholders.

PSP application		
Core service	**Service**	**Specification**

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

[34] Future requirements for the digital euro app will be detailed further in future version of the rulebook and/or other documentation.

General requirements	Functional services[35]	• Specification #3 – 4.1.1
	Non-functional services[36]	• Specification #3 – 4.1.2
Acces management[37]	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[38]	Manual funding of online holdings	• Specification #3 – 4.3.2
	Manual defuning 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 (Pay-by-Link) • Specification #3 – 4.4.1.5 (Alias) • Specification #3 – 4.4.1.6 (DEAN) • Specification #3 – 4.4.1.7 (Standing order)

[35] Including requirements on, supported form factors, user experience, accessibility, personalized settings, QR code service, NFC communication, user authentication, user activation, customer alerts, and visual consistency and branding. Some specifications have placeholders for a future version of the rulebook.
[36] 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.
[37] 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.
[38] 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.

	POS	• POS specifications will be included in a future version of the rulebook
	Balance inquiry and transaction management[39]	• Specificaiton #3 – 4.4.3
	Dispute management[40]	• Dispute management specifications will be included in a future version of the rulebook

PSP web page		
Core service	**Service**	**Specification**
General requirements	Functional requirements[41]	• Specification #3 – 5.1.1
	Non-functional requirements[42]	• Specification #3 – 5.1.2
Access management[43]	Ondboarding 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 life cycle management (individual user)	• Specification #3 – 5.2.1.3
	Account portability (individual user)	• Specification #3 – 5.2.1.4

[39] Transaction history will only be available for online digital euro payments.
[40] 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.
[41] Including requirements on, seamless navigation, responsive design, visual consistency and branding, smooth performance, accessibility, personalized settings, user experience. Some specifications have placeholders for a future version of the rulebook.
[42] 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.
[43] 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.

	Profile management (business user)	• Specification #3 – 5.2.2.1
Liquidity management[44]	Manual funding online holding	• Specification #3 – 5.3.2
	Manual defunding online holdings	• Specification #3 – 5.3.3
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[45]	• Specificaiton #3 – 5.4.2
	Dispute management[46]	• Dispute management specifications will be included a future version of the rulebook

4.4.2 Distributing PSP - Front-end requirements

The following table lists servics to be integrated in the distributing PSP service domain as depcited in figure 4.4.1. These are further detailed in specification #1 and specification #5.

Distributing PSP services

[44] 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.
[45] Transaction history will only be available for online digital euro payments.
[46] 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.

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 account for a digital euro transaction proper execution.	Specification #1 – 6.1 Specification #5 – 9: Notification service[47]
	Private money account: Private money 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 – 7: Private money account service
Liquidity management	**Funds management**: management of the rules to manage funds in private money accounts (debit, credit, block, release).	• Specification #5 – 8: Funds management service
Transaction management	**Payment initiation**: Management of payment requests initiated by a digital euro user (covering all form factors).	• Specification #1 – 8.1 • Specification #5 – 9: Notification service[48] • Specification #5 – 4: Alias look-up dispatch service • Specification #5 – 5: PSP identifier look-up dispatch service • Specification #5 – 6: Link creation service

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

		• Specification #5 – 11: Tokenization service
	Recurring payment: Management of rules to collect the user details data and store them.	• Specification #1 – 8.2
	Standing order: management of parameters defined by the user to request a standing order set-up.	• Specification #1 – 8.3
	Payment processing: Invoked ruing a payment transaction process after payment initiation in relation to the DESP	• Specification #5 – 10 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 – 13 Fraud and risk service
Dispute management	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 describe 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[49]. Specificiations for authentication services will be included in a future version of the rulebook.

Specification #6 (Technical standard) [50] and #7 (Data management) of Annex D1.1 (Front-end specifications) respectively describe security standards and the data model which distributing PSPs should adhere to.

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.

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

Alias Lookup Service (AL)	Payment with alias	Individual user payments 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 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	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 certificaton procedures as described in annex A1 (onboarding, certification and testing).

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 implementaion specifications are furhter detailed in annex D1 (Front-end impemenation specifications) annex D1.1 (Core data requirements)[51], and annex D2 (Back-end implementaion specifications)

Front-end requirments 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.10 Acquiring PSPs shall implement the specifications in annex D1.1. relevant to the digital euro payment servcies they offer

[51] The core data requirements are limited to the minimum requirements to initiate a digital euro payment transaction, the exhaustive list of all front-end data requirements is captured in specification #7 (Data management) of Annex D1.1 (Front-end implementation specifications).

TER.11 Acquiring PSPs shall use the the core data requirements in annex D1.2 relevant to the digital euro payment servcies they offer.

TER.12 Acquiring PSPs shall implement the specifications in annex D2 relevant to the digital euor 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 accessbile by acquiring PSPs through which digital euro payment services are executed as depicted in Figure 4-1. The tables refer to the relevant implement specifications and chapters in annex D1.1 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 ruelbook will include specifications for POS terminals. Moreover, some specifications in this overview may still have placholders.

Acquiring PSP acceptance solutions		
Acceptance solutions	**Service**	**Specification**
E-commerce	General requirements	• Specification #4 – 4.1.1 (Functional requirements[53]) • Specification #4 – 4.1.1 (Non-functional requirements[54]
	E-commerce payment	• Specification #4 – 4.2.2 (QR-code) • Specification #4 – 4.2.3 (Alias)

[52] Implementation specifications for the offline functionalities of the digital euro will be further detailed when a vendor for the offline solution is selected.
[53] Including, digital euro payment method, visual consistency and branding, user experience, online notifications to the customer
[54] Including, supported operating systems

		• 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
M-Commerce	General requirements	• Specification #4 – 5.1.1 (Functional requirements[55]) • Specification #4 – 5.1.1 (Non-functional requirements[56]

[55] Including, digital euro payment method, visual consistency and branding, user experience, online notifications to the customer
[56] Including, supported operating systems

	M-commerce payments via mobile App	• Specification #4 – 5.2
	Recurring payment on m-commerce	• Specification #4 – 5.3
	Pre-authorisation on m-commerce	• Specification #4 – 5.4
POS	POS specifications will be included in a future version of the rulebook	
ATM[57]	Manual funding	• Specification #4 – 7.1.2 (Card) • Specification #4 – 7.1.2 (QR code)
	Manual defunding	• Specification #4 – 7.2.2 (Card) • Specification #4 – 7.2.2 (QR code)
	Account balance inquiry and transactions history[58]	• Specification #4 – 7.3

4.5.2 Acquiring PSP front-end requirements

The following table lists servics to be integrated in the acquiring PSP service domain as depcited in figure 4.4.1. 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	• Specification #2 – 6.1

[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.

	checking the validity of the link to the private money account	• Specification #5 – 9: Notification service[59]
	Private money account: Private money 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 – 7: Private money account service
Liquidity management	**Fund management:** Management of rules to manage funds in private money account (debit, credit, block, release)	• Specification #5 – 8: Funds management service
Transaction management	**Payment initiation:** Management of payment requests: initiated by a digital euro user (covering all form factors)	• Specification #2 – 8.2 • Specification #5 – 4: Alias look-up dispatch service • Specification #5 – PSP identifier look-up dispatch service • Specification #5 – 11: Tokenization service • Specification #5 – 6: Link creation service • Specification #5 – 9: Notification service[60]
	Recurring payment: Management of recurring payment (set-up, modification,	• Specification #2 – 8.3 • Specification #5 – 9: Notification service[61]

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

	termination, periodic payment transaction)	
	Payment processing: Invoked ruing a payment transaction process after payment initiation in relation to the DESP	• Specification #5 – 10 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 – 13 Fraud and risk service
Dispute management	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 describe 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[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 D1.1 (Front-end specifications) respectively describe security standards and the data model 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).

