EUROPEAN CENTRAL BANK
EUROSYSTEM

ECB-PUBLIC

Digital euro market research

Answers to questions received

3 February 2023

This document summarises the answers to questions received in the Eurosystem market research on possible technical solutions for a digital euro. Answers are provided for the purpose of market research only and do not imply or commit the Governing Council to any potential decision on the implementation of a potential digital euro or on its final design, as a number of topics are still open.

A decision on whether the Eurosystem will enter into a further realisation phase of a digital euro, and its design, will only be made towards the end of 2023 (see also the digital euro pages on the ECB's website).

Main Clarifications and Errata

- **The costs provided for Development in Section 4.1 of Annex 2 should also include the costs for maintenance for a period of 5 years. Annex 2 has been replaced with a revised version including these clarifications. Also, the column description in Section 2.1 of Annex 2 has been adjusted to read "Development & Maintenance".**
- **The 5th requirement in Section 6.8.4 of Annex 1 related to the Integrated Banknote App SDK should read "Self-custodial wallet implementation"**

General questions

Question 1

Is the expectation that there will be one Digital Euro system across all Europe, or the design is still open for independent instances of such system in different EU countries that would however need to interoperate with the rest?

The technical implementation design is still open, the Eurosystem would like to better understand the pros and cons of each solution and its impact on development costs and implementation timelines.

Question 2

Chapter 7.2. of the main document relates to "Confidentiality/intellectual property". Hence, the last sentence of this chapter "Ownership of all information provided, and correspondence submitted to the ECB in response to this market research exercise passes to the ECB upon receipt" may need clarification.

Does ECB claim ownership of/rights on respondent intellectual property?

This is standard wording ensuring that the ECB can transmit the information provided to the Eurosystem project team and governance bodies and use the information provided solely as outlined in the Main Document associated with this market research. The ECB will decide at its own discretion which information to publish.

All information provided, all correspondence with the ECB and any potential design solution in response to the market research exercise shall be the property of the ECB.

Question 3

Do the words in attachments count as part of the 500 words? Referring to 'Please make sure that your responses are clear, concise and not longer than 500 words per free-text entry. Your answers should be in English. You may also submit attachments describing things like the components and/or related operational services.'

The limitation has been introduced to ensure that the number of expected responses can be processed in a limited timeframe. Respondents are kindly requested to try to adhere to this word count as much as possible. Content provided in additional annexes will be processed on a best-effort basis only.

Question 4

Can anybody send its input on questions to the specified email address (digitaleuro-marketresearch@ecb.europa.eu) or first ECB expect that experts submit their participation intention and then ECB selects certain experts which shall be requested to provide input?

Digital euro market research targets all relevant interested parties, who can respond to the market research by submitting a completed questionnaire to the email address mentioned. By the stated deadline, respondents should not only submit their intention to participate but also their complete input. The ECB will not conduct any preselection and, after the deadline has passed it will evaluate all responses received. It is also possible that some respondents may receive a request to be interviewed.

Question 5

“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.”

Which element of the system will be responsible for the policy limits for users?

Any interaction with end users will be done by the intermediaries based on the rules defined by the Eurosystem. For market research purposes only, digital euro components would not control limits per user for the online part. The off-line component will control the limit at a device level. Remuneration will be calculated as per the requirement in Section 6.4.4.

Question 6

Does the ECB only consider Technical Readiness Level (TRL) 9 as compliant with the notion that any Digital Euro component shall rely only on proven technologies (Annex 1, page 10), or will other TRL-levels also be considered for a possible solution?

The Eurosystem is researching on all potential technological solutions and is looking for the solutions that best fit the stated requirements. As such, systems with lower TRLs should also be proposed. The development time and costs provided in the answers to the questionnaire (Section 4.1 of Annex 2) should then include the time and costs needed to develop the technology to the level required for production use in a potential digital euro.

Question 7

In Annex 2, question 2.12, you ask for the Product Environmental Footprint (PEF) of the solution and measures to minimize the PEF. Do you expect a quantitative assessment (i.e., calculating the PEF as described in the PEF-Guide), or is a qualitative assessment sufficient (e.g. describing the main drivers of the environmental performance of the solution and how the environmental impact is minimized?)

A qualitative assessment is sufficient, with any further detailed insights being welcome.

Question 8

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).

Could you explain in detail what you mean by geographical regions? Is it linked to countries? Could you confirm that the minimum infrastructure consists of 6 sites with, at least, 500 kms between them on 3 different countries (2 sites per country)?

A geographical region is foremost to be a measure to withstand regional disasters. From this point of view, it is linked to a distance which is assumed a regional disaster would not span across, i.e. 500km. A minimum of six sites (two sites per region, three regions) is in line with the requirements. Solutions with three regions, each being in a different country, are welcome.

