EUROPEAN CENTRAL BANK

EUROSYSTEM

Annex 1: Functional and non-functional requirements linked to the market research for a potential digital euro implementation

13 January 2023

Table of contents

0. Preface

This annex provides further details on the design of a potential digital euro. It starts with an introduction highlighting the preliminary design decisions taken so far. Chapter 2 explains the different actors in the environment and then goes into further details of the digital euro components (functions that cannot be performed by intermediaries on their own) and describes the overarching non-functional requirements. Chapter 3 details the end-to-end flows for different use cases to illustrate the interactions between actors and the digital euro components, while Chapter 4 outlines the functional map and the subfunctions performed by the intermediaries and the Eurosystem. Chapter 5 sets out a high-level design of the components and their interactions, while Chapter 6 details the components of this market research. The design illustrated in this market research is subject to change and interactions between components are yet to be finalised. In that spirit, respondents are free to suggest alternative interactions between components if deemed relevant.

1. Introduction

A digital euro would be issued by the Eurosystem to allow end users (individuals, businesses and public institutions) to make and receive payments electronically. While a digital euro would be central bank money and hence risk-free, exactly like cash, its electronic format requires the development of technical components enabling, among other things, the issuance and redemption of digital euro; transaction initiation, processing and settlement; user and data management; and all necessary interfaces across the digital euro components and with its users. The Eurosystem will decide in autumn 2023 on the requirements for a digital euro and on a potential project realisation phase, prioritising the use cases of person-to-person payments and payments at the point of interaction (point of sale, e-commerce and with public institutions).[1]

This annex lists a preliminary set of high-level requirements for a digital euro. In this regard, interested market participants are asked to contribute with a view to broadening the Eurosystem's

[1] The launch of a project realisation phase would not prejudge the Eurosystem's decision on whether/when a digital euro might be issued. It is also worth noting that issuance of a digital euro is contingent upon EU legislators passing appropriate legislation.

understanding of the potential design solutions existing in the market, as well as their time to market and related costs.[2]

A digital euro would allow end users of retail payment instruments to access and transfer central bank money in electronic form. Every digital euro will, like cash, always be a central bank liability and will therefore be available to its holders to make and receive payments throughout the euro area. Having digital money issued by the central bank would provide an anchor of stability for the euro area monetary system. A digital euro would also strengthen the monetary sovereignty of the euro area and foster competition and efficiency in the European payments sector. The digital euro project aims at delivering this financial innovation while supporting the role of competitive and efficient payment service providers. The digital euro payment solution will be equally usable throughout the euro area and integrate with existing payment infrastructures and private payment solutions built until now around commercial bank money, while being a sufficiently distinctive payment solution for end users.

Following the Governing Council's preliminary decisions[3], the Eurosystem would:

- Onboard and manage every intermediary who will adhere to the digital euro scheme,
- Perform issuance and redemption of digital euro units,
- Perform the settlement activities of digital euro transactions (verification and recording) and manage the general ledger for all digital euro holdings,
- Allow intermediaries to (i) instruct payments, (ii) send funding and defunding requests, and (iii) query the general ledger on behalf of the end users.

Intermediaries would be responsible for providing user-facing services to end users of the digital euro. Therefore, they would have the following roles:

- End user management: lifecycle management of end users (incl. onboarding and offboarding) and their payment instruments (incl. provision of these instruments);

---

[2] The market research exercise seeks input on the different questions listed in Annex 2. It is not meant to obtain input on the high-level requirements. For what matters requirements, input is received from the market via the stakeholder engagement actions of the digital euro project involving consultations mainly with the Euro Retail Payments Board (ERPB) and the Market Advisory Group (MAG).

[3] See the first (sept. 2022) and the second (dec. 2022) ECB progress report on the investigation phase.

- Liquidity management: initiating funding and defunding of end users' holdings from/to private money or from/to cash;
- Transaction management: initiation, authentication (before every payment), validation, settlement instruction and post-settlement activities.

Personal and transaction data would only be accessible to intermediaries for the purpose of ensuring compliance with anti-money laundering and combating the financing of terrorism (AML/CFT) requirements and all other relevant provisions under EU law. Before transactions can be settled, the consent of the payer needs to be ensured. The intermediary may be required to carry out additional checks by of the payee.

User data obtained by intermediaries during the onboarding process would not be shared with the Eurosystem or other intermediaries, unless in specific cases where this was required by law or necessary to perform digital euro-related tasks.

The Eurosystem will not itself be able to monitor the holdings of any individual or track the transaction history or infer payment patterns of any user. Nonetheless, the Eurosystem should see which intermediaries are responsible for managing which sets of digital euro holdings, while it does not see their breakdown across their end users – leaving the mapping between holdings of digital euro dispersed across different one-time addresses in the general ledger and their holders to the relevant intermediaries providing wallet services.

The payment instruments available to an end user should enable both online and **offline payments** and include a mobile wallet, which the intermediary may integrate with its own app (optionally via a common **SDK**). The end user can decide to access digital euro via the **digital euro app**. Any payment instrument will interact with the systems of the end user's intermediary, which instructs the settlement of transactions in the Eurosystem's settlement component. In doing so, the intermediary could potentially make use of an **alias/proxy lookup service**.

Since excessive reliance on digital euro may have an impact on the financial stability of the euro area financial sector, the Eurosystem will incorporate limit and remuneration-based tools in the design of a digital euro to curb its use as a form of investment. The Eurosystem should as a minimum oversee this by relying on data and business intelligence tools at a more aggregated level.

Whereas intermediaries participating in the digital euro scheme are expected to operate their own systems and apply appropriate fraud and risk management processes, the digital euro scheme might support these with an additional **fraud detection/management** component.

Finally, a digital euro scheme might potentially help intermediaries resolve disputes with the possibility to provide a dedicated **dispute management** component.

2. High-level requirements

Three main groups of actors are involved in the digital euro environment: end users, intermediaries and the Eurosystem:

- **End users**

  An end user is an individual, business or public institutions transacting in digital euro. The end user can act as a payer or payee.

  Any end user interaction with a digital euro is considered one of the core competencies and responsibilities of intermediaries.

- **Intermediaries**

  An intermediary is an entity acting between the Eurosystem and end users. Intermediaries may include entities like credit institutions, electronic money institutions and payment institutions, in line with the definitions under the revised Payment Services Directive (PSD2).

  Each intermediary is responsible for several activities related to its end users, ranging from the onboarding/offboarding of end users and the provision of payment instruments to the (de)funding of accounts/wallets, the authentication of end users and the authorization of transactions.

- **Eurosystem**

  The Eurosystem comprises the European Central Bank (ECB) and the national central banks of those countries that have adopted the euro.

  The Eurosystem is responsible for several activities in the context of a digital euro including issuance and redemption of digital euro as well as settlement verification and recording of transactions.

Digital euro components

For the purposes of this market research, the term "digital euro components" refers to those functions that cannot be accomplished by an individual intermediary on its own, as described below.

When intermediaries onboard end users, a shared **onboarding repository** is used to control the number of accounts/wallets per user so that the number of accounts/wallets allowed per user is not exceeded.

For the purpose of this exercise, it is assumed that intermediaries will make use of a TARGET Dedicated Cash Account (DCA) specifically for digital euro purposes, open under the name of a TARGET participant to enable **(de)funding of end users**' digital euro on a 24/7 basis.

Three main payment use cases have been prioritized for the digital euro: person-to-person and government payments, proximity (POS) payments and remote (e-commerce) payments. When an end user issues a payment request, an intermediary would send a payment instruction to the digital euro service platform, which will then verify the transaction and record it in its ledger, resulting in final and irrevocable **settlement**.

The digital euro should support two transfer mechanisms with two different settlement models in parallel: online instant digital euro settlement and offline instant digital euro settlement. Apart from the dedicated **offline component**, all other components described in this document refer to online digital euro settlement.

Should an end user lack sufficient funds to complete a payment but have configured a link to a commercial bank account, the intermediary would initiate the payment instruction together with the funding instruction to make sure the payment is not rejected due to insufficient balance on the digital euro account/wallet. This scenario is known as a *reverse waterfall*. Should the holding limit of an end user be exceeded, the intermediary would initiate a defunding instruction at later point and defund the amount exceeding the holding limit, to a linked commercial bank account. This scenario is known as a *waterfall*.

Reference data, not including personal data, are needed to support the different functionalities of the digital euro components and would be accessible to intermediaries in a secure manner to help them perform their roles in support of payments in digital euro.

Other digital euro components, such as **dispute management, proxy lookup database and fraud and risk management**, could potentially ensure other functions related to digital euro transactions.

The digital euro components should be capable of offering scalable **performance**. This means that they should provide services to support a specific number of digital euro end users (served by intermediaries), daily digital euro transactions (average and peak) and daily digital euro queries (average and peak). The following table shows assumptions regarding matured volumes for three different uptake scenarios.

Digital euro volumes[4] (millions)		**Scenario**[5]		
		Small	**Medium**	**Large**
End users		30.00	110.00	200.00
Daily transactions[6]	Average	3.75	55.00	175.00
	Peak	37.50	550.00	1750.00
Daily queries[7]	Average	3.75	55.00	175.00
	Peak	37.50	550.00	1750.00

4 For Dispute Management 1% of the assumed volumes, for Digital euro App 10% and for Offline Solution 1%.

5 Volumes are based on two main figures derived from *Study on the payment attitudes of consumers in the euro area (SPACE) 2022*: (i) a population of 280 million (80% of euro area population) and (ii) an average of 2 payments per person per day (across all payment instruments and points of interaction in the euro area). The three scenarios are created on a purely statistical distribution of percentages of these two figures, assuming a user base of 10%, 40% and 70% (of the referred population) and usage of 5%, 20% and 35% (of the referred number of payments per person per day). These scenarios fulfill the purpose of receiving information about how different sized scenarios would influence the proposed solutions.

6 Digital euro transactions (payment, funding, defunding, combined funding and payment transactions); for further details see Settlement component (Section 6.1)

7 Digital euro queries (digital euro holding and digital euro transaction queries requiring real-time data); for further details see Settlement component (Section 6.1)

Regardless of the uptake scenario, the digital euro components should ensure (i) a processing latency for digital euro transactions[8] of one second (for 99% of all processed transactions) in order to support an end-to-end processing latency[9] of three seconds (for 99% of all processed digital euro transactions), and (ii) a processing latency for digital euro queries[10] of 0.5 seconds (for 99% of all processed digital euro queries). Furthermore, the architecture of the digital euro components is required to cope with volumes increasing over time (doubling each year) and to eventually handle the assumed matured volumes indicated for each uptake scenario. The digital euro components should scale horizontally and act elastically to varying volumes, such as seasonal effects, in order to consume the minimum resources possible. In general, the design and architecture of the digital euro components should provide a holistic, **eco-friendly** solution.

The digital euro components should demonstrate a high degree of **reliability** enabling them to be **available 24 hours every day of the year** by ensuring an availability rate of at least 99.99% – allowing for a maximum tolerable downtime of 13.15 minutes – calculated on a quarterly basis. The digital euro components should tolerate hardware and/or software failures so that overall performance and availability is still provided as intended, thus ensuring resilience in the face of component failures and local and regional disasters. Accordingly, the digital euro components should be distributed between at least two operational sites in each geographical region and across at least three geographical regions (defined as at least 500km between two operational sites belonging to different geographical regions). The digital euro components should ensure a

---

8 Processing latency for a digital euro transaction starts at the moment a digital euro transaction message is received at the Access Gateway component – includes the Access Gateway, the Settlement component and potentially the DCA Management component (in case of funding, defunding and combined funding and payment transactions) – and ends again at the Access Gateway component at the moment when a confirmation or rejection is sent to the intermediaries involved. Processing latencies consumed by intermediaries are excluded here as they count towards the end-to-end processing latency (see footnote below).

9 End-to-end processing latency starts at the moment when an intermediary receives a payment, funding or defunding request from an end user – including the processing latency described in the footnote above and therefore also including the reverse waterfall case (via a combined funding and payment transaction) but not including the waterfall case (as this is handled via two separate transactions with a potential time delay) – and ends at the moment when the intermediaries involved send a confirmation or rejection to the payer and payee.

10 Processing latency for a digital euro query starts at the moment a digital euro query message is received at the Access Gateway component – includes the Access Gateway and the Settlement component – and ends again at the Access Gateway component at the moment when the result is sent to the requesting intermediary.

Recovery Point Objective value of zero and a Recovery Time Objective of 45 seconds, even if a switchover to another operational site is required. The digital euro components should rely only on proven technologies (assessed using the European Commission's Technology Readiness Levels framework) and withstand attacks by malicious actors.

The digital euro will be trusted by end users and protect their privacy. Its components should support **end user privacy** by applying privacy-enhancing techniques, like information segregation, unlinking and hiding. They should facilitate unlinking between end user information and the data used in, and/or the payment patterns resulting from, end users' digital euro interactions. The digital euro components should enable end users to prove their access to digital euro holdings regardless of their selected intermediary in order to enhance portability by making it easy for end users to switch between different intermediaries even in emergency scenarios in which the current intermediary becomes unavailable.

The digital euro components should comply with the requirements resulting from a **security and cyber resilience** assessment. They should guarantee and maintain the integrity and confidentiality of managed data, using data encryption, digital signatures and/or physical safety measures, for instance. The digital euro components should ensure a secure audit trail for actions initiated by a user or a component (including manual entries, data queries, etc.). They should ensure the (legal) archiving of data over defined retention periods and process, store and archive such data within the euro area. The digital euro components should be designed so that it is possible to upgrade cryptographic primitives and algorithms while minimizing architectural impact, maintenance costs and operational downtime, with a view to ensure quantum-resistance.

The digital euro components should support **compatibility** by being network provider agnostic, interoperable and backwards-compatible with external components. They should do so by relying on open standards and protocols as well as best practices for interfacing. The digital euro components should support **maintainability** by applying best practices regarding modularity, reusability, modifiability, testability, future-proof concepts and IT service management. The digital euro components should be supported by an operator for responding to any operational or technical issue concerning the digital euro components raised by the Eurosystem or the intermediaries. The digital euro components should be supported by monitoring and alerting tools.

To **support a structured development and testing lifecycle**, the digital euro components should be available in **multiple environments**. In addition to the production environment, this comprises at least one development environment, one continuous integration testing environment, two pre-

production environments for testing with third parties (one for fixing urgent errors and one for longer time testing of new functionalities), both of which replicate the geographically distributed set-up of the production environment. Additionally, the two pre-production environments should permanently support a minimum capacity (in terms of assumed volumes for the production environment) of 10% but should be capable of periodically – multiple times per year – handling non-functional testing (performance, load, penetration, scalability) at full capacity for the planned duration of the testing. Respondents should consider the environment requirements in their cost estimations.

3. End-to-end flows

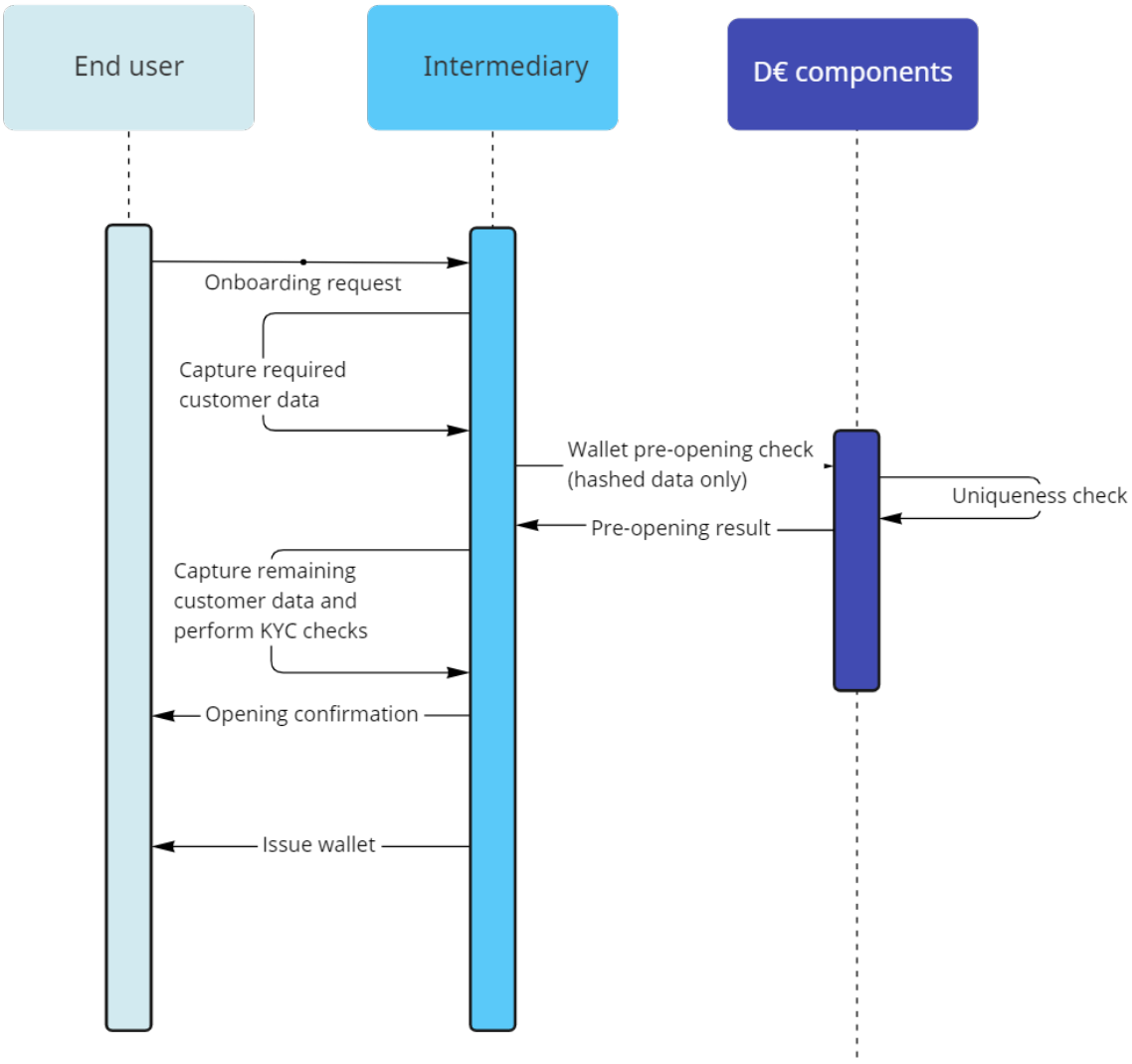
This chapter presents **high-level flow charts** to facilitate a better understanding of the flows considered:

- End user onboarding, including validation of the number of digital euro accounts/wallets based on hash values;
- funding and defunding operations, including automated waterfall considerations;
- transaction initiation, reflecting different flows depending on form factors supporting the three main use cases: person-to-person and government payments, proximity point of Sale (POS) payments and remote (e-commerce) payments;
- payment flow options, either payer- or payee-initiated.