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

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.
	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	PSP 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 commercial bank money. Defunding is a process whereby a digital euro user exchanges 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	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 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 certificaton procedures as described in annex A1 (onboarding, certification and testing).

5 Risk management requirements

RMR.01 PSPs shall comply with all risk management requirements as detailed in annex E1.

The risk management annex is confidential and is only available on a strict need to know basis, and is not made available as part of the rulebook.

General risk management principles may be added to this section in the future for transparency and awareness.

6 Dispute management requirements

6.1 Section overview

This section defines the requirements of the dispute management services for a 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[64] consists of:

(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 participant shall comply with the requirements governing the eligibility of a digital euro payment transaction for dispute:

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 schemeparticipant 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.

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

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	
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, 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 participant shall provide supporting documentation in any of the formats listed in the box 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, 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 update by either (1) one of 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 box below.

Possible statuses						
Status	Status trigger	Payer	Payer's PSP[65]	DESP	Payee's PSP[66]	Payee
Pre-dispute request accepted	The DESP has accepted the received pre-dispute request		Status notified	Updates status	Status notified	Status notified
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	

[65] Payer's distributing PSP
[66] 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)

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 remediating action has been carried out ❖ The payer's PSP has rejected the dispute response ❖ The dispute has escalated to an arbitration case	Status notified	Status notified	Updates	Status notified	Status notified
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 high-level process description, including applicable timeframes. 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 box below.

Functional requirements
General functional requirements:

DM-030-001	Disputes shall be initiated within [90-180] business days since the disputed transaction settlement date[67] 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 dispute 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 of dispute response received
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

Dispute management processes 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 parties 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.

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

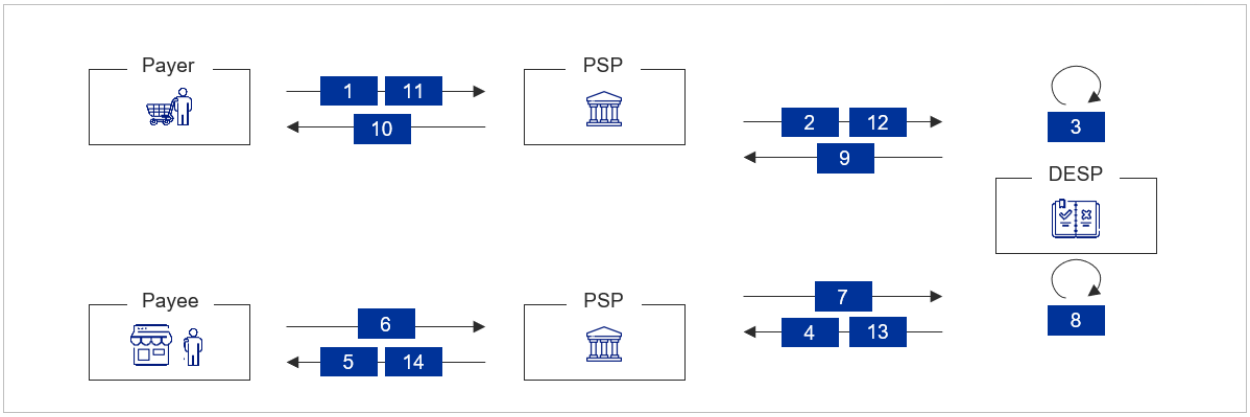

Figure 6-1 - High-level process flow for the pre-dispute phase.

Description of steps:

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

1. The payer's PSP reviews the information and documentation received, the sends a pre-dispute request to the DESP – Dispute component[68]

2. The DESP - Dispute component runs a pre-dispute request validation, based on dispute eligibility requierments (section 6.2.1.), supporting documentation rules (section 6.2.2), dispute process requirements (section 6.3.1.), 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 rejectes the pre-dispute request

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

6. The payee's PSP reviews the payee's response and sends a pre-dispute response to the DESP - Dispute[69] 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.), 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 request to the payer

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

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.

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

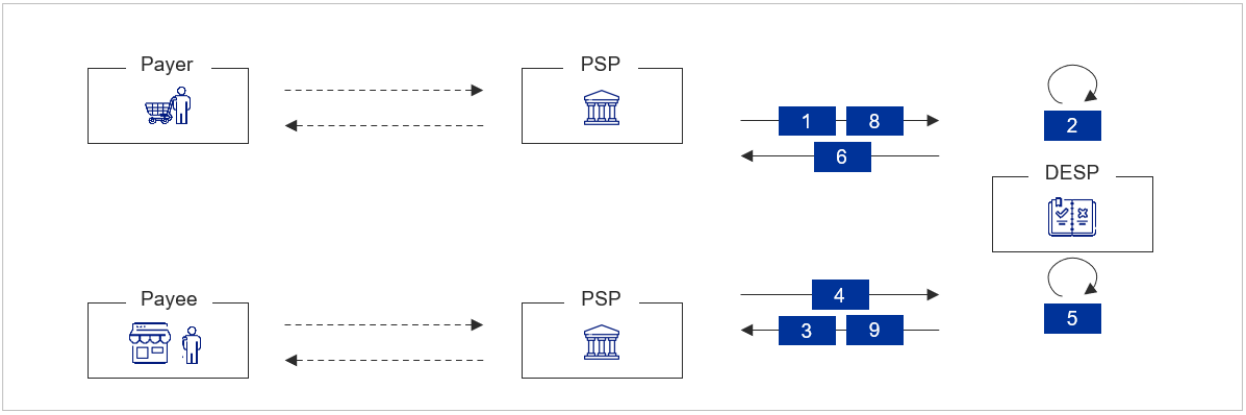

Figure 6-2 - High-level process flow for the dispute phase.

