

Digital Euro Scheme Rulebook

| | |
|-----------------|-----|
| Version: | 0.8 |
|-----------------|-----|

| | |
|----------------|--------------|
| Status: | DRAFT |
|----------------|--------------|

| | |
|--------------|------------|
| Date: | 06/12/2023 |
|--------------|------------|

DISCLAIMERS FOR DRAFT RULEBOOK V0.8**Preliminary and non-binding nature of version 0.8**

This document represents a preliminary draft version (version 0.8) 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 0.8, which was shared with the RDG members in January 2024², 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 0.8 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 0.8 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 0.8 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 be subject to public consultation, incorporate any future amendments stemming from legislative discussions among co-legislators on the European Commission's proposed regulation on the establishment of the digital euro³.

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

² See Update on the work of the digital euro scheme's Rulebook Development Group, 3.1.2024, available at: https://www.ecb.europa.eu/euro/digital_euro/timeline/profuse/shared/pdf/ecb.degov240103_RDG_digital_euro_schemes_update.en.pdf

³ 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 0.8 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 rulebook may require adjustment once the Regulation on the establishment of the digital euro and the Regulation on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro are adopted by the Union legislator. The discussion is ongoing between the Commission, the Parliament, and the ECB, which publishes opinion on the draft legal act.

All along this draft Rulebook, text highlighted in **yellow** refers to placeholders to be updated at later stage when associated decisions are made.

All paragraphs and lines are also numbered (within the left margin of the document) as a way to facilitate the provision of commentary from reviewers.

TABLE OF CONTENTS

| | | |
|-----------|--|-----------|
| 1. | Document information | 9 |
| 1.1. | References | 9 |
| 1.2. | Defined terms | 9 |
| 1.3. | Change history | 9 |
| 1.4. | Ownership of the document | 11 |
| 2. | Digital euro scheme: scope and interplay | 11 |
| 2.1. | Section overview | 11 |
| 2.2. | Vision and mission statement | 11 |
| 2.3. | Scope | 11 |
| 2.4. | Digital euro participation model overview | 13 |
| 2.4.1. | <i>Key actors in the scheme</i> | 14 |
| 2.4.2. | <i>Relationships</i> | 16 |
| 2.5. | Separation between scheme and infrastructure | 16 |
| 2.6. | Benefits of the scheme | 17 |
| 2.7. | Services | 18 |
| 2.8. | Fees | 18 |
| 3. | Functional and operational model | 19 |
| 3.1. | Section overview | 19 |
| 3.2. | Naming conventions | 19 |
| 3.3. | Overview of Services | 20 |
| 3.3.1. | <i>Access management</i> | 21 |
| 3.3.2. | <i>Liquidity management</i> | 39 |
| 3.3.3. | <i>Transaction management</i> | 46 |
| 3.4. | End-to-end flows | 64 |
| 3.5. | Illustrative user journeys | 64 |
| 3.6. | Core requirements, service endpoints and list of attributes (incl. interplay with standardisation initiatives) | 64 |
| 3.7. | Identification | 64 |
| 3.7.1. | <i>Identification and authentication of components</i> | 65 |
| 3.8. | Authentication | 65 |

| | | |
|-----------|--|-----------|
| 3.8.1. | <i>Digital euro app</i> | 65 |
| 3.8.2. | <i>Intermediaries' apps / environments</i> | 66 |
| 3.8.3. | <i>Authentication with no smartphone (inclusion use cases)</i> | 66 |
| 3.8.4. | <i>Authentication in environments other than the digital euro app and the intermediaries' apps</i> | 66 |
| 3.8.5. | <i>Authentication in "open intermediary" situations</i> | 66 |
| 3.9. | Dispute management principles | 66 |
| 3.10. | Minimum user experience standards | 67 |
| 4. | Adherence Model | 67 |
| 4.1. | Section Overview | 67 |
| 4.2. | Participation in the Scheme | 70 |
| 4.3. | Reachability & interoperability | 71 |
| 4.4. | Eligibility criteria | 71 |
| 4.5. | Becoming a participant | 72 |
| 4.6. | Scheme registers of participants | 72 |
| 4.7. | Obligations of participants | 72 |
| 4.7.1. | <i>General Obligations</i> | 72 |
| 4.7.2. | <i>Obligations related to the participants role as access manager</i> | 74 |
| 4.7.3. | <i>Obligations related to the participants role as liquidity manager</i> | 74 |
| 4.7.4. | <i>Obligations related to the participants' role as transaction manager</i> | 75 |
| 4.7.5. | <i>Obligations related to the participants' role as payee's intermediary</i> | 75 |
| 4.8. | Liability | 75 |
| 4.9. | Termination | 76 |
| 4.10. | Suspension | 77 |
| 4.11. | Intellectual property | 77 |
| 4.12. | Governing law(s) | 77 |
| 5. | Technical scheme requirements | 77 |
| 5.1. | Section overview | 77 |
| 5.2. | Foundational principles for the selection of technical standards | 78 |
| 5.3. | High-level IT infrastructure | 78 |
| 5.4. | Domains of actors | 79 |

| | | |
|----------------|--|------------|
| 5.4.1. | <i>End user domain</i> | 79 |
| 5.4.2. | <i>Payer and payee intermediary domain</i> | 95 |
| 5.5. | IT security | 97 |
| 5.6. | Non-functional requirements | 97 |
| 5.6.1. | <i>Availability and reliability requirements</i> | 98 |
| 5.6.2. | <i>Performance requirements</i> | 99 |
| 5.6.3. | <i>Compatibility requirements</i> | 99 |
| 5.6.4. | <i>Integrity requirements</i> | 99 |
| 6. | Risk management | 100 |
| 7. | Scheme management | 100 |
| 8. | Defined terms and abbreviations | 100 |
| Annex A | Functional and operational model | 117 |
| A.1 | Illustrative user Journeys | 117 |
| A.2 | E2E Flows | 117 |
| A.3 | Data management | 117 |
| A.4 | Illustrative user products | 117 |
| A.5 | Branding standards | 117 |
| A.6 | Limits and thresholds | 117 |
| Annex B | Adherence model | 117 |
| B.1 | Adherence agreement and related documents | 117 |
| B.2 | Onboarding document and toolkit | 117 |
| B.3 | Approval framework | 117 |
| B.4 | Certification and testing ecosystem | 117 |
| B.5 | Dispute Management | 118 |
| Annex C | Technical Scheme Requirements | 118 |
| C.1 | Service Level Requirements and Key Performance Indicators | 118 |
| C.2 | Reporting requirements and guidelines | 118 |
| C.3 | Incident management, disaster recovery, and business continuity management | 118 |
| C.4 | Dispute Handling | 118 |

| | | |
|----------------|---|------------|
| Annex D | Risk Management | 118 |
| Annex E | Scheme Management | 118 |
| Annex F | Scheme compatibility and interoperability | 118 |
| F.1 | Fee table | 118 |
| F.2 | Scheme compatibility and interoperability | 118 |
| Annex G | Implementation specifications | 119 |
| G.7 | Implementation specifications and technical standards | 119 |
| G.7.1 | Individual and business users | 119 |
| G.7.2 | Between individual users | 119 |
| G.7.3 | Individual users and PSPs | 119 |
| G.7.4 | Business users and PSPs | 119 |
| Annex H | Enforcement model | 119 |
| H.1.1 | Enforcement model | 119 |

1. Document information

1.1. References

This section lists documents referred to in the digital euro scheme rulebook. The convention used throughout is to provide the reference number only, in square brackets. Use of square brackets throughout is exclusively for this purpose.

Table 1.1-1 Documents referred to in the Rulebook

| N° | Document Number | Title | Issued by |
|-----|-----------------|--|---------------------|
| [1] | 2023/0212/COD | Proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro | European Commission |
| [2] | CON/2023/34 | Opinion of the European Central Bank of 31 October 2023 on the digital euro | European Commission |

1.2. Defined terms

The digital euro scheme rulebook makes reference to various defined terms which have a specific meaning in the context of this rulebook and are hence indicated with capital letters. Section 8 provides the list of defined terms.

1.3. Change history

Table 1.3-1: History of changes made to the Rulebook.

| 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. |
|--|--|--|

1.4. Ownership of the document

The digital euro scheme rulebook is owned by the Eurosystem.

2. Digital euro scheme: scope and interplay

2.1. Section overview

This section delineates the scope of the digital euro scheme, defining the actors, the services and the relationships orchestrated by the Rulebook. **Error! Reference source not found.** summarises these elements. This section also highlights the mission statement and intended benefits of the scheme.

2.2. Vision and mission statement

The digital euro scheme rulebook (the Rulebook) consists of a set of rules and standards (rights and obligations) allowing intermediaries to join, participate and operate in the scheme. The objectives of the Rulebook are:

- To support the vision and mission of the digital euro in line with the digital euro objectives.
- To describe the rights and obligations set by the scheme, potentially alongside with EU legislation, ECB regulatory acts, contractual provisions, concession contracts etc.

The Rulebook supports the vision and mission of the digital euro, as described in [1] (Procedure 2023/0212/COD - proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro).

2.3. Scope

The geographical scope of the Scheme is the Euro area, the EU and third countries – subject to the corresponding agreements.

As regards the material scope of the Rulebook, as depicted in Figure 2.4-1 below, it covers all functionalities that intermediaries are obliged to provide in supporting the execution of payment transfers in digital euro. The Rulebook will not cover the liquidity transfers between digital euro

DCA's and MCA (part of the TARGET framework), the provision and management of the back-end services by the DESP⁴ (a matter for the Eurosystem and respective ECB legal act/s) as well as the underlying contract between the payer and the payee (a matter of private law).

The following key provisions should, from a business viewpoint, be covered by the Rulebook:

- A set of rules, practices and standards under which all actors who have agreed and been authorised to participate are bound.
- Specifications of the functioning and limits of the following relationships:
 - Payer and payer's intermediary
 - Payee and payee's intermediary.
- The functionalities managed by the intermediaries, i.e.:
 - **Access Management**
 Access management describes onboarding and offboarding of end users in/from the digital euro environment. The onboarding consists of activities that provide an end user access and ability to use a digital euro account while the offboarding is a procedure initiated when an end user shall not use a digital euro account anymore. Access management also describes the recurring lifecycle management processes enabling end users to interact with the digital euro environment, including the option of digital euro account portability.
 Note: In the context of the digital euro intermediaries do not actually carry payment accounts with money in them but rather provide mere access to payment accounts held at the level of the Eurosystem. Also, at no point in time are the intermediaries legally entitled to digital euro amounts held with the Eurosystem for the end users.

⁴ Note: The DESP is a platform enabling the issuance and redemption of digital euro and providing functions (e.g., settlement and other functions) that cannot be accomplished by an individual intermediary carrying no settlement accounts in digital euro but only acting on behalf of end users.

61 ○ **Transaction Management**

62 Once successfully onboarded an individual will be able to pay and receive
63 payments in digital euro at anytime and everywhere in the euro area:

- 64 ▪ Payments from person-to-person (P2P), available online and offline;
- 65 ▪ Payments at E-commerce stores, available online (including consecutive
66 and recurring payments, and also includes payments to governments
67 initiated on websites hosted by governments); and
- 68 ▪ Payments at the point-of-sales (POS) (also includes payments to
69 governments at government agencies), available online and offline.

70 ○ **Liquidity management**

71 End users can choose to fund and/or defund their digital euro account from and
72 to cash as well as private money commercial bank account on a 24/7/365 basis
73 manually or automatically at a pre-defined moment in time.

- 74 • Specification of a minimum set of data elements to be exchanged by the different actors
75 when performing the functions as laid out in the Rulebook.
- 76 • The different use cases in which the Digital Euro can be used, and with what limitations.
- 77 • The Rulebook will not include any provision regarding the relationship between the
78 intermediaries and the Eurosystem for the access and use of the back-end services of
79 the DESP. The latter will be covered by the respective ECB legal act/s (still to be
80 defined) and respective contractual arrangements.

81 **2.4. Digital euro participation model overview**

82 The chosen distribution model for the digital euro requires the collaboration of the public and
83 private sector actors active in the euro retail payment ecosystem. End users will be able to open
84 digital euro accounts via intermediaries (like for other digital payments), exchange cash and
85 private money into digital euro and vice versa, and transfer digital euros between each other
86 (users).

2.4.1. Key actors in the scheme

Delivering the digital euro requires the orchestrated interaction of the following actors, both private and public. The **four private⁵ sector actors** are the payer, the payee, the payer's intermediary, and the payee's intermediary.

(1) The payer is a party in a payment transaction which agrees to the transfer of digital euro to the payee. In the context of the scheme, a payer might be an individual user, a business user, a government or other public authorities.

(2) The payee is a party in a payment transaction which receives digital euro from the payer. In the context of the digital euro project, a payee might be an individual user, a business user, a government or other public authorities.

An intermediary is an entity acting between a central bank and end users in the digital euro environment without becoming a holder of digital euro. Intermediaries can have different roles and they may be credit institutions or other payment service providers (payment institutions, e-money institutions).

(3) The payer's intermediary is the participant that receives the digital euro transfer instruction from the payer and acts upon arrival of the payment instruction by initiating the transfer of the digital euro from the payer to the payee to be undertaken in the DESP according to the information provided in the instruction and in accordance with the provisions of the scheme.

(4) The payee's intermediary is the participant that receives the notification from the DESP about the digital euro received and acts there upon, in accordance with the provisions of the scheme.

The payer's intermediary and the payee's intermediary may be the same entity.

The public sector actor is the **Eurosystem⁶** in the roles of:

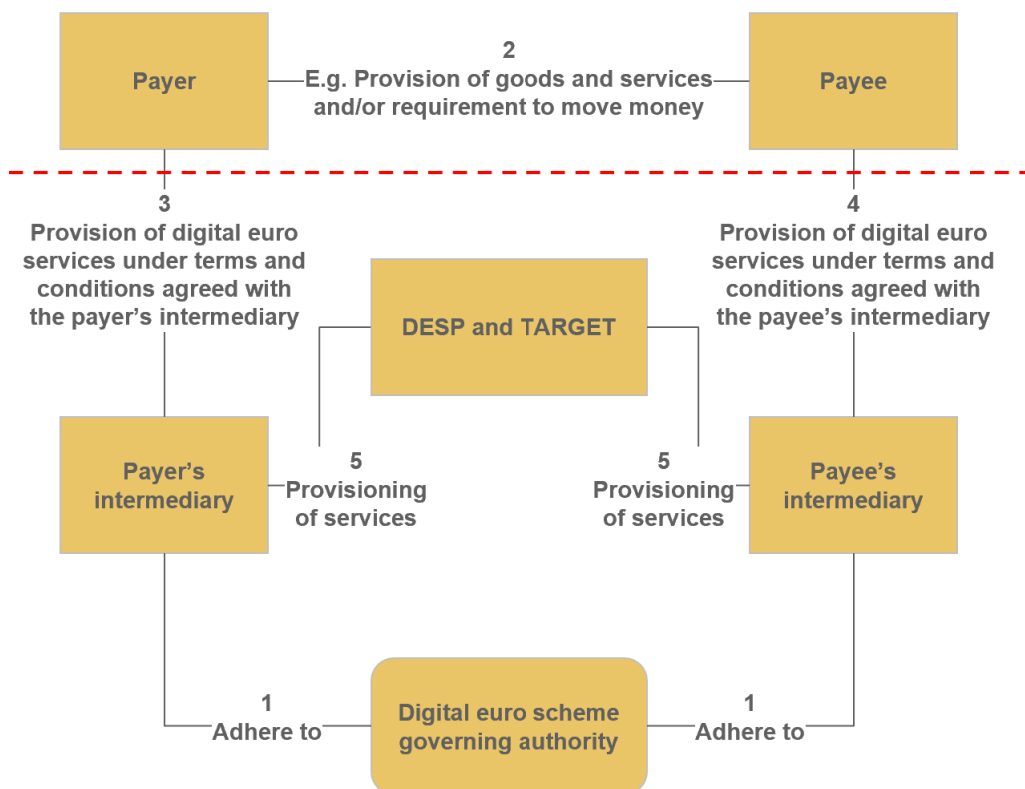
⁵ Note: Public sector entities may act as payers/payees as well.

⁶ The Eurosystem could act by means of the ECB Governing Council or a dedicated body duly delegated by the GovC, as governing authority of the scheme.

1. The scheme governing authority
2. A digital euro service platform (DESP) provider
3. The provider for the provision of funding and defunding in digital euro through TARGET.

The following **Error! Reference source not found.** presents an overview of the parties interacting in the digital euro ecosystem.

Figure 2.4-1 Relationships in the digital euro ecosystem



Note: Intermediaries may engage third party entities as agents or subcontractors supporting them in the provision of functions they are obliged by the Rulebook, while maintaining full liability. Such third party entities would from a contractual point of view not be an actor in the scheme.

2.4.2. Relationships

1. The relationship **between the Eurosystem** (as governing authority of the scheme) and **each participant** (“intermediary”) underlies the scheme. All participants will be bound through the Scheme Participation Agreement. While the legal architecture of the ECB’s legal acts on the digital euro is not finalised, it can be expected that the Rulebook is to form part of such acts or be incorporated by reference in them.
2. The underlying relationship between **the payer and the payee** does not form part of the is not directly governed by the scheme, and its validity does not influence the validity of payments effected through the scheme. Provision of goods and services and/or requirement to move money between payer and payees is one example for an interaction between payers and payees being outside the scope of the scheme.
3. The relationship between the **payer and the payer’s intermediary** concerning the digital euro services to be provided and their related Terms and Conditions. This relationship is not directly governed by the scheme, but the minimum requirements of the Rulebook related to user management, liquidity management and transaction management are expected to be imposed on the payer by its intermediary.
4. The relationship between the **payee and the payee’s intermediary** concerning the digital euro services to be provided and the related Terms and Conditions. This relationship is not directly governed by the scheme, but the minimum requirements of the Rulebook related to user management, liquidity management and transaction management are expected to be imposed on the payee by its intermediary.
5. The relationship between the **payer’s intermediary, the payee’s intermediary and the eurosystem** (as provider of the DESP and TARGET) concerning the back-end services provided and the related Terms and Conditions. These relationships are not governed by the scheme.

2.5. Separation between scheme and infrastructure

The digital euro scheme provides a set of rules, practices and standards to be followed by intermediaries (participants in the digital euro scheme). The digital euro service platform (DESP) will provide (part of) the digital euro infrastructure. The scope and rules of the DESP will be described in a **Eurosystem framework (still to be defined)**.

2.6. Benefits of the scheme

Citizens in the euro area benefit from a generally accepted means of payment – euro cash – which they can use freely across our monetary union. Cash has unique properties, including high standards for safety and privacy, and is valued by Europeans as a payment option, even when they choose not to use it. That is why the Eurosystem will continue to make euro cash available for everyone to use.

Nevertheless, the world is becoming increasingly digital, and payments are no exception. With the use of cash declining and the shift towards online shopping and digital payments accelerating in the wake of the pandemic, it is important to ensure that Europeans' money and payments remain secure, safe and future-proof. In this context, the digital euro has an essential role to play, as a public good provided to citizens and merchants by the central bank.

The digital euro is not to be tangible but brings key features of cash into the digital era. Like euro cash, the digital euro offers privacy and is widely accepted across the euro area. It provides an additional payment option to complement cash and private digital payment solutions (and does not replace them).

The digital euro is designed to have the highest possible level of privacy. The central bank has no interest in citizens' payment patterns and/or any commercial aspirations, and as such would neither access nor store users' personal data.

The digital euro is inclusive and ensures that all citizens have access to digital payments, even without a bank account, credit card and/or internet connection for some use cases and form factors. The digital euro is designed for use in physical and online payments, as well as for person-to-person transactions.

The digital euro protects universal access to safe money. The ability to convert money issued by private intermediaries into a completely risk-free form issued by the central bank anchors trust in the euro. To preserve this trust, the Eurosystem needs to ensure the euro remains fit for purpose in the digital era.

Payments are an essential part of citizens' lives and the digital euro ensures the continued smooth functioning of the payments system. It increases resilience against crises such as cyber-attacks and electricity outages. Likewise, it reduces dependence on non-European payment providers. It also fosters further innovation in the private sector by increasing market competitiveness.

Taking European integration a step further, the digital euro is a standardised means of payment, covering all payment needs across all euro area countries. It provides an unprecedented pan-European platform for innovative payment services.

Furthermore, a scheme-based distribution approach for the digital euro allows for the most degrees of freedom for the market to distribute the digital euro and develop innovative front-end solutions, while still fulfilling the two key objectives of the Eurosystem: digital euro as a monetary anchor as well as strategic autonomy and economic efficiency. This approach promotes a harmonised end-user payment experience through the specification of requirements for scheme members, whilst still allowing the flexibility to respond to local preferences and specificities.

2.7. Services

Digital euro services regulated by the scheme are grouped into three categories:

- **Mandatory services** that each scheme participant obliged to offer,
- **Conditional services** that some scheme participants are obliged to offer, depending on their status (in line with [1] Article 14 of Procedure 2023/0212/COD which stipulates proposal for a regulation of the European Parliament and of the Council on the establishment of the digital euro)
- **Optional services** for which the offered services are not mandatory but regulated by the scheme for intermediaries wishing to offering them

The list of mandatory, conditional and optional services is detailed in Section 4 of the Rulebook (adherence model), in line with the Regulation of the European Parliament and of the Council for details on the objectives of the proposal.

One aim of the digital euro scheme is to encourage innovation by making it easy to integrate services, e.g. through standardised application planning interfaces (APIs) and compatibility with existing standards (see Section 3.4). Thus, intermediaries will be enabled and encouraged to develop value-added services, in addition to the mandatory, conditional and optional services set out below.

2.8. Fees

Will be further detailed in next iterations of the Rulebook.

3. Functional and operational model

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 described by the means of end-to-end process flows. Summarised process flows are included in this section while detailed process flows are included in Annex A.2 – E2E flows. These process flows were designed on the basis of illustrative user journeys, available in Annex A.1 – Illustrative user journeys.

3.2. 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.

A **dataset** is defined as a set of attributes required by the Rulebook.

An **attribute** is defined as specific information to be used in the Rulebook.