Question 9

There is no page 74, but the footer indicates a Page x of 74. Could you confirm it’s a blank one?)

Yes, this is confirmed. Annex 1 consists of 74 pages including the cover page, but the page numbering only starts on page 2, hence the inconsistency.

Question 10

Ad Questionnaire, chapter 2, "General questions", Q 2.1: "Development only" vs. "Development, operation & maintenance": Does "Development only" mean only development of a first release of a component for the digital Euro, or will this also include the ongoing development of future releases of a component (which would in our understanding be maintenance)? Or vice versa: we would like to offer software development services including the development of future releases…

We would like to clarify that ''Development only" shall also include the ongoing development of updates (corrective maintenance) for a period of five years. The wording in Annex 2 (questionnaire) has been updated accordingly and a revised version has been published. The category is now called "Development incl. 5Y maintenance".

Question 11

Page 8: the figures shown in the table do not seem consistent with the percentages indicated in footnote 5. In particular, daily transactions' figures (3.75, 55.00 and 175.00 million) do not seem to correspond to the usage percentages indicated in the footnote (5%, 20% and 35%). Is there behind an assumption (not documented in the footnote) concerning an 'overhead' related to manual and automatic (de)funding transactions?

Yes, correct. There is an undocumented assumption of adding 25% transactions on top of the mentioned payment figures to cater for funding and defunding transactions.

Calculation example for the small scenario:

30 million end users using the digital euro for 0.1 payments per user per day (5% of the average of 2 payments per user per day) resulting in 3 million payments per day. Adding 25% on top for funding and defunding transactions results in 3.75 million daily transactions.

High-level requirements

Question 1

“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.”

Is an end user only an EU resident? As per 6.10.1 what are the entity values permissible to identify a user to control the user wallet limit?

The document Progress on the investigation phase of a digital euro – second report states that everyone in the euro area could pay and receive payments in digital euro, while more detailed end-user access criteria are still being analysed. Please refer to Section 6.10.2 of Annex 1 of the market research for the assumptions regarding identification of an end user.

Question 2

“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.”

Are push payments the only supported method? When verifying the transaction will this include available balance, fraud checks etc…?

Pull payments (payment requests) could also be supported (e.g. for recurring e-commerce payments). Indeed, transaction validation by intermediaries should include the checks on available balance, fraud checks, etc., as currently done for any payment.

Question 3

“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.”

What happens if the funding instruction is declined? Who / What determines what the holding limit is for a user?

The assumption for the market research is that holding limits for end users would be controlled by the intermediaries. If a funding instruction is declined, the whole “reverse waterfall” transaction, including the payment, will be rejected.

Question 4

“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.”

Is it possible to have some reference data examples?

Some examples of references data for intermediaries are:

- identifier: the ISO compliant identifier;
- type: e.g. credit institution, payment institution, electronic money institution;
- intermediary’s long and short names;

intermediary's address;
contact person of the intermediary and position of contact person;
contact person phone's number and e-mail address.

End-to-end flows

Question 1

"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." (§3)

Please clarify whether intermediaries are allowed to hold digital euro liquidity in order to satisfy end user funding requests internally, or whether any funding request must go through digital euro components.

Intermediaries do not hold digital euro and intermediaries' holdings in their TARGET dedicated cash account (DCA) are not regarded as digital euro. Any funding/defunding request should go through the digital euro components.

Question 2

Could "waterfall" and "reverse waterfall" procedures also be considered to be intermediaries' responsibilities, given that intermediaries also operate cash machines?

Waterfall and reverse waterfall would be facilitated by the intermediaries. The process would be triggered by the intermediary immediately before (reverse waterfall) or as soon as possible after (waterfall) the payment, provided there is a linked commercial bank account. I.e., "waterfall" and "reverse waterfall" procedures are considered intermediaries' responsibilities,

Question 3

"Funding and defunding can be done from/to a commercial bank account or cash (e.g. at ATMs)"

How will a transaction direct from the CBDC wallet direct to cash be facilitated?

Such defunding would be facilitated by the intermediaries. Upon receiving a defunding request from end user, the intermediary would send a defunding instruction to the digital euro components (to debit the end-user's account/wallet and credit their DCA) and would then provide to the end user the corresponding amount in cash (via a cash withdrawal at an ATM or in a branch).

Question 4

"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."

What is the exception process if for example the linked commercial account is no longer valid / available?

The intermediaries will check during the validation phase whether there is a linked valid commercial bank account. If there is not, the (de)funding cannot be executed, and the payment instruction will be rejected.

Component 1: Settlement

Question 1

In Section 6.1.1 Description (page 26)

“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."