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[70] within 5 business days of the pre-dispute closing; the status updates to "Dispute requested"

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.), 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[71], 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.), back-

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

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

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 box 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 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 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 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[72] and timestamp[73]
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 account • The payer authorised the transaction only once
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro 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	
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 account
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro 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

[72] Based on data element AuthorisationCode [Au1]
[73] Based on data element CreationDateTime [Tm1]

	• The respective digital euro transactions were processed, settled, and recorded in the payer's digital euro account
Supporting documentation	To be provided by the payer and payer's PSP: • Digital euro 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[74], but a different amount was recorded and debited from the payer's digital euro 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 account
Supporting documentation	To be provided by the payer and payer's PSP: • Link[75] or QR code[76] 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[77], country, remittance information or scheduled execution date.
Conditions for initiating a dispute	• The disputed transaction is either either consumer-to-business or peer-to-peer

[74] Based on data element Amount [Tr2])
[75] Based on data element Return URL [Tr46]
[76] Based on data element Transaction Token [Tr58]
[77] Based on data element CreditorAccountName [Ac14]

	• 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 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)
	  ○ 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 authorized 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 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 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 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 either consumer-to-business or peer-to-peer • The payer did not authorise the transaction • No Strong Customer Authentication (SCA) 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 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 account. The payer states that they retain possession of their payment instruments (e.g., card, digital euro mobile 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 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

ii. [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

a. [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

b. [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

iii. 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 participant 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 box 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[78], amount[79], currency[80], payee name[81]
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

[78] Based on data element CreationDateTime [Tm1]
[79] Based on data element Amount [Tr2]
[80] Based on data element Currency [Tr16]
[81] Based on data element CreditorAccountName [Ac14]

7 Minimum user experience requirements

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 applicable to all user journeys. Specific UX requirements 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 marked as [optional]. The selection has been made based on the principle of proportionality.

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.

7.1 Generic UX requirements

7.1.1 Authentication

UXR.01 Digital euro users shall be able to use authentication methods equivalent to those available for other means of payment.

UXR.02 Digital euro users shall be able to complete authentication in no more steps than are required for other means of payment.

UXR.03 Digital euro users shall not be required to complete authentication more often than with other means of payment and shall only need to do so once for the same authentication purpose.

UXR.04 Digital euro users shall be provided with multi-modal authentication methods, having access to at least one authentication method that does not depend on the possession or use of a smartphone, or any other digital channels.

UXR.05 Digital euro users shall have the option to select a preferred authentication method in their account management settings.

UXR.06 Digital euro users shall be able to use their European Digital Identity Wallet to authenticate as one of the options.

UXR.07 Digital euro users shall be clearly informed and provided with a straightforward way to retry or select an alternative method if authentication fails (e.g., biometrics not recognised).

UXR.08 Digital euro users shall always have a secure fallback authentication method (e.g., PIN) in place if primary method (e.g., biometrics) is unavailable.

UXR.09 Digital euro users shall not be logged out or forced to reauthenticate unnecessarily if activity is ongoing. If authentication times out, digital euro users shall be notified and given the opportunity to reauthenticate easily.

UXR.10 Digital euro users shall be able to explicitly confirm or reject an authentication request.

UXR.11 If seamless authentication is available for the digital euro, digital euro users shall be able to use it by default for mobile-initiated transactions without being redirected away from the current environment.

UXR.12 If redirection takes place for authentication, digital euro users shall have the choice to be redirected to their preferred digital euro-supporting app.

UXR.13 Participants shall display the consent screen with required transaction details on the device on which digital euro users authenticate a transaction.

UXR.14 Participants shall require a new authentication in case of any change in the amount or payee.

UXR.15 Participants shall require authentication before displaying personal data including the account balance.

7.1.2 Accessibility

UXR.16 All devices and services offered shall comply with the requirements outlined in the European Accessibility Act.

7.1.3 Branding

UXR.17 All devices and services offered shall comply with the branding requirements outlined in section 8 of the rulebook.

7.1.4 Controllability

UXR.18 Digital euro users shall be able to select the preferred digital euro-supporting app.

UXR.19 Payers shall be able to cancel the payment at any point throughout the transaction flow until the authentication process has started.

UXR.20 Payers shall be able to go back to the previous step throughout the entire transaction flow until the authentication process has started.

UXR.21 Payers shall be able to opt out of a specific digital euro solution (e.g., NFC, QR, alias).

UXR.22 [Optional] Payers may be able to refuse incoming payment requests by blocking payee based on their DEAN.

7.1.5 Error handling

Placeholder, subject to the outcome of the relevant workstream.

7.1.6 Feedback and information

UXR.23 Digital euro users shall be able to opt for notifications equivalent to other means of payment.

UXR.24 Digital euro users shall see a loading indicator if digital euro front-end service processes take longer than three seconds.

UXR.25 Digital euro users shall be informed on being redirected.

UXR.26 Participants shall validate fields before proceeding to the next screen.

UXR.27 User devices shall specify which field failed validation.

UXR.28 [Optional] Participants may perform field validation immediately after digital euro users complete the corresponding field.

UXR.29 Digital euro users shall receive all necessary information at the appropriate step, minimising the need to recall information.

UXR.30 Digital euro users shall be able to choose language according to their preferences equivalent to the languages offered for other means of payment in the same environment.

UXR.31 The information provided in the notifications shall be understandable and should not exceed the B2 (upper intermediate) complexity level of the Council of Europe's Common European Framework of Reference for Languages.

7.1.7 Positioning

UXR.32 Digital euro services shall be accessible via one of the main pages of the user interface on an equal footing with non-digital euro payment services.

7.1.8 Transactions

UXR.33 Payers shall be able to select a default option for using either online or offline digital euro to make a payment.

UXR.34 Payers' devices shall display, prior to 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.

UXR.35 Payers' devices shall display, before authentication of the transaction, that the reverse waterfall functionality will be triggered.

UXR.36 Payers shall have the option to receive a notification whenever the reverse waterfall functionality is triggered.

UXR.37 Payers shall have the option to receive a notification if a payment fails due to insufficient funds.

UXR.38 Payers shall have access to a shortcut for funding if a payment fails due to insufficient funds.

UXR.39 Payees shall have the option to receive a notification whenever the waterfall functionality is triggered.

UXR.40 Payee shall have the option to receive a notification if a payment fails because the balance exceeds the holding limit.

UXR.41 In case of a failed transaction, Participants shall provide an explanation or specifications of the next step in the error message.

UXR.42 Participants shall support transaction history for online digital euro.

UXR.43 Participants shall include in the Transaction history; amount, payee name if available, transaction ID, message if available, date and time.

UXR.44 Participants shall use the commercial trade name as payee’s name for the Transaction history, if applicable.

UXR.45 Participants shall label digital euro payments as such in the Transaction history.

UXR.46 Participants shall inform users that the alias is solely used for transaction or authentication purposes and never used for commercial purposes.

7.1.9 User support

UXR.47 Digital euro users shall be able to find accurate help and documentation in an easily accessible and intuitive manner, equivalent to other means of payment.

UXR.48 Participants shall provide customer support for digital euro services equivalent to that offered for other means of payment.

UXR.49 Participants shall provide customer support in an inclusive and accessible manner, using different methods of communication (e.g., visual and auditory) and offering it through more than one platform.

7.2 Specific UX requirements

Specific UX requirements are organised by illustrative user journey (Annex B1) and only apply to that specific user journey. Annex F1 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.