To facilitate the reading and the use of this Rulebook, structured identification numbers are used as follows:

| | |
|---------|--|
| Process | AM-xx, where AM represents access management flows and xx represents the unique alphanumeric sequence in this Rulebook |
| | LM-xx, where LM represents liquidity management flows and xx represents the unique alphanumeric sequence in this Rulebook |
| | TM-xx, where TM represents transaction management flows and xx represents the unique alphanumeric sequence in this Rulebook |
| | OT-xx, where OT represents other flows (not fitting in the categories AM, LM and TM) and xx represents the unique alphanumeric sequence in this Rulebook |

| | |
|---------------|---|
| Process steps | AM/LM/TM/OT-xx-yy, where yy is the unique sequence number of the process-step inside process xx |
| Datasets | DS-xx, where xx represents the unique sequence number |
| Attributes | AT-xx, where xx represents the unique sequence number |

3.3. Overview of Services

This section describes the digital euro focus areas of most relevance to end users.

Access management – registration and management of digital euro describes onboarding, offboarding, and lifecycle management processes of end users and intermediaries in/from the digital euro environment.

Liquidity management – distribution and control of amount in circulation of a digital euro describes the funding/defunding of the end user's digital euro account from and to a private money account on a 24/7/365 basis manually or automatic (reverse waterfall/waterfall) at a pre-defined moment in time.

Processing of digital euro transactions (transaction management): describe the services that enables users to transact in digital euro (through a one-off or recurring payment) and comprises activities including authentication, payment initiation service and payment confirmation/rejection.

242

Figure 3.3-1 Core and optional services⁷

| Access management | Liquidity management | Transaction management |
|---|-----------------------------------|---|
| Onboarding digital euro end-users | Funding (manual & automated) | Transaction initiation (one-off transactions) |
| Offboarding digital euro end-users | Reverse waterfall | Authentication |
| Payment instrument management (both provision and maintenance) | Defunding (manual & automated) | Payment confirmation/rejection notification |
| Linking digital euro holdings to commercial bank money account | Waterfall | Refunds |
| User lifecycle management processes (identification, data update, information display on balance and transactions, account portability and end user support) | | Dispute/exception management |
| Account information service | | Recurring payments |
| | | Pay-per-use enabled via pre- authorisation service |
| | | Payment initiation service |
| | | Core services |
| | | Optional services |

243

244 **3.3.1. Access management**245 **3.3.1.1. Onboarding of an end user**

246 Intermediaries⁸ are responsible for the onboarding of end users, which can take place both
 247 remotely or onsite.⁹ Onboarding consists of activities that provide an end user access and ability
 248 to use a digital euro including the provision of digital euro account number(s), the user's form
 249 factor and (voluntary) registration of alias(es).

250 A high level process flow for the onboarding of a user is included below.

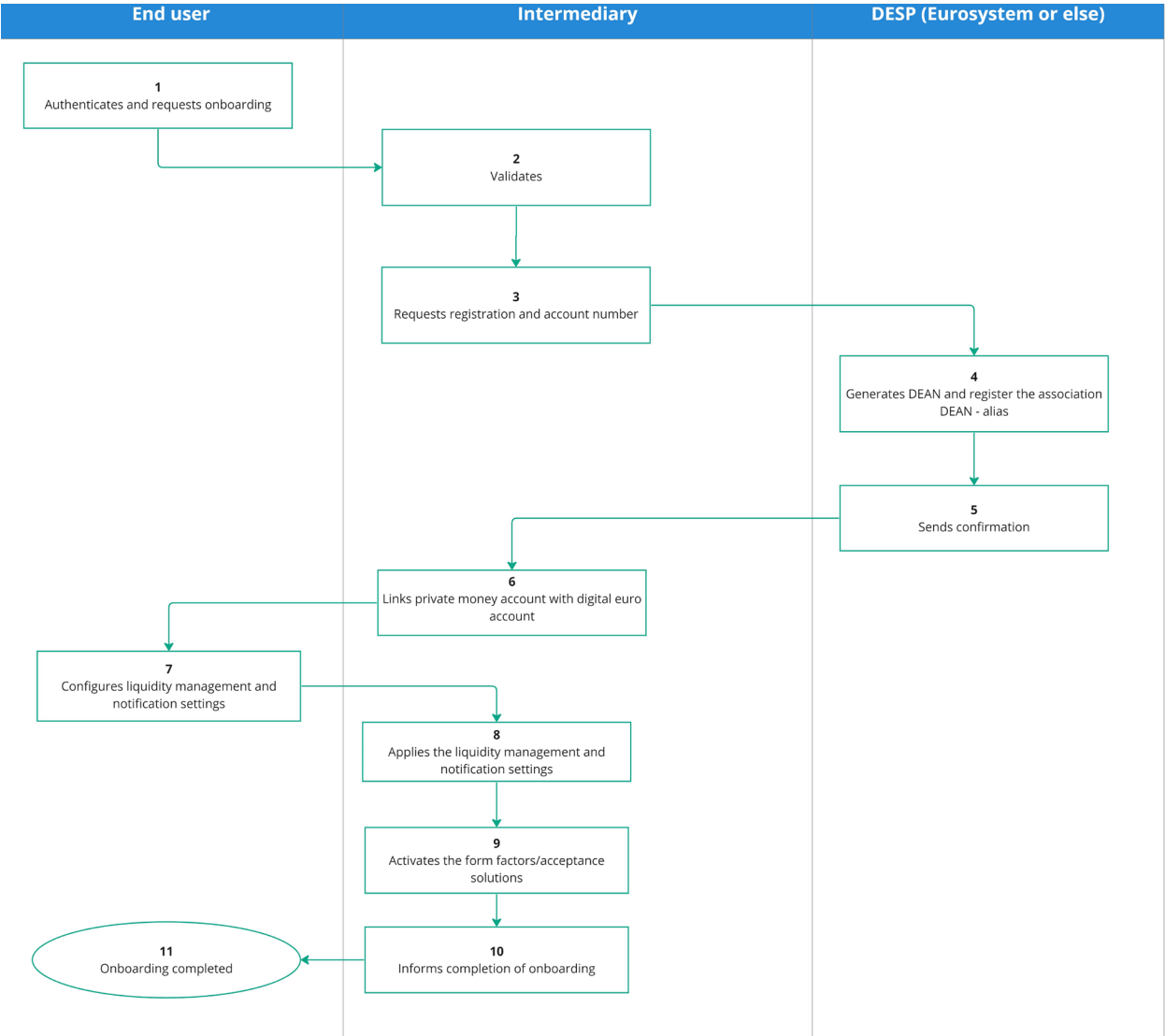
⁷ Digital euro payment initiation and account information services would be optional for PISPs and AISP to offer to end-users but digital euro ASPSPs would need to, as per PSD2, always support these services.

⁸ The intermediary that provides the onboarding services is called "access manager". An access manager is an intermediary that provides end 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.

⁹ 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.

251

Figure 3.3-2: High level process flow for the onboarding of a user



252

253 Description of steps:

254

1. The user authenticates and submits a request for onboarding the intermediary for digital euro services (assumption: the user is already a customer of the intermediary).

255

256

2. The intermediary validates the user credentials and the onboarding request.

257

3. The intermediary requests DESP to register the user (in a pseudonymised way), possibly an alias and to generate the digital euro account number (DEAN).

258

4. The DESP registers the user (in a pseudonymised way), possibly an alias and generates the DEAN.
5. The DESP confirms the registration and returns the DEAN
6. The intermediary receives and registers the DEAN and (if requested by individual user; mandatory for business users, optional for individual users) links a private money account to the digital euro account to enable automatic funding and defunding (including (reverse) waterfall)
7. The user sets up liquidity management preference (only if a linked account has been set up; e.g. reverse waterfall and/or periodic or threshold based ((de-)funding) and notification preferences
8. The intermediary registers the user's liquidity management and notification settings
9. The intermediary activates the user's form factors (this form factor activation may be combined with distribution (after preparation / configuration) in case of card)
10. The intermediary informs the user that the onboarding is completed and shares the DEAN
11. The user is informed about the completion of the onboarding

The following E2E flows detail this high-level process flow further:

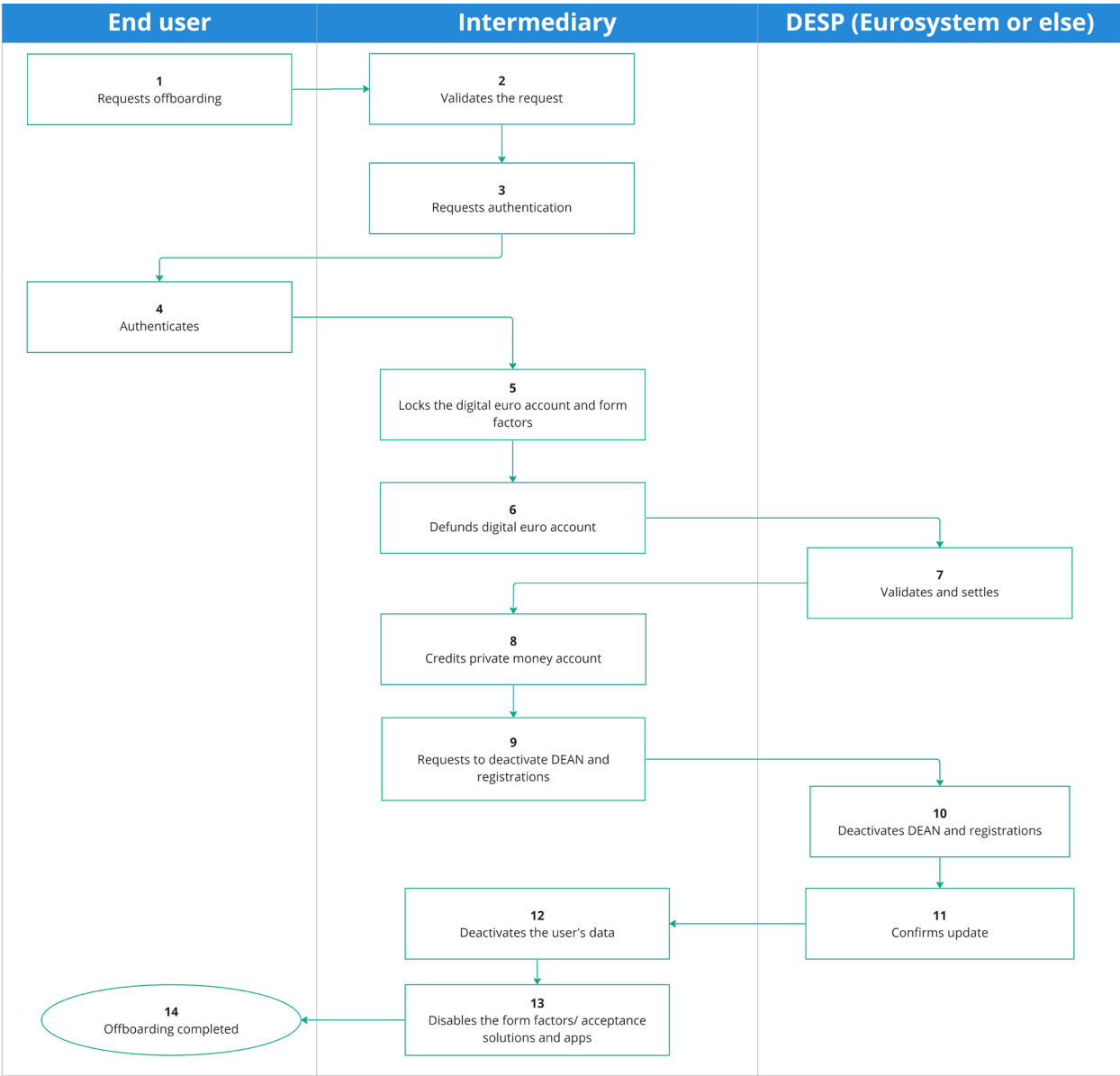
- AM – 01 onboarding of end user (individual)
- AM – 07 end user (business) onboarding

3.3.1.2. Offboarding of an end user

The offboarding is a procedure initiated when an end user chooses to close their digital euro account. The intermediary will be able to return the funds associated with a digital euro account number, deactivate recurring payments (if activated), resolve pending disputes, close all open transactions and disable access to form factors.

A high level process flow for the offboarding of a user is included below.

Figure 3.3-3: High level process flow for the offboarding of a user



Description of steps:

1. The user requests the intermediary to be offboarded for digital euro services.
2. The intermediary validates the user's offboarding request.
3. The intermediary prompts the user for authentication
4. The user authenticates

5. The intermediary locks the user's digital euro account and the user's form factors to ensure no payments can be initiated or received anymore
6. If the user has a positive (online) digital euro balance, the intermediary defunds the digital euros to either the linked private money account, a private money account specified by the user (if no private money account is linked) or a cash withdrawal
7. The DESP validates and settles the defunding instruction and confirms the defunding to the intermediary
8. Upon receiving the settlement confirmation from the DESP, the intermediary credits the user's private money account (if the private money account is serviced by another intermediary the process is more complex than the one shown in **Error! Reference source not found.**)
9. The intermediary requests the DESP to deactivate the user registration, DEAN and (if applicable) the user alias
10. The DESP deactivates the user registration, DEAN and (if applicable) the user alias
11. The DESP confirms the deactivation to the intermediary
12. The intermediary disables the user's data related to the digital euro service
13. The intermediary disables the user's form factors (which were blocked earlier) and apps and confirms the offboarding completion to the user
14. The user is informed about the completion of the offboarding.

The following E2E flows detail this high-level flow further:

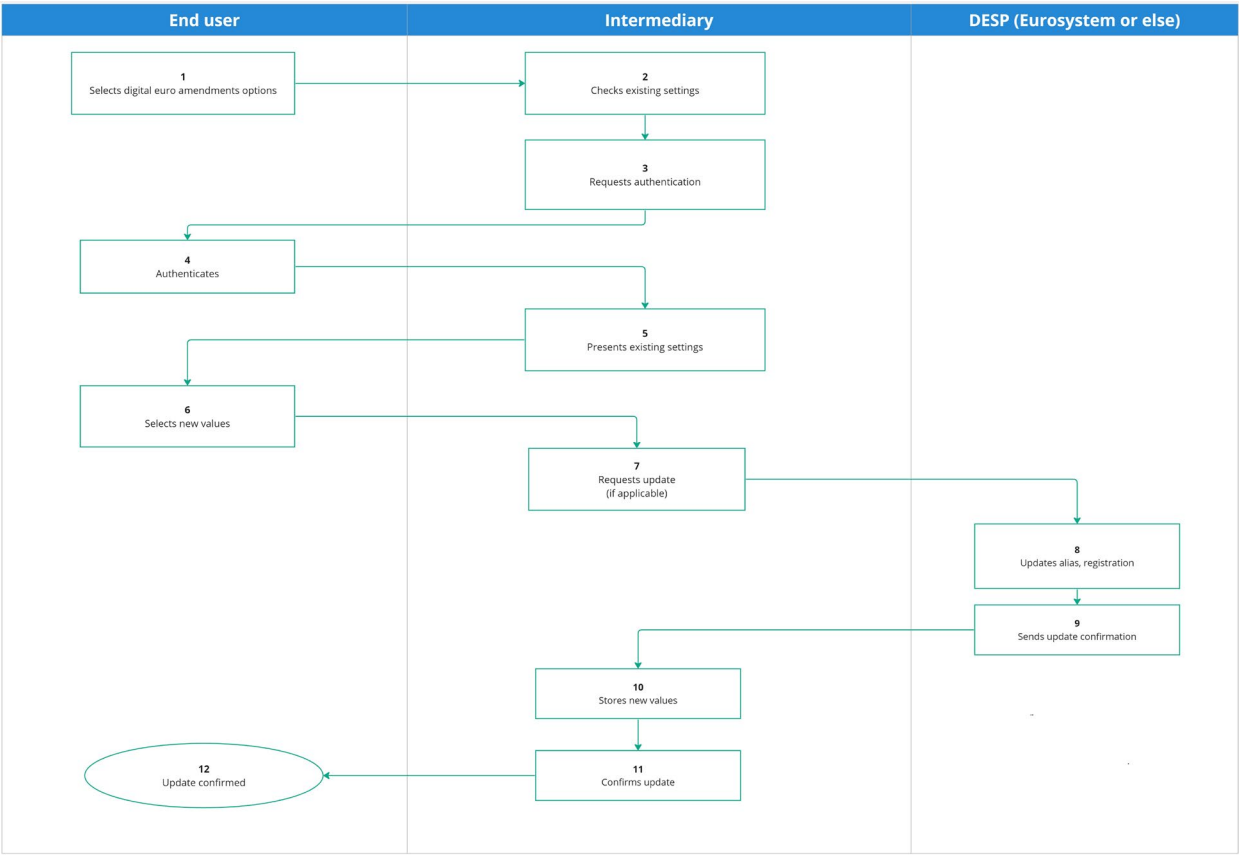
- AM – 05 end user (individual) offboarding
- AM – 08 end user (business) offboarding

3.3.1.3. User lifecycle management processes for end users

The lifecycle management processes for end users enables an end user to interact with the digital euro environment, including the option of adding/removing private money accounts used for funding/defunding/waterfall/reverse waterfall, digital euro account portability, see and edit different types of limits and thresholds, and checking digital euro balance & transaction history.

A high level process flow for the lifecycle management of a user is shown in Figure below.

Figure 3.3-4: High level process flow for the lifecycle of a user



Description of steps:

1. The user selects an amendment option
2. The intermediary checks the existing settings related to the amendment option selected by the user
3. The intermediary prompts the user for authentication
4. The user authenticates
5. The intermediary displays the existing settings related to the amendment option selected by the user
6. The user specifies the new values for the setting or activates or deactivates a setting

7. Depending on the amendment option selected by the user, the intermediary can request the DESP to update the user settings in DESP (e.g. alias)
8. If applicable, the DESP updates the user settings
9. If applicable, the DESP confirms the updates to the intermediary
10. The intermediary stores the new values
11. The intermediary confirms the updates to the user
12. The user is informed about the completion of the updates.

The following E2E flows detail this high-level flow further:

- AM – 06 end user (individual) amendments (including alias registration, account linkage, liquidity management settings and notification preferences)
- AM – 09 end user (business) amendments

3.3.1.4. Access Management business rules

The business rules provide a more detailed view on the responsibilities of scheme participants, complementing the responsibilities described in the adherence model. The business rules take the form of instructions (specifying what participants must do, either in general or when specific conditions are met) and constraints (specifying what is not possible or allowed under the scheme).

| Id | Business rule |
|-------------------|---|
| AM-001-001 | Upon receipt of an onboarding request from an individual user, the intermediary must check based on a mandatory PID whether the user already holds a digital euro account (either with the same or another intermediary). If that is the case, the user's request to onboard cannot be accepted. The intermediary should check if the user wishes to port the existing account instead. |
| AM-001-002 | If the intermediary accepts the individual user's onboarding request, it needs to request a DEAN and registration of the user in the DESP, |

| | |
|-------------------|--|
| | including the mapping to the responsible intermediary and possibly including an alias. |
| AM-001-003 | The intermediary must request tokenisation of the individual user's DEAN. |
| AM-001-004 | The intermediary must share the DEAN and technical proof with the individual user when onboarding is completed successfully. |
| AM-001-005 | If the intermediary accepts the individual user's offboarding request, it needs to first lock the user's digital euro account and the user's form factors, request the disablement of the user's token and alias (if applicable) in DESP and defund the user's online holdings. Subsequently, the user needs to request the deactivation of the user registration (including DEAN) and disable the user's digital euro account and the form factors. |
| AM-001-006 | An intermediary must allow individual users to link a private money account to their digital euro account for funding and defunding purposes, either during onboarding or at any later point in time |
| AM-001-007 | An intermediary must allow individual users to change or remove the link to a private money account at any point in time. If the user chooses to remove the linked account all automated liquidity management options (including waterfall and reversed waterfall) must be disabled as well. |
| AM-001-008 | An intermediary must allow individual users to activate or deactivate the reverse waterfall option |
| AM-001-009 | An intermediary must allow individual users to activate or deactivate the waterfall option |
| AM-001-010 | An intermediary must allow individual users to specify that the reverse waterfall option and automated funding can only be applied if the linked private money account holds sufficient balance, without the need for overdraft. |

| | |
|-------------------|---|
| AM-001-011 | An intermediary must allow individual users to set up, change and terminate either periodic funding or threshold based funding. In case of period funding the user must be allowed to specify the start date, frequency and funding amount. In case of threshold based funding the user must be allowed to specify the threshold amount and the funding amount. |
| AM-001-012 | An intermediary must allow individual users to set up, change and terminate either periodic defunding or threshold based defunding. In case of period defunding the user must be allowed to specify the start date, frequency and defunding amount. In case of threshold based defunding the user must be allowed to specify the threshold amount and the defunding amount. |
| AM-001-013 | An intermediary must allow individual users to modify or disable their automated funding and defunding settings at any point in time. If the user chooses to disable automated funding and/or defunding settings, any associated notification settings (including waterfall and reversed waterfall) must be disabled as well. |
| AM-001-014 | An intermediary must allow individual users to specify for which events they wish to receive notifications: <ul style="list-style-type: none"> - 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-001-015 | An intermediary must allow individual users to select the means of notification from a predefined range of options. |
| AM-001-016 | An intermediary must allow individual users to modify their notification settings at any point in time. |

| | |
|-------------------|--|
| AM-001-017 | <p>An individual user may request the porting of their digital euro account (keeping the same DEAN) from one intermediary to another intermediary at any time. Such a request can only be refused by the current intermediary for the following reasons:</p> <ul style="list-style-type: none"> - some or all of the user's digital euro holdings are reserved - there are (pre-)disputes related to transactions from or to the account that have not been resolved yet |
| AM-001-018 | <p>If an intermediary accepts a (standard) porting request from an individual user, it must request the transfer of digital euro holdings on the ledger from the previous intermediary to itself, generate the new technical proof and it must allow the user to port the transaction history and/or standing orders from the previous intermediary if the user wishes to do so.</p> |
| AM-001-019 | <p>If the user chooses to port the digital euro account without porting the transaction history, both the new and the old intermediary must allow the user to port the transaction history at a later date up to 30 days after the porting of the digital euro account.</p> |
| AM-001-020 | <p>If the user chooses to port the digital euro account without porting the transaction history, the old intermediary must allow the user to consult the transaction history for a minimum of 13 months after the porting of the digital euro account.</p> |
| AM-001-021 | <p>If the user chooses to port the transaction history, the old intermediary send the transaction history to the new intermediary and the new intermediary must make the transaction history available to the user.</p> |
| AM-001-022 | <p>Offline digital euros cannot be ported. They must be defunded prior to porting.</p> |
| AM-001-023 | <p>The previous intermediary must apply SCA to authenticate the user and obtain approval for the porting request before executing it.</p> |