1. What is the notion of privacy considered here and w.r.t. who? Does privacy refer to concealing the transactors (payer and payee and intermediaries) to the central bank or third parties that have access to the settlement component, as well as the transaction amount? If so, what would the audit requirements be in this system or visibility of regulators (.e.g, upon certain authorised request).

2. What are the transparency needs of the settlement component to the Eurogroup participants?"

1. Requirements regarding privacy can be found in the non-functional part of Section 6.1.4. Privacy refers to privacy of end users (payers, payees) against of the Settlement component or central bank and against other intermediaries (not chosen by the end user nor participating in a transaction with the end user). Transaction amounts should be visible to the Settlement component only and to the intermediaries involved in the transaction. In order to be compliant, upon certain authorised requests from regulators, the data in the Settlement component (or from legal archiving) regarding the request has to be provided.

2. It is assumed that intermediaries maintain the business relationship with end users, maintain their personal data and are the only parties able to link the digital euro holdings recorded in the Settlement component to an end user. Thus, there could only be transparency about money transfers between holding identifiers, and it should not be possible to construct payment patterns of a given user based on information processed by the settlement component.

Question 2

Should we provide for integration of the solution to existing Instant Payments infrastructure (SEPA Instant Credit Transfer Schemes)? so e.g. using the TIPS Dedicated Cash Accounts.

Integration with the existing Instant payments infrastructure is not required. The DCA Management component foresees the use of a dedicated cash account for the purpose of liquidity transfers and funding/defunding of end users’ digital euro holdings.

Question 3

Digital euro holdings need to have pseudorandom identifiers. Are intermediaries responsible to generate and maintain mapping of single use pseudorandom IDs of actual end-users?

Only an intermediary knows the identities of its end users and the mapping to the pseudorandom identifiers used in the settlement infrastructure. There is no requirement concerning who can or should generate these identifiers, but this should be clearly described when proposing a solution so that we can better understand the pros and cons.

Question 4

What privacy-enhancing techniques are to be considered in scope? Given that many PETs are relatively new, what level of (mathematical, scientific) maturity are deemed sufficient?

The Eurosystem is researching all potential technical solutions and is looking for the solutions that best fit the stated requirements. As such, systems with lower maturity (or lower TRLs) should also be proposed. The development time and costs provided in the answers to the questionnaire (Section 4.1 of Annex 2) should then include the time and costs needed to develop the technology to the level required for production use in a potential digital euro.

Question 5

Please clarify whether a layer 1 token-based digital euro system would generally be deemed to satisfy ECB's requirements.

The Eurosystem is researching all potential technical solutions. A solution needs to fulfil the stated functional requirements, like central verification and recording of each transaction, and non-functional requirements, like latency and scalability. If what you refer to as a "layer 1 token-based" system can do this, feel free to propose such a solution.

Question 6

Please clarify the envisioned mechanics of remuneration. According to our reading, there could be (at least) two possible interpretations:

i. Each intermediary receives remuneration based on their total holdings, and in turn each intermediary distributes to their customer.

ii. Each user receives remuneration based on their individual holding, but intermediaries are tasked with distributing the remuneration.

Please also clarify the feature interactions between remuneration, offline wallets, and portability of holdings (as set out in §6.1, p. 29).

Intermediaries will not hold digital euro, which rules out interpretation (i). Interpretation (ii) should be complemented with the constraint related to privacy, which implies that only the intermediary is able to compute the holdings and remuneration of individual end users while the Settlement component is able to check the intermediary's overall end user holdings. Remuneration requirements are stated in a component that is different from the Settlement component (see the subsection "Functionalities" in Section 6.4.4). When providing your solution, please elaborate on the chosen remuneration calculation method(s) and their pros and cons or reasons why they were chosen.

Regarding feature interactions: for the purpose of this market research, offline holdings shall not be remunerated. In the case of the porting of holdings, remuneration shall be paid before the move to another intermediary.

Question 7

Page 28: it is stated that 'The Settlement component interacts with […] the RDM component for receiving real-time reference data or general configuration data and using the results for authorization purposes or checking a maximum transaction limit, etc.' Can you confirm that the mentioned real-time propagation of reference data from RDM to Settlement is required only for a limited subset of data (e.g. blocking/unblocking of participants/holdings) and that a daily propagation of data is sufficient for all the other reference data? If this is not confirmed, could you please clarify the business rationale / use case for imposing a real-time propagation of all reference data from RDM to Settlement?

The Settlement component needs real-time access to reference data from the (Reference Data Management (RDM) component for all the reference data that are necessary for all tasks related to the real-time processing of transactions and queries.