The flows described below are for illustrative purposes only. They may be affected by design decisions yet to be made. Market participants may also suggest alternative flows.

End user onboarding

- Onboarding of end users is the responsibility of intermediaries.
- The digital euro components support the process by verifying whether the end user already has a digital euro holding, using a hash value derived from predefined end user data (e.g. national ID). This process helps to keep a check on that end users do not exceed the number of digital euro accounts/wallets per user.
- Depending on the internal processes of the intermediary, and the customer status prior to the onboarding to digital euro, the pre-opening check might be initiated
    - without capturing none, or limited, additional data, for existing customers of that intermediary,
    - after partial data capture sufficient to support the pre-check before the KYC process continues or
    - after the completion of the KYC process.

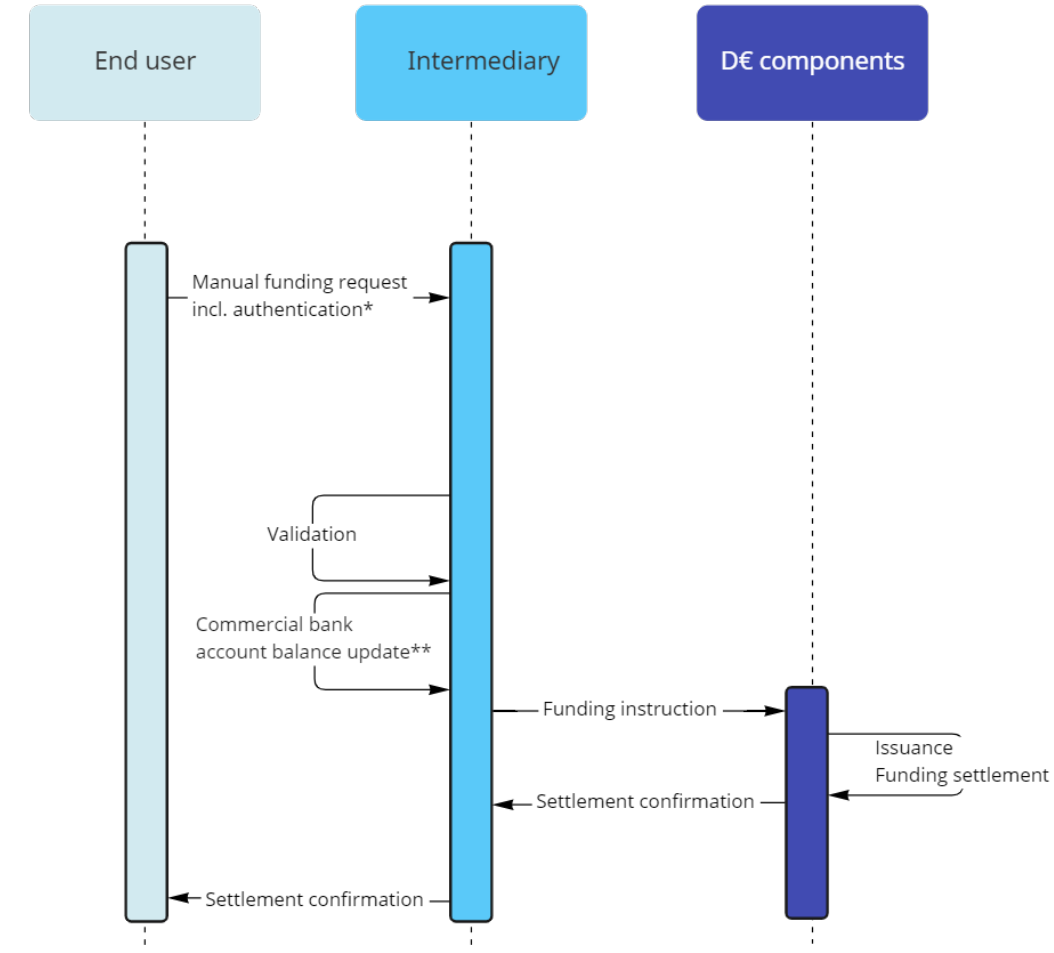


Funding/defunding

- Intermediary establishes processes to help end users fund or defund their wallets.
- Funding and defunding can be done from/to a commercial bank account or cash (e.g. at ATMs).
- Intermediaries should offer manual and automated funding/defunding functionalities – Automated functionalities would be activated at the end user's choice in case a linked liquidity source like commercial bank 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).

- In addition, there are automated defunding related to payments – waterfall, in case the holding limit is exceeded – and automated funding – reverse waterfall, to automatically load the digital euro account/wallet to allow the payment to be processed.
- Automated (de-)funding does not require and additional end user authentication for the specific automated (de-)funding occurrence.
- During the funding process intermediary's central bank money holdings are converted into digital euro (digital euro issuance) reducing intermediary's central bank money balance and crediting the end user. For defunding the opposite process applies.

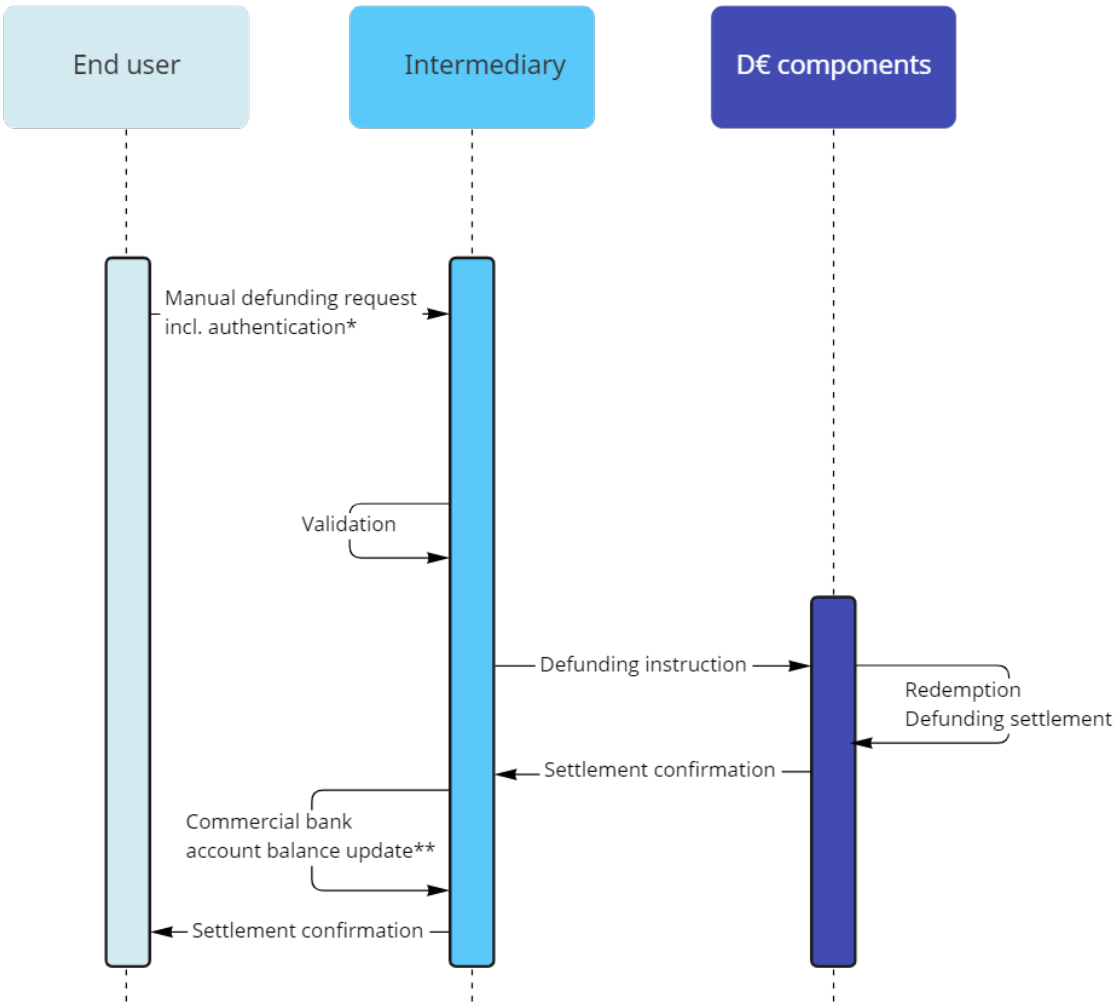
Funding



* For automated funding there is no end user authentication and the funding request is not initiated by end user

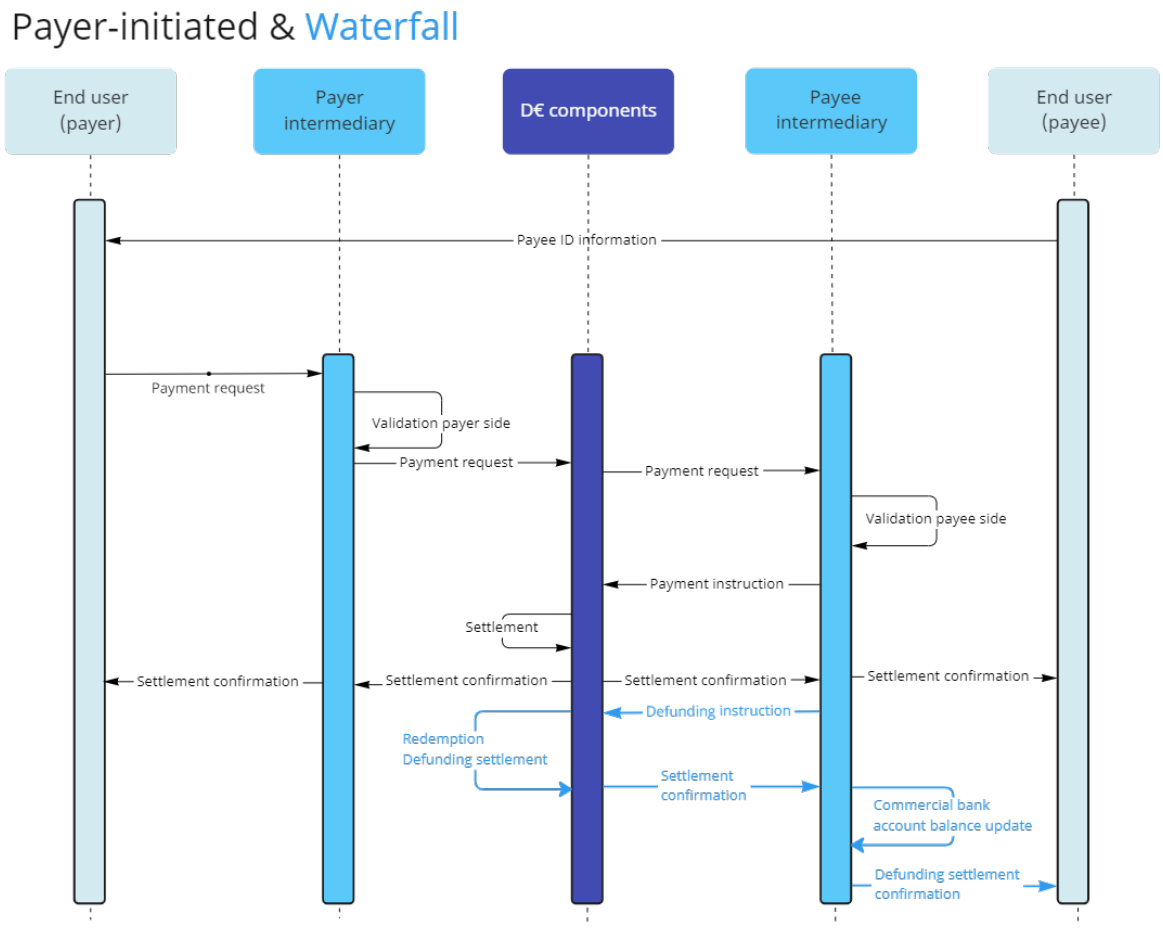
** Does not apply to funding from cash

Defunding



* For automated defunding there is no end user authentication and the defunding request is not initiated by end user

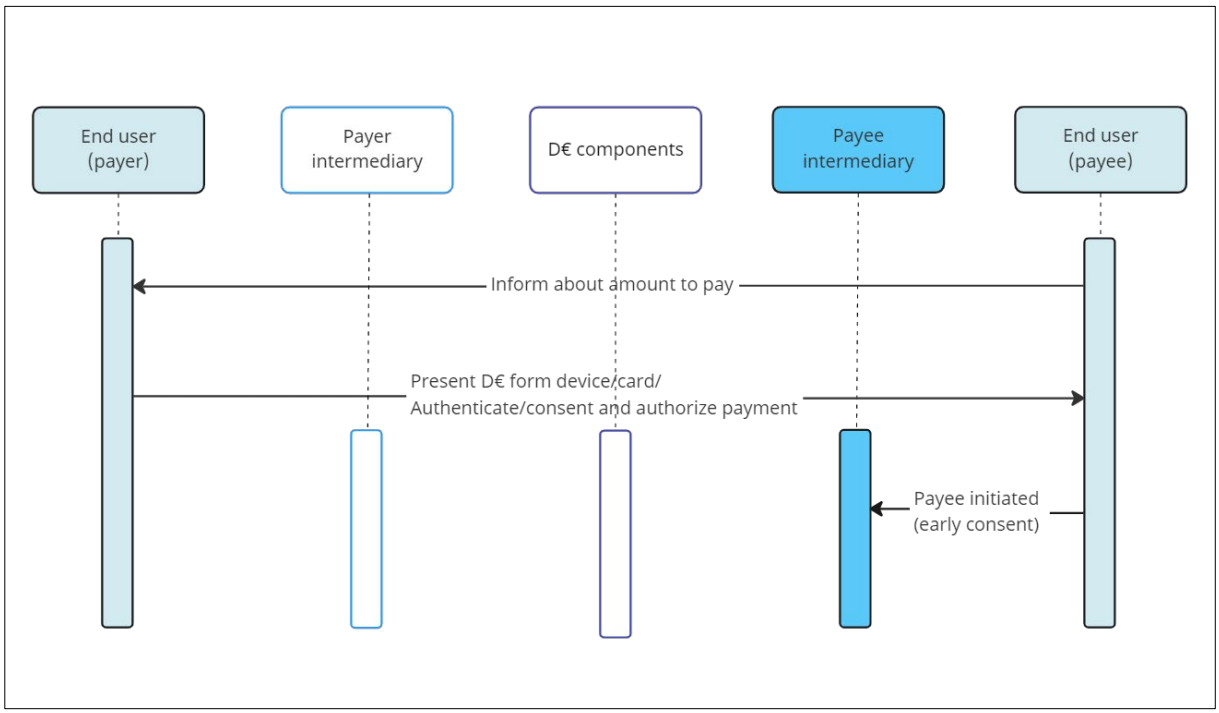
** Does not apply to defunding to cash



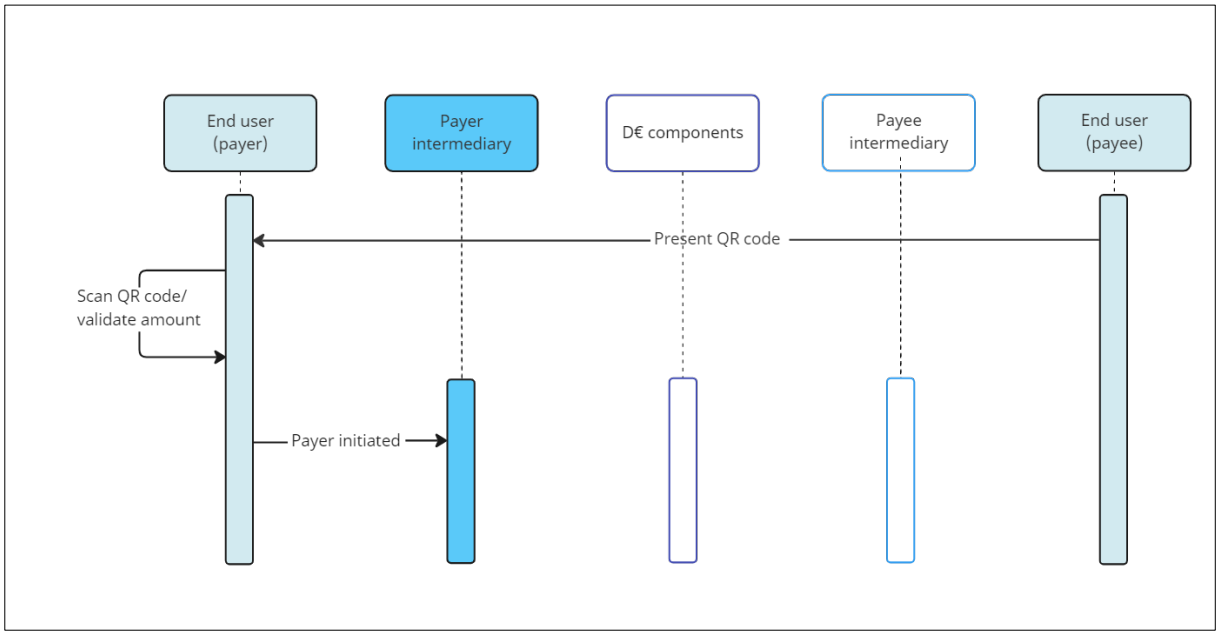
Transaction initiation

Three main use cases have been identified for the digital euro: person-to-person, government payments, proximity point of Sale (POS) payments and remote (e-commerce) payments. Depending on the use case, there are different ways of initiating digital euro payments, in line with the choice of form factor. The three flows shown below only depict transaction initiation using a different form factor. After transaction initiation, the flow continues using either the payer-initiated or the payee-initiated payment flows described in the next section.