| | |
|-------------------|--|
| AM-001-024 | If the previous intermediary accepts the porting request, it must send a positive reply to the request immediately and refrain from processing any further payment, funding or defunding requests involving the digital euro account. |
| AM-001-025 | Intermediaries are only allowed to register aliases for users to which they provide digital euro services |
| AM-001-026 | Intermediaries are only allowed to register aliases for individual users |
| AM-001-027 | Intermediaries must give individual users the possibility to register, change or disable an alias in the alias lookup service. Users can choose not to register an alias. |
| AM-001-028 | Registration of an alias, changes to an alias registration and disablement of an alias are subject to SCA. |
| AM-001-029 | Intermediaries shall only register an alias in the alias lookup service with the user's consent |
| AM-001-030 | Only one alias can be registered per digital euro account. |
| AM-001-031 | Intermediaries must verify that the alias provided belongs to the user. |
| AM-001-032 | Intermediaries must manage their user's aliases by promptly updating, amending and deactivating them as soon as a change occurs. |
| AM-001-033 | Intermediaries are responsible for the correctness of the association between the alias value and the customers account number and shall be liable for any damage caused by an incorrect association. |
| AM-001-034 | Intermediaries and their users are not permitted to use the alias lookup service for any other purpose than the initiation of a transaction. |
| AM-001-035 | Intermediaries 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 intermediary for e.g. compliance or fraud reasons). |

| | |
|-------------------|---|
| AM-001-036 | Intermediaries must give individual users the possibility to block, unblock, activate or deactivate their form factor(s) (e.g. card, app, offline wallet). Individual users can only unblock their form factor(s) if they have blocked it themselves (i.e. if it was not blocked by the intermediary for e.g. compliance or fraud reasons). |
| AM-001-037 | The intermediary must verify that the end user reporting a stolen or lost device is indeed the authorised end user of the device. |
| AM-001-038 | When a device connects online for reconciliation, the intermediary must check whether the device has been reported lost or stolen and if, so the status of the device shall be set as disabled. |
| AM-001-039 | A disabled device is not allowed to initiate or receive transactions, to fund or defund or to query transactions |
| AM-001-040 | The intermediary must change the status of the device from disabled to enabled when the device is reported found or recovered by the authorised end user. |
| AM-001-041 | If the intermediary accepts the individual user's onboarding request, it needs issue a card if requested by the user. |
| AM-002-001 | If the intermediary accepts an onboarding request from a business user, it needs to request one or multiple DEAN(s) and registration of the user in the DESP, including the mapping to the responsible intermediary. |
| AM-002-002 | The intermediary must share the DEAN(s) and the technical proof(s) with the business user when onboarding is completed successfully |
| AM-002-003 | If the intermediary accepts the business user's offboarding request, it needs to first lock the user's digital euro account(s) and disable the user's acceptance solutions and defund the user's online holdings. Subsequently, the user needs to request the deactivation of the user registration (including DEAN(s)) and disable the user's digital euro account(s). |

| | |
|-------------------|---|
| AM-002-004 | An intermediary must ensure that a business user's digital euro account has a private money account linked to it at all times. A business user is allowed to change the linked account, but not to close or unlink it. |
| AM-002-005 | <p>An intermediary must allow business users to specify for which events they wish to receive notifications:</p> <ul style="list-style-type: none"> - 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 - aggregated notifications for specific event types |
| AM-002-006 | An intermediary must allow business users to select the means of notification. |
| AM-002-007 | An intermediary must allow business users to modify their notification settings at any point in time. |
| AM-002-008 | A business user cannot port their digital euro account from one intermediary to another intermediary. |
| AM-002-009 | Intermediaries must give business users the possibility to block, unblock, activate or deactivate their acceptance solutions (e.g. POS terminal, payment gateway). Business users can only unblock their form factor(s) if they have blocked it themselves (i.e. if it was not blocked by the intermediary for e.g. compliance or fraud reasons). |
| AM-002-010 | Intermediaries must allow business users to open (a) new digital euro account(s) or close (an) existing digital euro account(s) and to change (a) private money account(s) linked to these digital euro account(s). |
| AM-002-011 | If the digital euro account to be closed happens to be the last digital euro account of that business user, the business user must be offboarded. |

| | |
|-------------------|---|
| AM-002-012 | If the intermediary accepts the business user's account closure request, it needs to first lock the user's digital euro account and disable the user's acceptance solutions and defund the user's online holdings. A digital euro account need to be maintained for the period specified in Annex A.6 after closure for refunds and claims. Subsequently, the user needs to request the deactivation of the user registration (including DEAN) and disable the user's digital euro account. |
| AM-003-001 | Users can request their intermediaries to be offboarded for digital euro services at any point in time. The intermediary can only reject such a request for the following reasons: - the user has a (pre-)dispute that has not been completed yet. - ... |
| AM-003-002 | The linked private money account can be any private money account held by the user at either the same intermediary which services the user's digital euro account or at another intermediary that is a participant in the digital euro scheme. |

348

349

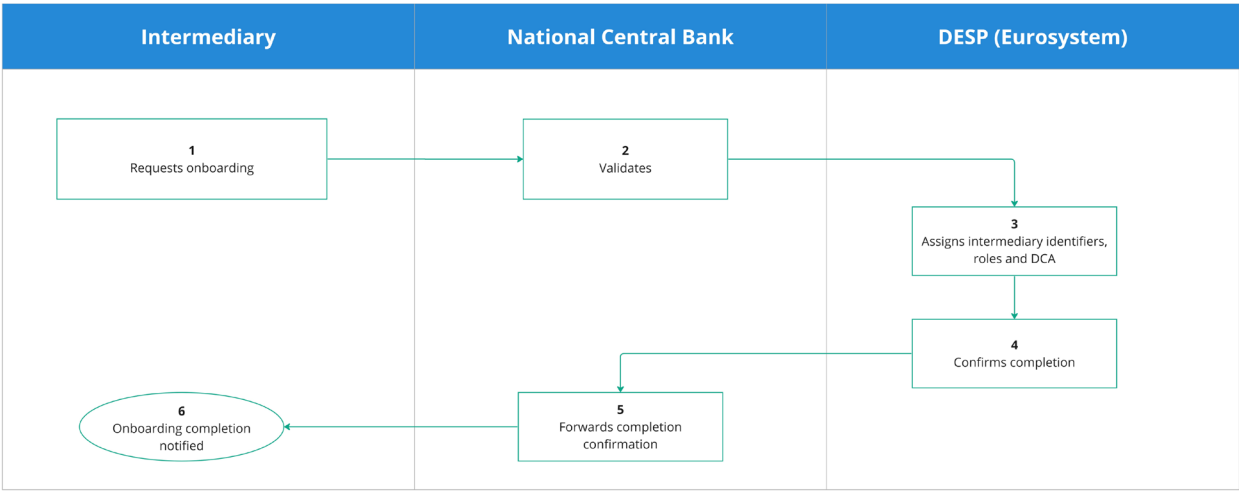
350 **3.3.1.5. Onboarding of an intermediary¹⁰**

351 The onboarding of an intermediary enables intermediaries to interact in the digital euro
 352 environment. The onboarding consists of activities including assigning intermediary identifiers
 353 and roles, and creating or granting access to dedicated cash account/(s) (DCA).

354 A high level process flow for the onboarding of an intermediary is shown in Figure below.

¹⁰ Business rules related to intermediary management are expected to be covered in specific documentation and are therefore not included in the rulebook.

Figure 3.3-5: High level process for the onboarding of an intermediary



Description of steps:

1. The intermediary requests its national central bank to be onboarded for digital euro services
2. The national central bank validates the intermediary's onboarding request, determines if the intermediary is eligible and if so, requests the DESP to register the intermediary
3. The DESP registers the intermediary (including the applicable roles, unique identifiers and the DCA to be used for funding and defunding)
4. The DESP confirms the registration to the national central bank
5. The national central bank confirms the onboarding to the intermediary
6. The intermediary is notified of the onboarding completion.

The following E2E flows detail this high-level flow further:

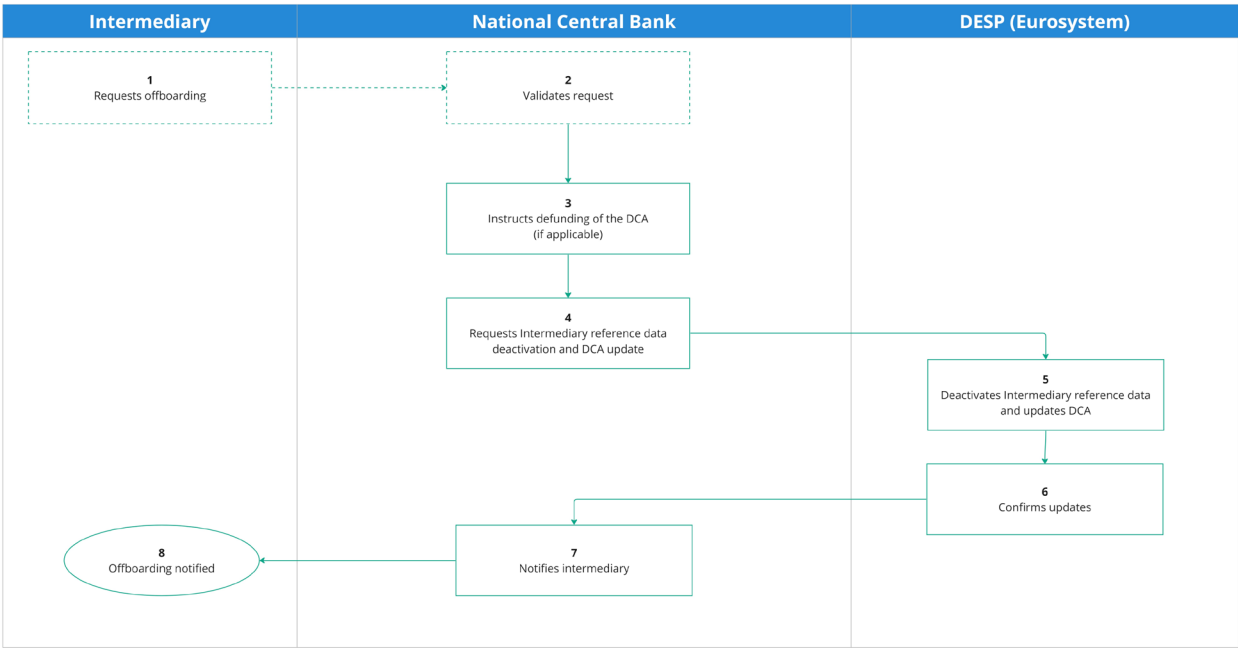
- IM – 01 intermediary onboarding (including creating an intermediary ID, assigning a DCA, optionally assigning a liquidity provider)

3.3.1.6. Offboarding of an intermediary

The offboarding of intermediaries is a procedure initiated when an intermediary will no longer participate in the digital euro environment with specific actions taken on-going actions related to

the intermediary, e.g. on-going transactions, disputes.. The National Central Bank (NCB) will instruct defunding of the DCA if there are available balances, then initiate intermediary reference data deletion/deactivation.

Figure 3.3-6: High level process flow for the offboarding of an intermediary



A high level process flow for the offboarding of an intermediary is included below.

Description of steps:

1. The intermediary requests its national central bank to be offboarded from the digital euro scheme. This step is optional. It would be skipped in case the national central bank takes the initiative to offboard the intermediary
2. The national central bank validates the intermediary's offboarding request. This step is optional. It would be skipped in case the national central bank takes the initiative to offboard the intermediary
3. If the intermediary has its own DCA and the DCA holds a balance, the national central bank instructs the defunding of the DCA

4. The national central bank requests the the DESP to deactivate the intermediary reference data and update the status of the intermediary's DCA (if applicable)
5. The DESP deactivates the intermediary reference data and updates the status of the intermediary's DCA (if applicable)
6. The DESP confirms the completion of the updates to the national central bank
7. The national central bank notifies the intermediary of the completion of the offboarding
8. The intermediary is informed about the completion of the offboarding.

Note: this flow is based on the assumption that the intermediary does not have digital euro users anymore.

The following E2E flows detail this high-level flow further:

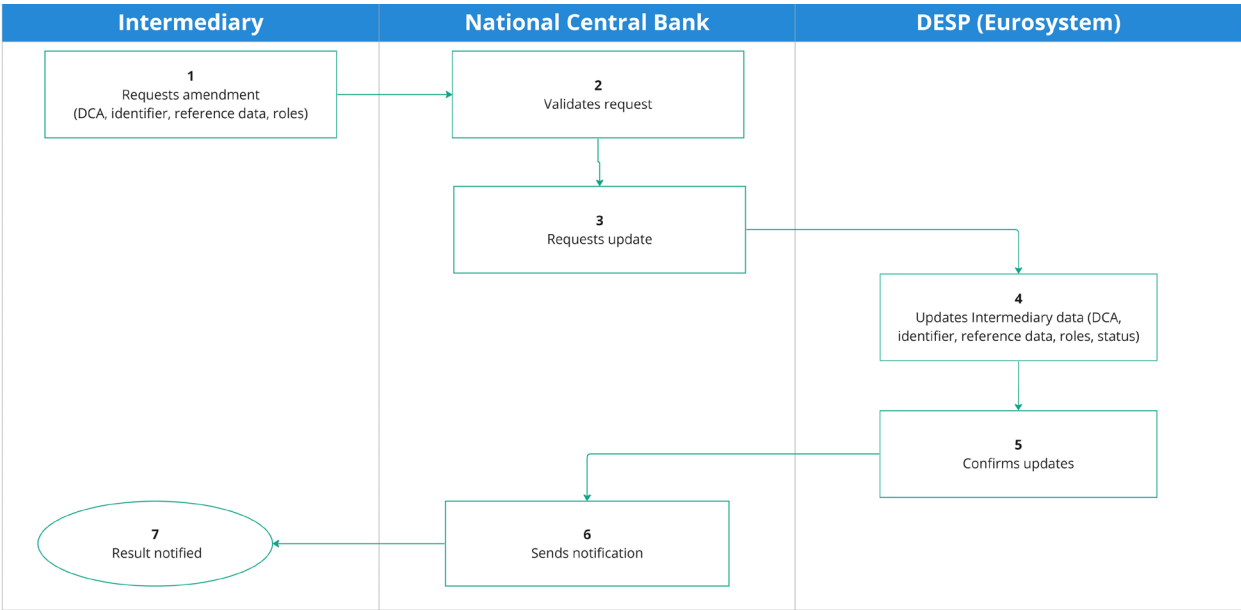
- IM – 02 intermediary offboarding

3.3.1.7. User lifecycle management processes for intermediaries

The lifecycle management processes for intermediaries consist of any changes that may be required including assigning identifiers, roles, recording reference data and managing their access to DCA. Intermediary management is performed by the NCB responsible for the intermediary.

A high level process flow for the lifecycle management of an intermediary is shown on Figure

Figure 3.3-7: User lifecycle management processes for intermediaries



Description of steps:

1. The intermediary requests its national central bank for an amendment (e.g. a change in DCA or roles)
2. The national central bank validates the intermediary's amendment request
3. The national central bank requests the DESP to update the intermediary's data
4. The DESP updates the intermediary's data
5. The DESP confirms the updates to the national central bank
6. The national central bank confirms the updates to the intermediary
7. The intermediary is notified of the completion of the amendments.

The following E2E flows detail this high-level flow further:

IM – 03 intermediary amendments (including creating an intermediary ID, assigning a DCA, optionally assigning a liquidity provider)

3.3.2. Liquidity management

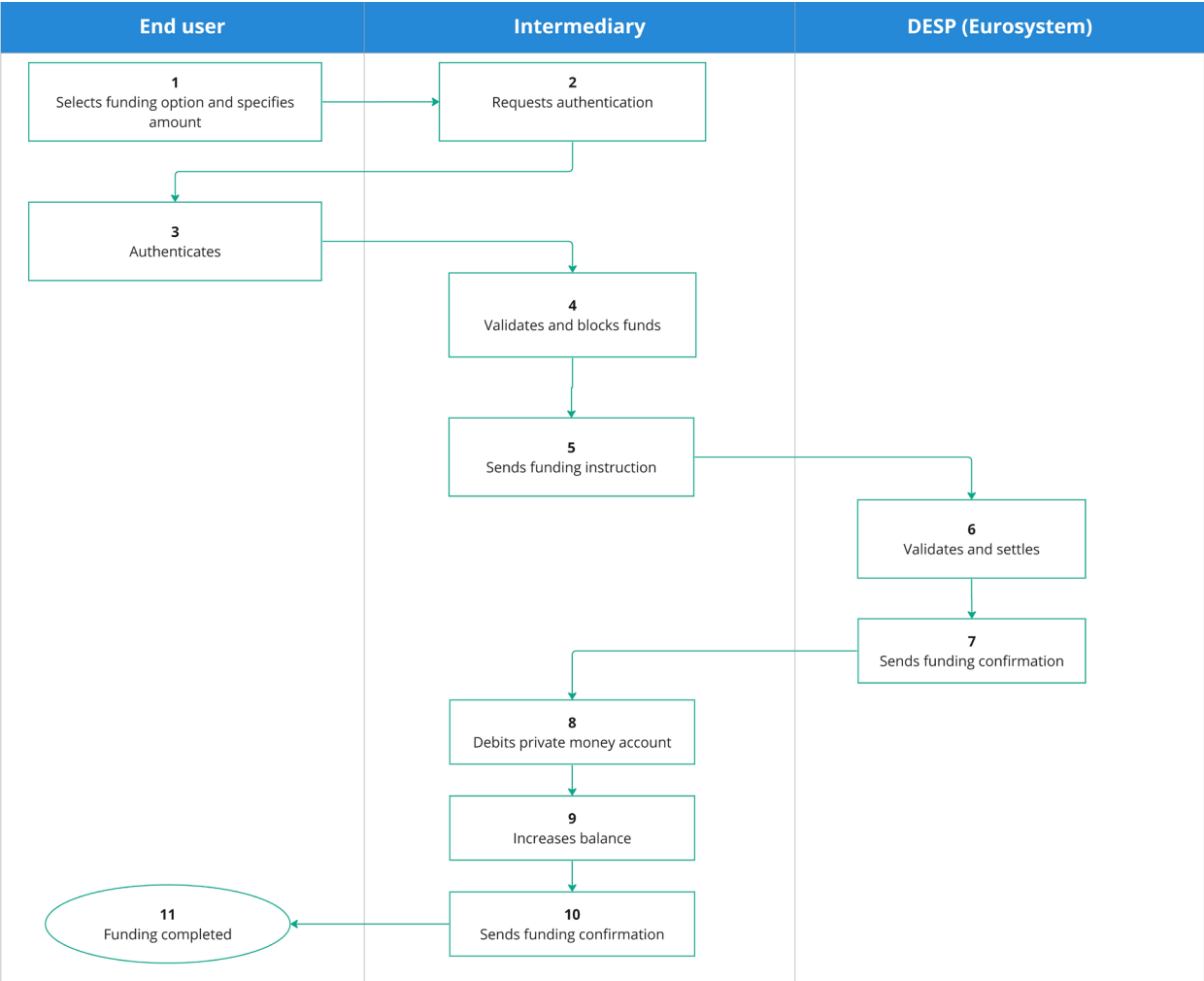
3.3.2.1. Funding

Funding can be done from a private money account or cash (e.g., at ATMs or intermediary branches). Intermediaries may offer manual and scheduled funding functionalities. An individual has the option to set a default balance of digital euro holdings (below a potential holding limit set by the Eurosystem), which gets automatically refilled if the set default balance is breached after an outgoing transaction.

A high level process flow for a funding operation is shown in Figure below. In the case of funding by cash, users would either access an ATM and insert notes or go to a branch of their intermediary and hand the cash to an employee (or be assisted in the use of the ATM). The broad outlines of the process remain the same, but inserting/handing over the cash would replace the debit of the private money account in the flow shown here.

433

Figure 3.3-8: High level process flow for a funding operation



434

435 Description of steps:

436

1. The user selects the funding option (in this case manual funding, but automated funding, based on a periodic fixed amount or a threshold based funding is also possible) and specifies the amount

437

438

439

2. The intermediary prompts the user for authentication

440

3. The user authenticates

441

4. The intermediary validates the funding request and blocks the required funds on the user's private money account or receives cash from the end user

442

443

5. The intermediary sends the funding instruction to the DESP

6. The DESP validates and settles the funding instruction by debiting the intermediary's DCA and issuing digital euros for the same amount
7. The DESP confirms the completion of the funding operation to the intermediary
8. In case of funding via private money, the intermediary debits the user's private money account for the funding amount
9. The intermediary increases the balance of the user's digital euro account with the funding amount
10. The intermediary confirms the completion of the funding operation to the user
11. The user is informed about the completion of the funding request.

The following E2E flows detail this high-level flow further:

- LM – 01 Manual funding from private money account – same intermediary
- LM – 02 Manual funding from private money account different intermediary (triggered by digital euro intermediary)
- LM – 05 Automated funding from private money account same intermediary
- LM – 06 Scheduled funding from private money account different intermediary (triggered by digital euro payee/payer intermediary)
- LM – 17.1 Manual funding of offline holdings from private money account

3.3.2.2. Reverse waterfall

An end user may (voluntarily) allow automatic transfers of money from the private money account if digital euro holdings are not sufficient to complete the digital euro payment. The reverse waterfall mechanism is mandatory for businesses to ensure zero holding limits when paying in digital euro ie. Refunds. This is only valid for online transactions. In case the end user does not have enough digital euro, the reverse waterfall mechanism will be activated. If there are not sufficient funds, the payments won't be processed. The settlement of reverse waterfall is fully integrated into the settlement of the transactions itself.