Question 8

Page 31: as a non-functional requirement, it is stated that '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.'

a. The points (i) and (ii) look actually pure functional requirements. Could you please clarify why you see them as non-functional requirements? Are we missing some specific technical requirements here?

b. The point (iii) may be a non-functional requirement, but we do not understand its rationale. Could you please clarify the reason why an intermediary should be allowed to query 'at least' a minimum number of holdings? What would be the drawback without this requirement?

This requirement and its subpoints are considered to be non-functional from the point of view of protecting end-user privacy, which is very important and essential to a digital euro solution (see the paragraph on end user privacy on page 10 in section 2 High-level requirements).

Ad (a), points (i) and (ii) aim to not jeopardise end-user privacy by revealing information to intermediaries other than those chosen by the end user. Potentially these may be seen as functional requirements, but the aim is to protect the non-functional end-user privacy.

Ad (b), point (iii) aims to not jeopardise end-user privacy by revealing information to the operator / central bank. An intermediary sending a query could reveal information about the end user via (meta) data, e.g. an end user's total digital holdings when querying all of them at the same time. Being required to query at least a minimum number of holdings is assumed to increase privacy in this regard because holdings of different users might be requested within one query.

When proposing a solution, any further considerations on how to improve end-user privacy against other intermediaries or the operator/central bank and the trade-offs these come with are welcome.

Component 2: DCA Management

Question 1

Page 32: it is stated that '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.'

a. Can you confirm that the mentioned real-time access consists in a real-time propagation of reference data from RDM to DCA Management and that it is required only for a limited subset of data (e.g. blocking/unblocking of participants/accounts, intraday creation/opening of new DCA) and that a daily propagation of data is sufficient for all the other reference data? If this is not confirmed, could you please clarify the business rationale / use case for imposing a real-time propagation of all reference data from RDM to DCA Management?

b. As DCA-related reference data shall also be propagated to and used by T2/CLM, can you confirm that the reference data propagation rules from RDM to DCA Management shall be consistent with those related to the reference data propagation from CRDM to T2/CLM. If this confirmed, ensuring consistency would obviously require aligning the two propagation processes also in terms of what shall be propagated real-time and what shall be propagated on a daily basis.

a. Only business-critical updates performed in the RDM component shall be immediately reflected in the DCA management component. Frequency and timeliness requirements of updates will vary for different configuration and reference data, depending on business need.

b. See point (a) and the related comment.

Question 2

Page 34: it is stated that '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.' This statement seems to imply that the DCA Management component shall not have its local reference data and make direct (real-time) use of reference data stored in the RDM component. This is most likely not feasible from a technical standpoint, as it would not allow fulfilling all the given non-functional requirements (e.g. transactions' latency requirements). Can you confirm that the statement only refers to the necessity, for the DCA Management component of receiving the most recent update of the reference data from the RDM component (with some reference data potentially to be propagated real-time and all the others propagated on a daily basis)?

Updates of business-critical configuration and reference data shall be reflected in the DCA component immediately, as soon as they are performed in the RDM component. Caching of configuration and reference data should be possible as a general rule, but specific constraints and/or exceptions might apply depending on the business need.

Question 3

As for question 3.2.1, could you please clarify which non-functional requirements you are referring to? In Annex I we did not find anything specific for this component. Furthermore, volumetric requirements related to (de)funding operations and liquidity transfers seem to be missing.

Please refer to the general non-functional requirements in Chapter 2 of Annex 1 of the market research.

With regard to the volumetrics of funding and defunding transactions, please see the clarification in the answer to Question 12 in the general questions. We assume the volumes of the liquidity transfers would be negligible in comparison to the funding and defunding.

Component 3: Reference Data Management

Main Clarifications and Errata

- With regards to the requirements for the RDM component:
    - Frequency and timeliness requirements of updates will vary for different configuration and reference data, depending on business need. The RDM component shall support several scenarios, e.g.
        - business-critical data updates that must be reflected immediately in dependent components, vs non-business-critical data updates that can be reflected in dependent components with a pre-defined acceptable delay;
        - frequent (e.g., intraday) updates vs infrequent (e.g., daily, weekly, monthly, occasional) updates;
        - scheduled updates vs on-demand updates.
    - The choice of paradigm, i.e., whether push or pull, can be considered a design detail at this stage; the most appropriate choice might depend on a number of additional factors (business and technical) that are not known at this time. As a guideline, non-time-critical updates could be performed in pull fashion, but the RDM component will nevertheless have to support both paradigms, and the respondents are free to make their own recommendations and proposals of interface paradigm.
    - Caching of configuration and reference data by the dependent component should be possible as a general rule, but specific constraints and/or exceptions might apply depending on the business need.