POS using NFC

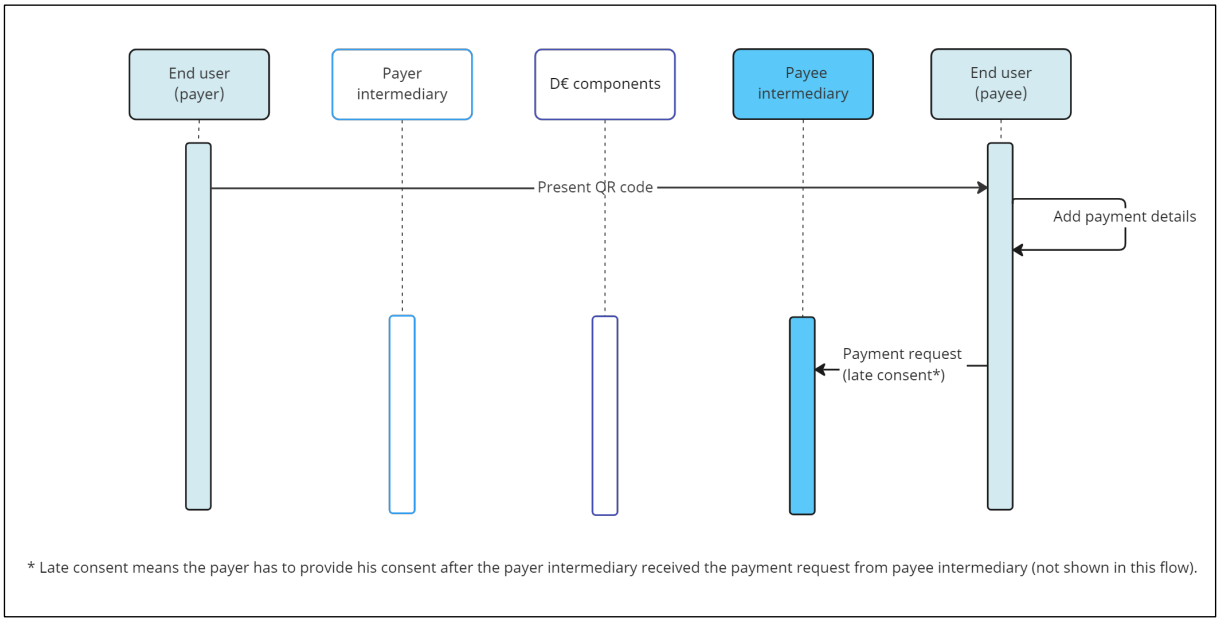


Merchant-presented QR code



The payee can either present a static QR code or a dynamic QR code. In case the QR code does not contain the amount, the payer should enter the amount and then validate, authenticate, and initiate the transaction.

Consumer-presented QR code

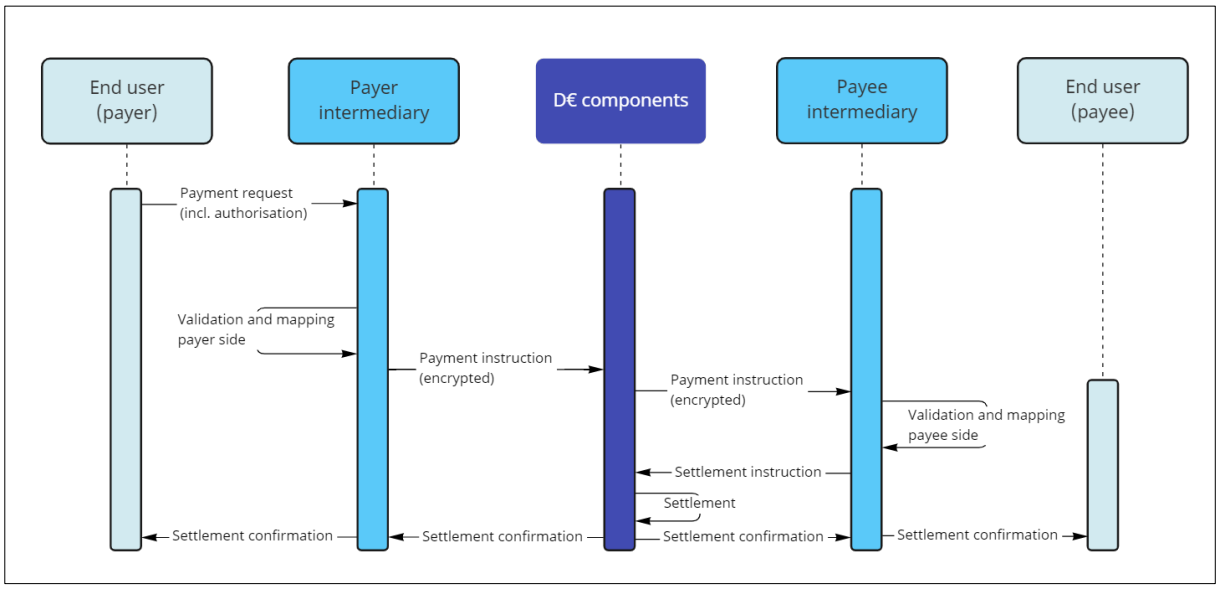


Payments

Depending on the use case, transactions can be initiated by either the payer or the payee. Both intermediaries (the payer's and the payee's) should validate the transaction. Depending on the final design, any private data that may be present and are not required for settlement should be encrypted.

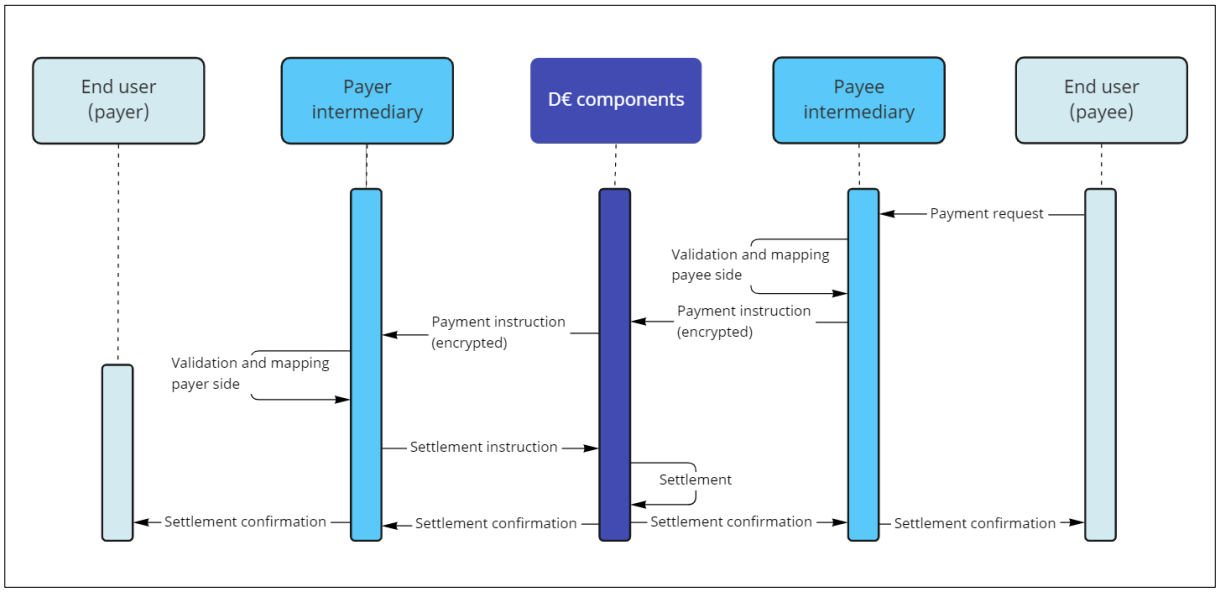
Payer-initiated

Flow representing the interaction with digital euro components after the transaction initiation process has been completed for a payer-initiated transaction:



Payee-initiated

Flow representing the interaction with digital euro components after the transaction initiation process has been completed for a payee-initiated transaction:

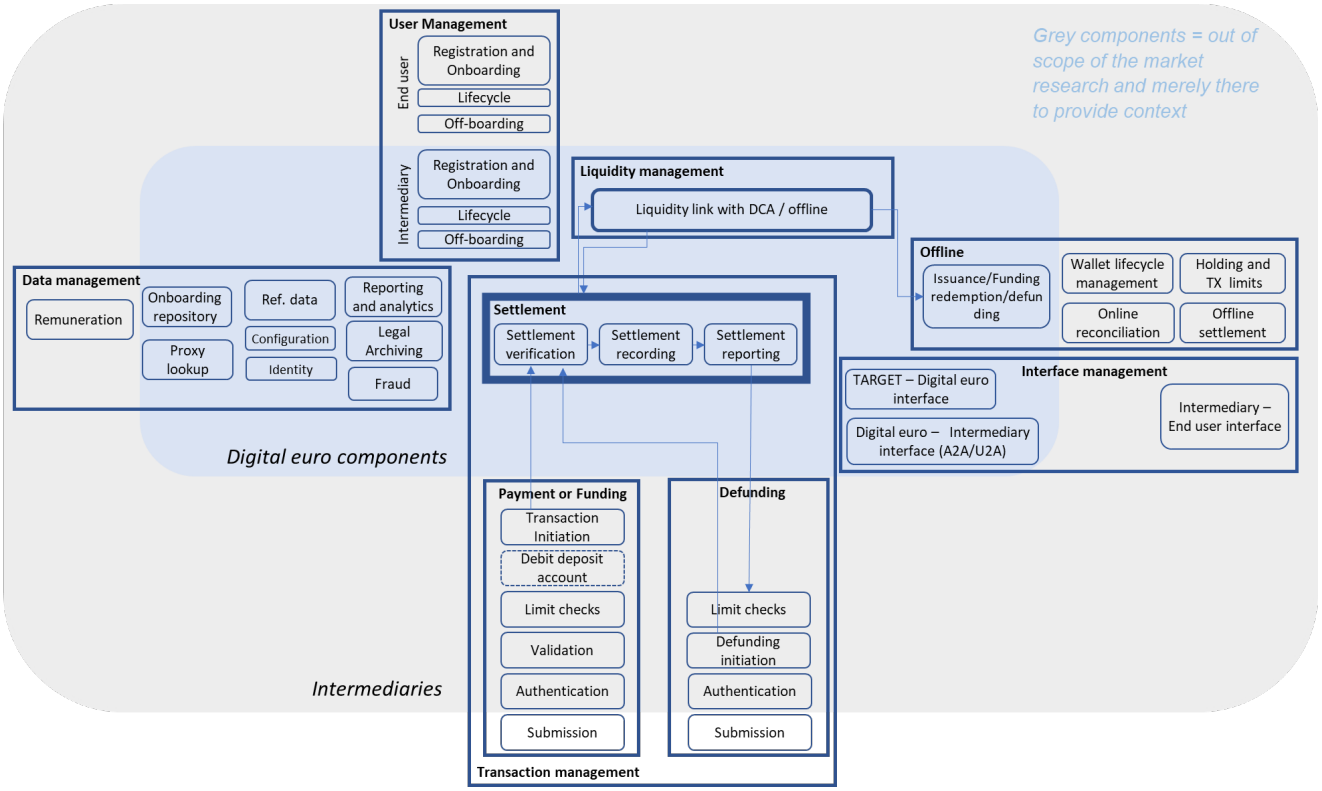


4. High-level functional map

The following function groups have been identified for the overall design of the digital euro environment. Some functions are fully managed by the digital euro components while others are performed jointly by the components and the intermediaries. The list of subfunctions performed solely by intermediaries is not exhaustive and would be defined as part of the digital euro scheme.

- Onboarding, lifecycle management and offboarding of users and intermediaries (**user management**).
- Management of liquidity transfers received and sent between TARGET Services and the digital euro components (**liquidity management**).
- Processing of digital euro transactions, including payments between end users, funding/defunding, waterfall (payment + defunding) and reverse waterfall (funding + payment) transactions (**transaction management**).
- Reference data, configuration and identity management, as well as transaction data stored for reporting, operational and legal purposes (**data management**[11]).
- Communication between directly connected actors and the digital euro service platform, and between the digital euro service platform and TARGET Services (**interface management**).
- In addition, specific **offline** functions to support peer-to-peer offline functionalities.

[11] The fraud component will be supporting, in addition to fraud checks done by intermediaries. Please refer to the fraud component description for more details.


Grey components = out of scope of the market research and merely there to provide context
User Management
End user
Registration and Onboarding
Lifecycle
Off-boarding
Intermediary
Registration and Onboarding
Lifecycle
Off-boarding
Liquidity management
Liquidity link with DCA / offline
Offline
Issuance/Funding redemption/defunding
Wallet lifecycle management
Holding and TX limits
Online reconciliation
Offline settlement
Data management
Remuneration
Onboarding repository
Proxy lookup
Ref. data
Configuration
Identity
Reporting and analytics
Legal Archiving
Fraud
Settlement
Settlement verification
Settlement recording
Settlement reporting
Interface management
TARGET – Digital euro interface
Digital euro – Intermediary interface (A2A/U2A)
Intermediary – End user interface
Digital euro components
Payment or Funding
Transaction Initiation
Debit deposit account
Limit checks
Validation
Authentication
Submission
Defunding
Limit checks
Defunding initiation
Authentication
Submission
Intermediaries
Transaction management

5. High-level conceptual architecture

Figure 1[12] provides a conceptual view of the high-level architecture of the digital euro. A conceptual architecture view shows the key architectural elements (the components) and their relationships (how the components collaborate and interact) at an abstract level.

The components shaded in grey are not in the scope of this market research exercise, but are nevertheless shown to provide a context for the components that are in scope.

A short description of the components in scope and the functions that they support is provided in Table 1. From the table, a hyperlink on each component's name leads to a dedicated section providing more details about the component, its interactions, and its functional and non-functional requirements.