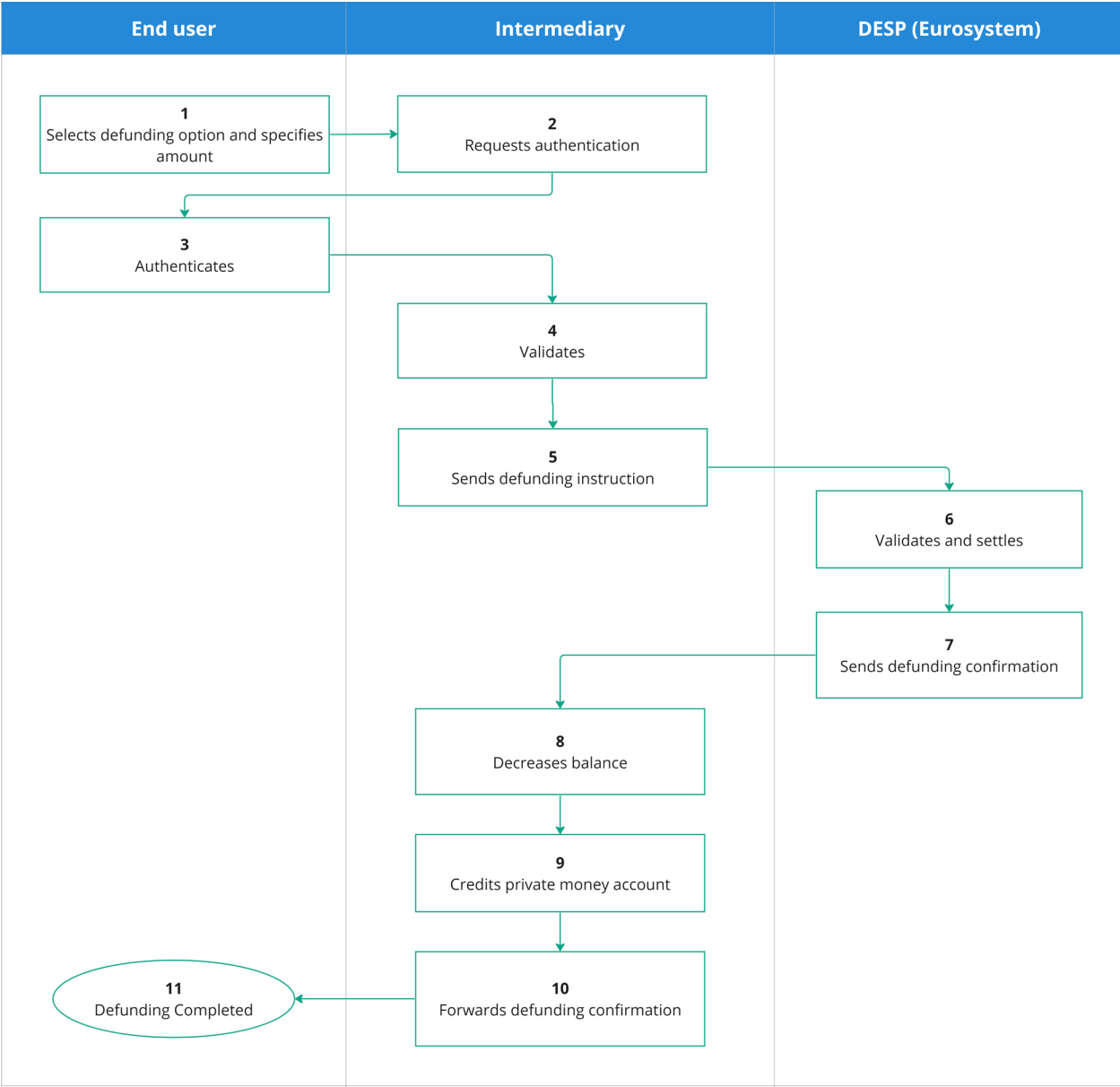
3.3.2.3. Defunding

Defunding can be done to a private money account or cash (e.g., at ATMs or intermediary branches). Intermediaries may offer manual and scheduled defunding functionalities. Scheduled functionalities will be activated at the individual's choice in case a linked liquidity source (like a private money account) exists and customised so that they can keep their digital euro holdings within their preferred range over time (in line with holding limits set by the Eurosystem).

A high level process flow for a defunding operation is included in Figure 3.3-9 below. In the case of defunding to cash, users would either access an ATM and withdraw notes or go to a branch of their intermediary and receive the cash from an employee (or be assisted in the use of the ATM). The broad outlines of the process remain the same, but receiving the cash would replace the credit of the private money account in the flow shown here.

482

Figure 3.3-9 High level process flow for a defunding operation



483

484 Description of steps:

- 485 1. The user selects the defunding option (in this case manual defunding, but automated
- 486 defunding, based on a periodic fixed amount or a threshold based defunding is also
- 487 possible) and specifies the amount
- 488 2. The intermediary prompts the user for authentication
- 489 3. The user authenticates

4. The intermediary validates the defunding request and checks if the balance on the digital euro account is sufficient
5. The intermediary sends the defunding instruction to the DESP
6. The DESP validates and settles the defunding instruction by redeeming the digital euros and crediting the intermediary's DCA for the same amount
7. The DESP confirms the completion of the defunding operation to the intermediary
8. The intermediary decreases the balance of the user's digital euro account with the funding amount
9. The intermediary credits the user's private money account for the defunding amount or provides cash to the end user for the defunding amount
10. The intermediary confirms the completion of the defunding operation to the user
11. The user is informed about the completion of the defunding request.

The following E2E flows detail this high-level flow further:

- LM – 03 Manual defunding to private money account same intermediary
- LM – 04 Manual defunding to private money account different intermediary (triggered by digital euro intermediary)
- LM – 07 Scheduled defunding to private money account same intermediary
- LM – 08 Scheduled defunding to private money account different intermediary (triggered by digital euro payer/payee intermediary)
- LM – 18.1 Offline manual defunding - private money
- LM – 24 Defunding

3.3.2.4. Waterfall

An individual user may allow automatic transfers of money to the private money account if digital euro holding limits are reached (i.e waterfall functionality). Moreover, an individual has also the option to customise a lower holding cap than defined by the Eurosystem holding limit. The activation of the waterfall functionality is mandatory for businesses to ensure zero holding limits when accepting digital euro payments. This is only valid for online transactions. The

settlement of waterfall is fully integrated into the settlement of the transactions itself. In exceptional circumstances an additional waterfall step after settlement in case of incoming payment to individual end user is required to handle the following scenario:

- Incoming 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 transaction 2 is received. 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 post settlement is performed.

3.3.2.5. Liquidity management business rules

| Id | Business rule |
|-------------------|---|
| LM-001-001 | The intermediary must offer users the possibility to exchange offline digital euros for online digital euros or vice versa. This requires the intermediary to request defunding first, followed by a funding request. |
| LM-001-002 | The intermediary must ensure that the sum of the balance of the digital euro account and the funding amount does not exceed the holding limit. |
| LM-001-003 | If the user has set up threshold-based funding and the user's digital euro balance drops below the defined threshold, the intermediary must check if sufficient balance is available on the user's private money account and if so, initiate funding. |
| LM-001-004 | If the user has set up threshold-based defunding and the user's digital euro balance exceeds the defined threshold, the intermediary must initiate defunding. |
| LM-001-005 | If the user has set up periodic funding and the specified funding amount is not available on the linked private money account, the funding process must be aborted and the intermediary must inform the user of the exception. |

| | |
|-------------------|---|
| LM-001-006 | If the user has set up periodic defunding and the specified funding amount is not available on the digital euro account, the funding process must be aborted and the intermediary must inform the user of the exception. |
| LM-001-007 | If the user has linked a private money account to the digital euro account, this linked account should be presented by the intermediary as the default source account for manual funding and the default destination account for manual defunding. However, the user should be offered the possibility to select another private money account instead of the linked account. |
| LM-001-008 | The payer intermediary must specify the digital euro holdings to be defunded (redeemed). |
| LM-001-009 | The DESP must verify that the digital euro holdings specified by the intermediary to be defunded exist and are available (not blocked/reserved). |

3.3.3. Transaction management

Transaction management outlines the methods of paying and receiving payments in digital euro at any time and everywhere¹¹ using different devices and interfaces (physical card, mobile device equipped with a mobile app, or wearable) supporting different data exchange technologies (chip, near field communication (NFC), quick response code (QR-code) and possibly an alias) across the prioritised use cases:

- Payments from person-to-person (P2P), available online and offline;
- Payments at E-commerce stores, available online (including consecutive and recurring payments, and also includes payments to governments initiated on websites hosted by governments); and

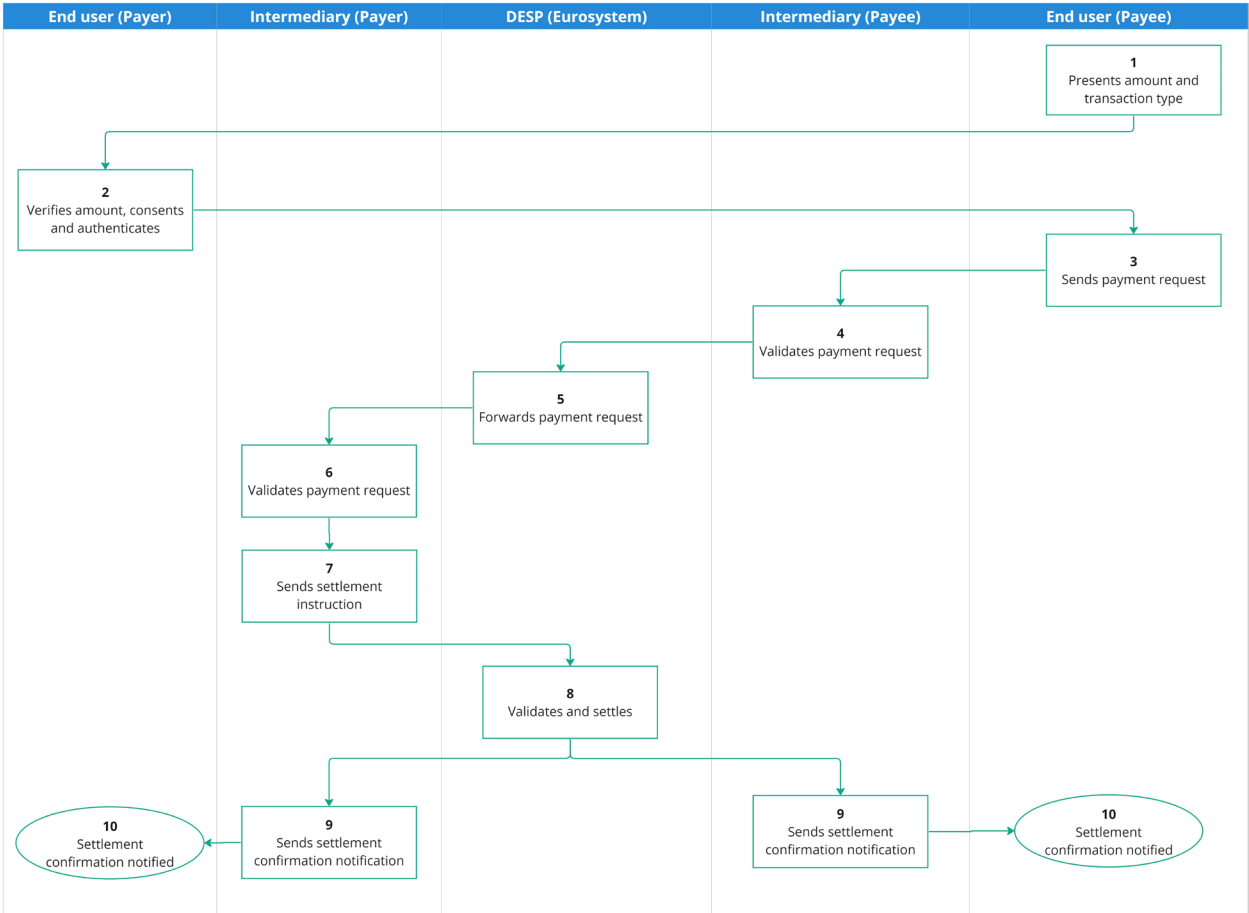
¹¹ As per design decisions, POS, P2P, e-commerce and G2X/X2G are the use cases prioritized for the first release of the digital euro. Other use cases might be included as part of potential subsequent releases such as Consumer-to-Business (C2B), Business-to-Consumer (B2C) and Business-to-Business (B2B) use cases

- Payments at the point-of-sales (POS) (also includes payments to governments at government agencies), available online and offline.

Digital euro end users will also be able to use a digital euro in full or partial payment refunds, and to dispute an (un-)successful payment.

A high level process flow of a payee-initiated transaction is shown on Figure below :

Figure 3.3-10: High level process flow of a payee-initiated transaction



Description of steps:

1. The payee presents the amount to be paid to the payer
2. The payer verifies the amount, consents to the payment and authenticates
3. The payee submits the payment request (including the consent details) to its intermediary

4. The payee's intermediary validates the payment request and sends it to the DESP
5. The DESP forwards the payment request to the payer's intermediary
6. The payer's intermediary validates the payment request
7. The payer's intermediary sends the settlement instruction (including funding instruction if reverse waterfall applies and/or defunding instruction if waterfall applies) to the DESP
8. The DESP validates the settlement instruction, settles the transaction and confirms the settlement to both the payer's intermediary and the payee's intermediary
9. The intermediary sends the settlement confirmation to the end user
10. The end user is notified of the completion of the settlement of the transaction.

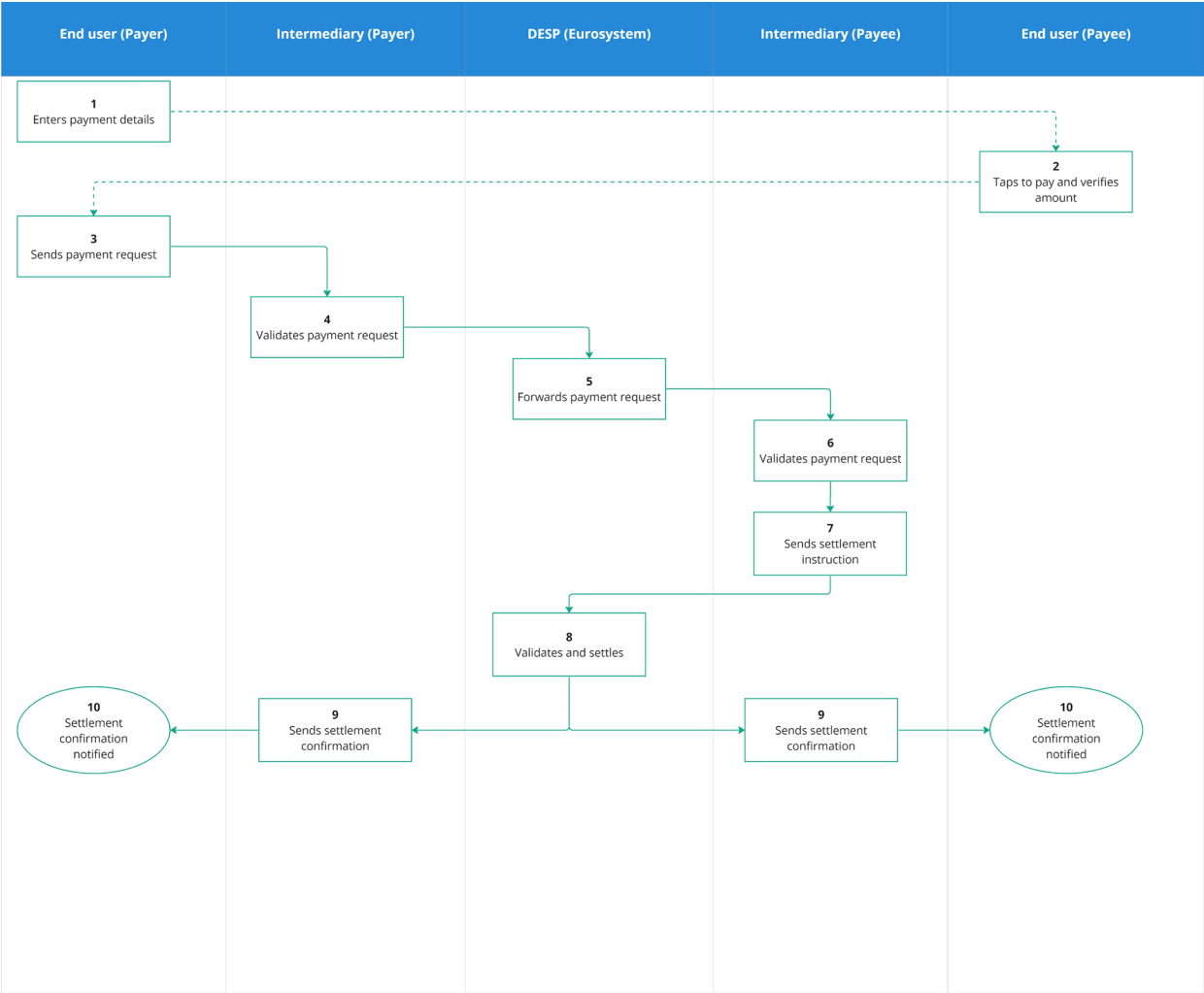
The following E2E flows detail this high-level flow further:

- TM - 03 POS payment with NFC (online) Centralised Tokenisation
- TM – 16 P2P payment with NFC (online), payee-initiated
- TM - 48 POS payment with NFC (online) – different intermediaries

A high level process flow of a payer-initiated transaction is shown in Figure below:

566

Figure 3.3-11 High level process flow of a payer-initiated transaction



567

568 Description of steps:

569

1. The payer enters the payment details

570

2. The payee verifies the amount, consents and taps to accept the payment (optional, only in case of NFC)

571

572

3. The payer submits the payment request to its intermediary

573

4. The payer's intermediary validates the payment request and sends it to the DESP

574

5. The DESP forwards the payment request to the payee's intermediary

575

6. The payee's intermediary validates the payment request

7. The payee's intermediary sends the settlement instruction (including funding instruction if reverse waterfall applies and/or defunding instruction if waterfall applies) to the DESP
8. The DESP validates the settlement instruction, settles the transaction and confirms the settlement to both the payer's intermediary and the payee's intermediary
9. The intermediary sends the settlement confirmation to the end user
10. The end user is notified of the completion of the settlement of the transaction.

The following E2E flows detail this high-level flow further¹²:

- TM – 15 P2P payment with NFC (online), payer-initiated
- TM – 08 E-Com (incl. C2G) payment with alias/proxy
- TM – 09 M-Commerce payment (in-app)
- TM – 18 P2P payment with Alias/Proxy
- TM – 53 P2P payment request with Alias and/or EU identifier (Payee initiated)
- TM – 01 POS payment with Payee-generated QR Code
- TM – 07 E-Com (incl. C2G) payment with QR Code
- TM – 10 P2P payment with Payee-generated QR code
- TM – 19 P2P payment with payment request by link
- TM – 51 E-Com (incl. C2G) payment with pay by link

3.3.3.1. Transaction management business rules

| Id | Business rule |
|----|---------------|
|----|---------------|

¹² Please note that initial steps may differ or additional steps may be involved depending on the specific characteristics of the form factor. These are described in detail in the end-to-end flows.

| | |
|-------------------|---|
| TM-000-001 | <p>The intermediary ensures the authenticity of the instruction received from its user, validates the correctness of its content, and (if valid and correct) completes and forwards it immediately to the DESP.</p> <p>If the intermediary cannot accept the request, it informs the user immediately and it provides the reason for rejecting the request.</p> |
| TM-000-002 | <p>Upon receipt of a payment request from the DESP, the intermediary verifies if it can process the payment and executes various validations and (if valid) submits the settlement instruction to the DESP.</p> <p>If the intermediary cannot accept the request, it informs the DESP immediately and it provides the reason for rejecting the request.</p> |
| TM-000-003 | <p>Intermediary must check all digital euro transactions against sanctions/embargo lists. If parties involved in the transactions are on the sanctions list, the transaction must be rejected.</p> |
| TM-000-004 | <p>Upon receipt of the settlement confirmation from the DESP, the intermediary immediately updates the user's digital euro balance and notifies the user in accordance with the user's notification preferences.</p> |
| TM-000-005 | <p>The payer intermediary must verify that the payer either</p> <ol style="list-style-type: none"> 1) holds sufficient digital euros to complete the transaction, or 2) has a linked private money account which holds sufficient balance to compensate for the insufficient digital euro holdings and has activated the reverse waterfall option. <p>The payer's liquidity manage settings determine if only the available balance or the balance plus overdraft facilities can be used.</p> |
| TM-000-006 | <p>If the payee is an individual user, the payee intermediary must verify that the transaction either</p> <ol style="list-style-type: none"> 1) would not push the payee's digital euro balance over the holding limit, or 2) would push the payee's digital euro balance over the holding limit but the payee has a linked private money account set up and the waterfall |

| | |
|-------------------|---|
| | option activated. In that case the payee's intermediary must trigger the waterfall mechanism. |
| TM-000-007 | If the payee is an individual user and the payee does not have a linked private money account, the payee intermediary must reject any further incoming transaction while an incoming transaction is still being processed. |
| TM-000-008 | If the payee is a business user, the payee intermediary must trigger the waterfall mechanism upon receipt of each incoming online digital euro payment. |
| TM-000-009 | If waterfall is required, the payee intermediary must instruct the defunding of the amount above the holding limit (current balance + transaction amount - holding limit) |
| TM-000-010 | Intermediaries must credit the user's private money account immediately after receiving the confirmation form DESP that the defunding (including waterfall) instruction has been settled. |
| TM-000-011 | If reverse waterfall is required, the payer intermediary must instruct the funding of the transaction amount minus the payer's current digital euro balance. |
| TM-000-012 | If a transaction including reverse waterfall fails, the payer's intermediary must reverse the debit or reservation made on the user's private money account |
| TM-000-013 | After having processed an outgoing transaction/made a debit to the user's digital euro account, the intermediary must check if the available balance on the user's digital euro account has dropped below the lower threshold value specified by the user (if applicable). If it has, the intermediary must |