Specific UX requirements for additional user journeys will be included in a future version of the rulebook.

8 Brand rules

8.1 Introduction

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 has the intent to "facilitate a harmonised user experience, regardless of payment service providers involved and the front-end services used" (digital euro legislative proposal, article 59).

These brand rules will apply to all relevant use cases and channels where the digital euro brand is used.

To accommodate for the various brand implementation scenarios that apply for payment service providers (PSPs) and future applications, the rules are split into three parts:

- General brand rules – applicable across all channels and uses of digital euro brand, both physical and digital, to ensure consistent display and clarity,
- Specific brand rules - applicable to some use cases due to their specific features,
- Brand style guide – [PLACEHOLDER: add link to the style guide].

8.2 General brand rules

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

8.2.1 Logo requirements

BRR.01 The full brand logo may be comprised of a combination of text and graphical elements, as specified in the brand style guide.

BRR.02 The full logo shall be used whenever possible, with preference for animated branding. For guidance on the use of animated branding, see section 8.2.1.2 Sensory branding. If the use of graphical logo, full colours or size is not possible, alternatives are made available in section 8.2.6 Small and limited display of this section.

BRR.03 Only approved and unaltered versions of brand logo and branding elements (e.g., banners, icons, trademarks) shall be used. All approved branding elements can be found in the brand style guide.

BRR.04 Digital euro branding shall be displayed with any registered trademark symbol, as detailed in the brand style guide.

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

8.2.1.1 Logo placement

BRR.05 The logo and other branding elements shall be displayed in all relevant scenarios following the indications provided in the user journeys, implementation specifications and brand style guide wherever applicable.

BRR.06 By default, the brand 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 in 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
- Marketing materials promoting digital euro products and services. Adherence to the brand style guide is required for consistent representation in all communications relating to the brand. [PLACEHOLDER: add link to the style guide].

8.2.1.2 Sensory branding

BRR.07 Sensory branding is a form of animation and sounds, serving to provide consumers with auditory and visual cues, enhancing brand recognition, and providing additional audio-visual confirmation upon a successful transaction.

BRR.08 Animated branding is preferred whenever possible and shall be displayed with equivalent prominence to animations of other brands.

BRR.09 If animations cannot be displayed legibly, static branding elements shall be used.

BRR.10 Sensory branding shall use assets as specified in the brand style guide. [PLACEHOLDER: add link to the style guide].

BRR.11 Animations shall be displayed in a minimum size ensuring legibility, without any alterations to colour treatment, proportions or speed.

8.2.1.3 Minimum size

BRR.14 The logo shall be displayed in a minimum size that ensures legibility and equal prominence to other brands.

BRR.15 Specific print & digital requirements can be found in the brand style guide: [PLACEHOLDER: add link to the style guide].

BRR.16 For branding alternatives to be used on small and limited displays, refer to subsection 2.6 Small and limited displays of this section.

8.2.1.4 Spacing

BRR.17 Minimum free space around the logo shall be included to ensure recognition and unobstructed view.

BRR.18 Specific print & digital requirements can be found in the brand style guide: [PLACEHOLDER: add link to the style guide].

8.2.1.5 Background

BRR.19 The logo shall be placed on a simple or solid colour background providing sufficient contrast and legibility in accordance with European Accessibility Act (EAA).

8.2.1.6 Colour

BRR.20 The logo shall be displayed in colours specified in the brand style guide unless the grayscale alternative needs to be used.

BRR.21 The use of colours outside the defined colour palette is not permitted.

BRR.22 Full colour branding shall be used whenever possible.

BRR.23 Grayscale version of the logo and other assets shall be used when full colour in display or print are not supported.

BRR.24 When using grayscale alternatives, other requirements regarding placement, minimum size, sufficient contrast with the background and spacing remain applicable.

BRR.25 The use of grayscale branding shall maintain equal prominence to other brands, meaning that other brands need to also be displayed in grayscale. When other brands are displayed in full colour, digital euro branding shall also be displayed in full colour.

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

8.2.2 Accessibility

BRR.26 Branding implementation shall conform to the accessibility principles as outlined in European Accessibility Act (EAA).

8.2.3 Brand integrity

BRR.27 Digital euro branding shall be used in accordance with the brand rules, specifications outlined in the brand style guide.

BRR.28 It is not permitted to alter the logo design, place any additional text within the logo, change the proportions, rotation, aspect ratio, include 3D elements or add any other visual alterations or filters to the logo and other branding elements.

BRR.29 The logo requirements described in section 8.2.1 Logo requirements shall be maintained in all content, use cases and channels including co-branding and partnerships that use digital euro branding.

BRR.30 The logo must not be used in text as a part of the sentence and shall instead include the brand name in text format.

BRR.31 Any trademark symbols indicated in the brand style guide shall be used as specified and not altered or resized independently of the logo, maintaining consistency in brand representation.

BRR.32 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.33 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. This includes making false, confusing, or misleading statements, or failing to disclose important information (e.g., any information necessary to make informed decisions)

BRR.34 For visual references on correct usage of the logo design and other branding elements, see the brand style guide **[PLACEHOLDER: add link to the style guide]**.

8.2.4 Physical brand visibility rules

8.2.4.1 Signalling acceptance

BRR.35 Brand acceptance signage shall be prominently displayed at point-of-sale (POS), terminals, cash registers, self-checkout and ATMs using brand approved acceptance signage assets (for digital screens); or ready-made sticker designs or stand-up displays if digital on-screen acceptance signalling is not possible.

BRR.36 The digital euro acceptance sticker shall be prominently displayed on a main entry door or window near the property entrance, ensuring it will be easily visible from the outside.

BRR.37 Digital euro acceptance signage and stickers shall be displayed with equal prominence in relation to other leading brands, ensuring that it is prominently visible and easily recognisable as a separate payment means for the consumers.

BRR.38 Business digital euro users shall notify customers if a specific digital euro payment method is not accepted at the merchant location (e.g., no QR, no NFC or only contact card available) prior to the payment.

BRR.39 Only unaltered acceptance signage provided in the brand style guide shall be used to signal digital euro acceptance.

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

8.2.4.2 Receipts

BRR.40 Receipts of digital euro transactions shall include the full brand name in text with specified capitalisation as outlined in the brand style guide **[PLACEHOLDER – add link to the style guide].**

BRR.41 If using full brand name in text is not possible, shortened version of the brand name shall be used with specified capitalisation as outlined in the brand style guide.

8.2.5 Digital brand visibility rules

8.2.5.1 E-commerce/M-commerce

BRR.42 The full digital euro logo shall be displayed with equal prominence and proportionately to other payment methods in all digital channels. The brand display shall follow indications in minimum user experience requirements [section 7] and the brand style guide.

BRR.43 By default, the brand shall be represented in following situations:

- When signalling acceptance of available payment methods;
- When representing digital euro credentials in payment interfaces (e.g., stored DEAN, alias);
- Pre-purchase:
  - in payment method selection screen;
  - at check-out, within immediate proximity of the payment trigger;
- Post-purchase – for any payments made with digital euro:

- during consent & authentication;
- on payment result / confirmation page;

- in notifications (e.g., push, email, digital receipts; in transaction history).