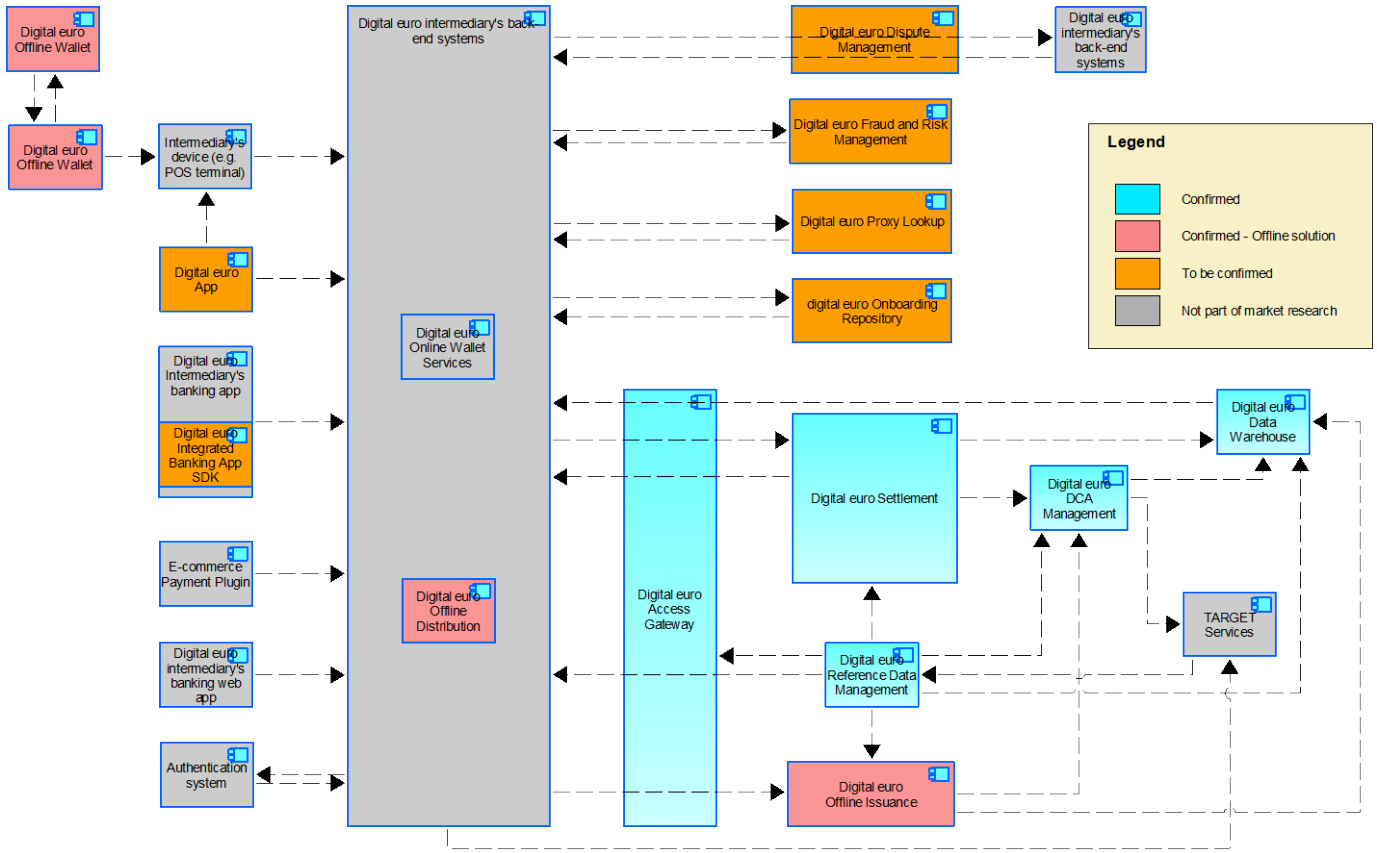


Figure 1: High-level conceptual architecture view

[12] The chart in Figure 1 uses the ArchiMate modelling language.

Table 1

Components in the scope of the digital euro service platform		
Component name	**Component description**	**Functions associated with component**
Settlement	The main functions of this component are to perform settlement verification and settlement recording tasks (including those resulting from funding/defunding) and to maintain the digital euro ledger. This component also handles queries that require real-time data from the ledger.	Settlement verification, settlement recording, settlement reporting Transaction management: payments, funding, defunding, waterfall, reverse waterfall, query processing
DCA Management	This component serves to manage intermediaries' digital euro dedicated cash accounts (for both online and offline digital euro) and interfaces with the TARGET central liquidity management component.	Transaction management: funding, defunding (including Waterfall and reverse waterfall) Liquidity management: liquidity link with DCA / off-line
Reference Data Management	The RDM component acts as a database for reference data, the configuration and identity management of in the digital euro service platform.	Data management: reference data management, configuration management, identity management User management: intermediary registration and onboarding, lifecycle management, offboarding
Data Warehouse	The Data Warehouse component collects data from other components, provides data and tools for historical, statistical and regulatory reporting and archives legally relevant data for regulatory purposes.	Data management: reporting and analytics, legal archiving

Components in the scope of the digital euro service platform		
Component name	**Component description**	**Functions associated with component**
Offline Solution	Offline Wallet The component(s) available to end users, i.e. software running on the offline wallet, either as an applet running on the secure element or a combination of a mobile app and the applet, with the ability to settle digital euro transactions locally.	Offline: wallet lifecycle management, holding and transactions limits, offline settlement
	Offline Distribution The component(s) running at an intermediary, interacting with the devices for funding and defunding operations, and also for the online reconciliation of each device.	Offline: online reconciliation
	Offline Issuance This component is designed to ensure that issuance of funds is always monitored by the Eurosystem and always associated with a corresponding balance adjustment in a dedicated cash account belonging to the relevant intermediary, maintaining full control of the aggregated amount of offline digital euro in circulation.	Liquidity management: liquidity link with DCA / offline Offline: issuance/funding redemption/defunding
Access Gateway	This provides a single point of access for all Eurosystem-provided digital euro services (A2A and U2A).	Interface management with intermediaries, interface management with TARGET
Digital euro App	This Eurosystem-branded mobile app provides a subset of digital euro functionalities to end users. The Digital euro App will act as a user gateway to	Interface management intermediaries <– > end users

Components in the scope of the digital euro service platform		
Component name	**Component description**	**Functions associated with component**
	digital euro services that are provided by an intermediary.	
Integrated Banking App SDK	The SDK(s) (one per mobile OS) is used by digital euro intermediaries to integrate digital euro services into their mobile banking apps in a harmonised way, in accordance with the scheme rulebook specifications.	Interface management intermediaries <– > end users
Proxy Lookup	This component allows intermediaries to pair mobile phone numbers (or other aliases, such as email addresses) with the corresponding account/wallet details of end users. Data are entered into the repository usually during the onboarding of an end user, if an end user decides to share proxy data (e.g. a mobile phone number). The repository will be queried to retrieve the relevant details that are required to instruct a digital euro transaction.	User management: end user onboarding, lifecycle management, offboarding Transaction management: validation
Onboarding Repository	This is a repository of data that supports the check on the number of digital euro end user accounts/wallets. It makes it possible to limit the number of digital euro accounts/wallets to only one per end user.	User management: end user onboarding, lifecycle management, offboarding
Dispute Management	This component supports the exchange of pre-dispute messages regarding additional transaction details and dispute messages for financial chargebacks, streamlining and	Interface management with intermediaries (depending on final design and interactions with other components)

Components in the scope of the digital euro service platform		
Component name	**Component description**	**Functions associated with component**
	structuring the communication between intermediaries.	
Fraud and Risk Management	The Fraud and Risk Management component supports fraud prevention, ex post fraud detection and fraud reporting.	Transaction management: transaction validation Data management: fraud

6. Digital euro components

6.1 Settlement

6.1.1 Description

The Settlement component provides 24/7 instant gross settlement functionality. Settlement is defined as the completion of a transaction with the aim of irrevocable and unconditional discharging of payment obligations through the transfer of money. The Settlement component is mainly responsible for the settlement (i.e. settlement verification and settlement recording) of **digital euro transactions**, which include **payment**, **funding**, **defunding** and **combined** (payment and funding) transactions, and for settlement reporting (i.e. sending settlement confirmations and rejections). It functions in a way that protects **end user privacy**. It records **digital euro holdings** in the main ledger when processing digital euro transactions. When processing **digital euro queries** (which require real-time data) the Settlement component provides information about recorded digital euro holdings or transactions.

6.1.2 Assumptions

To impede the identification of end user payment patterns in the settlement ledger and thus protect end user privacy vis-à-vis the Eurosystem, the recorded end users' digital euro holdings must be represented in discrete holdings linked to one-time pseudorandom identifiers[13].

6.1.3 Interactions

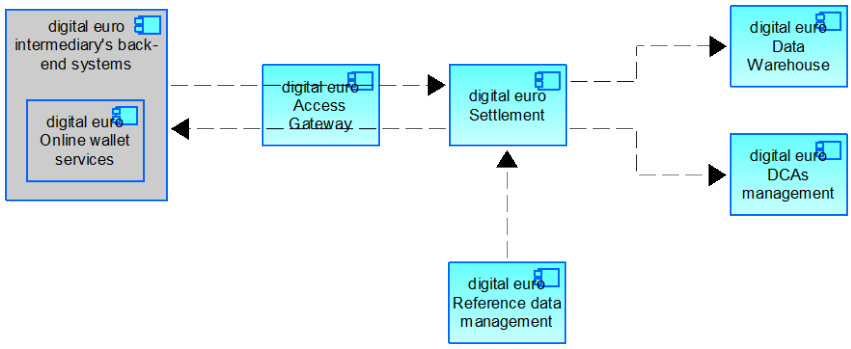


Figure 2: Settlement – interactions

[13] Digital euro holdings need to have pseudorandom identifiers that are not linkable to each other. Thus, such an identifier should not be used multiple times but only once. This concept needs to be supported by intermediaries as ensuring it in the Settlement component might be challenging.

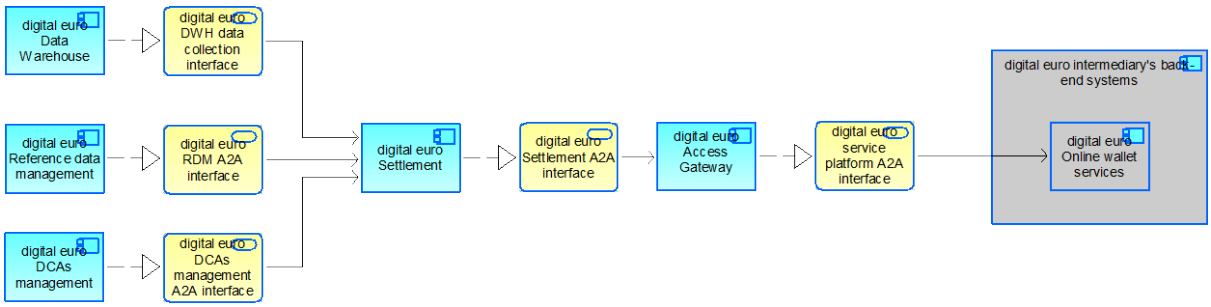


Figure 3: Settlement – interfaces

The Settlement component interacts with the following components:

- Via the Access Gateway component:
  (i) receiving digital euro transactions (i.e. payment, funding, defunding and combined – payment and funding – transactions) and returning settlement notifications (i.e. settlement rejection or settlement success);
  (ii) receiving digital euro queries (i.e. digital euro holding query, digital euro transaction query) and returning the respective real-time information.
- The DCA Management component for processing funding and defunding transactions atomically by instructing a credit (defunding) or a debit (funding) of the DCA holdings involved at the same time as a credit (funding) or debit (defunding) of end users' holdings.
- The RDM component for receiving real-time reference data or general configuration data and using the results for authorisation purposes or checking a maximum transaction limit, etc.
- The Data Warehouse, by pushing data to the Data Warehouse at a predefined frequency.

6.1.4 Requirements

Functional requirements

General

- The Settlement component should verify if the sender of incoming interactions is authorised for the intended interaction.
- The Settlement component should terminate any interaction when it encounters an error and notify the sender accordingly.
- The Settlement component should settle digital euro transactions immediately, in parallel, for the full amount(s) specified, without any netting functionality.

- The Settlement component should handle digital euro transactions containing at least the holding(s) to debit, the holding(s) to credit, a creation timestamp, a message identifier and the digital signatures of the intermediaries involved.
- The Settlement component should handle digital euro queries (requiring real-time data) requested by intermediaries about digital euro holdings they manage for their end users and return information containing at least the holding identifier(s), the associated amount(s) and the message identifier(s) of associated digital euro transaction(s).
- The Settlement component should handle digital euro queries (requiring real-time data) requested by intermediaries about digital euro transactions (within a configurable time span in the magnitude of days) they are involved in and return information containing at least the message identifier(s), the debited holding(s) (if requested by the intermediary of the payer's side), the credited holding(s), and the creation timestamp(s).
- The Settlement component should enable end users to prove their access to digital euro holdings irrespective of their selected intermediary in case they want or need to choose a new intermediary to manage their holdings, e.g. because the previous intermediary suddenly ceases to operate. This proof should not be known to the digital euro components and may be known to the intermediary.

Settlement verification

- The Settlement component should perform technical and message checks on digital euro transaction sent by an intermediary.
- The Settlement component should terminate settlement verification and send a rejection message to the intermediaries involved when it encounters the first error or has a time-out based on a configurable parameter.
- The Settlement component should verify the message signatures provided by the intermediaries involved, thereby confirming that authentication and validation were executed on intermediary level before settlement. When the message signature of one intermediary – and thereby the confirmation of authentication and validation at their level before settlement – is missing, it needs to be requested from the respective intermediary.
- The Settlement component should verify that the digital euro transaction's creation timestamp is within a configurable time window.
- The Settlement component should verify that the digital euro transaction's amount to be transferred is within a configurable range (i.e. higher than zero and below a maximum transaction limit, should one be imposed).

- The Settlement component should verify that the sum of the amounts of all holdings to debit is equal to the sum of the amounts of all holdings to credit.
- The Settlement component should verify settlement by executing a money availability check, which involves checking that the amount of money to be transferred as specified in the digital euro transaction exists in the settlement ledger.

Settlement recording

- The Settlement component should record the settlement of a transaction by reflecting the money transfer between the holding(s) to debit and the holding(s) to credit – of end users in case of a payment or of an intermediary and (an) end user(s) in case of a funding, defunding or a combined payment and funding transaction – in the settlement ledger.
- The Settlement component should send a settlement confirmation after the settlement is reached.

Combined settlement (funding and payment within one digital euro transaction)

- The Settlement component should enable combined payment and funding settlement, involving technical and message checks, settlement verification and settlement recording, to prevent intermediaries having to send two separate messages, thereby avoiding synchronisation logic and race conditions and improving latency.
- The Settlement component should settle a funding combined with the processing of a payment when the digital euro transaction message contains the optional funding data required for settlement. A digital euro transaction message including payment data and funding data indicates that additional money is required on the payer side for a successful payment. It triggers the settlement of a funding directly in the Settlement component based on the incoming data from the digital euro transaction message. In general, a funding could be triggered by an intermediary acting on behalf of the payer to make money available for the payment before a separate subsequent payment is triggered. This requires the complete end-to-end chain of all entities involved to be executed twice (first for the funding and second for the payment). This is seen as sufficient for manual or regular automated (time- or event-based) fundings but a reverse waterfall funding occurs during a payment and is therefore time-critical.
- The Settlement component should execute a combined payment and funding atomically, meaning it will either do both (i.e. funding and payment) successfully or nothing (i.e. no funding and no payment) at all in case of an error occurring.

Non-functional

- The Settlement component should apply privacy-enhancing techniques to protect the privacy of end users.
- The Settlement component should apply information-unlinking techniques to support the unlinking of end user data from (i) the data used for their digital euro transactions, and/or (ii) the payment patterns resulting from their digital euro transactions.
- The Settlement component should (i) have no information about end users (including no single static pseudonym linked to one end user and no balance information of one specific end user) and (ii) support a one-time random identifier per digital euro holding.
- The Settlement component should apply information-unlinking techniques to support the unlinking between end user data and the (meta) data derivable from processed digital euro queries.
- The Settlement component should allow an intermediary to send digital euro queries (i) only for digital euro transactions in which this intermediary was involved, (ii) only for digital euro holdings that this intermediary manages for its end users and (iii) only when querying a minimum number (configurable parameter) of different digital euro holdings.

6.2 DCA Management

6.2.1 Description

DCA Management is a component providing intermediaries that have their own dedicated cash accounts (DCAs) with liquidity management functionalities to allow (i) transfers of liquidity between the digital euro service platform and TARGET Services, and (ii) the funding and defunding of end users' digital euro holdings.

Liquidity transfers would be settled by moving the liquidity through transit accounts[14] (or using a comparable mechanism). Two different types of liquidity transfer can be distinguished: inbound (from the main cash account in the CLM (central liquidity management) to a DCA in the digital euro service platform) and outbound (from a DCA in the digital euro service platform to a main cash account in the CLM). The liquidity transfer process is defined so as to ensure that, in absolute terms, the sum of all the positions (DCAs) held by the intermediaries and all the positions held by end users is always equal to the difference between the inbound liquidity transfers and outbound liquidity transfers settled in the digital euro service platform (see assumptions below).

With regard to the latter, intermediaries can use their dedicated central bank reserves in the DCA Management component to fund (and defund) digital euro holdings by means of either the Settlement component or the Offline Solution when the network connectivity is active.

The Eurosystem creates and maintains DCAs for intermediaries and sets up the appropriate assignment of liquidity management access rights in the Reference Data Management component. Real-time access to the Reference Data Management component should ensure that both the creation of DCAs and data changes related to DCAs become effective in the DCA Management component.

[14] Inbound and outbound liquidity transfers between TARGET Services are settled by moving the liquidity through transit accounts. The transit accounts are technical accounts (one per settlement currency) that reflect any movement across the various settlement services (CLM, RTGS, T2S and TIPS). In order to ensure consistency between TARGET Services, all liquidity transfers affecting dedicated positions held by intermediaries within the digital euro components need to be processed and monitored using a mechanism compatible with the one based on transit accounts.

6.2.2 Assumptions

- A dedicated pool of liquidity held by intermediaries for the purpose of facilitating a convenient funding and defunding process should be established in the form of a new digital euro DCA in TARGET Services.
- The liquidity source of such digital euro DCAs is the central liquidity management (CLM) component in TARGET. In this context, intermediaries facilitate its conversion into digital euro held by end users and the liquidity held in such digital euro DCAs will not be digital euro, since it remains central bank money owned by an intermediary, until issuance which will only take place upon a funding request of an end user.