| | |
|-------------------|---|
| | initiate the funding of the account as per the user's liquidity management settings. |
| TM-000-014 | After having processed an incoming transaction/made a credit to the user's digital euro account, the intermediary must check if the available balance on the user's digital euro account exceeds the upper threshold value specified by the user (if applicable). If it has, the intermediary must initiate the funding of the account as per the user's liquidity management settings. |
| TM-000-015 | The payer intermediary must specify the digital euro holdings to be transferred and (if applicable, in case reverse waterfall applies) the amount to be debited from the DCA associated with the intermediary. |
| TM-000-016 | If an intermediary receives a rejection notification from DESP in response to a settlement instruction, the intermediary must inform it's user of the rejection of the transaction. |
| TM-000-017 | An intermediary submitting a settlement instruction to the DESP must ensure that the sum of debit amounts in the settlement instruction equals the sum of credit amounts. |
| TM-000-018 | An intermediary submitting a settlement instruction to the DESP must ensure amounts in the settlement instruction have two decimals. |
| TM-000-019 | An intermediary submitting a settlement instruction to the DESP must ensure that at least one debit or credit amount in the settlement instruction belongs to an end user. |
| TM-000-020 | If a reservation including reverse waterfall fails or expires, the payer's intermediary must reverse the debit or reservation made on the user's private money account. |
| TM-000-021 | If a reservation includes reverse waterfall and the final amount is lower than the reservation amount, the payer's intermediary must adjust the |

| | |
|-------------------|--|
| | amount of the debit made on the user's private money account for the difference. |
| TM-000-022 | When reserved holdings are released by DESP due to a (partial) cancellation, by settlement of the final amount or when the expiry date and time are reached, the payer intermediary notifies the payer of the release of the digital euro holdings. |
| TM-000-023 | When reserved holdings are released by DESP due to a (partial) cancellation, by settlement of the final amount or when the expiry date and time are reached, the payee intermediary notifies the payee of the release of the digital euro holdings. |
| TM-000-024 | A reservation can be used either as a whole or in part, including by means of multiple settlements. |
| TM-000-025 | An existing reservation can be modified (increase or decrease the amount, change of expiry date). A change of an existing reservation requires SCA of the payer. |
| TM-000-026 | To increase the reservation amount, the payer's intermediary must provide the id's of the additional holdings to be blocked. |
| TM-000-027 | To decrease the reservation amount, the payer's intermediary must provide the id's of the holdings to be released. |
| TM-000-028 | To change the expiry date of a reservation the payer's intermediary must provide the id's of the holdings to be updated. |
| TM-000-029 | The payer's intermediary must accept for processing all payment requests received from either DESP or the payee that conform to the scheme specifications, unless the identified payer account is closed, invalid or being monitored for suspected fraudulent or other illegal activity. |
| TM-000-030 | The payee's intermediary must accept for processing all payment requests received from either DESP or the payee that conform to the |

| | |
|-------------------|--|
| | scheme specifications, unless the identified payee account is closed, invalid or being monitored for suspected fraudulent or other illegal activity. |
| TM-000-031 | The user's intermediary must make the status/result of a transaction known to the end user immediately (if and as required by customer-defined notification preferences). |
| TM-000-032 | Intermediaries must give business users the possibility to specify in a payment request the private money account to be used for for funding or defunding instead of the linked account. |
| TM-000-033 | The transaction amount must not exceed the amount specified in Annex A.6. |
| TM-000-034 | Reservations/pre-authorisations are possible for an amount up to the holding limit. |
| TM-000-035 | Payer intermediaries are obliged to request fraud scoring from the DESP fraud service in real time for each payment request they receive. After receiving the fraud score from the DESP fraud service, the intermediary decides whether it accepts the payment request or not. |
| TM-000-036 | Intermediaries are obliged to report fraud cases to the DESP as further detailed in the DESP legal documentation for standards fraud cases. Exceptional fraud cases are to be reported to the Scheme Governing Authority. |
| TM-000-037 | Intermediaries receive periodic fraud related reports from DESP and are obliged to review (and if needed, adjust) their fraud controls based on these reports. |
| TM-000-038 | A transaction cannot be cancelled once a request has been sent to the DESP. |
| TM-000-039 | A reservation/pre-authorisation can be cancelled by the business user or the business users intermediary from the moment they have received |

| | |
|-------------------|--|
| | confirmation that the digital euro holdings have been blocked in the ledger until the expiry date and time of the reservation. |
| TM-001-001 | Payment requests in the form of pay by link must be tokenised by the payee's intermediary through the DESP tokenisation service. |
| TM-001-002 | In case of a payment requests in the form of pay by link, the payee's intermediary must provide the payer with a possibility to identify/select the payer's intermediary. |
| TM-004-001 | Intermediaries must allow their users to identify the counterparty in the transaction by an alias. |
| TM-004-002 | When the intermediary receives an instruction containing an alias, the intermediary must request resolution of the alias from the DESP alias look-up service. |
| TM-004-003 | When the payer sets up a standing order using an alias to identify the payee, the intermediary must request resolution of the alias from the DESP alias look-up service. |
| TM-004-004 | If a merchant has received an alias as an identification of the payer, the merchant may store the alias as well as the associated DEAN for future use (consecutive & recurring payments). |
| TM-005-001 | For the purpose of initiating recurring payments, the merchant is obliged to store the payers details in tokenised form. The merchant must request tokenisation of these details via it's intermediary. |
| TM-005-002 | The payee's intermediary must request detokenisation of the payer's details from the DESP before submitting the payment request to the DESP. The payee's intermediary is not allowed to share the untokenised payer details with the merchant. |

| | |
|-------------------|---|
| TM-005-003 | <p>For the purpose of initiating recurring payments, the merchant is obliged to obtain consent from the payer regarding:</p> <ul style="list-style-type: none"> - the recurring payment amount (fixed or variable, a maximum amount if variable) - the recurring payment frequency - expiry date/end date of the recurring payments (optional) - whether or not the payer's consent is required for each subsequent transaction, the payee sends the request including the recurring payment parameters to the payer's intermediary (via the payee's intermediary and DESP) and the payer's intermediary presents the request to the payer and obtains consent through SCA. |
| TM-005-004 | <p>After the payer has authenticated and confirmed the recurring payments parameters, the payer's intermediary must store these for the purpose of validating subsequent payments.</p> |
| TM-005-005 | <p>When receiving a recurring payment request from a payee's intermediary (via DESP) for one of its users, the intermediary must validate the recurring payment against the (maximum) amount and frequency authorised by the payer. In addition, the intermediary must check if the payer's consent must be obtained for the payment. If so, the intermediary must notify the payer and request the payer to consent to the payment. If not, the intermediary must accept and process the payment request.</p> |
| TM-005-006 | <p>A payer intermediary must allow the payer to terminate a recurring payment. Termination of a recurring payment is subject to SCA. The intermediary must notify the payee (via the DESP and the payee's intermediary) of the termination. Any subsequent payments received under the mandate of the terminated recurring payment, must be rejected.</p> |

| | |
|-------------------|--|
| TM-005-007 | A payer intermediary must allow the payer to modify the parameters of a recurring payment. A modification of the parameters of a recurring payment is subject to SCA. The intermediary must notify the payee (via the DESP and the payee's intermediary) of the change. |
| TM-005-008 | A payer intermediary must allow the payer to terminate a recurring payment. The intermediary must notify the payee (via the DESP and the payee's intermediary) of the termination. Any subsequent payments received under the mandate of the terminated recurring payment, must be rejected. |
| TM-005-009 | A payer intermediary must allow the payer to request modification of the parameters of the recurring payment. The change in these parameters is subject to the payer's consent. |
| TM-005-010 | After the payer has authenticated and confirmed the modified recurring payments parameters, the payer's intermediary must store these for the purpose of validating subsequent payments. |
| TM-005-011 | Intermediaries must allow individual users to set up recurring future payments with a fixed amount and fixed frequency (standing orders). |
| TM-006-001 | Offline transactions are possible up to the holding limit assigned to the offline wallet or a lower single transaction limit set by the Eurosystem. |
| TM-006-002 | The number of offline transactions that a device is allowed to initiate before being required to go online for reconciliation is limited to the maximum set by the Eurosystem as specified in Annex A.6. |
| TM-006-003 | The number of offline transactions that a device is allowed to receive before being required to go online for reconciliation is limited to the maximum set by the Eurosystem as specified in Annex A.6. |
| TM-006-004 | An offline digital euro device cannot initiate transactions after the maximum number of days as specified in Annex A.6 have passed since the last time it was reconciled online. |

| | |
|-------------------|--|
| TM-006-005 | An offline digital euro device cannot receive transactions after the maximum number of days as specified in Annex A.6 have passed since the last time it was reconciled online. |
| TM-006-006 | Offline digital euros received by business users must be defunded as soon as technically feasible (as soon as the offline device is able to go online). However, defunding should happen before the maximum period specified in Annex A.6. Any further payments must be rejected if this maximum period is exceeded. |

596 3.3.3.2. General and other business rules

597

| Id | Business rule |
|-------------------|--|
| GE-001-001 | The currency in all transactions and instructions must be EUR. |
| GE-001-002 | Validations (including those by ATMs, POS terminals, other devices and software solutions) must be performed as per the implementation specifications. |
| GE-001-003 | Reject messages should be clear and easy to understand in the language as set in the language preferences offered by the intermediary to the end user. |
| GE-002-001 | At no point in time shall the total sum of digital euro held by an individual user exceed the individual user holding limit. |
| GE-002-002 | The holding limit for accounts held by business users is €0,- any digital euros received by business users must be defunded as soon as technically possible. |
| GE-002-003 | The user's intermediary is responsible for enforcing the user's holding limit. |
| GE-002-004 | An online account owned by an individual user has a holding limit assigned to it. This holding limit can never exceed the overall holding limit set by the scheme. |

| | |
|-------------------|--|
| GE-002-005 | An offline wallet owned by an individual user has a holding limit assigned to it. This holding limit can never exceed the overall holding limit set by the scheme. |
| GE-003-001 | An individual user can have only one offline digital euro wallet. |
| GE-003-002 | An business user can have an unlimited number of offline digital euro wallets. |
| GE-004-001 | An individual user can have only one online digital euro account. |
| GE-004-002 | An business user can have an unlimited number of online digital euro account. |

598

| Id | Business rule |
|-------------------|--|
| OT-001-001 | Intermediaries must allow their users to submit a pre-dispute regarding a previous transaction. |
| OT-001-002 | Both the intermediary and the DESP must check that the transaction to which the pre-dispute refers has been processed no more than x days/months before the submission of the a pre-dispute. |
| OT-001-003 | The user must provide a reason for the pre-dispute. |
| OT-001-004 | The receiving intermediary must respond to a received pre-dispute within x days. |
| OT-001-005 | The receiving intermediary may either respond to the pre-dispute itself (if it has sufficient information to do so) or request it's user for the required information and send the response when that information has been received. |
| OT-001-006 | If the outcome of the pre-dispute is not satisfactory to the submitting user, the intermediary must allow the user to submit a dispute. |

| | |
|-------------------|---|
| OT-001-007 | Intermediaries shall not open a dispute without a preceding pre-dispute which has either been completed or for which the response deadline has been exceeded without a response from the other intermediary. |
| OT-001-008 | The receiving intermediary must respond to a received dispute within x days. |
| OT-001-009 | The intermediary must verify the correctness of the transaction information provided by its user |
| OT-002-001 | The user's intermediary must inform the user of the current online digital euro balance at the user's request |
| OT-002-002 | Intermediaries can in exceptional circumstances query the holdings of all their users in the DESP. |
| OT-002-003 | For privacy reasons, intermediaries are not allowed to query the holdings of a single user in the DESP. |
| OT-002-004 | An intermediary must provide its users an overview of online digital euro transactions initiated or received up to at least 13 months in the past. |
| OT-003-001 | If a merchant initiates a refund at the point of sale, the merchant can either use the payer token which was used for the original transaction, request the payer to share the token stored on the payer device or request the payer to share the payer details by scanning a QR code. In all cases, the merchant must include the tokenised payer data in the refund request |
| OT-003-002 | If an e-commerce or m-commerce merchant initiates a refund, the merchant can either use the payer details or payer token which was used for the original transaction or request the payer to share the payer details by scanning a QR code. |
| OT-003-003 | The payee's intermediary is not allowed to request detokenisation of the payer token received as part of a refund request. Only the payer intermediary is allowed to request detokenisation. |

| | |
|-------------------|--|
| OT-003-004 | When the payer's intermediary receives a refund request, it must request the DESP tokenisation service to detokenise the payer token prior to validation or acceptance of the refund request. |
| OT-003-005 | When the payer's intermediary receives a refund request, it must verify that the refund either 1) would not push the user's digital euro balance over the holding limit, or 2) would push the user's digital euro balance over the holding limit but the user has a linked private money account set up and the waterfall option activated. In that case the user's intermediary must trigger the waterfall mechanism. |

3.3.3.3. Notification events

| Event | Outcome | DESP to Payer Intermediary | DESP to Payee Intermediary | Payer intermediary to Payer | Payee intermediary to Payee | Intermediary to user | DESP to DCA holder |
|--|---------|--|--|--|--|----------------------|--------------------|
| Payment request validation | Success | None | None | None | None | n.a. | n.a. |
| | Failure | Mandatory if payer initiated, otherwise none | Mandatory if payee initiated, otherwise none | Mandatory if payer initiated, otherwise none | Mandatory if payee initiated, otherwise none | n.a. | n.a. |
| Standing order | Success | None | None | None | None | n.a. | n.a. |
| | Failure | n.a. | n.a. | Mandatory | n.a. | n.a. | |
| Settlement instruction validation | Success | None | None | None | None | n.a. | n.a. |
| | Failure | Mandatory | Mandatory | Mandatory if payer initiated, otherwise none | Mandatory if payee initiated, otherwise none | n.a. | n.a. |
| Settlement verification | Success | None | None | None | None | n.a. | n.a. |

| | | | | | | | |
|---|---------|-----------|-----------|--|--|-----------|------|
| | Failure | Mandatory | Mandatory | Mandatory if payer initiated, otherwise none | Mandatory if payee initiated, otherwise none | n.a. | n.a. |
| Settlement recording | Success | Mandatory | Mandatory | None | None | n.a. | n.a. |
| | Failure | Mandatory | Mandatory | Mandatory if payer initiated, otherwise none | Mandatory if payee initiated, otherwise none | n.a. | n.a. |
| Update of the user digital euro balance | n.a. | n.a. | n.a. | Mandatory | Mandatory | n.a. | n.a. |
| Reservation expiry | n.a. | Mandatory | Mandatory | Mandatory | Mandatory | n.a. | n.a. |
| Reservation release | n.a. | Mandatory | Mandatory | Mandatory | Mandatory | n.a. | n.a. |
| Max. number of days offline exceeded (initiate) | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory | |
| Max. number of days offline exceeded (receive) | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory | |
| Max. number of received offline transactions exceeded | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory | |
| Max. number of initiated offline transactions exceeded | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory | |

| | | | | | | | |
|------------------------------------|---------|-----------|-----------|-----------|-----------|------|-----------|
| (Pre)dispute update | all | Mandatory | Mandatory | Mandatory | Mandatory | n.a. | n.a. |
| Inbound Liquidity Transfer | Success | n.a. | n.a. | n.a. | n.a. | n.a. | Optional |
| | Failure | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory |
| Outbound Liquidity Transfer | Success | n.a. | n.a. | n.a. | n.a. | n.a. | Optional |
| | Failure | n.a. | n.a. | n.a. | n.a. | n.a. | Mandatory |

601

602 **3.4. End-to-end flows**

603 The end-to-end flows are included in the digital euro scheme Rulebook – Annex A.2 E2E flows
604 document.

605 **3.5. Illustrative user journeys**

606 The illustrative user journeys are included in the digital euro scheme Rulebook – Annex A.1
607 Illustrative user journeys document.

608 **3.6. Core requirements, service endpoints and list of attributes (incl. interplay with**
609 **standardisation initiatives)**

610 Please see workstream F1 reports and associated XLS file listing potential standard to be
611 reused for each interaction in the E2E flows. This work will be the foundation for writing this
612 section in the next iterations of the Rulebook.

613 **3.7. Identification**

614 When requesting a Digital Euro Account Number (DEAN) from the Digital Euro Service Platform
615 (DESP) in order to create a new digital euro account, intermediaries are expected to provide a
616 pseudonymised digital euro end-user unique identifier mirroring the attributes of Personal
617 Identifiers (PID) foreseen by the eIDAS2 regulation.

618 Digital Euro Account Numbers (DEANs) to follow a “EU-IBAN” structure by to be used by
619 intermediaries subject to definition of DESP user requirements. Users can also use an “alias”,
620 mapped to the corresponding DEAN, for identifying themselves and using digital euro services.

Such “alias” could take different forms, such as a phone number and/or an email address. When using a card as a form factor, the personal account number (PAN) written on the card (and associated to a DEAN) can also be used to identify users.

3.7.1. Identification and authentication of components

Identification and authentication of components is necessary to ensure the security and integrity of the ecosystem. Only components that have been registered with the scheme shall be permitted to operate within the envisaged digital euro transaction flows. This shall be facilitated by outlining (as per the figure below) the interactions between various components and

| Relevant Component | Interaction with component (Standards & Authentication requirements) | | | | | | | | |
|------------------------------------|--|------------------------------------|--|---|--|---|---|--|---|
| | ATM | Physical POS or virtual POI (eCom) | mDevice (e.g. Smartphone, Tablet) | | Merchant, ATM operator | Intermediary API (payer) | Intermediary API (payee or ATM) | mApp ECB | mApp Intermediary |
| ATM | | | ID: DEAN Authentication: CDCVM (fingerprint/face recognition/device passphrase) | ID: Terminal ID Authentication: ATM operator space, keys | | | ID: DEAN, Terminal ID Authentication: cryptogram | ID: DEAN, Terminal ID Authentication: cryptogram | ID: DEAN Authentication: encrypted PIN, cryptogram |
| Physical POS or virtual POI (eCom) | | | ID: DEAN Authentication: CDCVM (fingerprint/face recognition/device passphrase) | ID: Terminal ID Authentication: Acquirer space, keys | ID: DEAN Authentication: cryptogram | ID: DEAN Authentication: cryptogram | ID: DEAN, Terminal ID Authentication: cryptogram | ID: DEAN, Terminal ID Authentication: cryptogram | ID: DEAN Authentication: encrypted PIN, cryptogram |
| mDevice (e.g. Smartphone, Tablet) | | | | | | | ID: DEAN, Terminal ID Authentication: secret key (sandbox) | | ID: DEAN Authentication: encrypted PIN, cryptogram |
| Merchant, ATM operator | | | | | ID: Merchant ID, DEAN Authentication: n/a | ID: Merchant ID, DEAN Authentication: Acceptor ID / keys | ID: DEAN via Link / QR-code Authentication: cryptogram | ID: Acceptor ID Authentication: cryptogram | |
| Intermediary API (Payer) | | | | | | | ID: DEAN, device fingerprint Authentication: cryptogram / certificates | ID: DEAN Authentication: cryptogram | |
| Intermediary API (Payee or ATM) | | | | | | | ID: DEAN Authentication: cryptogram / certificates | ID: DEAN Authentication: cryptogram | |
| mApp ECB | | | | | | | | ID: DEAN, Intermediary credentials Authentication: cryptogram | ID: DEAN Authentication: cryptogram? |
| mApp Intermediary | | | | | | | | | ID: DEAN Authentication: cryptogram? |
| d€ chipcard | | | | | | | | | |

Figure 3.7-1: Digital euro transaction flow facilitation

appropriate identification of the component by the actors operating such components.

3.8. Authentication

3.8.1. Digital euro app

Intermediaries are expected to implement and make available invisible embedded authentication within digital euro app, as further specified in the implementation specifications¹³.

¹³ Authentication requirements for offline digital euro transactions may be revisited with a progressed understanding of such transactions

3.8.2. Intermediaries' apps / environments

Intermediaries can decide how to authenticate users in their apps / websites as long as they comply with specified guidelines and relevant regulations (for instance PSD2 and associated Regulatory Technical standards).

3.8.3. Authentication with no smartphone (inclusion use cases)

Intermediaries expected to cater for the authentication of users who do not use a smartphone and/or present disabilities preventing them from using some forms of authentication mechanisms, respecting the provisions of the European Accessibility Act (EAA) .

3.8.4. Authentication in environments other than the digital euro app and the intermediaries' apps

Intermediaries are expected to conduct authentication of users in the context of merchant in-app payments based on redirection towards either the digital euro app or the users' intermediary app depending on end-user preferences.

3.8.5. Authentication in "open intermediary" situations

"DEAN holding intermediary" is expected be enabled to conduct one single authentication of the user in situations where the user is using two different intermediaries for accessing their digital euro account and associated services (the "DEAN holding intermediary") and funding their digital euro account (the "private money holding institution") – a situation referred to as "open intermediary situation".

3.9. Dispute management principles

The Rulebook provides the rules for resolving disputes between scheme participants and ultimately End Users, depicted in **Annex B.5 (to be developed in the next iterations of the Rulebook)**. The following types of disputes are covered by the Rulebook:

- Pre-disputes: right to obtain additional information from an end user (payer, payee) through their intermediary in relation to technical and fraud disputes
- Technical disputes: disputes resulting from technical glitches such as duplicates of transactions, errors in authorisation and/or validation steps within the process flows...the exhaustive list of situations falling into that category of disputes is provided in **Annex B.5**

- Fraud disputes: disputes resulting from fraudulent activities such as identity theft, merchant identity fraud, counterfeit goods... the exhaustive list of situations falling into that category of disputes is provided in **Annex B.5**

The resolution of commercial disputes are not covered by the Rulebook and can be offered as a value-added service by intermediaries. Commercial disputes result from situations such as the non-provision and/or the provision of a good and/or service with diverging expectations between the provider and the recipient.

Disputes that cannot be solved directly between intermediaries are escalated to an arbitration party.

The management of (pre) disputes will require scheme participants to develop dedicated interfaces, as described in section 5 of the Rulebook and to be further elaborated in next iterations of the rulebook.

3.10. Minimum user experience standards

Will be provided in next iterations of the Rulebook.