BRR.44 If the display of the full-sized logo is not possible, it is permitted to use a brand approved icon and/or full brand name in text with specified capitalisation, as outlined in the brand style guide.

BRR.45 For digital receipts, transaction history and other post-purchase notifications that do not allow for display of the full logo or full brand name, the shortened name in text shall be used with specified capitalisation, as outlined in the brand style guide. **[PLACEHOLDER – add a link to the style guide].**

BRR.46 Digital euro direct check-out buttons shall be displayed with equal prominence to the direct check-out buttons of other payment means.

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

8.2.6 Small and limited displays

BRR.47 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.48 **If the minimum size logo is too large**, the brand approved icon and/or full name in text shall be used with specified capitalisation as outlined in the brand style guide.

BRR.49 The maximum size of the icon cannot be larger than the minimum size of the full logo.

BRR.50 If the display **does not support graphics**, the full name in text shall be used with specified capitalisation as outlined in the brand style guide.

BRR.51 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 brand style guide.

Downloadable scalable icons can be found in the brand style guide. [PLACEHOLDER: add link to the style guide]

8.2.7 Display with other brands and co-branding

When digital euro branding is represented alongside other brands, the following logo requirements in terms of minimum size, spacing, colour and background are applicable:

BRR.52 The digital euro branding shall maintain equal prominence to other brands, meaning that the size, colour treatment, frequency and location of digital euro branding shall match that of other payment methods and brands.

BRR.53 The brand shall be represented by using approved assets provided in the brand style guide. It is not permitted to alter the logo and other brand designs.

BRR.54 The digital euro brand logo shall be displayed with equal prominence to other leading payment methods and clearly shown as a separate means of payment.

BRR.55 The digital euro branding shall be placed in a way that makes it easily noticeable for consumers. It must not be placed in the 'others' tab (or its equivalents).

BRR.56 When displayed with animations of other brands, digital euro animations shall be displayed with equal prominence.

8.2.8 Adaptation in international use

BRR.57 When using digital euro branding, scheme participants shall consider localisation and ensure all branding elements are aligned with the localisation guidance found in the digital euro brand style guide. **[PLACEHOLDER: add link to the style guide]**

8.2.9 Card design

BRR.58 Digital euro branding is required on all physical cards supporting digital euro-based services.

BRR.59 Digital euro branding shall be always prominently positioned on the front of the card while ensuring that the name and credentials on the card are clearly legible and not obscured by the branding elements.

BRR.60 Digital euro cards shall include accessibility features in accordance with principles set forth in the European Accessibility Act (EAA).

BRR.61 To further facilitate accessible use, cards are recommended to include embossed print, braille markings for the brand and credentials on the card, it is also recommended to include notches to indicate the type of the card and correct position for inserting it. (optional)

[PLACEHOLDER: Branding placement on the offline battery powered card and bridge device if needed]

BRR.62 The placement of the branding elements on the card shall follow specifications in the digital euro brand style guide. **[PLACEHOLDER: add link to the style guide].**

8.2.9.1 Digital card representations

BRR.63 Digital card representations shall follow the physical card design, including name and expiry date. It must not show the chip or add any additional shading or 3D elements.

BRR.64 When the digital euro card is represented alongside other digital cards, it shall maintain equal legibility and prominence.

8.3 Specific rules

8.3.1 QR codes

BRR.65 QR code user journeys shall follow the requirements outlined in section 8.2.5 Digital brand visibility rules (for digital user journeys) and section 8.2.4 Physical brand visibility rules (for physical user journeys) whenever applicable.

BRR.66 Additionally, QR codes for digital euro payments shall be made recognisable as such by including digital euro logo within close proximity to the QR code and other required branding elements as prescribed by the brand style guide. The logo shall be placed within a protected area either at the top or the bottom of the QR code.

BRR.67 QR codes shall be placed on a background that allows for sufficient contrast and in a size that ensures easy scanning.

BRR.68 The branding of the QR codes shall follow specifications in the digital euro brand style guide. **[PLACEHOLDER: add link to the style guide].**

8.3.2 In PSP-app/portal/wallet integrations

BRR.69 In PSP-app/portal/wallet integrations shall follow the requirements outlined in section 8.2.5 Digital brand visibility rules, whenever applicable.

BRR.70 If the specified digital euro colour scheme does not match the existing PSP environment, it is allowed to use grayscale alternatives of the logo, other branding elements and text.

BRR.71 The use of grayscale branding shall maintain equal prominence to other brands, meaning that other brands need to also be displayed in grayscale. When other brands are displayed in full colour, digital euro branding shall also be displayed in full colour.

BRR.72 Digital euro branding shall be integrated on par with other brands and displayed with equal prominence.

BRR.73 Additionally, when digital euro services are integrated in an app or a portal, the app/portal shall feature a section containing all relevant digital euro user journeys displayed with digital euro branding to make them recognisable as such. Including:

- 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 accounts
- Prominently representing available digital euro-based payment options and features

BRR.74 When a digital euro feature or payment method is selected, digital euro branding shall always be displayed in a protected area, either in the header or the footer of the screen, for all digital euro user journeys (e.g., payment set-up, sending/requesting money, generating and scanning QR codes, generating payment links, viewing account etc.)

BRR.75 The implementation of digital euro branding in PSP-app/portal/wallet integrations shall follow specifications in the digital euro brand style guide. **[PLACEHOLDER: add link to the style guide].**

9 Digital euro fees, limits and thresholds requirements

[Placeholder]

10 Scheme rulebook management

[Placeholder]

11 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 technical or functional factors which enable the initiation and the acceptance of digital euro payment transaction. Digital euro solutions are certified by certifying entities either as acceptance solutions or as distributing solutions.
Access management	A service offered by a scheme participant enabling digital euro users to hold digital euro and conduct digital euro payment transactions.
Access manager	A scheme participant that provides digital euro users with access to the digital euro service platform (DESP). An access manager can act as an instructing party or authorise a third party to act on its behalf. An access manager performs onboarding, lifecycle management and offboarding of digital euro users to, in, or from the DESP.
Account information service	An online service to provide consolidated information on one or more payment accounts held by the payment service user with either another payment service provider or with more than one payment service provider[82].
Account information service provider (AISP)	A payment service provider pursuing account information services[83].
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[84].