6.2.3 Interactions

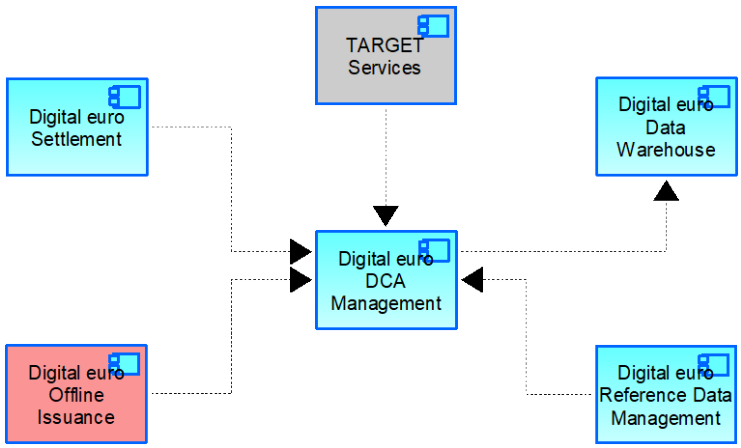


Figure 4: DCA Management – interactions

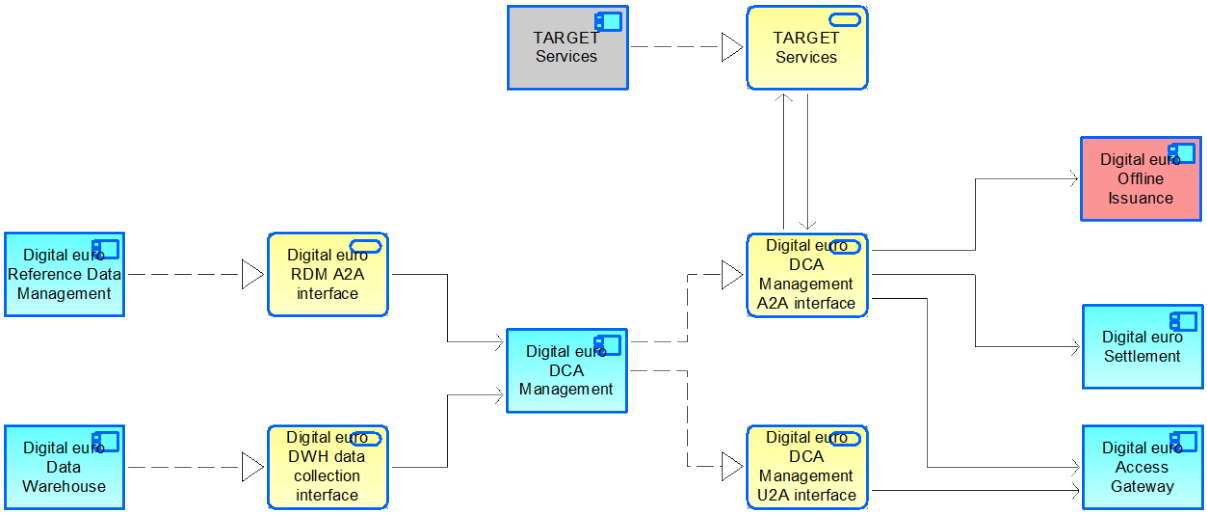


Figure 5: DCA Management – interfaces

- The DCA Management component would access the RDM component in real time and retrieve all the data related to DCAs (e.g. creations of new DCAs, updates of existing DCAs, report configurations, etc.) and the liquidity management access rights profiles of users' intermediaries and central banks within the Eurosystem.
- The DCA Management component would interact with TARGET Services to transfer the liquidity needed to support the funding and defunding processes:
    - to be informed about the current status of TARGET Services, needed for the validation of inbound and outbound liquidity transfers;
    - to be informed about the current TARGET business date and the moment of change of business date. When informed about the change of business date, the DCA Management component would provide the end-of-day information related to DCAs and the relevant transit account (or comparable mechanism) for the past business date.
- The DCA Management component would interact with the Settlement component for the processing of funding and defunding operations.
- The DCA Management component would interact with the Offline Solution for the processing of funding and defunding operations.
- The DCA Management component should support user access in both A2A and U2A mode.

- The DCA Management component should push relevant data for statistics and archiving purposes to the Data Warehouse at a predefined frequency.
- The DCA Management component should pull relevant data from the Reference Data Management component (e.g. access rights profiles) in real time.

6.2.4 Requirements

- Digital euro DCAs are central bank money positions opened in the books of a central bank within the Eurosystem and are dedicated solely to the funding and defunding of digital euro holdings.
- Inbound and outbound liquidity transfers are triggered by intermediaries and only if needed by central banks within the Eurosystem, in either the CLM or the DCA Management component.
- The DCA Management component should be available for funding/defunding operations 24/7 and allow the transfer of funds between the CLM and a DCA during TARGET operating hours.
- Information related to DCAs should be collected and provided to the CLM for the purpose of accounting and minimum reserve calculations. Such information should be provided only after all pending liquidity transfers from/to the CLM have been finalised.
- The DCA Management component should offer queries and reports to the intermediaries and the Eurosystem to support monitoring and reconciliation. Critical queries and reports for liquidity management (e.g. account balance queries and blocking account status queries) should be made available 24/7.
- The DCA Management component should differentiate between intermediaries with different level of access. These are (i) intermediaries that own a DCA; (ii) intermediaries that do not own a DCA but have a contractual agreement with other intermediaries to use their DCAs; (iii) entities (e.g. intermediaries and third parties) that communicate directly with the component and can instruct on their own behalf or on behalf of others, (via) the central banks within the Eurosystem that can, if needed, act on behalf of their intermediaries.
- The DCA Management component should provide tools that enable the Eurosystem to monitor each DCA (e.g. balance, amount received from the CLM, overall amount distributed to end users).

6.3 Reference Data Management

*The Reference Data Management component should **not** store the reference data or configuration of individual end users.*

6.3.1 Description

The Reference Data Management (RDM) component acts as a database for (i) reference data (as a consistent and uniform set of identifiers and extended attributes of each entity), (ii) configuration (as a set of data objects associated with each entity), and (iii) identity objects (supporting the identity management of system users).

6.3.2 Assumptions

- Each intermediary is associated with a **unique identifier,** such as a business identifier code (BIC) or legal entity identifier (LEI);
- A subset of intermediaries active in the digital euro service platform will also remain active as TARGET participants. Among others, this relates to credit institutions with headquarters or branches in the euro area which are subject to minimum reserve requirements and hold a main cash account (MCA) in TARGET. Thus, the RDM should ensure consistency of data in the RDM with data in TARGET Services.

6.3.3 Interactions

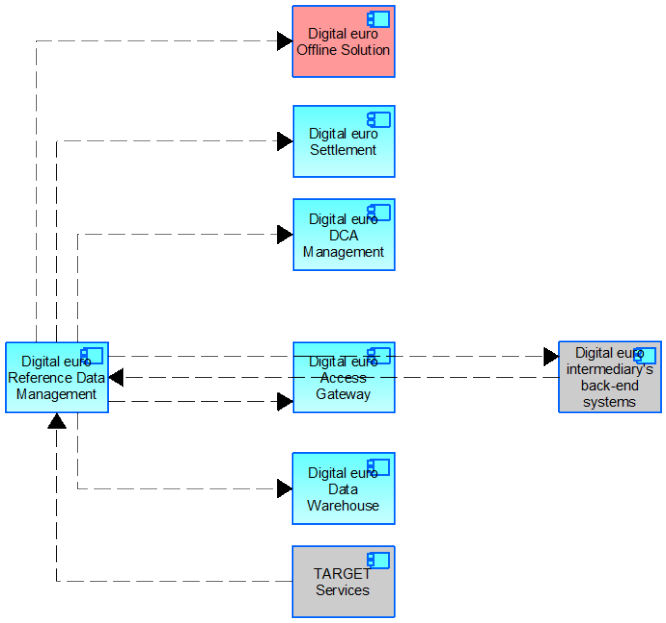


Figure 6: Reference Data Management – interactions

The RDM component **interacts with the other components** by:

- providing real-time access to identity objects (e.g. rights profiles of users), pulled by all other components;
- providing real-time access to reference data and configuration, pulled by the following components:
    - Settlement (e.g. input for authorisation of intermediaries)
    - DCA Management (e.g. DCA details, input for authorisation of intermediaries)
    - Access Gateway (e.g. input for authentication of intermediaries)

- pushing relevant data to the Data Warehouse at a predefined frequency;
- ensuring consistency of reference data for intermediaries present both on the digital euro service platform and in TARGET Services.

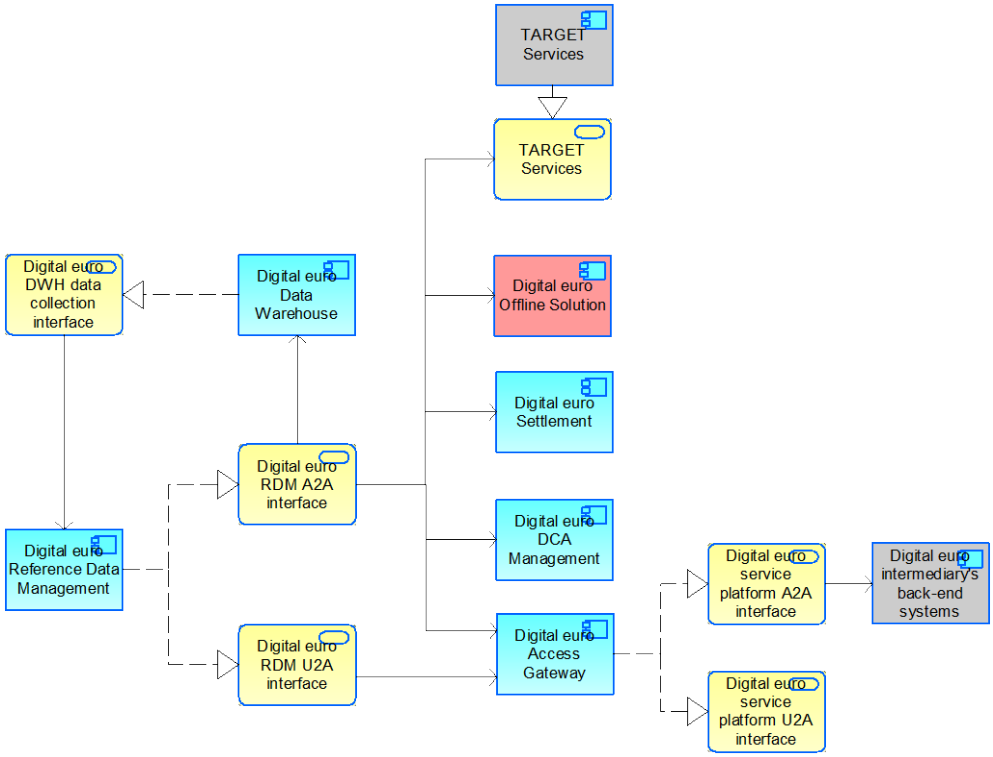


Figure 7: Reference Data Management – interfaces

RDM should support the **user access**:

- in A2A mode: inbound and outbound communication between applications;
- in U2A mode: online screen-based activities performed by the relevant entities, including bulk data loading. At the same time, RDM should make it possible to ensure data integrity and perform data requests and communications using a dual authorisation concept". According to this concept, a second independent verification and confirmation is required, if requested for a specified set of reference data operations, before an operation becomes active in RDM.

6.3.4 Requirements

Data scope

- RDM should serve as a database for reference data, configuration and identity objects;
- RDM should cover data of the operator, the Eurosystem, intermediaries and end users (i.e. common configuration for all end users, such as holding limits);

- RDM should store data that are shared across different digital euro components or are specific to one component.

Data collection

- RDM should facilitate the creation of new data and the amendment and deletion of existing data;
- RDM should execute all data maintenance instructions immediately;
- Updates to most of the data stored in RDM should be accessible to all other components of the digital euro service platform in real time, following a "pull" propagation by a given component from RDM. For selected business-critical data (e.g. in the event of insolvency blocking an intermediary or an account belonging to an intermediary), a "push propagation" from RDM to the remaining components should be available to ensure that the modified data are immediately available across the digital euro environment.
- Reference data of intermediaries in RDM should remain synchronised with the reference data of the same TARGET participants. Thus, RDM should rely on the data already available in the CRDM component of TARGET Services. If an intermediary present in the digital euro environment does not exist in TARGET, its reference data will be created and maintained in RDM and not in the CRDM.

Functionalities

- RDM should allow intermediaries and the Eurosystem to query data in real time in line with the hierarchical data model (i.e. each intermediary can query its own data, and each central bank within the Eurosystem can query its own data and the data of all intermediaries belonging to its community).

6.4 Data Warehouse

6.4.1 Description

The Data Warehouse acts as a database for data related to the activity of intermediaries and the Eurosystem. Its purpose is to (i) archive legally relevant data for regulatory purposes[15]; and (ii) provide data and tools for historical, statistical and regulatory reporting, as well as advanced analytics, respecting the general privacy requirements of the digital euro components.

For archiving, the Data Warehouse provides features to gather all messages from intermediaries with a legal relevance (i.e. mainly settlement-related messages and messages changing reference data or transaction data), including signed messages in their original content and format which cannot be modified. Archived messages should be stored for a predefined retention period, which may be different for different data types and components.

For reporting, the Data Warehouse stores all transactions and business information at a predefined frequency, supports a range of predefined reports and enables third parties to design their own queries.

6.4.2 Assumptions

- Legally relevant data stored in the Data Warehouse can be **accessed only by the operator** which is responsible for retrieving the archived information at the request of the Eurosystem. The Eurosystem can also request the retrieval of archived data on behalf of one of the intermediaries in its community.

6.4.3 Interactions

The Data Warehouse **interacts with the rest of digital euro components** by:

- receiving at a predefined frequency (e.g. hourly, daily, weekly) data produced by the relevant components (e.g. Settlement) and pushed to the Data Warehouse;
- pulling in real-time data from the Reference Data Management (RDM) component (e.g. access rights profiles).

[15] For the purpose of market research, the description and functionalities of legal archiving are included in the Data Warehouse, while it might become a separate technical component.

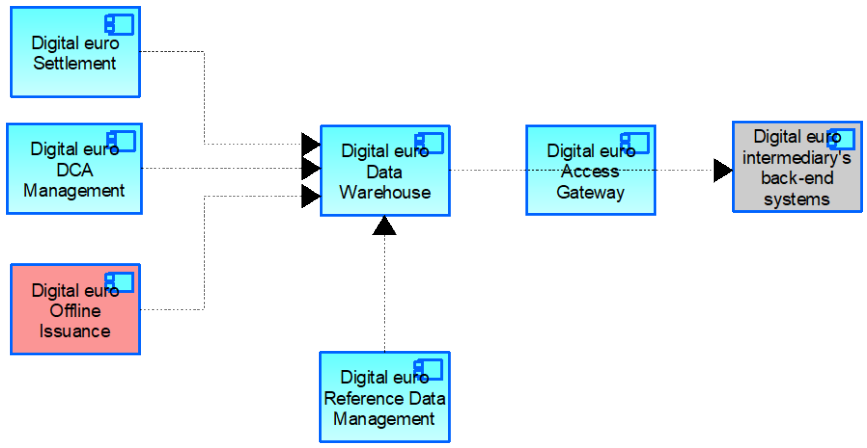


Figure 8: Data Warehouse – interactions

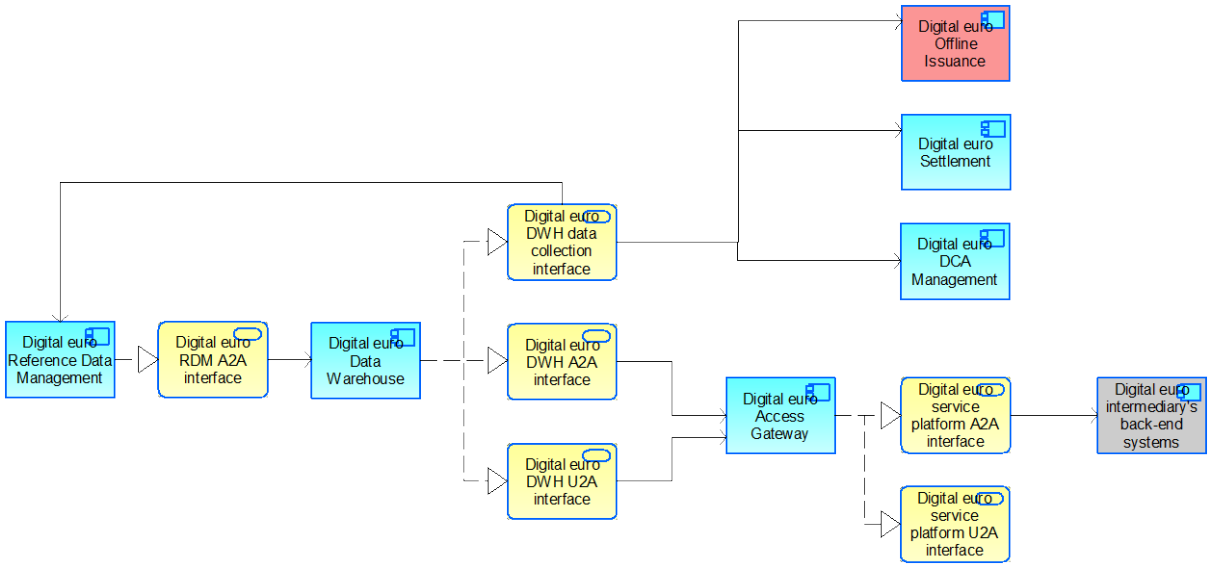


Figure 9: Data Warehouse – interfaces

6.4.4 Requirements

Data scope

- For legal archiving, the Data Warehouse should store transaction data (i.e. individual payment transactions settled/not settled between end users and between end users and intermediaries);
- For reporting, the Data Warehouse should store all transactions and business information (e.g. automated and manual funding/defunding of digital euro wallets, changes to the balances of

digital euro wallets, changes to the balances of DCAs, liquidity transfers crediting/debiting DCAs).