Question 1

RDM should ensure consistency of data in the RDM with data in TARGET. It is expected that TARGET/CRDM is to be mastering the common data, are we correct?

Please refer to:

- the assumption on Page 36 of Annex 1: “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”;

- the requirement on Page 39 of Annex 1: “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.”

The Common Reference Data Management (CRDM) component of TARGET holds the master records for data of intermediaries active in both TARGET services and digital euro. For such data, CRDM will act as the “source of truth” Thus creation and maintenance will be performed in CRDM only, and the data will be propagated to / retrieved by the RDM component. For intermediaries active in the digital euro but not in TARGET services, creation and maintenance will be performed in RDM and no propagation/retrieval in TARGET is required.

Question 2

Do you envision to use RDM as a meta data infrastructure storing reference identifiers and lineage in order to resolve a settlement or dispute or supporting surveillance requirements upstream?

Settlement, Dispute Management or any other component might request some intermediary master data from RDM if required for processing purposes. However, RDM should not store any transaction-related identifiers. Any transaction references should be stored as part of the transaction data record as unique transaction identifiers assigned during transaction processing.

Question 3

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. Is Reference Data Management expected to be synced REAL time with the Target system data?

The synchronisation between RDM and CRDM should be ensured in real-time, consistent with the availability of the CRDM component (22 hours a day, on weekdays).

Question 4

What is the definition of real-time in terms of speed that data update is propagated to other dependent components? E.g., updating the master reference data, how fast should this update be available to the dependent components?

Updates of business-critical configuration and reference data shall be reflected in the dependent components immediately as soon as they are performed in the RDM component.

Question 5

What authentication mechanism is planned to allow different components to access to RDM?

Since RDM should contain data belonging to different components, segregation principles need to be put in place to make sure that relevant data are made available to each component depending on individual needs. In this respect certain reference data (e.g. country, currency) are fully available – they are made available to every component without distinction. Other reference data are component-specific and are made available in full to a single component. Finally, certain reference data are available to multiple components, but the data are segregated and made available to a given component based on the values of specific attributes that link each instance to a specific component, either directly or indirectly.

Question 6

What is the plan in terms of metadata management? Would there be a central metadata platform that can be leveraged across systems?

The respondent can make proposals and describe how metadata management would be addressed in their solution.

Question 7

What are the requirements for data lineage?

At the current stage and in relation to RDM, a first set of general requirements has been identified (outside the scope of the market research) in terms of audit trail, data history and data consistency.

Question 8

Page 37: it is stated that the RDM component provides real-time access to all other D€ components. This is most likely not feasible from a technical standpoint, as it would not allow fulfilling all the given non-functional requirements (e.g. transactions' latency requirements); furthermore, it appears implausible that one single physical data model (in RDM) would ensure optimal performance in the real-time access of a multitude of different components. Can you confirm that the statement only refers to the necessity, for the different D€ component of receiving a consistent and up-to-date set of reference data from the RDM component (with some reference data potentially to be propagated real-time and all the others propagated on a daily basis)?

Frequency and timeliness requirements of updates will vary for different configuration and reference data, depending on business need. The RDM component shall support several scenarios, e.g.

- business-critical data updates that must be reflected immediately in dependent components, vs non-business-critical data updates that can be reflected in dependent components with a pre-defined acceptable delay;
- frequent (e.g. intraday) updates vs infrequent (e.g. daily, weekly, monthly, occasional) updates;
- scheduled updates vs on-demand updates.

Question 9

Page 38: it is stated that bulk loading shall be available in U2A mode. Can you confirm this refers e.g. to the upload of reference data via .txt files, .xls spreadsheets, etc.?

Yes. The upload should be available in U2A mode via a file containing the reference data to be created in RDM. In principle, the file could be generated in Excel or comma separated value format.

Question 10

Page 39: it stated that '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.' This statement seems to confirm the following two important points:

a. That a reference data propagation process shall exist between RDM and the other components (which means the different components have their own local reference data and do not have to access real-time RDM to perform their processing activities).

b. That such a reference data propagation process shall be real-time only for a subset of data (and not for all them), which implies the existence of a daily reference data propagation process, too.

Can you confirm our understanding is correct? Furthermore, can you confirm the 'pull' real-time propagation is not really necessary and can be better implemented by means of 'push' real-time propagation, so to increase the efficiency of the propagation process and reduce its complexity?

(a) : Caching of configuration and reference data should be possible as a general rule, but specific constraints and/or exceptions might apply depending on the business need.

(b) : please refer to the answer to Question 8.