[82] Article 4(16) of Title 1 of Directive [4]
[83] Article 4(17) of Title 1 of Directive [4]
[84] Article 4(44) of Title 1 of Directive [4]

Acquiring payment service provider (PSP)	A scheme participant contracting with the payee that is responsible for accepting and processing of digital euro payment transactions resulting in a transfer of digital euro funds to the payee.
Automated (de)funding	A functionality that allows funding or defunding of a digital euro user's 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.
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[85].
Alias look-up service	A service that maps an identifier (alias) linked to a digital euro user—such as an (optional) mobile phone number or digital euro account number (DEAN)—to the corresponding payment service provider (PSP).
Anonymity	A situation in which no personal data (i.e. data relating to an identified or identifiable natural person) can be retrieved.
Application to application (A2A) interface	An interface permitting the interaction between software applications without human interaction.
Application programming interface (API)	A set of a set of rules or protocols that enables software applications to communicate with each other.
Assisted use	Any situation in which a digital euro user accesses digital euro payment services via an access manager and receives support (inter alia by interactions with the access manager's staff in one of its branches or via its telephone service) as well as systems mimicking human interaction.
Archived data retention period	Defines the timeframe that Data Warehouse and Legal Archive or the operational component itself shall store its operational data when it has a dedicated historic data storage.
Back-end infrastructure	All hardware and software components necessary for recording of digital euro holdings in the Eurosystem ledger and processing of digital euro payment transactions. The infrastructure interacts with front-end services or other back-end infrastructures via defined interfaces.

[85] Article 2(28) of Chapter 1 of the draft Regulation [1]

Business continuity risk	In the context of the digital euro scheme, this refers to the risk of disruptions to digital euro operations and services due to external events (e.g., natural disasters, pandemics, terrorist attacks, power outages), system failures, or resource unavailability.
Business digital euro user	A natural or legal person, acting in the course of a business activity.
Business-to-business (B2B) digital euro payment transactions	A payment made by one business digital euro user to another.
Central bank(s)	The European Central Bank (ECB) and the National Central Banks (NCBs) of those countries that have adopted the euro.
Central bank money (CeBM)	Central bank liabilities, in the form of either banknotes, central bank reserves or digital euro held with the Eurosystem.
Commercial bank money	A commercial bank liability, in the form of deposits held at the commercial bank.
Commercial bank money payment service provider (PSP)	A payment service provider (PSP) that provide non-digital euro payment accounts.
Communication technology	Technology used for the transmission of data between two devices.
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[86].
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[87].
Confidentiality	An obligation enforced through a set of rules and operational measures which restricts the accessibility and interpretability of data to authorised users within a specific context.
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.

[86] Article 2(25) of Chapter 1 of the draft Regulation [1]
[87] Article 2(17) of Chapter 1 of the draft Regulation [1]

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[88].
Credit Memorandum Balance (CMB)	A limit set by the DESP DCA Holder for the use of liquidity on the DESP DCA by a specific Access Manager.
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 jurisdictions.
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
Customer Due Diligence (CDD)	A process to obtain sufficient knowledge of digital euro users (e.g. via know your customer (KYC)) enabling obliged entities under Directive (EU) 2015/849 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, to determine the money laundering and terrorist financing risks of digital euro users or digital euro payment transactions.
Customer-to-business (C2B) digital euro payment transaction	A digital euro payment order from an individual digital euro user to a business digital euro user. Typical customer-to-business (C2B) digital euro payment transactions include point-of-sale (POS) payment orders in shops and e-commerce payment orders over the internet.
Defunding	The process whereby a digital euro user exchanges digital euro with cash or other funds[89].
De-tokenisation	A process of retrieving digital euro payment transactions-related data and/or other sensitive data from a surrogate value.
Device	A piece of equipment attributed to a digital euro user that could be used for authorising digital euro payment transactions and digital euro user authentication.

[88] Article 4(1), point (1), of Regulation [8]
[89] Article 2(12) of Chapter 1 of the draft Regulation [1]

Digital euro service platform (DESP) dedicated cash account (DCA) Holder	A scheme participant which owns one or multiple dedicated cash account(s) (DCAs) in TARGET.
Digital euro	A digital form of the single currency available to natural and legal persons[90].
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 account number (DEAN)	A unique identifier of a digital euro account. Digital euro account number (DEAN) is provided by digital euro service platform (DESP).
Digital euro component	A part or element that contributes to the overall functionality of the digital euro service platform (DESP).
Digital euro service platform dedicated cash account (DESP DCA)	A TARGET account in central bank money, held and operated by a TARGET participant (i.e., DESP DCA holder) for the purpose of enabling funding and defunding of digital euro payment accounts at the request and on behalf of digital euro users.
Digital euro ecosystem	All the legal entities that are either scheme participant, the scheme governing authority and the digital euro service platform (DESP) governing authority.
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[91].
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[92].
Digital euro payment order instruction	Any instruction by a payer or payee to its payment service provider (PSP) requesting the execution of a digital euro payment transaction.

[90] Article 2(1) of Chapter 1 of the draft Regulation [1]
[91] Article 7(2) of Chapter 3 of the draft Regulation [1]
[92] Article 2(5) of Chapter 1 of the draft Regulation [1]

Digital euro scheme rulebook	A single set of rules, standards and procedures for the provision of digital euro payment services.
Digital euro payment service	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[93].
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[94].
Digital euro payment transaction identifier	A unique identifier for a digital euro payment transaction.
Digital euro payment transaction management	Services offered by scheme participants to digital euro users related to the administration and processing of digital euro payment transactions.
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 PSP on its own.
Digital euro settlement infrastructure	The settlement infrastructure of the digital euro adopted by the Eurosystem[95].
Digital euro solution	A combination of technical or functional factors which enable the initiation and the acceptance of digital euro payment transaction. Digital euro solutions are certified by certifying entities either as acceptance solutions or as distributing solutions.
Digital euro user	Anyone making use of a digital euro payment service in the capacity of payer, payee, or both[96].
Digital euro wallet	An electronic payment instrument that can receive and hold digital euro, and execute digital euro payment transactions, by storing secure information related to the digital euro user's balance.
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

[93] Article 2(8) of Chapter 1 of the draft Regulation [1]
[94] Article 2(3) of Chapter 1 of the draft Regulation [1]
[95] Article 2(19) of Chapter 1 of the draft Regulation [1]
[96] Article 2(4) of Chapter 1 of the draft Regulation [1]

	network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions[97].
Direct access	A model in which a digital euro user's scheme participant directly handles all onboarding, distribution, and/or other digital euro services for the user, without involving outsourcing service providers.
Distributing payment service provider (PSP)	A scheme participant distributing digital euro payment services to individual digital euro users potentially through an outsourcing service provider.
Distributing solution	A combination of payment instrument (e.g. mobile app), communication technology (e.g. near-field communication (NFC)), and processes as prescribed in the rulebook used by a customer to initiate a digital euro payment transaction.
E-commerce	A remote digital environment to purchase goods and services online.
E-commerce digital euro payment transaction	A purchase in a remote digital environment using digital euro as a means of payment.
Electronic money (e-money)	Electronically, including magnetically, stored monetary value as represented by a claim on the issuer which is issued on receipt of funds for the purpose of making payment transactions, and which is accepted by a natural or legal person other than the electronic money issuer[98].
Electronic money institution (EMI)	A legal person that has been granted authorisation to issue electronic money[99].
Entries	Records in the Eurosystem ledger in the back-end infrastructure of the digital euro holdings held by a digital euro user.
European Data Protection Representatives (EDPB)	Representatives in the EU (with regard to obligations under the General Data Protection Regulation) of non-EU firms, which act as controller or processor of personal data while offering goods or services, irrespective of whether a payment of the data subject is required, to data subjects in the EU.