Data collection

- For legal archiving, the data are collected upon entry (i.e. all inbound/outbound messages and files processed by the digital euro Access Gateway and inbound/outbound messages and files related to digital euro liquidity management) and stored in the Data Warehouse with immediate effect;
- For reporting, the data are collected daily and stored in the Data Warehouse as of the next business day.

Data retention

- The retention period for data collected in the Data Warehouse for reporting purposes is set at ten years.
- The retention period for data collected in the Data Warehouse for legal archiving is set at ten years.

Data format

- For legal archiving, the data collected in Data Warehouse should be protected and secured in the original format. Neither changes nor deletions should be possible once information is legally archived.
- For reporting, after the collected original data are captured, they should be transformed (e.g. cleaned, collated, aggregated) and stored appropriately (e.g. views, data marts) in order to enable the efficient execution of the queries and reports needed for the digital euro.

Data access

- Data access is limited for legal archiving, as intermediaries and the Eurosystem do not have direct access to the archived data. The intermediaries and the Eurosystem can ask the operator to provide a specific subset of the archived data provided they present a valid regulatory reason. The operator should provide the requested archived data via external means (e.g. secured e-mail).
- For reporting, the Data Warehouse should be accessible to the Eurosystem and intermediaries in line with the hierarchical data model.

Functionalities

- For reporting, the Data Warehouse should provide intermediaries with functionality to:

  - query their data scope according to specific settings (e.g. select the data type and conditions, filter, sort, apply statistical functions and limit the results);
  - save the settings of a query as an ad hoc report, to be performed in the future by the same intermediary or shared with another intermediary/central bank within the Eurosystem for processing within its own data scope;
  - run predefined reports available to all financial intermediaries/the Eurosystem within their own data scope (e.g. DCA statement, volume and value of payment transactions during a business day/calendar month, number of financial intermediaries or DCAs within the data scope of a Eurosystem central bank). These reports would also support the constant monitoring of the overall amount of digital euro in circulation.
  - schedule the reception of ad hoc and predefined reports.
- Furthermore, the Data Warehouse should provide advanced analytics and business intelligence tools (e.g. licenses and integration of such tools) to allow the Eurosystem to create custom analyses and models (including machine learning models) using the warehouse data.
- In addition, the component should be able to calculate the remuneration for each intermediary under the general requirement to calculate the remuneration of the digital euro. This calculation would be based on the cumulative amount of digital euro holdings of end users under the intermediary's management, the period (the number of business days for which the remuneration is applied) and the remuneration rate. The remuneration rate could be two-tiered, composed of a zero or positive remunerated first tier for holdings below a given threshold and a remunerated second tier (including the possibility of 0% remuneration).

6.5 Offline Solution

6.5.1 Description

The offline payment functionality would allow end users to make and receive final, irrevocable payments even in the absence of network connectivity. For the verification and recording of the transaction, this would rely solely on the two end users' devices that are interacting at the moment the transaction takes place.

The envisioned solution uses Secure Elements (SEs) on the end user devices, to ensure the proper execution of application logic, including required cryptographic primitives.

Although treated as a single component for the purposes of this market research – mainly because of the expected coupling between technical elements – the solution may be considered composed of at least three sub-components:

- The component(s) for end users: the device the end users will use as an offline wallet, with a software component running on it, either as an applet running on the Secure Element or a combination of a mobile app and the applet mentioned above.
- The component(s) running at an intermediary ("Offline Distribution"), capable of interacting with the devices for funding and defunding operations, also for the online reconciliation of the device.
- The component(s) running at the Eurosystem ("Offline Issuance"), designed to ensure that issuance of digital euro is always monitored by the Eurosystem and always associated with a corresponding balance adjustment in a DCA belonging to the relevant intermediary.

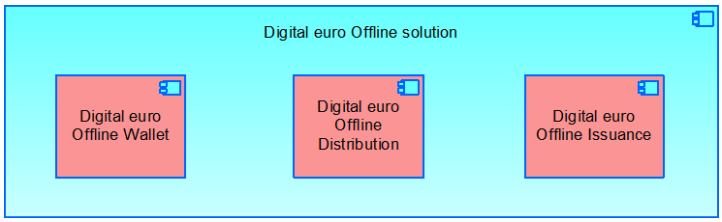


Figure 10: Offline Solution – potential sub-components

The devices are expected to go online (interacting with their own intermediary) from time to time, both to account for technical limitations (e.g. available storage on the devices) and to mitigate the risks associated with potential financial fraud. It should be possible for the Eurosystem to customize the frequency of such updates, depending on technical constraints and its risk tolerance. For the remainder of the section, this operation is called online reconciliation, although

the term is not meant in the accounting sense. Reconciliation is intended to enable the online counterpart of the system to complete the operations described in the following table.

Operation	Description/comments
Reset the balance on the device	The exact implementation of the operation depends on the data model used. It may entail exchanging the list of transactions or tokens stored on the device with a single transaction or token (signed by the intermediary).
Check the health status of the device	At reconciliation time, the system may run device diagnostics to check the device's health status (security status, app version, certificate validity, etc.).
Ensure maintenance/lifecycle management	Online reconciliation provides a good opportunity to exchange configuration data with the device, within the constraints imposed by the SE-backed architecture.

6.5.2 Assumptions

- The use of Secure Elements (i.e. silicon chips that are able to securely store confidential information and execute basic cryptographic operations)[16] in the devices is considered mandatory.
- A "prefunded approach" of the offline device has been chosen, as opposed to a "delayed settlement", requiring the funds to be available on the payer's device to execute the transaction.
- Each transaction completed and confirmed by the two interacting devices must be considered final and irrevocable and properly recorded in the local storage, implying that the transfer of value between the two secure elements prevents the payer from spending that amount again and in the case of a peer to peer transaction allows the payee to spend it with another user, without the need for a third party to verify and record the transaction.

[16] A Secure Element is a hardware device component which offers tamper-resistant secure services to the rest of the device (including tamper detection, secure memory, cryptographically secure random number generation, cryptographic services, secure generation of keys, secure monitoring of system resources, secure execution of software modules, secure counting of events, secure time measurements, tamper resistant unique identifier and so on). See Vauclair, M., "Secure Element", in van Tilborg, H.C.A. and Jajodia, S. (eds.), *Encyclopedia of Cryptography and Security*, Springer, 2011.

- Funding and defunding operations happen by connecting the device to the system of an intermediary (over-the-air or via a suitably equipped ATM or similar device).
- Technical constraints may make it impossible to indefinitely store long lists of transactions in the devices, and as a consequence:
    - a limit in the number of transactions per device may be applied;
    - the need for a periodic online reconciliation for the offline devices is considered in the scope.
- While the respondents are allowed maximum flexibility in the design of the solution, we assume that the platform will require at least the following three sub-components:
    - Offline Wallet
    - Offline Distribution
    - Offline Issuance
- A mobile app form factor and a card-based solution should be supported.

6.5.3 Interactions

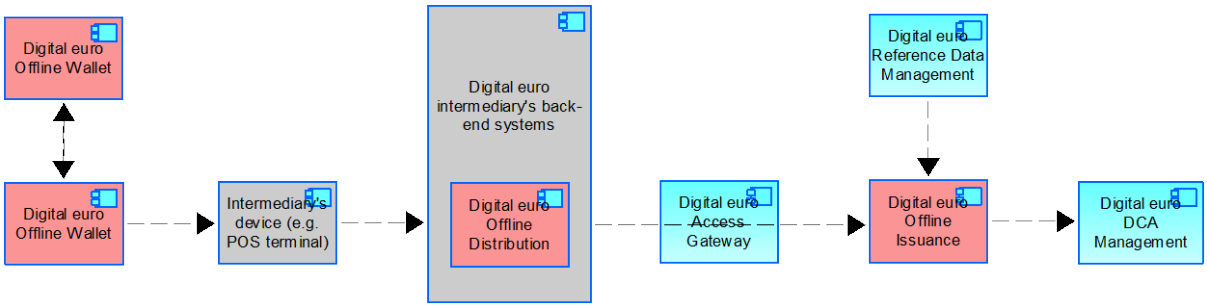


Figure 11: Offline Solution – interactions

The Offline Solution is expected to work with a certain degree of independence from the online counterpart. Each Offline Wallet would interact:

- with other offline wallets, including offline-capable merchant (POS) devices;
- with the Offline Distribution component, at the intermediary, for both online reconciliation and funding and defunding operations.

During online reconciliation, some information related to the status of the device is exchanged.

The Offline Distribution component also interacts with the Offline Issuance component which, in turn, interacts with the DCA management component, transmitting issuance or redemption instructions.

The digital euro components should always keep an up-to-date overview of the total amount of offline digital euro in circulation.

6.5.4 Requirements

Issuance and redemption of funds

- The offline digital euro components should permit the issuance or redemption of offline digital euro upon approval by the Eurosystem only. The authenticity of the operation must be provable.

Wallet initialisation/lifecycle management

- The wallet should be opened through an intermediary.
- Each citizen can only have one offline wallet.
- Merchants may have multiple wallets but will not be allowed to initiate transactions as payers, and funds acquired in a transaction should be defunded as soon as technically possible.
- A wallet owner can ask for an empty wallet to be deleted or the device to be replaced or reinitialised.
- After the online reconciliation, the wallet should revert to a clean state, with the (technical) capacity to record a new set of transactions.

Funding and defunding

- An offline digital euro wallet should only be funded in an interaction with an intermediary.
- End users can fund or defund their wallets using banknotes in an appropriate intermediary device (e.g. an ATM).

The following requirements are based on the underlying assumption that an offline wallet can be "securely funded" over-the-air (i.e. using a network connection provided by the mobile device when online, for example).

- The wallet owner can instruct a defunding operation from the wallet itself to a commercial bank account associated with the same individual.

- The wallet owner can instruct a funding operation involving the exchange of commercial bank account holdings associated to the same individual for funds that are transferred to the offline wallet.

Peer-to-peer and POS offline transaction

- Devices need to authenticate themselves before engaging in a transaction. This requires both devices to prove their identity and the authenticity of the running code. This may include the need to ensure the device is not rooted.
- A payer can initiate a transaction by keying in the amount to be paid using the device user interface. The actual transaction with the payee's device starts once the devices are in sufficient physical proximity to exchange information and when authorised by the user.
- The payer's device must be active (e.g. device unlocked, wallet app open).
- After a successfully completed transaction, a payee can use funds received offline (plus any balance available beforehand) in a subsequent offline transaction.
- An offline wallet can employ local proximity and NFC connectivity to pay at a store if the merchant has an offline-capable device.

Holding and transaction limits[17]

- The solution should allow for the secure and immutable configuration of a maximum number of payments to be executed between two online reconciliation operations. Once the device has reached maximum number of payments, it would need to go on-line for reconciliation and then would be able to process payments again
- The solution should allow for the secure and immutable configuration of a time-threshold, preventing the device processing payments unless it has been reconciled online in the recent past (parameter configurable by the Eurosystem). Devices that have not been reconciled during the defined period would need to go online for reconciliation before being able to process payments again.
- A single transaction (and cumulated transactions in a defined period of time) with a digital euro offline wallet cannot exceed a set amount.
- A single end user wallet should have its holding limit up to a threshold set by the Eurosystem.

[17] To avoid the risk of the limits being altered, and hence circumvented, we assume that these limits are enforced in the logic running in the Secure Elements.

- The mentioned limits will not be modifiable by the intermediaries.

Non-functional requirements

Performance

- A single transaction between two offline wallets should take no more than four seconds to complete.
- Funding an offline wallet should take no more than ten seconds to complete.

Lock-in/interoperability

The solution is not constrained by lock-in with specific suppliers and implementations can be certified against security and quality criteria. **To this end, the respondent should consider the production of the following deliverables in the cost estimates**:

- Technical product specifications, including both high-level and low-level specifications, that should allow different providers to implement interoperable solutions.
- Specific Protection Profiles according to ISO/IEC 15408 and the Common Criteria (CC), at a minimum for the solution used for the Offline Wallet, but potentially also for intermediaries' components.

6.6 Access Gateway

6.6.1 Description

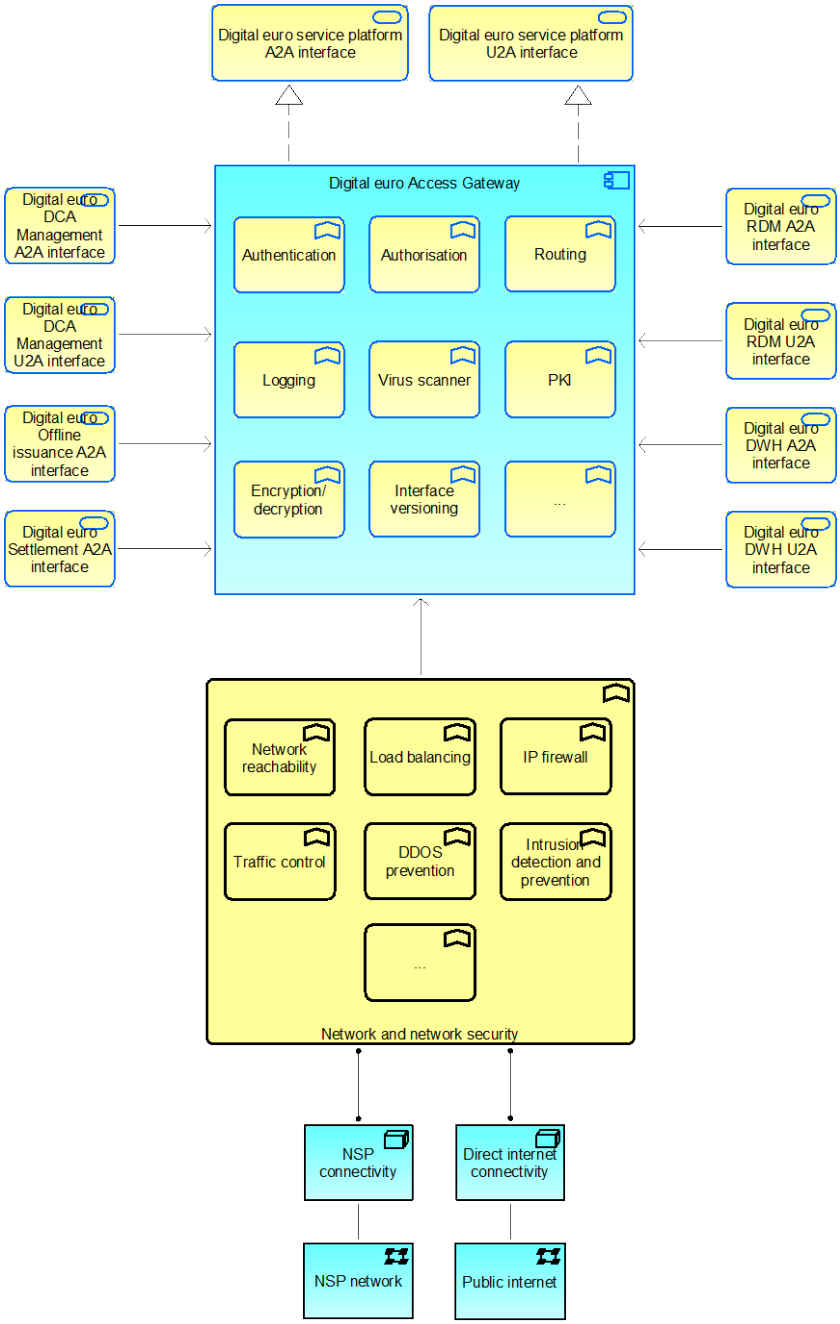


Figure 12: Conceptual view of the Access Gateway.

The functions depicted are indicative – only a few are listed to illustrate the principles.

External actors (applications or humans) that are users of the digital euro components need to access to them over a network. The **Access Gateway** is the component which enables network connectivity and communication interfaces between external actors and the digital euro components. It acts as a single entry point providing a unified interface to all these components, hiding the complexity of the individual components in the architecture and decoupling it from its users, and providing additional technical services (e.g. for security and reliability).

The Access Gateway must support connectivity via different private and public networks. For example, its services may be exposed on the network of one or more network service providers (NSPs), such as SWIFT or NEXI, or also on the public internet.

The following list is indicative and not exhaustive of the type of functionality that the Access Gateway comprises:

- **Infrastructure**: IP firewalling, load balancing, traffic control, intrusion detection and prevention, DDOS prevention, etc.
- **Application**: Validation, routing, logging, monitoring, message reliability, non-repudiation, protocol/interface versioning, rate limiting, public key infrastructure, traffic encryption/decryption, authentication, authorisation, digital signatures, virus scanner, etc.

The list of example functions for each layer is not exhaustive and may need to include others, determined by the functional requirements of the other components.

6.6.2 Assumptions

The design of the Access Gateway should encompass the following assumptions.

- The digital euro service operates in a redundant set-up from at least three geographically separate sites.
- The connectivity between operating sites is not assumed within the scope of the Access Gateway.

6.6.3 Interactions

The Access Gateway interacts with the following:

- software applications in the intermediaries' back-end systems in application-to-application (A2A) mode to communicate with components of the digital euro (see Section 6.6.4 below);
- human actors, acting on behalf of an intermediary, via web access in user-to-application (U2A) mode (see Section 6.6.4 below).