Regarding the choice of paradigm, i.e. whether push or pull, we would like to clarify that we consider this a detailed design detail; the most appropriate choice might depend on a number of additional factors (business and technical) that are not known at this time. As a guideline, non-time-critical updates could be performed in pull fashion, but the RDM component will nevertheless have to support both paradigms, and the respondents are free to make their own recommendations and proposals of interface paradigm.

Question 11

Can you confirm RDM is not expected to be available 24x7? If this is not confirmed, could you please clarify the business rationale / use case for RDM to be a 24x7 component?

The main requirement related to the availability of data is that critical updates should be immediately available to the relevant component.

Question 12

As for question 3.3.1, could you please clarify which non-functional requirements you are referring to? In Annex I we did not find anything specific for this component. Furthermore, volumetric requirements related reference data maintenance operations seem to be missing.

Please refer to the general non-functional requirements in Chapter 2 of Annex 1 of the market research.

Component 4: Data Warehouse

Question 1

What are the data types the DWH Component needs to be able to handle or for now is it fair to assume that most data will be structured, but also unstructured data (like documents) need to be stored in the Data Warehouse?

Both structured and unstructured data should be assumed.

Question 2

Processing latency for digital euro queries is expected at 0.5 seconds (for 99% of all processed digital euro queries). This requirement is related to Access Gateway and Settlement. Which performance expectation applies for the DWH component?

The Data Warehouse component will not serve real-time queries, but only analytical and reporting queries with performance requirements depending on the business need, which cannot be provided at this stage.

Question 3

Will the DWH be used for operational purposes only, e.g., monitoring, troubleshooting?

No.

Question 4

Is the historical data for archiving non-CSI (Confidentiality Statistical Information) – hence, can it be stored in a (public) cloud storage solution?

It cannot be excluded that CSI will be present in the archived data. For the purposes of the market research, no constraints on cloud-based solutions are given.

Component 5: Offline Solution

Question 1

In Section 6.5.1: "The envisioned solution uses Secure Elements (SEs) on the end user devices, to ensure the proper execution of application logic, including required cryptographic primitives."

The traditional definition of Secure Elements, such as given in Vauclair, M., "Secure Element", in van Tilborg, H.C.A. and Jajodia, S. (eds.), Encyclopedia of Cryptography and Security, Springer, 2011, does not include the execution of "custom" application logic as the envisioned solution relies on. Perhaps the use of hardware-based trusted execution environments (TEEs) as defined by the Open Modile Terminal Platform (OMTP) should be considered instead.

We confirm the need to have custom logic running in a protected environment with tamper-resistant capabilities.

Question 2

"After a successfully completed transaction, a payee can use funds received offline (plus any balance available beforehand) in a subsequent offline transaction."

How is a successfully completed transaction defined? Is that a tx that has been signed with the help of the SE? What if a rooted device can use the SE, in particular, a TPM to sign an invaild tx and send it offline to the receiver?

A "successfully completed transaction" is a transaction that has been stored on the payee device (after being completed on the payer's device). The payee device needs to check the authenticity of the payer's wallet (via solutions that this market research is exploring) and validate the signature of the received transaction. Proposed solutions should ensure – at the protocol level – the ability to distinguish an *invalid transaction, e.g. by chaining it with previous (signed) attestations.*

Question 3

"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"

Please clarify this requirement with respect to unpowered hardware devices without trusted clock.

We are interested in understanding whether this requirement can also be met in the unpowered device scenario, considering that, to complete the transaction, the other interacting device needs to provide power. We confirm that a local clock (e.g., from the interacting device) should not be by default trusted.

Question 4

Do PETs also apply to offline transactions?

One of our design goals is to limit the exposure of personal data. Every solution that improves privacy for the transacting parties (without creating challenges, e.g. in terms of computational / storage resource required) is welcome. Data minimisation and privacy enhancing techniques should also be evaluated also by taking into account the need to ensure the integrity of the system, specifically by ensuring that there can be no double spending or unauthorised creation of money.

Question 5

“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.”

Will the offline transactions still be passed for fraud checks when the device is back online, or does it just reconcile the balances within the system?

Offline wallets may be checked at the time of reconciliation (e.g. against a list of stolen / lost wallets), but not transactions. The ECB is at the same time willing to explore any solution that – can improve the overall security of the system while still aiming for a high level of privacy.

Component 6: Access Gateway

Question 1

Could you please confirm the Access Gateway is the component responsible for the routing of messages/requests between two intermediaries (and not only between one intermediary and the D€ component)? This seems obvious when looking at some of the end-to-end flows diagrams, but it is not stated explicitly in the text.

The Access Gateway could be the component responsible for the routing of such messages if no further functional processing is required. The respondent can propose alternative solutions.

Component 7: Digital Euro App

Question 1

"The question refers to the use-case where the payer exchanges euro with the merchant through POS (e.g., through NFC).