[97] Article 3(1) of Chapter (1) of Regulation [5]
[98] Article 2(2) of Chapter 1 of Directive [9]
[99] Article 2(1) of Chapter 1 of Directive [9]

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[100].
Front-end layer	All elements specifying the context (e.g. point of interaction (POI), initiation and acceptance devices, proximity/remote environment, applications) necessary to provide a digital euro payment service to digital euro users. The front-end layer interacts via defined interfaces with back-end services.
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[101].
Fraud risk	In the context of the scheme, 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 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").
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[102].

[100] Article 3(42) of Regulation [10]
[101] Article 2(20) of Chapter 1 of the draft Regulation [1]
[102] Article 2(11) of Chapter 1 of the draft Regulation [1]

Funding request	An API call submitted by a payment service provider (PSP) to digital euro service platform (DESP) to start the settlement process of a funding transaction.
Government or other public authorities	A public authority or government that in the context of digital euro payment transaction is acting as business digital euro user.
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.
Hashing	A computational operation that transforms a string of characters into a fixed size output string from which it is not possible to re-construct the original input. It is used to verify the integrity of data without revealing them.
Heartbeat mechanism	A mechanism in which payment service provider (PSP) send periodic signals to the digital euro service platform (DESP) to confirm their availability and status.
Identification	A process of identifying an individual digital euro user's, business digital euro user's, government or other public authorities' identity.
Indirect access	A model in which a scheme participants outsource digital euro user interactions to provide onboarding, distribution and/or other digital euro services.
Individual digital euro user	A natural person who is allowed to open a digital euro account on which to hold digital euro, subject to certain holding limits.
Individual holding limit	A maximum amount of digital euro that can be held by a single individual digital euro user at any time[103].
Instructing party	A party initiating a request by sending a message to the instructed party.
Inter-PSP fee	A fee paid for each digital euro payment transaction directly or indirectly between two scheme participants.
Intermediated access	A model in which the Eurosystem does not directly serve digital euro users, but instead relies on supervised PSPs (scheme participants) 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).

[103] Recital (39) of the draft Regulation [1]

Issuance of digital euro	A process 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 management	The processes to support from or to digital euro payment accounts necessary for the provision of digital euro payment service.
Liquidity provider	A payment service provider (PSP) that monitors central bank money liquidity transfers providing reserves dedicated positions on a DCA through dedicated mechanisms which are compatible with the one based on transit accounts in the relevant real-time gross settlement (RTGS) system.
Liquidity transfer	The process to transfer reserves between a scheme participant's central bank reserves and central bank reserves dedicated for use in the digital euro environment. It is executed 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.
Local storage settlement model	A settlement model referring to secure element (SE) in the digital euro user's devices performing the technical tasks of verification and registration of holdings, in line with the rules set by the Eurosystem.
M-commerce	A subcategory of e-commerce where the payment and the purchase are made on the same mobile device.
Machine-to-machine (M2M) payment	Individual payments initiated without human interaction as part of a transfer solution.
Main cash account (MCA)	A maximum amount of digital euro that can be held by a single individual digital euro user at any time[104].
Manual (de)funding:	A functionality that allows a digital euro user to manually fund or defund their digital euro payment account.

[104] Recital (39) of the draft Regulation [1]

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	A fee paid by the payee to a payment service provider when acquiring a digital euro payment transaction[105].
Mobile device	A device that enables digital euro users to authorise digital euro payment transactions online or offline including, in particular, smart phones, tablets, smart watches and wearables of all kinds[106].
National central bank (NCB)	A national central bank of a Member State whose currency is the euro[107].
Near-field communication (NFC)-based payment transaction	A payment transaction conducted with NFC (frequently referred to as contactless) technology that enables communication between devices when in proximity.
Network service provider	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 payment service provider (PSP) which holds funds not classified as digital euro.
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.
Offboarding of a digital euro user	A set of activities conducted by a scheme participant to revoke the possibility of a digital euro user to carry out digital euro payment transactions through it.
Offboarding of a payment service provider (PSP)	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 combination of hardware and software that allows a digital euro user to receive, store and transfer offline digital euro without the intervention of a third party.

[105] Article 2(24) of Chapter 1 of the draft Regulation [1]
[106] Article 2(31) of Chapter 1 of the draft Regulation [1]
[107] Article 2(13) of Chapter 1 of the draft Regulation [1]

Offline digital euro payment transaction	A digital euro payment transaction made in physical proximity, where authorisation and settlement take place in the offline digital euro device of both payer and payee.
Offline distribution	The component(s) of the Offline Solution that are running at an intermediary, interacting with the devices for funding and defunding operations.
Offline Issuance	The component(s) of the Offline Solution that are designed to ensure that issuance of funds is always monitored by the Eurosystem and always associated with a corresponding balance adjustment in a DCA belonging to the relevant intermediary, maintaining full control of the aggregated amount of offline digital euro in circulation.
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 (PSP)	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).
Onboarding repository service	A service that supports enforcing the holding limits and ensuring the emergency switching (i.e., account portability) of digital euro payment accounts in emergency situations upon the request of the digital euro user.
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.
Operator	An entity operating one or more digital euro component(s) in the digital euro service platform (DESP).
Operational data retention period	Defines the timeframe that an operational DESP component in the must retain data in its final processing state before its propagation to historic storage and its physical deletion from the operational data storage.
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.
Outsourcing	A category of third-party service relationships where a scheme participant uses a service provider to perform, on a recurrent or an

	ongoing basis, services, or parts thereof, that would otherwise be undertaken, or could reasonably be undertaken, by the scheme participant itself.
Outsourcing service provider	An entity or individual that provides services to one or more scheme participants under an outsourcing arrangement.
Pay-by-link	An online digital euro payment transaction use case in which a payee generates a digital euro payment request link and sends it to the payer via a third-party communication channel (e.g. email, SMS, messaging application).
Payee	Anyone who is the intended recipient of funds which have been the subject of a digital euro payment transaction[108].
Payee-initiated digital euro payment transaction	A digital euro payment transaction initiated by instruction from a payee to the acquiring payment service provider (PSP) and submitted to the digital euro service platform (DESP).
Payer	Anyone who has a digital euro payment account and allows a payment order from that digital euro payment account[109].
Payer-initiated transaction	A digital euro payment transaction submitted to the digital euro service platform (DESP) by the distributing payment service provider (PSP).
Payment account	An account held in the name of one or more payment service users which is used for the execution of payment transactions[110].
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[111].
Payment institution	A legal person that has been granted authorisation to provide and execute payment services throughout the Union[112].