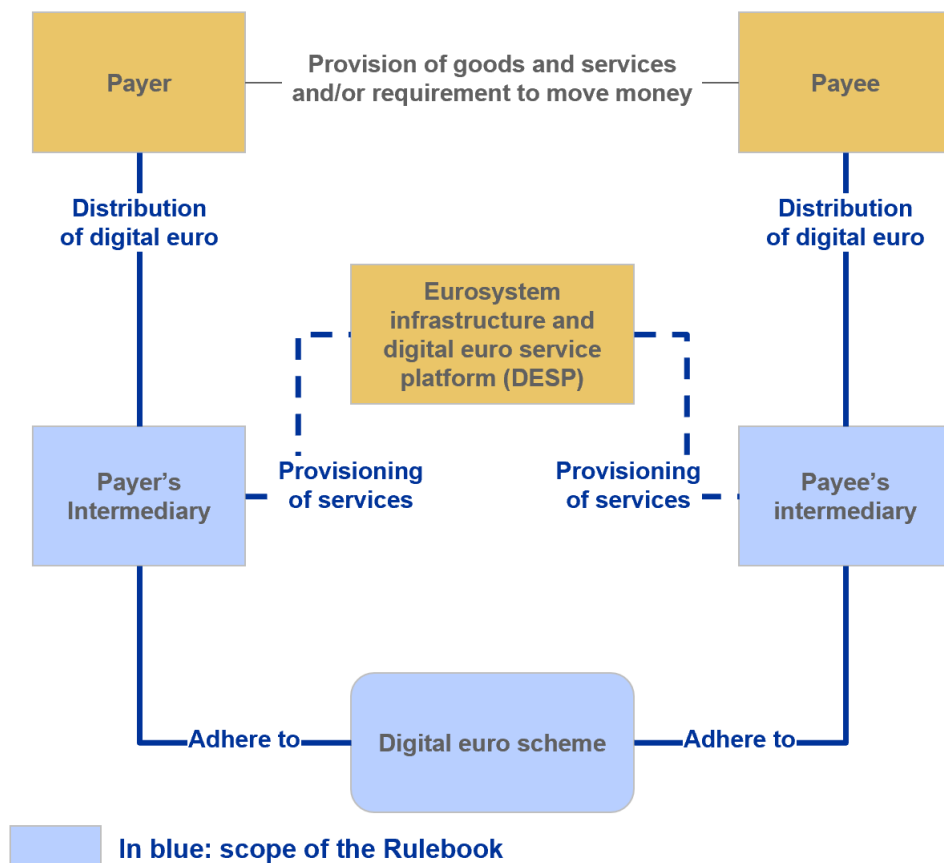
4. Adherence Model

This section, as the rest of the rulebook, may require adjustment once the Regulation on the establishment of the digital euro and the Regulation on the provision of digital euro services by payment services providers incorporated in Member States whose currency is not the euro are adopted by the Union legislator. This applies in particular to sections 4.2, 4.4., 4.5, and 4.7 – 4.10 of the adherence model.

4.1. Section Overview

Figure 4.1-1 below, as well as Table 4.1-1, provides an overview of the scope of the adherence model covered by the digital euro scheme rulebook and highlights the boundaries with (1) the intermediary to end-user legal terms (which are not governed by the rulebook and must respect core provisions of the rulebook) and (2) the intermediary to DESP legal terms (which are governed by a separate legal documentation).

689

Figure 4.1-1: Scope of the Rulebook

690

Table 4.1-1: Core legal provisions on the services in scope

| Sphere [Relationships] from figure 2.4-1 | Digital euro core services to be covered in legal documentation | | |
|---|---|--|---|
| | Access Management | Transaction management | Liquidity Management |
| End User documentation for which the Rulebook | Provisions on digital euro account servicing. | Provisions concerning the transfer of digital euros between payers and payees. | Provisions on the (automated) exchange of private money into digital euro and vice versa to accommodate (a) (reverse) waterfall |

| Sphere | Digital euro core services to be covered in legal documentation | | |
|--|---|---|--|
| | Access Management | Transaction management | Liquidity Management |
| <p>[Relationships] from figure 2.4-1</p> <p>provides core provisions</p> <p>Payer / Payee to Intermediary</p> <p>[3], [4]</p> <p>Scheme participation agreement¹⁴</p> <p>Intermediary to Scheme Governing Authority governing authority [1]</p> <p>Digital Euro Service</p> | <p>Amongst others enabling the intermediary to act as agent of the end user towards the Eurosystem. Hence, including the front-end services (digital euro app) provided by the DESP.</p> <p>Scheme defines rights and obligations for intermediaries. Amongst others enabling the intermediaries to distribute the digital euro towards the end user.</p> <p>Note: Access management is linked to the digital euro end user account and facilitated by the intermediary</p> <p>Rules governing the provision of</p> | <p>Note: The actual digital euro settlement is covered by the DESP legal documentation.</p> <p>Note: End user liquidity management as laid out above is primarily in the contractual sphere of the Intermediary.</p> <p>Resulting settlement instructions are covered by the DESP legal documentation.</p> <p>Rules governing the provision of back-end</p> | <p>and (b) min/max digital euro holdings, as requested by the end user.</p> <p>CLM – DE DCA movements.</p> |

¹⁴ Note: should the scheme be of a fully regulatory nature, no need would be materialising for individual participation contracts.

| Sphere [Relationships] from figure 2.4-1 | Digital euro core services to be covered in legal documentation | | |
|--|--|--|---|
| | Access Management | Transaction management | Liquidity Management |
| Platform Legal documentation | back-end services on the DESP (e.g. onboarding) | services on the DESP (e.g. settlement) | |
| Intermediary to Eurosystem infrastructure [5] | A legal bridge to the DESP will be required through a DESP servicing contract, ensuring that they will be made available to intermediaries and making them a condition to joining and remaining in the scheme. | | A legal bridge to digital euro back-end services is required, e.g. by the means of a new annex to the TARGET guideline. |

Legend for the colour coding in Table 4.1-1 above.

- Blue: what falls under the obligations derived from scheme participation contract
- Orange: what falls under the obligations derived from a specific agreement with intermediaries for digital euro back-end services offered by the Eurosystem or subject to related decisions by the private sector. Back-end services provided by the Eurosystem are contracted elsewhere and are outside the scope of the Rulebook services potentially provided by the private sector will be specified within the Rulebook.
- Green: what falls under the obligations which would derive from TARGET guideline.

4.2. Participation in the Scheme

Participation in the scheme is on the basis of the ECB legal acts, **the legal construction of which is still to be analysed**, and in compliance with the following guiding principles:

- Participants shall comply with the Rulebook, its annexures including amendments as and when they are made and properly communicated to participants;
- Participants need to ensure that all applicable laws and regulations are adhered to. These include but are not limited to future regulation on the the digital euro and relevant

future ECB legal acts, the Regulation on Information on the payer accompanying transfers of funds and the provisions of the Payment Services Directive¹⁵.

The parties to the scheme are the [ECB;Eurosystem]¹⁶ and each participant. A participant shall ensure that its clients, employees, its agents and the employees of its agents comply with all applicable obligations under the Rulebook.

4.3. Reachability & interoperability

Each participant shall offer services relating to the scheme in the capacity of an intermediary by providing access to digital euro accounts, liquidity management, and transaction management for digital euro under the Scheme and to providing them according to the rules of the scheme. The scope of services to be provided by the participant is further specified under 4.7 Obligation of participants. As such they may operate as payer's or payee's intermediary and assure reachability and interoperability.

4.4. Eligibility criteria

In order to be eligible as a participant, a participant must at all times:

- (1) Be incorporated and licensed by an appropriate EEA regulatory body and supervised by competent authorities incorporated in EEA Member States as CI, PI, EMI., or third party providers;
- (2) Having signed a servicing contract with the operator of the digital euro servicing platform (DESP);
- (3) Have access to a digital euro DCA, i.e. being able to be debited/credited in a DCA as part of a funding/defunding operation, but not necessarily owning or even being able to directly instruct a DCA;

¹⁵ Note: To be transferred divided to the future Payment Services Regulation and new Payment Services Directive (PSR and PSD3).

¹⁶ Note: Topics requiring further clarification are covered in [] and marked in **amber**.

(4) Having the effective risk control measures that, on top of the ones required to be licensed, are required in the Rulebook and further detailed in the Risk Management Annex D.

A participant shall notify the scheme governing authority of any matter that is material to its eligibility as a participant under this section 4.4. The scheme governing authority shall take reasonable steps to bring such notifications to the attention of all other participants.

4.5. Becoming a participant

Any undertaking which is eligible under section 4.4 above may apply to become a participant. Some might be required by law to join the scheme while others may join on a voluntary basis. Applications shall be submitted to the scheme governing authority in accordance with the application procedures set out in the internal rules. To apply to become a participant, the applicant shall submit to the scheme governing authority an original and duly signed participation agreement as well as supporting documentation as further detailed in the internal rules. The scheme governing authority may require additional information from the applicant in support of its application. The applicant needs to fulfill and prove its compliance with the technical requirements for the digital euro as laid out in the internal rules. An applicant becomes a participant on an admission date specified by the scheme governing authority in accordance with the internal rules. Names of applicants which will become participants at a future date may be pre-published, and a date designated and published when they will become participants.

4.6. Scheme registers of participants

The scheme governing authority will operate and provide a register of participants.

4.7. Obligations of participants

4.7.1. General Obligations

As further specified in Section 3 and 5 of the Rulebook, in respect of each of its end user, an intermediary shall:

- (1) Comply fully with applicable regulations in particular in respect of anti-money laundering, countering the financing terrorism (AML/CFT), including sanctions restrictions, which are to be applied to all activities related to access, transaction and liquidity management;

- (2) Ensure the ongoing compliance of its own rules, procedures and agreements with the regulatory and supervisory requirements applicable to the intermediary;
- (3) Comply at all times with the Rulebook and its annexures;
- (4) Comply with applicable provisions issued in relation to risk management as set out in the Rulebook;
- (5) Ensure that terms and conditions of the participants with each end user exist, governing the provision and use of services relating to the scheme;
- (6) Ensure that such terms and conditions of the participants with the end user are consistent with the Rulebook as laid out in the internal rules;
- (7) Enter into an end user agreement governing the provision and use of services relating to the scheme only after applying the principles of Know Your Customer;
- (8) Ensure that such end user agreement is consistent with the Rulebook and that such agreement is complete, unambiguous and enforceable;
- (9) Provide end users with adequate information on their risks as well as the respective rights and obligations of the payer, payee, payer intermediary and payee intermediary, where relevant, including those specified in the applicable legislation, in relation to the digital euro as well as to the scheme in question, and information about the service level offered and any charges that apply to the service being performed;
- (10) Immediately report to the scheme governing authority about unmitigated risks¹⁷ of scheme wide importance and about major incidents that affect the smooth functioning of the scheme. This includes but is not limited to notifications to the central fraud detection and prevention function within the DESP about unmitigated fraud risks;
- (11) Without delay report to the scheme governing authority about issues or complaints related to digital euro transactions that were raised by payers or payees and about internal or external audit findings, where such issues, complaints or findings are of scheme-wide importance;

¹⁷ Note: Only unknown and / or new risks are to be reported.

(12) Be able to provide access to digital euro holdings, provide liquidity management services and process digital euro instructions and transactions as defined in the Rulebook, 24 hours a day on all calendar days of the year. This includes all business continuity arrangements set up by the intermediary itself;

(13) Enable access to digital euro holdings, liquidity management services, and digital euro instructions and transactions via its channels, i.e., the intermediary website, the intermediary payment app, via ATMs in case provided by the payer intermediary;

4.7.2. Obligations related to the participants role as access manager

(14) As further specified in Section 3 and 5 of the Rulebook, in respect of each of its end users, an intermediary shall: enable access to digital euro holdings, liquidity management services (incl. the linking of a private money account¹⁸ to its digital euro account), and digital euro transactions via API access to the digital euro app. Intermediaries servicing private users shall issue digital euro cards as further specified in the implementation specifications;

4.7.3. Obligations related to the participants role as liquidity manager

(15) Enable the individual users to conduct liquidity management instructions via the intermediary website, via payment app, via ATMs where provided by the payer intermediary, or via the digital euro app. End users shall be able to provide liquidity management instructions either manually or automated based on specific parameters as set by the end user and further specified in the end user implementation specifications. Intermediaries shall thereby enable the private users to choose between private money account and digital euro online holdings as source for funding and defunding the digital euro offline solution;

(16) Enable individual users to withdraw cash from their digital account in their branch network where cash services are offered. This includes but is not limited to ATM services offered in branch even if outsourced or contracted otherwise;

¹⁸ The private money account is held with a scheme participant

4.7.4. Obligations related to the participants' role as transaction manager

Note: There is no role for the intermediary in the offline transactions. However, subject to legislation, the analysis or ex-post verification of transactions may still be required.

4.7.4.1. Obligations related to the participants' role as payer's intermediaries

As further specified in Section 3 and 5 of the Rulebook, in respect of each of its payers, a payer intermediary shall:

- (17) Enable the payer to create, change, and delete recurring payments, via the intermediary website or the intermediary payment app in case provided by the payer intermediary
- (18) Prior to the final execution of a digital euro transaction, conduct the legally required fraud as well as AML/CFT (including sanctions / embargo) checks based on the information the payer's intermediary would use for payment transactions, while taking full responsibility for the execution or non-execution of the transaction. With regards to the fraud checks performed by the payer's intermediary, payer's intermediary shall further inform its own fraud rating by the fraud scoring provided by the central fraud detection and prevention function within DESP;
- (19) Provide the payer with an explanation of the reasons for terminating the relationship as an access manager in such case. Intermediaries can only terminate digital euro related services in isolation for business users if they fail to meet merchant specific requirements as further specified in the know your merchant requirements;

4.7.5. Obligations related to the participants' role as payee's intermediary

As further specified in Section 3 and 5 of this Rulebook, in respect of each of its payees, a payee's intermediary shall:

- (20) Receive the digital euro credit notifications from the DESP and immediately notify the corresponding payee, provided that applicable AML/CFT and fraud regulations have been complied with.

4.8. Liability

The liability regime between the PSPs and the Eurosystem depends on the ECB legal act regulating the Rulebook, which requires further analysis till fully developed and agreed. Once

this is progressed further the adherence section in general and the obligations in particular might be subject to change.

4.9. Termination

The criteria, which may result in termination of scheme participant, will be further defined in the preparation phase and may or may not apply only to voluntary services.

A participant may terminate its status as a participant as legally permitted by giving no less than [xx] months' prior written notice to the scheme governing authority, such notice to take effect on a designated day (for which purpose such a day will be designated at least one day for each month). As soon as reasonably practicable after receipt of such notice, it or a summary shall be published to all other participants in an appropriate manner. Notwithstanding the previous paragraph, upon receipt of the participant's notice of termination by the scheme governing authority, the participant and the scheme governing authority may mutually agree for the termination to take effect on any day prior to the relevant designated day. A former participant shall continue to be subject to the Rulebook in respect of all activities which were conducted prior to termination of its status as a participant and which were subject to the Rulebook, until the date on which all obligations to which it was subject under the Rulebook prior to termination have been satisfied. A former participant shall continue to be subject to all confidentiality obligations. Upon termination of its status as a participant, this former participant shall not incur any new obligations under the Rulebook. Further, upon such termination, the remaining participants shall not incur any new obligations under the Rulebook in respect of such former participant. In particular, no new scheme related obligations may be incurred by the former participant or in favour of the former participant. The effective date of termination of a participant's status as a participant is (where the participant has given notice in accordance with the first paragraph of section 4.9) the effective date of such notice, or (in any other case) the date on which the participant's name is deleted from the scheme register of digital euro participants, and as of that date the participant's rights and obligations under the Rulebook shall cease to have effect except as stated in this section 4.9. This section, sections 4.8, 4.10, 4.11 [and Annex] of the Rulebook shall continue to be enforceable against a participant, notwithstanding termination of such participant's status as a participant.

4.10. Suspension

The criteria, which may result in suspension of scheme participant, will be further defined in the preparation phase and may or may not apply only to voluntary services.

The scheme governing authority may suspend participants in case they fail to meet their obligations as laid out on in section 4.7. In case of grave omissions of the participant the suspension may be rendered mandatory without discretion by the scheme governing authority. A suspension can exclude the participant from all or some of the scheme services and would be notified by a suspension note released by the scheme governing authority. This note will state the reasons for suspension, the scope of services being affected by the suspension, immediate actions being required by the participant as well as activities to be conducted by the participant in order to resolve its suspension status. The scheme governing authority shall monitor the progress of the participants in the resolution of the reasons for its suspension and unsuspend the participant as soon as reasonably possible. A suspended participant can be excluded from the scheme as laid out in section 4.9.

As soon as reasonably practicable after receipt of such notice of suspension and or unsuspension, it or a summary shall be published to all other participants in an appropriate manner.

4.11. Intellectual property

The participants acknowledge that any copyright in the Rulebook belongs to the [ECB;Eurosystem]. 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;Eurosystem] in the Rulebook.

4.12. Governing law(s)

A thorough analysis of pros and cons of different governing laws is to be conducted by DG-L.

5. Technical scheme requirements

5.1. Section overview

This section depicts the functional architecture foreseen for the digital euro. This includes the description of the interactions and necessary interfaces between end users, devices and

intermediaries. Figure 5.3-1 provides a visual summary of the foreseen architecture. Besides, this section also outlines non-functional requirements to be met by scheme members.

5.2. Foundational principles for the selection of technical standards

The digital euro scheme aims to leverage existing standards and market solutions provided that it would not introduce intellectual property constraints and/or critical governance dependencies for the Eurosystem and the participants of the digital euro scheme.

5.3. High-level IT infrastructure

The high-level functional architecture for the digital euro depicted in Figure 5.3-1 below describes the interplay between end-users, Intermediaries and the digital euro access gateway and associated digital euro service platform.

(1) End user domain (cf. Section 5.4.1) consists of

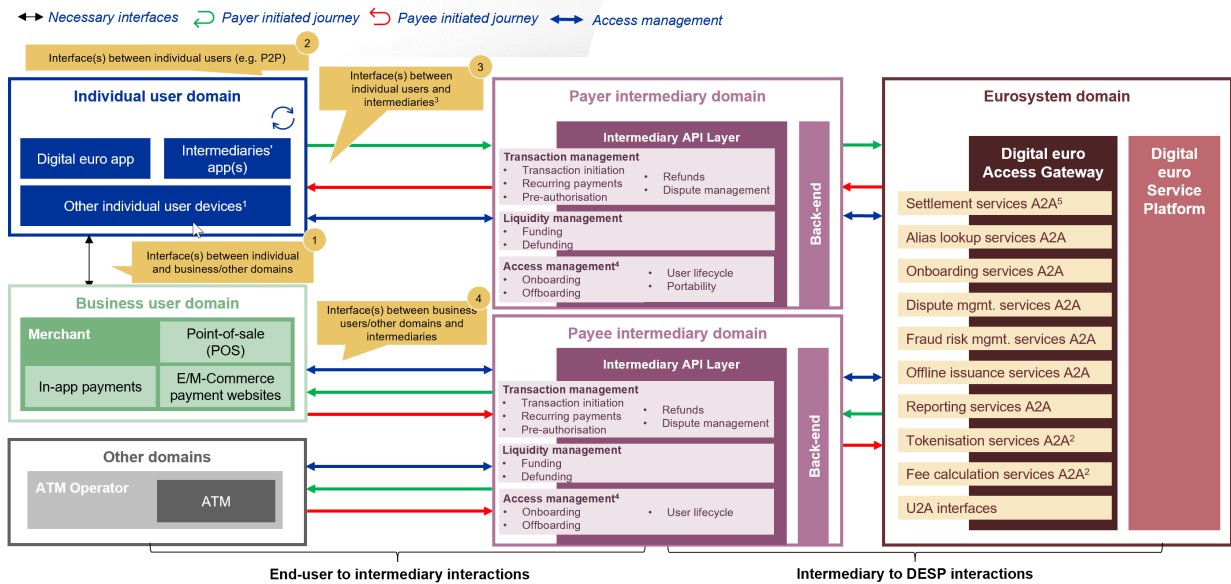
- a) Individual users providing the perspective of individuals using digital euro,
- b) Business users providing the perspective of digital euro acceptors, i.e., merchants, governments and other public authorities,
- c) Other domains including ATM operators.

(2) Intermediary domain (cf. Section 5.4.2) consists of

- a) payer intermediaries also referred to as distributing payment service providers (distributing PSPs) providing access and required payment instruments to individual users of digital euro,
- b) payee intermediaries also referred to as acquirers providing access and required acceptance solutions to business users and
- c) associated providers acting on behalf of the intermediaries and/or providing complementing technical services (e.g., technical processors, payment gateways)

(3) Eurosystem domain consisting of digital euro access gateway and associated digital euro services, which are described in the digital euro service platform (DESP) agreement.

922 **Figure 5.3-1 High-level architecture**



5.4. Domains of actors

5.4.1. End user domain

5.4.1.1. Individual user domain¹⁹

Access managers provide digital euro services through the digital euro app as well as provide such services by their own access channels such as an intermediary app.



5.4.1.1.1. Intermediaries' app(s) or website

Access managers may integrate digital euro scheme support into their own (existing) intermediary apps and websites. In any case access managers shall support the digital euro app integration and related APIs. Person-to-Person (P2P) as well as Person-to-Business payments may be conducted in proximity (QR-code, NFC, offline digital euro) and remote environment (Qr-code, alias or pay-by-link).

¹⁹ Partial overlaps to business user as further specified in the section exist.

935 In parallel to the mandatory integration of the digital euro app intermediaries might optionally re-
 936 use a dedicated, customised set of APIs to facilitate the integration of digital euro into existing
 937 intermediary apps or to support specific value-added-services (VAS).

938 **Table 5.4-1: Summary of the components that will need to be interfaced with the digital**
 939 **euro-enabled intermediaries' apps.**

| Interaction between | Nature of interaction | Interface supporting this interaction |
|---|--|---|
|  <p>End user and App (U2A²⁰)</p> | <p>The intermediary app communicates with the user via the device for returning feedback from intermediary, performing authentication, initiating transactions or funding / defunding operations, etc.</p> <p>The user experience of the intermediary app might deviate from the unified user experience of the digital euro app but will need to meet minimum UX requirements set by the digital euro scheme.</p> | Intermediary app via user-to-app interface |
|  <p>End user device and other device (individual for P2P,</p> | <p>The intermediary's app interacts with other devices (e.g., attended and unattended POS terminals, ATMs, payer and payee devices for P2P transactions and remote transactions) for exchanging payment information using contactless communication with QR codes or NFC technology.</p> | NFC Interface, QR Code Interaction, Interface to support offline digital euro |

²⁰ U2A = User-to-Application interface

**acceptance for
P2B) (A2A²¹)**



**End user
device and
intermediary
(A2A)**

The intermediary's banking app forwards its user's interactions (e.g., requests or authentication data) to the intermediary API and receives feedback from the intermediary, which for some use case relate to subsequent interactions with DESP.