In iOS the only wallet capable of emulating a card on the NFC hardware is the Apple Wallet itself. How do you envisage to pay through their app without using the Apple Wallet? Do you plan to use Apple Wallet in the end?"

We are aware of the limitation of NFC usage in iOS devices. Respondents are welcome to explore and discuss different design options, including, for example, the use of QR codes as an equivalent option.

Component 8: Integrated Banking App SDK

Question 1

“Custodial wallet implementation: integration with mobile OS key management, signing of transaction messages with signing keys (incl. cryptographic algorithms implementation)"

Please clarify this point further. Are private keys stored on mobile? Would this be used to sign payments for a custodial wallet on an intermediary? Or would this mean the custodial wallet is on the phone? Prepared by box in article author name author last name, box in article author name author last name and box in article author name author last name

The requirement should read “Self-custodial wallet implementation”. In the case of a self-custodial wallet, cryptographic material may have to be stored on end-user devices, hence the requirement. In the case of a custodial wallet, cryptographic material will be managed by the end-user’s intermediary.

Component 9: Proxy Lookup

Question 1

The Proxy Lookup component would consist of a shared repository (either centralised or distributed) that allows intermediaries to pair mobile phone numbers…with the corresponding account/wallet details of end users. Is Alias/Proxy lookup envisioned through Data Replication across the intermediaries and National Banks - the document states that it is NOT to be shared but contained locally - in that case, is it envisioned that the Proxy lookup will only happen at the intermediary level, or does it need to be surfaced at the ECB level as well - given there maybe AML/KYC implications?

For market research purposes, Proxy Lookup is considered part of the digital euro components, with all intermediaries being able to populate the database and retrieve relevant transaction data from it. Proxy Lookup is not expected to have a role in performing AML/KYC related processes/tasks.

Question 2

Page 62: it is stated that '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.' We do not see the use case for using the Proxy Lookup when the payer is identified with a proxy, as in this case the intermediary (of the payer) should know already the account identification of the payer itself. Could you please clarify how such a use case would work?

The use case you are referring to is a request to pay use case, where a payee provides proxy data of the payer to the intermediary. The payee's intermediary would need to be able to resolve the payer's proxy data, in order channel the request to pay to the payer's intermediary.

Question 3

Page 64: it is stated that '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).' We did not find specific requirements related to the Proxy Lookup in Chapter 2. Could you please clarify the performance requirements (e.g. throughout, latency) you are expecting for this component?

Please refer to the scenarios from the table on page 8 and describe their impact on the design of the Proxy Lookup. The inclusion of the Proxy Lookup should not limit the number of daily transactions processed, as indicated for each of the three scenarios from the table, or negatively affect an end-to-end processing latency of three seconds (for 99% of all processed digital euro transactions).

Question 4

As for question 3.9.6, could you please clarify what it is meant exactly with incorporating existing proxy lookup solutions in the Proxy Lookup component? Do you mean reusing/enhancing one already existing proxy lookup solution to build the requested Proxy Lookup component? Or do you mean building the Proxy Lookup component in a way that is interoperable with already existing proxy lookup solutions? Or do you mean something else?

Please describe your proposal for an implementation of the Proxy Lookup that could benefit from existing proxy lookup solutions on the market. As you have indicated, there are different approaches to achieving this, which can be suggested as a solution in the market research.

Question 5

As for question 3.9.7, we have the same doubt that we illustrated for question 3.9.6. Could you please clarify whether 'incorporating', in this context, means leveraging on an already existing solution to build the Proxy Lookup component, or to make the Proxy Lookup component interoperable with an already existing solution, or something else?

Please base your answer to this question on the proposed implementation approach(es) you described in your answer to Question 3.9.6.

Question 6

In Annex 1 (Functional and non-functional requirements linked to the market research for a potential digital euro implementation) page 9, it is mentioned that the processing latency for all digital euro queries is 0.5 seconds. Does this timeframe include a processing time of the proxy lookup service as well? Could it be considered that the Proxy request processing timeframe is not included in the digital euro processing timeframe? What is the required desirable max time to process a proxy lookup request?

The inclusion of the Proxy Lookup should not increase an end-to-end processing latency of three seconds (for 99% of all processed digital euro transactions).

Question 7

Could you elaborate more on the Directory service for the Proxy Lookup component (referring to the scheme on page 62 of Annex 1) and explain should the Proxy Lookup component includes Directory service functionality or Directory Service is simply treated as an external service that ensures interaction between the Proxy Lookup Repository and the corresponding proxy lookup services?