- the components of the digital euro that need to be accessed by intermediaries (see Section 6.6.4 below);
- the Reference Data Management component to retrieve reference data needed for its operations, including access rights for authorisation purposes, etc.;
- TARGET Services, as needed.

6.6.4 Requirements

The Access Gateway supports connectivity indirectly via various network service providers (**NSP connectivity**) and directly via the internet (**direct internet connectivity**)[18]. In the case of NSP connectivity, the Access Gateway could make use of existing network infrastructure, security infrastructure, services, protocols and interfaces provided by an NSP. For direct internet connectivity, such infrastructure, services and protocols are not usually provided by ISPs and will thus have to be provided as part of the Access Gateway component. The respondent must additionally specify, describe and quote the infrastructure, services and protocols required (on both sides: intermediaries and digital euro) for direct internet connectivity in the questionnaire in Annex 2.

The requirements applicable to both connectivity modes are described below.

Network reachability

The intermediaries' back-end systems must be able to reach all active operational sites of the digital euro components via the Access Gateway.

Interfaces

The Access Gateway should enable connectivity to all core digital euro components[19] which interact with external actors and, depending on the implementation, TARGET Services. It should therefore connect to the **internal interfaces** for Settlement, DCA Management, Offline Issuance, Reference Data Management, Data Warehouse and possibly TARGET Services. The Access Gateway also provides **external interfaces** to reach each of these components from the outside. Different communications protocols may be used to support the communication between the

[18] The Access Gateway must *support* both modes of connectivity. A decision on which connectivity modes to eventually enable is subject to an on-going analysis of risks and threats.

[19] Excluding the orange components in Figure 1 on page 21.

intermediary's back-end system and the Access Gateway, depending on the digital euro service component that needs to be reached. These may include:

- Interfaces for accessing different digital euro services in A2A mode using a suitable protocol at the application level (HTTP API, WebSocket, RPC-style, message-based, file-based, etc.). These should be implemented for both NSP-based connectivity and direct internet connectivity. Various protocols may be available for each A2A interface, depending on requirements.
- Web-based interfaces for accessing different digital euro services in U2A mode for human activities performed by the relevant activities. These can also be used for retrieving data files (e.g. in .csv, .pdf, .xlsx or .txt format), such as generated reports.

Services

The Access Gateway offers services to enable the validation and (reliable) routing of messages, non-repudiation, a web portal for U2A mode, user authorisation for the different access modes, and so on, subject to the requirements of the connected components. Additional services could also be related to service lifecycle management, such as governance, incident management and monitoring.

Security

The Access Gateway should satisfy high security requirements regarding confidentiality, integrity and availability. The following requirements are non-exhaustive and may depend on requirements imposed by the components that the Access Gateway interacts with.

- **Security policy**: The provider is required to have a documented IT security and risk management framework in place, in line with industry standards and applicable oversight frameworks. The provider will offer guidance on security services to intermediaries, cooperate on security risk mitigation with the operators of the digital euro components and ensure the application of these practices through documented procedures.
- **Data confidentiality**: All data in transit through the gateway must be encrypted; access to sensitive data (e.g. secret key material) should be protected by employing tamper-proof devices.

- **Data integrity**: The Access Gateway should offer support for data integrity validation, in line with all the required messaging models.[20]
- **Authentication and PKI**: Any A2A connection should be mutually authenticated at the transport layer (e.g. using mTLS). The Access Gateway should be provided complete with a public key infrastructure (PKI), whose root key material should be adequately protected. The provider should manage all the issuance and revocation activities related to the certificates used. U2A channels should be protected by multi-factor authentication.
- **Availability**: The Access Gateway should offer a level of availability for the connection and service that is compatible with the distributed design (in terms of geographical sites) and the non-functional requirements described in Section 2. It should allow for maintenance procedures that do not require service downtime.
- **Forensic**: The Access Gateway should log relevant security events and operator activities and protect the logs to support forensic investigation if required.
- **Endpoint protection**: Exposed endpoints should offer protection against the typical network and application-level threats, including traffic flooding (network level DDOS) and transmission of malware.

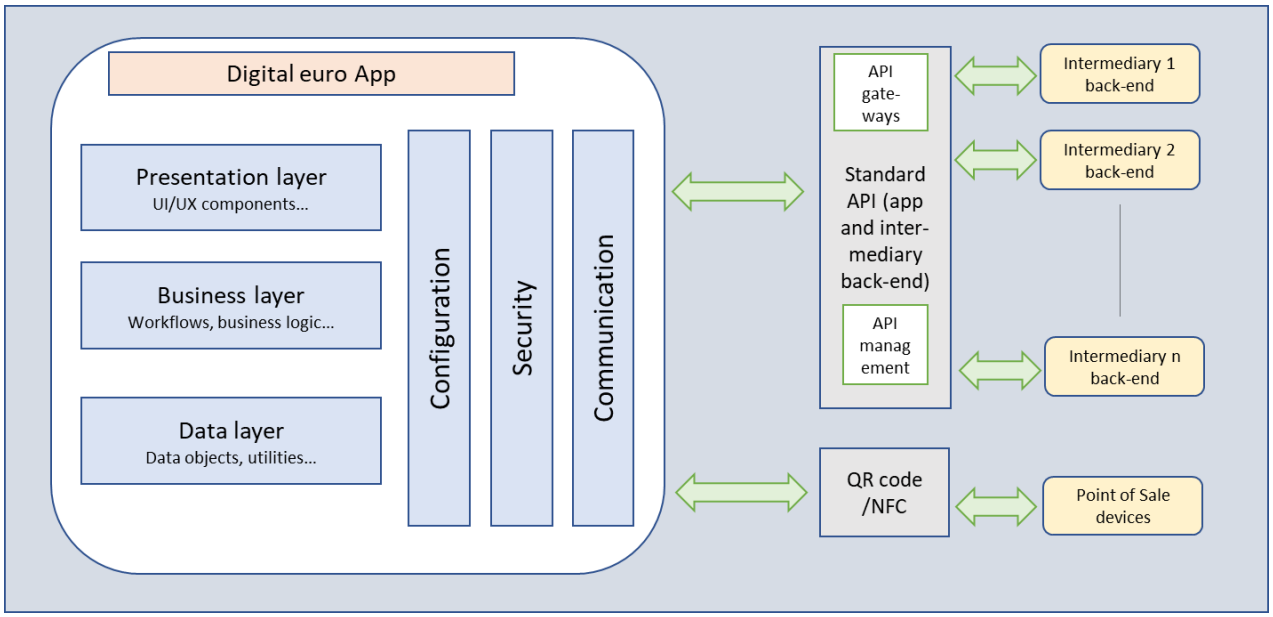
[20] For connection-oriented models, this is ensured at the transport level, while for message-oriented models, this may include reliable messaging and message integrity validation.

6.7 Digital euro App

	*The Digital euro App component may be considered to enhance the overall functionality and, ultimately, the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.*

6.7.1 Description

A digital euro app would provide strong visibility for the digital euro and promote a standard user experience. The app should have a uniform look and feel that will facilitate a standardised approach to connecting users to intermediaries. It would allow intermediaries to initiate payments in response to end user actions. The underlying objective is to provide the market with the minimum required development, ensuring that all intermediaries can maintain their roles in digital euro distribution. The app would satisfy the preferences of some end users who want an independent access channel supporting basic functionalities. The app should offer a harmonised entry point to end users connecting them to intermediaries providing operational and information services. It acts only as a portal to the services offered by the intermediary and does not provide the services independently.



6.7.2 Assumptions

A standardised API layer is defined in the digital euro scheme that all intermediaries' back-end systems need to implement and comply with.

6.7.3 Interactions

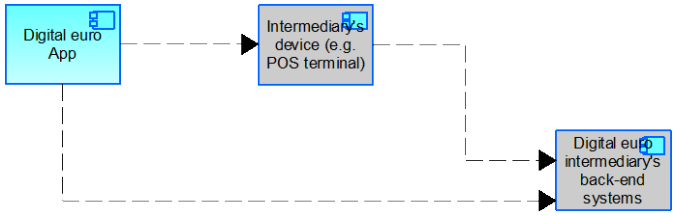


Figure 13: Digital euro App – interactions

Users interact with the app to carry out authentication, initiate funding/defunding, initiate transaction-related activities, check balances and view transaction histories. The app also interacts with other POI devices to exchange information using contactless communication with QR codes or NFC technology.

The app forwards the user interactions and associated data to the intermediary back-end.

The app communicates the feedback from the intermediary back-end (such as the result of authentication, funding/defunding, transaction, queries) to the user to enable further user interaction.

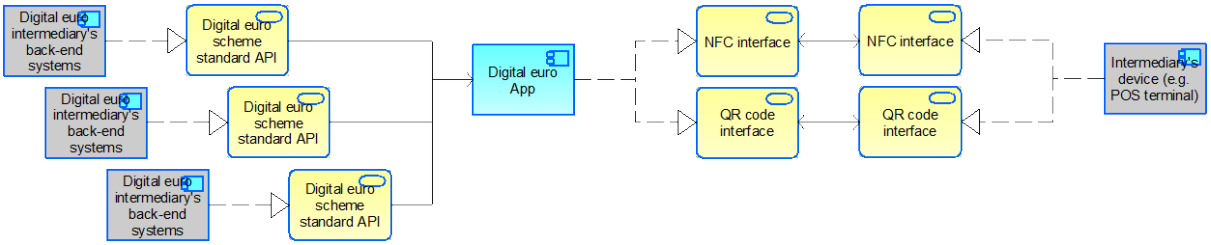


Figure 14: Digital euro App – interfaces

6.7.4 Requirements

The app should support all official European Union languages and provide enhanced accessibility options. The app should feature a help section including a demonstration of how to use the app as well as other content aimed at easing adoption by end users.

The app should allow the users to connect with their intermediary for onboarding.

The app should allow users to authenticate and activate themselves after onboarding with the relevant intermediary. Upon activation, users should be able to identify the intermediary issuing their digital euro account/wallet and link the digital euro account/wallet with the app. They should also have an option to deregister/delink a current intermediary or existing digital euro account/wallet.

The app should support various authentication methods to foster strong customer authentication, as required by the PSD2 regulation, while maintaining a minimum of required personal data. The app should enforce user authentication at login as well as before a user action is confirmed or any of the other services offered by the app are requested.

The app should allow the end user to communicate with the linked intermediary to initiate a transaction (funding/defunding/payment) and to request processing of the transaction.

The app should offer contactless communication using QR codes (to scan and read codes) and NFC. If the Proxy Lookup functionality is implemented, the app should enable users to enter a proxy (e.g. a mobile number) manually or view the contacts stored in the device and select a contact as payee or payer and subsequently enter the amount and associated message.

In addition, the app should allow users to:

- view transaction details and approve or reject a transaction;
- check the current digital euro balance;
- filter and view the transaction history.

When a user starts one of these functions, the app should initiate communication with the linked intermediary to obtain and display the relevant information for the user.

The app should receive settlement confirmations and rejections from the linked intermediary and display the relevant confirmation or rejection for the user.

The app should communicate the relevant user interaction and the associated details (such as authentication and transaction data) securely to the intermediary back-end. The app should communicate with the intermediary back-end using a standardised API layer defined in the digital euro scheme that all the intermediaries back-end systems should support. Once it has received feedback from the intermediary's back-end, the app should communicate the feedback to the end user for information or take necessary action (such as approve/reject).

The provider of the app should follow the update timelines of the relevant mobile operating system and update the app as appropriate to ensure compatibility.

The provider of the app should run functionality to monitor the API endpoints of the connected intermediaries for any connectivity or technical issues. The app should provide a feature to initiate a support request in case of issues, which should be then forwarded to the relevant intermediary.

The app should store only as little information as is required for it to operate. All data stored must be encrypted.

Non-functional requirements

The app should be developed for the latest versions of the mobile operating systems under the Android and iOS platforms and should be downloadable from the official app stores.

The app should also support older versions of the mobile operating systems which fall under the manufacturer's support cycle for backward compatibility.

The app should support installation on smart devices including, but not limited to, smartphones, tablets and smart watches.

The provider must hold the relevant licenses and permissions required to host the app in the official app stores under Android and iOS.

6.8 Integrated Banking App SDK

	*The Integrated Banking App SDK component may be considered to enhance the overall functionality and, ultimately, the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.*

6.8.1 Description

In addition to the Digital euro App, users will have the option of accessing digital euro services via their intermediary's existing mobile banking app, if the intermediary provides one. The Integrated Banking App SDK is a software development kit that helps intermediaries to integrate digital euro services into their own existing apps.

6.8.2 Assumptions

- A standardised API layer is defined in the digital euro scheme that all intermediaries' back-end systems should comply with and implement.

6.8.3 Interactions

The SDK is embedded in the intermediary's mobile banking apps as a software library and provides a client to the API layer integrated into the intermediary's back-end system.

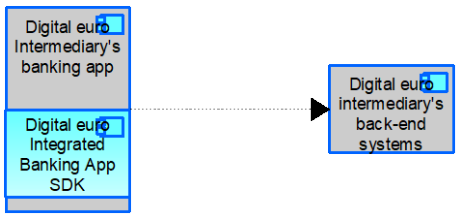


Figure 15: Integrated Banking App SDK – interactions

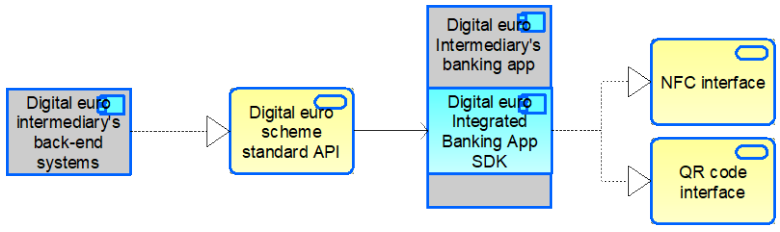


Figure 16: Integrated Banking App SDK – interfaces

6.8.4 Requirements

The functionalities supported are the same as for the Digital euro App. The SDK provides software libraries, documentation and artifacts for the following (non-exhaustive list):

- API client for standardised API layer provided by intermediaries
- NFC interface
- QR code interface (displaying and scanning)
- Association with a URI scheme (e.g. digitaleuro://) for integration with other apps (e.g. for payment flows)
- Custodial wallet implementation: integration with mobile OS key management, signing of transaction messages with signing keys (incl. cryptographic algorithms implementation)
- Push notifications
- UI kits

Non-functional requirements

- The SDK should be developed for the latest versions of the mobile operating systems in the Android and iOS platforms.
- The SDK should also support older versions of the mobile operating systems which fall under the manufacturer's support cycle for backward compatibility.

6.9 Proxy Lookup

The Proxy Lookup component may be considered to enhance the overall functionality and, ultimately, the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.

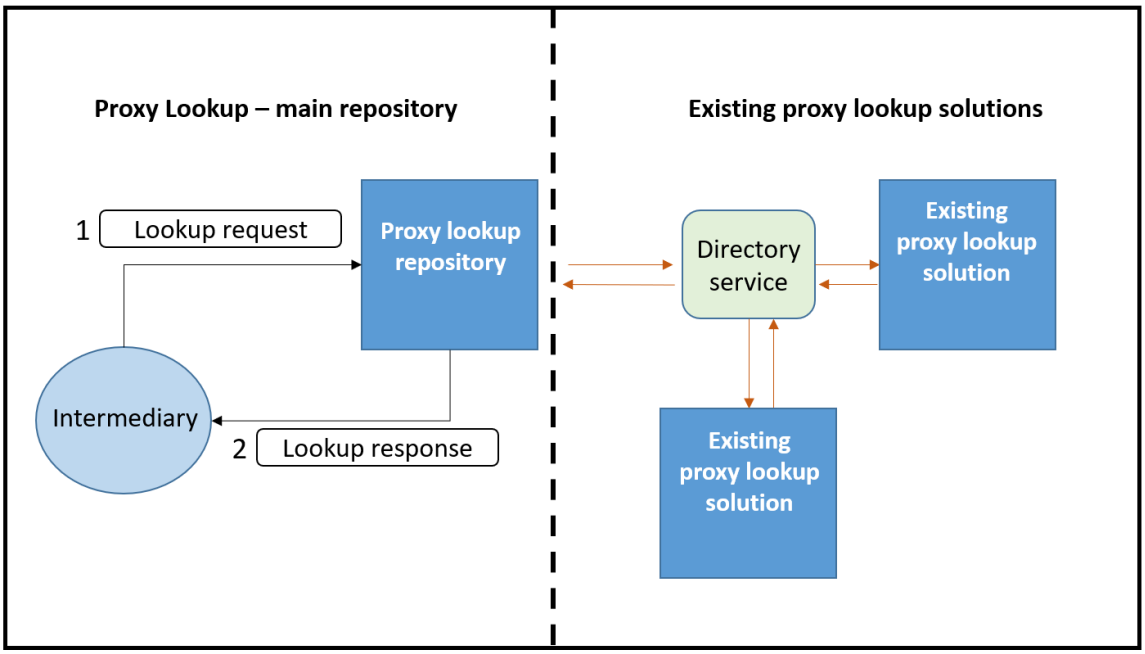
6.9.1 Description

The Proxy Lookup component would consist of a shared repository (either centralised or distributed) that allows intermediaries to pair mobile phone numbers (or other identifiers, such as email addresses) with the corresponding account/wallet details of end users. Data are usually entered in the repository during end user onboarding,[21] if the end user decides to share proxy data (e.g. a mobile phone number). The repository can be queried by means of a lookup request to retrieve the relevant details that are required to instruct a digital euro transaction. Such details are provided to the requestor via a lookup response.