Digital euro scheme standard API or customised intermediary API

The app interacts via intermediary APIs to support pay-by-link and alias payments.

5.4.1.1.2. Digital euro app

Access managers shall support digital euro app by providing related APIs as further specified in the end user Implementation specifications.

The digital euro app is a stand-alone mobile application and due to its integration with all intermediaries offering digital euro services to individual users accessible to all end users. It builds upon a standardised set of APIs allowing individual users to manage their profiles, liquidity, digital euro payment form factors and to initiate (and monitor) transactions.




The app will communicate directly with the user's intermediary using a standardised API layer. As such, participants of the digital euro scheme must support the standardised API layer by providing the respective API endpoints for communication between the backend of the intermediary and the digital euro app.

The first time the app is opened by the user, it will prompt the user to select their intermediary, which will configure which of the intermediaries' API endpoints will be used by the app to contact the appropriate back end.

The app will be available for smartphones and might include additional operating systems to support other bearer instruments such as wearables. The operating systems to be supported is clarified in the end user implementation specification.

²¹ A2A = Application-to-Application interface




Table 5.4-2: Summary of the components that is to be interfaced with the digital euro app.

| Interaction between | Nature of interaction | Interface supporting this interaction |
|---|--|---|
|  End user and app (U2A) | The digital euro app communicates with the user via the device for returning feedback from intermediary, performing authentication, initiating transactions or funding / defunding operations, etc. | Digital euro app U2A interface |
|  End user device and other device (individual for P2P, acceptance for C2B) (A2A) | The digital euro app interacts with other devices (e.g., attended and unattended POS terminals, ATMs, payer and payee devices for P2P transactions and remote transactions) for exchanging payment information using contactless communication with QR codes or NFC technology. | NFC Interface, QR code interaction, Interface to support offline digital euro |
|  End user device and intermediary (A2A) | The digital euro app forwards its user's interactions (e.g., authentication data, payment request or balance inquiry) to the user's intermediary via the dedicated Eurosystem API and receives responses from the intermediary, which for some use case relate to subsequent interactions with DESP. | Digital euro scheme standard API The app interacts via APIs to support pay-by-link and alias payments. |

5.4.1.1.3. Other individual user devices

Individual users can also use digital euro services through other devices such as a physical card. Table 5.4-3 below provides a summary of the components that will need to be interfaced with the digital euro physical cards.

963 **Table 5.4-3: Summary of the components that will need to be interfaced with the digital**
964 **euro physical cards**

| Interaction between | Nature of interaction | Interface supporting this interaction |
|---|---|--|
|  <p>End user and end user device (interface n/a)</p> | <p>End-user presents the card - or enters the card number in remote environment for an alias-based digital euro transaction - for transaction initiation in the next step.</p> | <p>n/a</p> |
|  <p>End user device and other end users' devices / acceptance channels (A2A)</p> | <p>The card interacts with acceptance devices (e.g. attended and unattended POS terminals, ATMs, payer devices for P2P transactions) for exchanging payment information using contactless communication with NFC technology. In remote environment, an alias in the form of a card number is entered.</p> | <p>Contactless NFC as preferred interface; contact chip transactions for specific use cases not allowing to deploy contactless technology will apply (e.g. due to infrastructure limitations) and/or offline digital euro. Manual alias entry in remote environment.</p> |
|  <p>End-user device and intermediary's back-end systems (i) NFC (or contact chip) online for proximity environment, (ii) Alias for remote environment, (iii) Offline digital euro</p> | <p>The physical card as such cannot interact directly with the intermediary. It interacts with acceptance devices. Acceptance devices then interact themselves with the relevant intermediaries, based on the information shared by the card such as the number (used as an alias) and/or other information (e.g., reconciliation for offline, transaction history, etc.)</p> | <p>Transaction - purchase, (de-)funding - notification from intermediary to end-user via defined communication channel.</p> <p>No interaction for offline digital euro payment per transaction but interface for regular reconciliation of offline activities required.</p> <p>Funding and defunding interface for offline digital euro.</p> <p>Transaction history interfaces, e.g. web or statement.</p> |

The following table 5.4-4 specifies the applicable form factors respectively means of connectivity for interactions between individual users. They are further specified in Annex G.7.2 and G.7.3.

Table 5.4-4: Applicable form factors respectively means of connectivity for Interactions between individual users

| | | Individual payee's device | | | |
|---------------------------|-----------------------|---|---|---|--|
| | | Digital euro app | Intermediary app | Card | Other (e.g. wearable) |
| Individual payer's device | Digital euro app | <ul style="list-style-type: none"> • QR code • NFC²² • Alias • Pay-by-link • NFC offline²³ | <ul style="list-style-type: none"> • QR code • NFC • Alias • Pay-by-link • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline • QR code if applicable* |
| | Intermediary app | <ul style="list-style-type: none"> • QR code • NFC • Alias • Pay-by-link • NFC offline | <ul style="list-style-type: none"> • QR code • NFC • Alias • Pay-by-link • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline • QR code if applicable |
| | Card | <ul style="list-style-type: none"> • NFC • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline | • n/a | Might apply (power supply): <ul style="list-style-type: none"> • NFC • NFC offline |
| | Other (e.g. wearable) | <ul style="list-style-type: none"> • NFC • NFC offline | <ul style="list-style-type: none"> • NFC • NFC offline | Might apply: <ul style="list-style-type: none"> • NFC • NFC offline | Might apply (power supply): <ul style="list-style-type: none"> • NFC |

²² 'NFC' represents here contactless online digital euro transactions, the technologies for offline digital euro transactions are still to be discussed.

²³ Offline d€ might be contactless or a contact transaction, subject of final solution design. However, it is not expected that in P2P environment an individual user has a device with contact transaction capabilities.

| | | | | | |
|--|--|-------------------------|-------------------------|--|---------------|
| | | • QR code if applicable | • QR code if applicable | | • NFC offline |
|--|--|-------------------------|-------------------------|--|---------------|

969

970 **5.4.1.2. Business user domain**

971 In the business user domain, the requirements differ depending on the payment channel
972 (proximity or remote) and the acceptance device type.

973 Digital euro transactions can be conducted either in proximity or remote environment.

974 Proximity payments are conducted in an environment in which payer and payee (device) are at
975 the same physical location, using one of applicable proximity technologies i.e., QR code, NFC,
976 offline digital euro or card contact chip.

977 A special type of proximity transactions are use cases addressing funding transactions at so
978 called cash recycling machines (CRMs) and defunding – or withdrawal of cash for end users –
979 at automated teller machines (ATMs) and at cash-over counter terminals in bank branches.

980 Remote payments are conducted in an environment in which payer and payee are interacting
981 remotely like in e-commerce or m-commerce transactions using payment technologies such as
982 QR code, alias or pay-by-link.

983 Digital euro scheme specific offline digital euro transactions are only applicable in proximity
984 environment.

985 The following subsections describe both channels and address their specific requirements.

986 **5.4.1.2.1. Acceptance devices in proximity environment**

987 The business user domain can be broken down by several criteria which result in dedicated
988 technical requirements for (un)attended POS types, which are further specified in Annex G.7.1
989 and G.7.4.

- 990 • Attended terminals
 - 991 ○ Standard POS terminal
 - 992 ○ Industry specific solutions e.g., for lodging or car rental with integration to
 - 993 dedicated back-end systems of business users.

- 994 ○ Bank branch terminals for cash advance or funding transactions
- 995 ○ mobile POS (mPOS) such as smartphone or tablet
- 996 • Unattended terminals
 - 997 ○ Unattended terminals can be further divided into different subtypes, e.g., with or
 - 998 without pinpad
 - 999 ○ Industry specific solutions (e.g., fuel dispenser, vending machines)


1000 **Physical POS system**



1001 A physical POS is part of a sales system which consists of several components. While
 1002 unattended POS are usually considered as fully integrated stand-alone systems, attended POS
 1003 environments will need to meet component specific requirements as further specified in Annex
 1004 **G.Error! Reference source not found.**7.1 and G.7.4.

1005 **POS system interfaces**

- 1006 • A POS terminal management system (TMS) is operated by an intermediary to manage
 1007 POS configuration, software updates and patches, implementation and activation of
 1008 additional terminal functions. The interface supports management of online and offline
 1009 digital terminal application.
- 1010 • Electronic cash register (ECR) interface
 1011 ECR is part of the business user payment environment.
- 1012 • Transaction interface
 1013 The transaction interface is used for the transaction (reference to Annex G.7.1 and G.7.4
 1014 and table with transaction types) and liquidity management use cases (funding, cash
 1015 withdrawal or combination of both (e.g., purchase with cashback).
- 1016 • API for QR code tokenisation and QR code generation
 1017 A POS supports dynamic payee-presented QR codes interacting with the tokenisation
 1018 service via the intermediary (acquirer), either by displaying the QR Code directly on the
 1019 terminal and/or displaying it on an another screen connected to the ECR.
- 1020 • Internal or external NFC reader.

1021 **Table 5.4-5: Description of interactions between POS and end users, devices and**
1022 **intermediary systems**

| Interaction between | Nature of interaction | Interface supporting this interaction |
|--|---|---|
|  <p>End user and POS (U2A)</p> | <p>There is a difference between attended and unattended terminals.</p> <p>At unattended terminals any interaction happens between end user and the terminal.</p> <p>At attended terminals some operations will be conducted by the cashier. An interaction between cashier and payer might be required e.g., asking/requesting a cashback transaction.</p> <p>A POS interacts with user presenting to be scanned QR code on a built-in or external display and/or displays a message to user to conduct a contactless transaction or a contact transaction with card.</p> <p>If applicable, the POS might ask for selection of online/offline digital euro.</p> <p>User enters a PIN via the POS Pinpad if required.</p> <p>Unless an electronic receipt is available, POS provides a paper receipt.</p> | <p>Display, Pinpad, printer, optional separate POS unit operated by the cashier and/or an electronic cash register (ECR).</p> |




| | | |
|---|--|--|
|  <p>End user device and POS (A2A)</p> | <p>A POS interacts with payer (device) for exchanging payment related information and transaction initiation.</p> <p>The actual interactions depend on the form factor used as described in the following sections.</p> | <p>QR code on display.</p> <p>Contactless interface.</p> <p>Chip contact reader.</p> <p>Offline digital euro interface (NFC or contact chip)</p> |
|  <p>POS and intermediary's back-end systems (A2A)</p> | <p>POS requests (i) dynamic QR codes to be presented to user via tokenisation service and (ii) receives response from Acquirer back-end regarding the approval or decline of the transaction via defined interfaces and possible intermediate 3rd party gateways.</p> | <p>Tokenisation service API.</p> <p>Back-end interface to initiate transaction and to receive approval/decline which might include intermediate 3rd party gateways.</p> <p>Terminal management system interface</p> |

1023 5.4.1.2.2. Acceptance devices in remote environment

1024 There are no physical devices in remote environment, the distinction can be made between

- 1025 • Virtual terminals represented by terminal IDs used as reference in the transaction
- 1026 process.
- 1027 • Merchant apps which are either smartphone-optimised versions of the e-commerce
- 1028 website with similar payment process as in e-commerce or dedicated payment m-
- 1029 commerce payment process including interaction with and redirection to payer apps.

Table 5.4-6: Description of interactions between payment page and end users, devices and intermediary systems

| Interaction between | Nature of interaction | Interface supporting this interaction |
|--|---|---|
|  End user and payment page (U2A) | <p>For completion of an online purchase/order the user is redirected to a payment page where digital euro can be selected as payment method.</p> <p>A selection of the applicable digital euro payment options must be provided (e.g., alias, QR-code or pay-by-link).</p> <p>After selection of the preferred payment option the user needs to authenticate themselves and consent the transaction which might include another device such as a smartphone.</p> <p>After the successful payment the user receives a payment confirmation and a transaction receipt (e.g., by Email).</p> | <p>Internet browser</p> <p>Alias field on payment page/website.</p> <p>Email</p> <p>Authentication device</p> |
|  End user device and payment page (A2A) | <p>The payment page interacts with payer (device) for exchanging payment related information and transaction initiation.</p> <p>The actual interactions depend on the form factor used as described in the following sections.</p> | <p>QR-code on payment page/website.</p> <p>Pay-by-link initiation button on payment page/website.</p> <p>Authentication webpage or dedicated device (e.g., smartphone with d€ or intermediary app).</p> |
|  Payment page and intermediary's | <p>The payment page requests (i) dynamic QR-codes to be presented to user via tokenisation service and (ii) receives response from acquirer back-end regarding the approval or decline of the transaction via defined interfaces and possible intermediate 3rd party gateways.</p> | <p>Tokenisation service API.</p> <p>Alias lookup service.</p> <p>Pay-by-link service.</p> <p>Back-end interface to initiate transaction and to receive</p> |



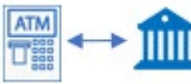
| | |
|---------------------------------------|---|
| back-end systems (A2A) | approval/decline which might include intermediate 3 rd party gateways. |
|---------------------------------------|---|

1030

1031 **5.4.1.3. Other user domains**

1032 **5.4.1.3.1. ATMs**

1033 **Table 5.4-7: Description of interactions between ATM and end users, devices and**
1034 **intermediary systems**

| Interaction between | Nature of interaction | Interface supporting this interaction |
|---|---|--|
|  <p>End User and ATM (U2A)</p> | <p>ATM interacts with user by presenting a QR-code. The user would scan the QR-Code, insert chip or tap card in case of NFC to trigger further actions.</p> <p>Selection online/offline digital euro must be offered.</p> <p>If applicable, an online and/or offline balance might be presented.</p> <p>User enters a PIN or a code via the Pinpad. Authentication can also be via mobile phone.</p> | <p>Screen, pinpad; NFC, card reader, receipt printer</p> |
|  <p>End user device and ATM (A2A)</p> | <p>The ATM interacts with payer devices (e.g. digital euro or intermediary app) for exchanging payment information via QR-code or NFC if the ATM already supports NFC; or using a digital euro card via NFC or contact chip.</p> | <p>NFC Interface, display to present QR Code (for online only) and card reader, Interface to support offline digital euro</p> |
|  <p>ATM and intermediary (A2A)</p> | <p>ATM requests (i) dynamic QR-codes to be presented to user via tokenisation service and (ii) receives response from ATM acquiring API regarding the approval or rejection of the transactions via defined interfaces, via dedicated ATM gateways.</p> <p>The ATM forwards the user's interactions (e.g., requests or authentication data) to the intermediary API and receives feedback from the intermediary, which for some use case relate to subsequent interactions with DESP.</p> | <p>Intermediary API supporting transaction initiation for respective form factors and to receive approval/decline responses.</p> <p>QR-code tokenisation requires tokenisation request and response.</p> |

5.4.2. Payer and payee intermediary domain

The following table 5.4-8 specifies the applicable form factors and respective means of connectivity for interactions between individual and business users / other domains domain. They are further specified in Annex G.7.1 and G.7.4.

Table 5.4-8: Form factors for interactions between individual and business users / other domains

| | | Business' device / channel / ATM | | |
|---------------------------|------------------------|---|---|--|
| | | POS (ATM) | e/mCom | In-app |
| Individual payer's device | Digital euro app | <ul style="list-style-type: none"> • QR code • NFC • Offline d€ • Chip card | <ul style="list-style-type: none"> • QR code • Alias • Pay-by-link | <ul style="list-style-type: none"> • DEAN • Alias • Pay-by-link |
| | Intermediary app | <ul style="list-style-type: none"> • QR code • NFC • Offline d€ | <ul style="list-style-type: none"> • QR code • Alias • Pay-by-link | <ul style="list-style-type: none"> • DEAN • Alias • Pay-by-link |
| | Card | <ul style="list-style-type: none"> • NFC • Offline d€ | <ul style="list-style-type: none"> • Alias • <i>DEAN entry (tbd)</i> | • n/a |
| | Other (e.g., wearable) | <ul style="list-style-type: none"> • NFC • Offline d€ | <ul style="list-style-type: none"> • Alias • <i>DEAN entry (tbd)</i> | • n/a |

In addition, intermediaries act for end users as entry point to central scheme services like alias lookup and tokenisation service and support appropriate APIs.

The functions which access managers expose via the Intermediary API layer depend on the role and scope of service the offer to the end users, in particular:

- Individual users can transact with digital euro at any point of interaction using any of the applicable use cases. Therefore, access managers of individual users must support the full range of functions defined by the scheme, including portability function for interface type access management as further specified in the end-user implementation specification.

- Access managers of business users (acquirers) support via their API layer all mandatory functions as defined by the scheme and further specified in the end user implementation specification. In contrast to access managers of individual users there are conditional requirements for acquirers, depending on the supported business scope. E.g., acquirers addressing e-commerce merchants only are not mandated to implement POS specific requirements and vice versa.

Table 5.4-9: Overview of the functions to be supported

| Interface type | Function | Access manager for Individual Users | Access manager for Business Users ²⁴ |
|---------------------------------|------------------------------------|--|--|
| Access management | Onboarding | mandatory | mandatory |
| | Lifecycle management | mandatory | mandatory |
| | Offboarding | mandatory | mandatory |
| | Portability | mandatory | n/a |
| Liquidity management | Funding at ATM | mandatory | conditional |
| | Funding at cash- over-counter | mandatory | conditional |
| | Funding (money transfer) | mandatory | n/a |
| | Defunding at ATM | mandatory | conditional |
| | Defunding at cash- over-counter | mandatory | conditional |
| | Defunding (money transfer) | mandatory | n/a |

²⁴ Business users can be either merchants or ATM operators. Merchant acquirers providing services to merchants do not have to support ATMs and vice versa, ATM acquirers do not have to support merchant acquiring.

| | | | |
|-------------------------------|----------------------------|-----------------|-------------|
| Transaction management | P2P Transaction initiation | mandatory | n/a |
| | Transaction initiation | mandatory | mandatory |
| | Recurring payments | mandatory | conditional |
| | Pre-authorisation | mandatory | conditional |
| | Refunds | mandatory | mandatory |
| | Dispute management | mandatory | mandatory |
| Other | Waterfall | mandatory | mandatory |
| | Reversed waterfall | mandatory | mandatory |
| | Alias lookup | mandatory | mandatory |
| | QR-code tokenisation | mandatory (P2P) | mandatory |
| | NFC tokenisation | mandatory | n/a |

1057 5.5. IT security

1058 Security requirements which apply to data in transit (connectivity) and data at rest (storage) are
1059 further specified in the Annex G.7. Implementation specifications and technical standards as
1060 well as Annex **Error! Reference source not found.**⁴ Certification and testing ecosystem.

1061 5.6. Non-functional requirements

1062 The digital euro scheme is designed as always online²⁵ 24/7, relying on 24/7 instant settlement
1063 in central bank money.

1064 The attractiveness of a payment scheme depends on a set of non-functional aspects which are
1065 described in this section, in particular availability, reliability (5.6.1) and performance (5.6.2).

²⁵ Dedicated SLRs and KPIs might be applicable and must be defined for 'offline digital euro'.

1066 A frictionless user experience is ensured by scheme compatibility (5.6.3) and integrity (5.6.4.)
1067 requirements.

1068 The scheme reserves the right to request proofs or certifications and/or the right to conduct
1069 announced on-site reviews for auditing purposes, in particular in case of recurring non-
1070 compliance events.

1071 The scheme reserves the right to monitor intermediaries' compliance with the set out non-
1072 functional requirements in day-to-day operations. Intermediaries must be prepared to support
1073 monitoring messages as defined in the end user implementation specifications.

1074 Different requirements apply for online and offline digital euro. In particular, while 24/7
1075 availability and performance is key for online digital euro as instant settlement scheme, most
1076 important offline digital euro aspects are the prevention of double-spending and loss of funds
1077 which might be considered as reliability requirements.

1078 **5.6.1. Availability and reliability requirements**

1079 International Organisation of Standardisation (ISO) 25010 suggests that availability is a subtopic
1080 of reliability.

1081 Intermediaries participating in digital euro scheme and critical third parties which provide ICT
1082 (Information Communication Technologies)-related services to digital euro intermediaries shall
1083 comply with all regulations in place related to operational resilience.

1084 The scheme reserves the right to monitor e2e availability sending regular ping messages or
1085 dummy transactions initiated via e.g., the digital euro app. Intermediaries must be prepared to
1086 support such messages.

1087 To address cases where e2e availability monitoring is not applicable intermediaries are required
1088 to provide monthly availability reporting as defined in Annex C.1 Service Level Requirements
1089 and Key Performance Indicators.

1090 In order to ensure 24/7 reachability, the intermediaries are required to provide during the
1091 onboarding phase all necessary contact details of involved IT operation centres.

1092 In terms of reliability in offline digital euro context prevention of double-spending and loss of
1093 funds are key requirements as further specified in end user implementation specifications.

5.6.2. Performance requirements

Intermediaries and any 3rd parties acting on their behalf must ensure compliance with target key performance indicators (KPIs) set out in Annex C.1.

Intermediaries must establish processes for volume projections, in particular for predictable peak times (e.g., public holidays) to ensure target transaction performance indicators as set out in Annex C.1.

The scheme reserves the right to monitor the performance, measuring timeout-ratio or UTC time stamp of an e2e transaction process and underlying messages.

5.6.3. Compatibility requirements

Intermediaries and any 3rd parties acting on their behalf must be compliant with scheme standards to ensure interoperability with other parties, integrity of the scheme and minimisation of exceptions resulting in technical errors, rejects/recalls, timeouts, (pre-)disputes or even fraud.

The scheme Rulebook describes mandatory certification requirements to be completed before (i) intermediaries can initiate digital euro activities and (ii) activate to be certified services and/or components as described in Annex B.4.

The scheme reserves the right to monitor intermediaries' day-to-day operation compliance after activation of digital euro by the intermediary.

Specific compatibility metrics are described in Annex C.1.

Intermediaries and any 3rd parties acting on their behalf must support scheme change management processes as set out in Section 7.1 of the Rulebook.

Intermediaries and any 3rd parties acting on their behalf must support incident management best practices as described in Annex. C.3.

5.6.4. Integrity requirements

Intermediaries and any 3rd parties acting on their behalf must comply with technical standards which include non-repudiation and anti-replay capabilities. The same requirement applies to all components operated by intermediaries and any 3rd parties acting on their behalf.