[108] Article 2(10) of Chapter 1 of the draft Regulation [1]
[109] Article 2(9) of Chapter 1 of the draft Regulation [1]
[110] Article 4(12) of Title 1 of Directive [4]
[111] Article 4(15) of Title 1 of Directive [4]
[112] Article 4(4) of Title 1 of Directive [4]

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[113].
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[114].
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 is executed between a payer and payee without any 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).
Person-to-person (P2P) digital euro payment transaction	A digital euro payment transaction from one individual digital euro user to another.
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[115].
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.

[113] Article 4(14) of Title 1 of Directive [4]
[114] Article 4(11) of Title 1 of Directive [4]
[115] Article 4(1) of Chapter 1 of Regulation [7]

Provider of support services	One or more entities, appointed by the European Central Bank, that provide services to all payment service providers distributing the digital euro that are aimed at facilitating the smooth functioning of digital euro payment transactions[116].
Proximity payment	A payment initiated when payer and payee are in physical proximity.
Payment instruction	An API call submitted by a payer's payment service provider (PSP) to digital euro service platform (DESP) to start the settlement process of a payment transaction.
Payment service provider (PSP) identifier	An identifier used to uniquely identify a scheme participant in the digital euro service platform.
Payment service provider (PSP) solution	A combination of technical or functional factors that enable the initiation and acceptance of a digital euro payment transaction. Digital euro solutions are certified by certifying entities either as acceptance solutions or as distribution solutions.
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 information 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. Such data include, but are not limited to, payment service provider (PSP) type, name, address, contact persons, roles in the digital euro payment scheme, number of the dedicated cash account (DCA), status.
Payment request	An API call submitted by a payee payment service provider (PSP) to digital euro service platform (DESP) to start the settlement process of a payment transaction.
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, presented by the payee to the payer.

[116] Article 2(11) of Chapter 1 of draft Regulation [1]

Recovery point objective (RPO)	The maximum amount of time for which data updates (creations, modifications, deletions) can tolerably remain lost/unrecovered as a result of a failure or disaster event. Data changes that precede a failure or disaster event by at least this amount of time are preserved by a recovery.
Recovery time objective (RTO)	The maximum tolerable amount of time required to restore one or more applications and associated data to a correct operational state after a failure or disaster event has compromised availability.
Recurring digital euro payment transaction	A digital euro payment transaction for which a merchant has previously stored the payer's information and for which the payer has given pre-authorisation (e.g. fixed amount, frequency, end date).
Redemption of digital euro	A process which results in the destruction of digital euro units and of the corresponding liability on the Eurosystem balance sheet.
Refund	Return of a previous payment amount to the original payer by the original payee.
Remote payment	A payment that is initiated in a remote environment.
Reservation (Pre-authorisation)	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.
Request to pay	A request initiated by a payee to a payer, requesting the payer to pay a certain amount to the payee. A request to pay always requires authorisation by the payer. The payer may accept, reject or ignore the request. If the payer accepts the request, the digital euro payment transaction is generally executed automatically and immediately.
Residence	The place where a natural person is legally resident in the Union[117].
Reverse waterfall	A functionality whereby commercial bank money from a linked non-digital 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 participant	A payment service provider (PSP) that participates in the digital euro payment scheme, meeting the rules and requirements as set by the digital euro payment scheme rulebook.

[117] Article 2(16) of Chapter 1 of the draft regulation [1]

Secure element (SE)	A tamper-proof chip with pre-installed software that can store confidential and cryptographic data and run secure applications.
Secure Exchange of Payment Information (SEPI)	A process of substituting payer data or payee and transaction data with a surrogate value that in itself does not provide information on the digital euro payment transaction but allows the authorised payment service provider (PSP) to retrieve the necessary data elements to instruct settlement.
Settlement	The completion of a digital euro payment transaction resulting in discharging digital euro users' payment obligations.
Settlement instruction	An API call submitted 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.
Settlement model	A model according to which the two technical settlement tasks, namely settlement verification and settlement recording, are allocated among operational entities, or to the local storage devices possessed by digital euro users.
Settlement provider	An entity that performs technical settlement tasks, namely settlement verification and/or settlement recording.
Settlement recording	Bookkeeping of performed payment transactions characteristics
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[118].
Surrogate value	A set of characters that represents and replaces (sensitive) information so information can be processed safely
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[119].
Technical acquirer	An entity that enables business digital euro users, governments or other public authorities to technically accept digital euro payment orders (e.g. terminal provision). It does not hold digital euro users' digital euro and does not necessarily participate in the digital euro payment scheme.
Technical proof	The technical proof / master seed (kept by the user) is the hash of a generated 24-word passphrase (kept secret by the user). The technical proof / master seed (kept by the user) is kept by the user and used to generate Entry-IDs (used by the PSP for settlement instructions).
Termination	The process of terminating a 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 of the European Union.
Third-party service provider	An entity or individual that provides services to one or more scheme participants under a third-party service relationship, meaning a formal arrangement for the provision of one or more services, or parts thereof.
Third party-validated digital euro	A technical solution in which a third party determines the validity of a digital euro payment transaction between payer and payee.
Timestamp of completion	The moment on which a digital euro payment is finalised by transferring the funds that a payer obliges towards a payee.

[118] Article 4(30) of Title 1 of Directive [4]
[119] Article 2(26) of Chapter 1of the daft Regulation [1]

Trusted execution environment (TEE)	An isolated processing environment that ensures (i) the integrity and confidentiality of the data that are being processed and (ii) the authenticity of the software/application running on it.
User authentication	"User authentication" as defined in the proposal for a Regulation of the European Parliament and of the Council on the establishment of the digital euro (COM/2023/369 final).
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[120].
User journey	A scenario-based sequence of steps that a digital euro user takes to accomplish a specific goal within digital euro services.
User to application (U2A) interface	An interface suitable for human interaction to permit the exchange of information between software applications of the digital euro and a digital euro user through a graphical user interface.
Validation of a digital euro payment transaction	A process of checking at the level of scheme participants to ensure that the payer is entitled to make a digital euro payment transaction, or that the digital euro payment transaction fulfils all technical standards.
Value added services (VAS)	Services that go beyond the core features of a product or service, providing additional value and benefits to the customer.
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[121].
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 account, indicated by the digital euro user.

[120] Article 2(27) of Chapter 2 of the draft Regulation [1]
[121] Article 2(22) of Chapter 1 of the draft Regulation [1]

Wearable	A broad category of worn or carried physical devices which include a variety of options from less complex devices (e.g. tags) to smart watches.
Wireframe	A simplified visual outline of the layout and structure of a digital euro service, showing key elements and user interface components.

12 Annexes

A1: Certification, testing and onboarding

B1: Illustrative user journeys

B2: End-to-end process flows

C1: Reporting requirements

[Placeholder]

D1.1. Front-end implementation specifications

D.1.2 Core data requirements

D2. Back-end implementation specifications

E1: Risk management requirements - CONFIDENTIAL

F1: Minimum UX requirements

G1: Rulebook change request form

[Placeholder]