In addition, existing proxy lookup solutions can be incorporated in the repository if they abide by the set of rules, practices and standards (to be identified in a second stage) that makes them interoperable with the repository[22]. In such cases, they would be queried by intermediaries and interoperable with the main repository and one another through a directory service.

[21] A data element can also be entered in the repository at a later stage, or an existing data element can be updated if an end user changes mobile phone number, for instance.

[22] Ensuring the legal basis for personal data processing includes the availability of the personal identifier in the proxy lookup system.



6.9.2 Assumptions

- Only one proxy data element (e.g. a mobile phone number) is initially supported, but additional proxy data elements (e.g. an email address, user name) could be added later.
- A proxy lookup request is optional and initiated by an intermediary only if it receives a payment request in which the payer or the payee is identified with a proxy.

6.9.3 Interactions

Figure 17: Proxy Lookup – interactions

Only intermediaries interact directly with the Proxy Lookup component (which may incorporate existing proxy lookup solutions). The Proxy Lookup API should support the processing data update requests and the retrieval of the identifiers required to process and settle the payment transaction. In both cases, the intermediary initiates the communication with the proxy lookup service provider and waits for its response.

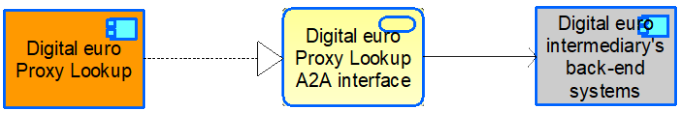


Figure 18: Proxy Lookup – interfaces

6.9.4 Requirements

Data update

- The Proxy Lookup should ensure the uniqueness of any proxy lookup data (one proxy data element can only be mapped to one digital euro account/wallet identifier).
- The Proxy Lookup should store the following information regarding an end user: a digital euro account/wallet identifier, a proxy data element (mobile phone number) and the identifier of the intermediary acting on behalf of the end user in the digital euro components.
- After every proxy database update request, the relevant intermediary should be informed if a proxy database was updated (proxy data element provided is unique) or not (proxy data element provided is already in use).
- The Proxy Lookup should support the updating of existing data entries (e.g. if an end user changes mobile phone number) and the deletion (deactivation) of data (e.g. if an end user is being offboarded).
- The database(s) should be restorable from a contingency data snapshot, and an audit trail of all the update activities should be kept.
- The Proxy Lookup should provide an intermediary with a report that details all intermediary's update requests registered in the last calendar day. Such reports should provide details of all maintenance activities and are provided to the relevant intermediary as soon as available.
- End users' data should be well protected against an unauthorised use due to a security breach or cyberattack. All data processing related to the functioning of the Proxy Lookup should adhere to the highest security and privacy standards.

Data retrieval

- The Proxy Lookup should include in the positive response all the data required to instruct a digital euro transaction.

- The Proxy Lookup should indicate in the negative response to the intermediary that the validation of a proxy query failed or that the proxy lookup element does not exist in the database.
- If existing proxy lookup solutions are incorporated in the repository, the main repository or the proxy lookup solution that receives the request should be queried first when an intermediary initiates a proxy lookup request. If the query does not return a result, the main repository/existing proxy lookup solution should forward the lookup request to a directory service with a view to identifying where the information is stored. Once the relevant data have been retrieved, the directory service should deliver it to the intermediary through the main repository/existing proxy lookup solution queried in the first place.

Non-functional requirements

- The Proxy Lookup should ensure authentication and authorisation of an intermediary in all interactions.
- The Proxy Lookup should support the use of privacy-enhancing techniques when processing data.
- The Proxy Lookup should be available 24/7 and meet performance requirements (e.g. throughput, latency) to support data update and data retrieval interactions (please refer to high-level requirements in Chapter 2).

6.10 Onboarding Repository

	*The Onboarding Repository component may be considered to enhance the overall functionality and, ultimately, the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.*

6.10.1 Description

The Onboarding Repository is a database needed to uniquely identify and differentiate between digital euro end users across the digital euro environment. Identification is based on a digital euro end user identifier which is created by hashing a unique national personal identifier (e.g. a taxpayer ID). A digital euro end user identifier is communicated to the Onboarding Repository by the intermediary that onboards the end user. A digital euro end user's identifier is not used in any other digital euro components, and only the end user's intermediary can link an identifier to other personal data (such as the digital euro account/wallet identifier of a digital euro end user).

For market research purposes, only one digital euro account/wallet per end user is envisaged. During onboarding, the intermediary would check if the Onboarding Repository already contains a corresponding end user identifier. If it does not, onboarding can continue as the digital euro end user does not have an existing digital euro account/wallet.

The Onboarding Repository should also allow a digital euro end user identifier to be updated (e.g. in case a digital euro end user relocates to another country and receives a new unique personal identifier) and data to be deleted or deactivated (e.g. when a digital euro end user is offboarded).

6.10.2 Assumptions

- One identifier (derived from a unique national personal identifier) is distinct enough to identify and differentiate between end users.
- The unique national personal identifier is ideally the same for all relevant countries.

6.10.3 Interactions

Only intermediaries interact directly with the Onboarding Repository. The Onboarding Repository should support APIs required to process data update requests and queries.

Figure 19: Onboarding Repository – interactions

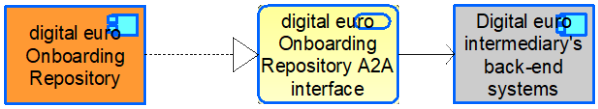


Figure 20: Onboarding Repository – interfaces

6.10.4 Requirements

- The Onboarding Repository should store a digital euro end user identifier (i.e. a hash value of a unique national personal identifier) and an intermediary's identifier.
- The Onboarding Repository should be able to store more than one digital euro end user identifier if a digital euro account/wallet is owned by multiple end users.
- After an Onboarding Repository update has been requested, an intermediary should be informed if the repository was updated (the end user does not have an existing digital euro account/wallet – onboarding can continue) or not (the end user already has an existing digital euro account/wallet – onboarding should be cancelled).
- The Onboarding Repository should support the updating of existing data entries (e.g. if there is a change in a unique national personal identifier) and the deletion (deactivation) of data (e.g. when an end user is offboarded).
- The Onboarding Repository should provide an intermediary with a report detailing all intermediary's update requests registered in the last calendar day.
- The Onboarding Repository should assist in prevention or reconciliation of errors resulting from an end user presenting a wrong unique personal identifier to an intermediary. (An end user might accidentally enter a unique personal identifier of another person in the onboarding form.)
- The Onboarding Repository consisting of interoperable databases managed by multiple operationally independent entities. would be preferred over a centralised implementation.
- If possible, the repository should also reuse existing databases (such as national banking account repositories).

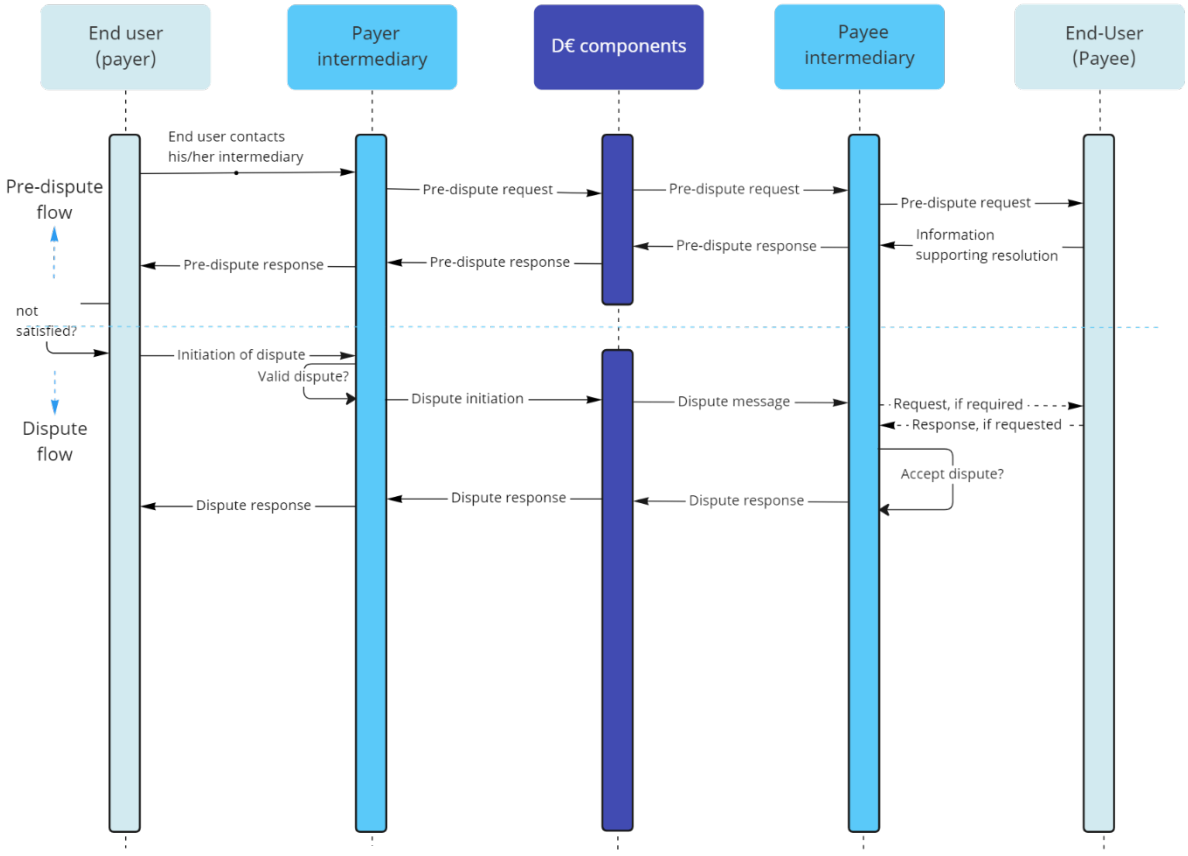
Non-functional requirements

- The Onboarding Repository should ensure authentication and authorisation of intermediaries in all interactions.
- The Onboarding Repository should be restorable from a contingency data snapshot, and an audit trail of all the update activities should be kept.
- The Onboarding Repository should support the use of privacy-enhancing techniques when processing data; only hashed data are processed in the Onboarding Repository.
- The Onboarding Repository should be available 24/7. The query of the Onboarding Repository does not negatively affect digital euro end users' onboarding experience (i.e. an intermediary receives an instant reply from the Onboarding Repository).

6.11 Dispute Management

	*The Dispute Management component may be considered to enhance the overall functionality and, ultimately, the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.*

6.11.1 Description



Dispute resolution can be divided into three phases: pre-dispute, dispute and arbitration.

Pre-dispute

The pre-dispute phase enables the payer and payee to clarify the issues between each other directly, supported by a tool-based, structured process. In particular, two scenarios are addressed during this phase.

- The payer does not recognise the transaction because transaction details are missing or they simply do not remember the transaction. Provision of additional information from payee to payer might help to resolve the issue at this stage.
- The payer does not accept the payment for legitimate reasons[23] arising after payment was completed. For example, the payer has been debited twice or more, the transaction was cancelled but still debited, or goods or services have not been delivered. The payee can refund the payer, offer another form of compensation or deliver a replacement.

The dispute management infrastructure logs the pre-dispute communication/messaging between payer and payee for possible use in any subsequent steps.

Ideally, the issue will have been resolved by the payer and payee during the pre-dispute process. If this is not the case, the dispute process would be initiated.

Dispute

If the pre-dispute process is not successful because the payee did not react or the payer does not accept the proposed solution, the payer – or the intermediary on behalf of the payer – initiates the dispute process.

The dispute management infrastructure logs the dispute communication/messaging for possible use in any subsequent step.

Arbitration

Arbitration is the final step in process. If the intermediaries representing the end users cannot reach agreement on the issue in dispute, the scheme – or a selected entity acting on behalf of the scheme – steps in to take a decision.

[23] Legitimate reasons to be defined in the scheme rulebook

6.11.2Assumptions

- The digital euro scheme will support dispute resolution via a dedicated component transmitting messages between the intermediaries.
- The settlement process for financial disputes will be similar to the process for usual digital euro payments and marked as dispute-related to faciliate identification.
- Both exchange of information (pre-dispute phase) and financial messages (dispute resolution phase) will be supported; the arbitration process is considered out of scope of the market research.

6.11.3Interactions

Figure 21: Dispute Management – interactions

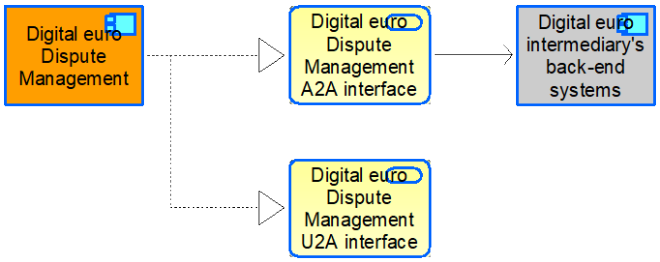


Figure 22: Dispute Management – interfaces

- In addition to interacting with the intermediaries' back-end systems, the Dispute Management component might also interact with the Access Gateway (see Section 6.6) and Reference Data Management (see Section 6.3) components.

6.11.4Requirements

- The (pre-)dispute function should support the exchange of dispute messages between intermediaries.
- A (pre-)dispute API should be available to intermediaries to initiate and respond to (pre-)dispute requests.

- Incoming (pre-)dispute request messages from the payer's intermediary should be forwarded to the payee's intermediary.
- Incoming (pre-)dispute response messages from payee's intermediary should be forwarded to the payer's intermediary.
- The (pre-)dispute API should support the provision of documentation together with the (pre-)dispute response.
- The dispute-related data exchanged between intermediaries required for subsequent processes, reconciliation and statistical/reporting purposes should be stored.
- The data from the component should be accessible via user-to-application (U2A) and application-to-application (A2A) interfaces.
- The component should be capable of managing user access rights.
- For data elements of the (pre-)dispute message which might contain personal data end user privacy-preserving GDPR compliant solutions should apply.

6.12 Fraud and Risk Management

The Fraud and Risk Management component may be considered to enhance the overall functionality and ultimately the customer experience. It represents an option that may or may not be included in the final scope, it is not a fixed element of the current design and its interactions with other components are yet to be finalised.

6.12.1 Description

Digital euro scheme rules and regulations might expect or require intermediaries to perform risk management and carry out fraud prevention and detection measures and to monitor the digital euro activities within their area of responsibility. Ideally, the risk and fraud management specific to the digital euro will be integrated into existing infrastructures and applications that are used to manage risk and fraud for other retail payment schemes.

Although intermediaries will operate their own systems and apply appropriate fraud and risk management processes, a Fraud Monitoring and Management capability might be required at scheme level to identify suspicious activities across many participants which cannot be monitored at intermediary level.

The Fraud and Risk Management component under consideration should support fraud prevention during the validation process, in support of intermediaries (i.e. by scoring the risk profile of a transaction) taking online real-time decisions to identify fraudulent or suspicious transactions before these are recorded in the Settlement component. Furthermore, the Fraud and Risk Management component should identify fraudulent patterns across completed and settled transactions.

Accordingly, fraud prevention rules should be continuously improved to prevent future fraud.

6.12.2 Assumptions

- The Eurosystem will support fraud management in addition to any fraud management tools currently used by intermediaries.

6.12.3 Interactions

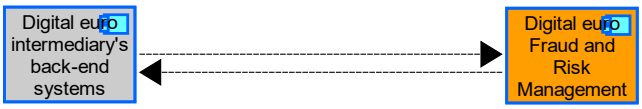


Figure 23: Fraud and Risk Management – interactions

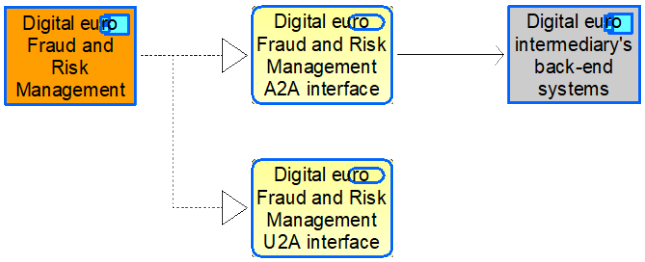


Figure 24: Fraud and Risk Management – interfaces

- The component should interact with intermediaries during payment validation, providing a transaction risk profile assessment result in the validation message.
- The fraud-related data and/or fraud management results required for subsequent processes (e.g. for statistical/reporting purposes) should be stored.
- The data from the component should be accessible via user-to-application (U2A) and application-to-application (A2A) interfaces.
- The component should be capable of managing user access rights.

6.12.4 Requirements

- Fraud and Risk Management should support fraud prevention during the validation process.
- Fraud and Risk Management should support ex post fraud detection to identify fraud and support the definition of new and/or modification of existing fraud prevention rules.
- Fraud and Risk Management should support the provision of fraud-related reporting.
- The privacy of digital euro end users should be safeguarded. Adequate privacy-protecting techniques should be applied so that transaction data required for fraud detection and prevention should be safeguarded and not be accessible to the Eurosystem.