The requirements include transaction recovery capabilities such as support of audit trails to reconstruct user activities, to identify exceptions or information security events.

1122 Specific integrity metrics are described in Annex C.1.

1123 6. Risk management

1124 Will be further detailed in next iterations of the Rulebook.

1125

1126 7. Scheme management

1127 Will be further detailed in next iterations of the Rulebook.

1128

1129 8. Defined terms and abbreviations

1130

1131 *Terms marked with an asterix indicate Rulebook specific definitions, currently being aligned
1132 with the formal digital euro glossary.

| Term | Definition |
|---------------------|---|
| Digital euro | The digital form of the single currency available to natural and legal persons. |
| Acceptance solution | A combination of a device for business digital euro users (e.g. a terminal at the POS), a user interface (e.g. a payment application) and a communication technology (e.g. quick response (QR) code-based payment or near field communication (NFC)), together supporting the exchange of payment transaction information between payer and payee for payment initiation and user authentication. |
| Actor* | A stakeholder in an environment that uses or provides services and can have one or more roles. In the context of the digital euro project, the main actors in a retail CBDC environment are end users, (supervised) intermediaries and the central bank. |
| Access management | Services offered by payment service providers (PSPs) enabling digital euro users to hold digital euro and conduct transactions. These services include the opening of digital euro payment accounts, |

| Term | Definition |
|--|--|
| | managing aliases, configuring a waterfall account and providing form factors or acceptance solutions. |
| Access manager | A payment service provider (PSP) 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. |
| Account information service | An online service to provide consolidated information on one or more payment accounts held by the payment service user with one or more payment service provider (PSP). |
| Account information service provider(AISP) | A payment service provider (PSP) pursuing account information services. |
| Account portability | <p>Upon a digital euro user's request, transferring from one payment service provider (PSP) 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.</p> <p>This process is also known as 'switching'.</p> |
| Acquiring of payment transactions | A payment service provided by a payment service provider (PSP) contracting with a payee to accept and process payment transactions, which results in a transfer of funds to the payee. |
| Alias | A unique pseudonymous identifier, such as the digital euro payment account number, which is unique to a given digital euro payment account, used to protect user's identity when processing digital euro payments that can only be attributable to an identifiable natural or |

| Term | Definition |
|-------------------------|---|
| | legal person by the payment service provider (PSP) distributing the digital euro or by the digital euro user. |
| Alias look-up service | A service that stores digital euro users' aliases and connects them to the respective access manager identifier and DEAN. The service enables this information to be looked up when a payment is initiated, thus enhancing usability and the digital euro user's payment experience. |
| Anonymity | A situation in which no personal data (i.e. data relating to an identified or identifiable living individual user) are used. |
| Assisted use | Any situation in which a digital euro user accesses digital euro services via an access manager and receives additional support, e.g. by interactions with the access manager's staff in one of its branches or using its telephone service as well as systems mimicking human interaction. |
| Authentication | A procedure which allows the payment service provider (PSP) to verify the identity of a payment service user or the validity of the use of a specific payment instrument, including the use of the user's personalised security credentials. |
| Authorisation* | The process of ensuring that an authenticated individual or entity has the permission to conduct certain activities. |
| Back-end infrastructure | All hardware and software components (e.g. servers, applications) necessary for recording of digital euro holdings and processing of digital euro payment transactions. The infrastructure interacts with front-end services or other back-end infrastructures via defined interfaces. Its functions include processing payment instructions and storing data on updated digital euro holdings. |
| Business user | A natural or legal person allowed to open multiple digital euro accounts, each with a holding capacity of zero. Payments received on the digital euro account(s) are immediately transformed into private |

| Term | Definition |
|---|--|
| | money (waterfall) as soon as technically feasible and refunds made from the digital euro account(s) are instantly funded from private money (reverse waterfall). |
| Business-to-business (B2B) payment | A payment from one business digital euro user to another. |
| Central bank money (CeBM)* | Central bank liabilities, in the form of either banknotes, bank reserves or digital euro held at the Eurosystem. |
| Chip* | The physical microchip embedded on smart cards used for contact payments |
| Conditional payments | A digital euro payment transaction which is instructed automatically upon fulfilment of pre-defined conditions agreed by the payer and by the payee. |
| Confidentiality | An obligation enforced through a set of rules and operational measures which restricts the accessibility and interpretable 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 support terrorist acts or organisations. As a minimum, the check includes customer due diligence and the monitoring, detection and reporting of suspicious transactions. |
| Credit institution | An undertaking the business of which is to take deposits or other repayable funds from the public and grant credits for its own account, as defined in Article 4(1), point (1), of Regulation (EU) No 575/2013 of the European Parliament and of the Council. |
| Credit Memorandum Balance (CMB) | A limit defined by the holder of a dedicated cash account (DCA) on the usage of the liquidity of that dedicated cash account (DCA) by an access manager. The number of credit memorandum balances defined for a given dedicated cash account (DCA) is unlimited. |

| Term | Definition |
|------------------------------------|---|
| Customer Due Diligence (CDD) | A process to obtain sufficient knowledge of digital euro users (e.g. via know your customer (KYC)) enabling obliged entities to determine the money laundering and terrorist financing risks of digital euro user relationships or transactions. |
| Customer-to-business (C2B) payment | A payment from an individual user to a business user. Typical C2B payments include point-of-sale (POS) payments in shops and e-commerce payments over the internet. |
| Dedicated Cash Account (DCA) | An account in central bank money, owned and used by a PSP (i.e. DCA holder) for the purpose of enabling digital euro funding and defunding requests at the request and on behalf of digital euro users. |
| DCA Holder | A PSP which owns one or multiple dedicated cash accounts (DCA) in the digital euro service platform (DESP). |
| Defunding | The process of reducing a digital euro user's digital euro holdings in their account or device through digital euro redemption, in combination with an increase of digital euro user's private money or an increase in the digital euro user's cash holdings. See funding and waterfall approach.. |
| De-tokenisation | A process of retrieving transaction-related data and/or other sensitive data based on surrogate value, referred to as token. |
| Device | A piece of equipment attributed to an end user digital euro user that could be used for authorising digital euro transactions and user authentication. Examples include smartphones, wearables, and cards. |
| Digital euro account number (DEAN) | The compulsory unique identifier of a digital euro account. |
| Digital euro payment | A transfer of digital euro between digital euro users. |

| Term | Definition |
|--------------------------------------|--|
| Digital euro payment account | An account held by one or more digital euro users with a payment service provider (PSP) to access digital euro recorded in the digital euro settlement infrastructure to initiate or receive digital euro payment transactions, irrespective of technology and data structure. |
| Digital euro payment scheme | A single set of rules, practices, standards and / or implementation guidelines for the execution of digital euro transactions and which is separated from any infrastructure or payment system that supports its operation, and includes any specific decision-making body, organisation or entity accountable for the functioning of the scheme. |
| Digital euro service | A payment service or other service accessible to a digital euro user in a digital euro environment. |
| Digital euro service platform (DESP) | A technical platform enabling the issuance and redemption of digital euro and providing functions (e.g., settlement) that cannot be accomplished by an individual intermediary on its own. |
| Digital euro wallet | A service that enables digital euro users to initiate digital euro transactions by storing secure information related the digital euro holdings of a digital euro user, which are either with the Eurosystem or local in an offline digital euro device. |
| Digital operational resilience | The ability of a financial entity to build, assure and review its operational integrity and reliability by ensuring, either directly or indirectly through the use of services provided by ICT third-party service providers, the full range of ICT-related capabilities needed to address the security of the network and information systems which a financial entity uses, and which support the continued provision of financial services and their quality, including throughout disruptions, as defined in article 3, point (1), of the Regulation (EU) 2022/2554 of the European Parliament and of the Council. |

| Term | Definition |
|------------------------------------|---|
| Direct access | A type of access to a retail central bank digital currency (rCBDC) for which the central bank provides onboarding, distribution and settlement services directly to digital euro users. |
| Distributed system | An infrastructure where multiple independent components appear as a single coherent unit to its users, which requires these components to collaborate on their tasks, typically via the exchange of messages over a network. These components can be made redundant and/or be separated geographically to increase performance, scalability, availability and/or resilience, e.g. to avoid single points of failure or to mitigate geographic concentration risks. The components can be operated either by a single entity or multiple entities –. |
| Distribution of digital euro* | A process of transferring digital euro to digital euro users' accounts or devices through the processes of digital euro issuance and funding. |
| E-commerce payment | An electronic payment between two digital euro users for the purchase of goods or services via the internet. |
| 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. |
| Electronic money institution (EMI) | A legal person that has been granted authorisation, to issue electronic money. |
| Entries | Recordings in back-end infrastructure representing the holdings that are available to a digital euro user. |
| Environment | A combination of IT platforms, actors and their roles that enables digital euro services to be provided to digital euro users in accordance with the relevant legal framework and technical documentation. |
| European Data Protection | Representatives in the EU (with regard to obligations under the General Data Protection Regulation) of non-EU firms which act as |

| Term | Definition |
|--|---|
| Representatives (EUDPR) | 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. |
| Form factor | A combination of a device from an individual digital euro user (e.g. mobile device, physical card), a digital euro user interface (e.g. a payment application) and a communication technology (e.g. Quick response (QR) code-based payment or near field communication (NFC)), together supporting the exchange of payment information between payer and payee for payment initiation and authentication. |
| Front-end layer* | All elements (applications, components, schemes, software, devices, etc.) necessary to provide a service to end users. The front-end layer interacts via defined interfaces with back-end services. |
| Funding | The process of increasing a digital euro user's holdings in their account or device through digital euro issuance, in combination with a reduction of another liquidity source from the digital euro user (e.g., cash or private money). See defunding and reverse waterfall approach. |
| Government or other public authorities | Public authorities allowed to open multiple digital euro accounts, each with a holding capacity of zero. Payments received on the digital euro account(s) are immediately transformed into private money (waterfall) and refunds made from the digital euro account(s) are instantly funded from private money (reverse waterfall). |
| Government-to-person or business (G2X) Payment | A payment from a government or other public authorities to an individual user or business user (e.g. subsidies and rebates). |
| Hashing | Hashing is a computational one-way operation that transforms a string of characters into a fixed size output string from which it is not |

| Term | Definition |
|--------------------------|---|
| | possible to re-construct the original input. It is used to verify the integrity of data without revealing it. |
| Holdings | An amount of digital euro available to a digital euro user. Holdings may be accessed by digital euro users under their contractual relationship with digital euro payment service providers (PSPs). The holdings increase or decrease as the result of a successful payment, funding or defunding operation |
| Identification | The process of determining an individual user's, business user's, government or other public authorities' identity. |
| Individual holding limit | The maximum amount of digital euro that can be held by each digital euro user. |
| Individual user | A natural person who is allowed to open a digital euro account on which to hold digital euro, subject to certain holding limits. |
| Initiation channel | Technological means through which a payment can be initiated and verified by a payment service provider (PSP). This differs based on the type of payment environment, particularly remote payments versus proximity. |
| Instructing party | An intermediary or third entity acting on behalf of an intermediary that can instruct digital euro transactions and receive notifications and reports sent by the digital euro service platform (DESP). See access manager. |
| Instruction | An order issued by a digital euro user to its payment service provider (PSP). |
| Intermediated access | A type of access to a retail central bank currency (rCBDC) in which the central bank does not interact directly with digital euro users but relies on intermediaries to provide onboarding, authentication, distribution or other payment services. |

| Term | Definition |
|----------------------------------|--|
| Interoperability | The use of common rules, standards and processes across different payment services. |
| Inter-PSP fee | A fee paid for each transaction directly or indirectly (i.e. through a third party) by the payment service provider (PSP) involved in acquiring digital euro to the payment service provider (PSP) involved in distributing digital euro. The net compensation or other agreed compensation is part of the inter-PSP fee. |
| Issuance of digital euro | A process which results in the creation of digital euro units on the Eurosystem's balance sheet and the redemption of central bank reserves. |
| Know-your - customer (KYC) check | A check aimed at identifying digital euro users and risks attached to providing services to them. The check is also aimed at ensuring that these services are used in line with intermediaries' expectations and for legitimate purposes. See customer due diligence (CDD). |
| Legal tender | The mandatory acceptance of a means of payment, at full face value, with the power to discharge from a payment obligation. |
| Liquidity management | The processes to support the distribution of the digital euro, i.e., liquidity transfer and funding/defunding. |
| Liquidity transfer | The process to move central bank reserves between a payment service provider's (PSP) main central bank reserves and central bank reserves dedicated for the use in the digital euro environment. It is executed upon request by payment service providers (PSP) to satisfy the expected demand from digital euro users controlled and performed by the Eurosystem. |
| M-commerce* | A virtual location at which goods and services are sold and paid for, accessed through a mobile app. |
| Merchant | A business user providing products or services to individual users in exchange for payment in digital euro. |

| Term | Definition |
|--|--|
| 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 | <p>A fee paid by the payee to the acquirer in relation to card-based payment transactions as defined in point (12) of article 2 of Regulation (EU) 2015/751 of the European Parliament and the Council.</p> <p>In the context of the digital euro, a merchant service charge is interpreted as a fee paid by the payee to the payment service provider (PSP) acquiring a digital euro payment transaction.</p> |
| National Central Bank (NCB) | A national central bank of a European Union Member State whose currency is the euro. |
| Near field communication (NFC) - based payments* | A payment made with a short-range wireless (frequently referred to as contactless) connectivity technology that enables communication between devices when in proximity. |
| Offboarding of a digital euro user* | A set of activities conducted by the access manager to revoke the possibility of an end user to hold digital euros and pay. |
| Offboarding of a PSP | A set of activities conducted by a back-end infrastructure operator to revoke a payment service provider's access to the infrastructure. |
| Offline payment | A payment in which authorisation and settlement takes place between payer's and payee's devices, without the need for any connection to the internet or other computer network and therefore only in physical proximity. |
| Offline digital euro device | A combination of hardware and software that allows a digital euro user to pay offline with offline holdings that are stored on the digital euro user's device, without the intervention of a third party. |
| Onboarding of a digital euro user* | A set of activities conducted by the access manager to enable an end user to hold digital euros and pay. |

| Term | Definition |
|-----------------------------|---|
| Onboarding of a PSP | A set of activities conducted by a back-end infrastructure operator to enable a payment service provider to access the infrastructure. |
| Online payment | A payment in which settlement requires that at least one of the payer or the payee is connected to a network. A third-party validated solution is considered in the current project. |
| Operator | An entity operating one or more digital euro services, e.g. a alias lookup service or an onboarding repository service. |
| Pay-by-link* | Pay-by-link is an online payment method in which a payee generates a payment request link and sends it to the payer via a communication channels (e.g. email, SMS, WhatsApp). Subsequently, the payer receives the link, clicks or taps on it, and is then directed to a page on which payers selects their intermediary and authenticate with their intermediary to authorize the payment. |
| Payee | A natural or legal person who is the intended recipient of funds which have been the subject of a payment transaction. |
| Payee-initiated transaction | A transaction involving an instruction from a payee to a payment service provider (PSP) to debit a payer. |
| Payer | A natural or legal person who holds a payment account and allows a payment order from that payment account, or, where there is no payment account, a natural or legal person who gives a payment order. |
| Payer-initiated transaction | A transaction involving an instruction from a payer to a payment service provider (PSP) to credit a payee. |
| Payment account | An account held in the name of one or more payment service users which is used for the execution of payment transactions. |
| Payment authorisation | The consent given by a payer, or a third party acting on behalf of the payer, to pay. |

| Term | Definition |
|--|---|
| Payment initiation | A legal person that has been granted authorisation in accordance with Article 11 of Regulation (EU) No 2015/2366 of the European Parliament and of the Council to provide payment services throughout the European Union. |
| 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 (PSP). |
| Payment initiation service provider (PISP) | A payment service provider (PSP) pursuing payment initiation services. |
| Payment instrument | <p>A personalised device(s) and/or set of procedures agreed between the payment service user and the payment service provider (PSP) and used in order to initiate a payment order.</p> <p>Examples of electronic payment instruments include payment cards, credit transfers and direct debits.</p> |
| 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. |
| Peer-to-peer validated digital euro* | A digital euro payment solution in which a payment between a payer and payee does not require validation by a third party. |
| Person or business-to-government (X2G) payment | A payment from an individual user (or a business user) to a government or other public authorities (e.g. payments of taxes, . duties and fines). |
| Personal data | Any information relating to an identified or identifiable living person, individual user or business user. |

| Term | Definition |
|---------------------------------------|--|
| Person-to-person (P2P) payment | A payment from one individual user to another. |
| Point of interaction (POI) | A physical premise (point-of-sale) or virtual space (e.g., eCommerce and mCommerce) of the merchant at which the payment transaction is initiated. |
| Point of sale (POS) | The address of the physical premises of the merchant at which the payment transaction is initiated. |
| PSP identifier | An identifier used to uniquely identify an payment service provider (PSP) in the digital euro service platform (DESP). |
| PSP mapping | A process of linking a digital euro user's digital euro account number (DEAN) and (if applicable) other aliases to the corresponding PSP identifier to enable forwarding of payment data between involved payment service providers (PSPs). |
| PSP reference data | A set of information of a payment service provider (PSP) that are relevant for establishing a contractual relationship with the Eurosystem, for connecting to the digital euro service platform and for the services it provides (e.g., intermediary type, name, address, contact persons, roles in the system, dedicated cash account, status). |
| Private money | Money issued by a private entity. |
| Quick reponse (QR) code-based payment | Payment initiated via the use of a two-dimensional matrix barcode in the form of a machine-readable optical label with digital information, shared between payer and payee . . |
| 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. |

| Term | Definition |
|--------------------------------------|--|
| Recovery time objective (RTO) | The maximum tolerable amount of time required to restore one or more applications and associated data back to a correct operational state after a failure or disaster event has compromised its availability. |
| 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. |
| Request to pay* | Request to pay is a way to request a payment initiation. The payee fills the details including the amount and sends it via the payers intermediary to the payer, who can reject the request or approve the payment. |
| Reverse waterfall | A method for facilitating the use of a digital euro whereby private money from a linked liquidity source chosen by a digital euro user (e.g. a private money account) is automatically converted into digital euro when the digital euro user's digital euro holdings are not sufficient to make a payment. See waterfall approach and funding. |
| Secure element (SE) | A tamper-proof chip with pre-installed software that can store confidential and cryptographic data and run secure applications. |
| Settlement | The completion of a payment with the aim of discharging digital euro users' obligations. |
| 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. |
| Technical proof | A cryptographic proof or authority, over entries (holdings) or identity in the digital euro settlement infrastructure. |

| Term | Definition |
|-------------------------------------|---|
| Third party entity | An entity which provides communication and interaction services with the digital euro service platform to the intermediaries without having a contractual relationship with the Eurosystem. |
| Third-party validated digital euro | A solution in which a third party determines the validity of a transaction between payer and payee. |
| Token | A substitute value which replaces payment account reference, end-user identification data, or potentially transaction related data. |
| Tokenisation | A process of substituting transaction-related data and/or other sensitive data based on a surrogate value, referred to as a token. |
| Transaction | A transaction could be a payment or a funding or a defunding, or a reservation or a combination of the previous (e.g., a payment that requires a defunding). |
| Transaction management | Services offered by intermediaries to digital euro users related to the administration and processing of transactions. |
| Transaction identifier | A unique identifier for a digital euro transaction. |
| Trusted execution environment (TEE) | An isolated processing environment that ensures (i) the integrity and confidentiality of the data that is being processed and (ii) the authenticity of the software/application running on it. |
| User to application (U2A) interface | An interface suitable for human interaction to permit the exchange of information between software applications of a retail central bank digital currency and a digital euro user through a graphical user interface. |
| 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. |

| Term | Definition |
|-------------------------------|--|
| Validation of a transaction | A process of checking at the level of payment service providers (PSPs) to ensure that the payer is entitled to make a payment, or that the payment fulfils all technical standards. |
| Verification of a transaction | A set of processes to check the availability of the payer's holdings and perform any other task that may be necessary for the verifying entity, or entities, to assess whether the transaction can be settled. |
| Waterfall approach | A method for facilitating the use of a digital euro by automatically converting the amount of digital euro that exceeds a defined holding threshold into private money, in a linked liquidity source chosen by the digital euro user such as a private money account. See reverse waterfall approach and defunding. |

Annex A Functional and operational model

A.1 Illustrative user Journeys

Please refer to separate document.

A.2 E2E Flows

Please refer to separate document.

A.3 Data management

Will be further detailed in next iterations of the Rulebook

A.4 Illustrative user products

Will be further detailed in next iterations of the Rulebook.

A.5 Branding standards

Will be further detailed in next iterations of the Rulebook.

A.6 Limits and thresholds

Will be further detailed in next iterations of the Rulebook.

Annex B Adherence model

B.1 Adherence agreement and related documents

Will be further detailed in next iterations of the Rulebook.

B.2 Onboarding document and toolkit

Will be further detailed in next iterations of the Rulebook.

B.3 Approval framework

Will be further detailed in next iterations of the Rulebook.

B.4 Certification and testing ecosystem

Will be further detailed in next iterations of the Rulebook.

B.5 Dispute Management

Will be further detailed in next iterations of the Rulebook.

Annex C Technical Scheme Requirements

C.1 Service Level Requirements and Key Performance Indicators

Will be further detailed in next iterations of the Rulebook.

C.2 Reporting requirements and guidelines

Will be further detailed in next iterations of the Rulebook.

C.3 Incident management, disaster recovery, and business continuity management

Will be further detailed in next iterations of the Rulebook.

C.4 Dispute Handling

Will be further detailed in next iterations of the Rulebook.

Annex D Risk Management

Possible placeholder

Annex E Scheme Management

Possible placeholder

Annex F Scheme compatibility and interoperability

F.1 Fee table

Possible placeholder

F.2 Scheme compatibility and interoperability

Possible placeholder

Annex G Implementation specifications

G.7 Implementation specifications and technical standards

G.7.1 Individual and business users

Implementation specifications will be further detailed in next iterations of the Rulebook.

G.7.2 Between individual users

Implementation specifications will be further detailed in next iterations of the Rulebook.

G.7.3 Individual users and PSPs

Implementation specifications will be further detailed in next iterations of the Rulebook.

G.7.4 Business users and PSPs

Implementation specifications will be further detailed in next iterations of the Rulebook.

Annex H Enforcement model

H.1.1 Enforcement model