The directory service enables interoperability of different proxy databases in the case of distributed implementation of the Proxy Lookup, but it is not needed if the implementation of the Proxy Lookup follows a centralised approach. The visual on page 62 and corresponding requirement related to data retrieval (page 64, second bullet point) stipulate that the directory service is used to connect the main proxy lookup repository with existing proxy lookup solutions. Our assumption is that some existing (national) proxy lookup solutions can also be reused to store digital euro related data, while if no suitable proxy lookup solution exists (for example, for specific Member State) the digital euro proxy data are stored in the proxy lookup repository. The directory service should also have some underlying logic to improve data retrieval from existing proxy lookup solutions (for example, a mobile phone number starting with +49 has a higher probability of being in an existing "German" proxy lookup solution than in any other). The directory service could be developed for the purpose of the Proxy Lookup, or an existing external service could be reused (if it is available on the market). Finally, please do not refrain from providing alternative and potentially more efficient approaches to implementing the Proxy Lookup in the case of distributed implementation.

Question 8

Could you, please, share more details on what you see could be Digital Euro Wallet Id? Could it be metadata like IBAN?

An identifier would most likely be a string (of numbers or letters) in predefined format, resembling today's IBANs.

Question 9

Referring to page 62, paragraph 6.9.2. assumptions: it is stated that only one proxy data element is required to be linked to the Digital Euro Wallet initially and additional proxy data elements could be added later. Could you explain if those proxy data elements must be different types, e.g., one mobile phone number, one email address, one username, etc. per one particular Digital Euro Wallet? Or is it allowed that two of the same type proxy data elements can be linked to the same Digital Euro Wallet, e.g., two different mobile phone numbers are linked to that one particular Digital Euro Wallet?

The only limit is that the same proxy data element is not linked to more than one digital euro account/wallet. However, we believe that the potential support for more than one proxy data element of the same type per end user (for example, for digital euro accounts/wallets with shared ownership) would be an optional service rather than a requirement for a standard proxy lookup service.

Question 10

In page 63, paragraph 6.9.4. Requirements: Data update: it is stated what kind of information regarding end user must be stored in the Proxy Lookup repository. Among this information, could other end user information be stored in the Proxy Lookup Repository, such as end user Name and Surname or Company name?

Owing privacy considerations, we do not foresee other end-user data being stored in the Proxy Lookup. Such data should only be stored by the intermediary providing the digital euro account/wallet to the end user.

Question 11

On page 64, paragraph 6.9.4. Requirements: Data retrieval: it is stated that "<...>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". Could you elaborate more on the requirements for the technical solution for forwarding proxy lookup requests to a Directory Service? Can options be proposed if there is no such solution foreseen at the moment?

Please refer to the answer to Question 7 (Proxy Lookup) for additional details.

Question 12

Referring to page 62, paragraph 6.9.3. Interactions: it is stated “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” Could you elaborate more on what you see these “identifiers” could be?

In the most likely scenario, the intermediary would receive a reply from the Proxy Lookup containing information on (1) which digital euro account/wallet identifier and (2) which intermediary identifier is linked to the proxy data element included in the data retrieval message.

Question 13

Referring to page 62, paragraph 6.9.3. Interactions: it is stated “Only intermediaries interact directly with the Proxy Lookup component (which may incorporate existing proxy lookup solutions)” Could you please elaborate more on what do you see as “incorporate existing proxy lookup solutions”? Do you mean interaction with external proxy lookup solution using Directory Service or do you see it as an incorporation of other systems to ECB digital euro proxy lookup solution?

The part “which may incorporate existing proxy lookup solutions” refers to the possible distributed implementation of the Proxy Lookup. Please also refer to the answer to Question 7 (Proxy Lookup) for additional details.

Component 10: Onboarding Repository

Question 1

In Section 6.10.4: “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.”

Isn’t the intermediary of a person confidential?

Intermediaries will enable the end user to use digital euro. During the onboarding, the intermediary will transmit the digital euro end-user identifier hash to the Onboarding Repository (required to perform the check that the number of accounts/wallets per user does not exceed the limit). In addition to the digital euro end user identifier, the Onboarding Repository will also also store an intermediary identifier (each intermediary will have a unique identifier). This is required, as only the intermediary who requested the specific digital euro end-user identifier to be entered into the Onboarding Repository can modify or change this entry at a later stage (for example, request to update a digital euro end-user identifier or request to deactivate/delete an entry when an end user is offboarded). The intermediary identifier is not personal data and not confidential.

Question 2

"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.

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.

Does this limitation to one relate to the accounts or is there also any limitation of Wallet Apps / SDKs being used (e.g. on different smart phones) - or in other words: Shall it be possible to connect to the same account from different wallets?

Is there a 1:1 relation intended between digital euro account and commercial bank account provided by the intermediary? If yes, how can the digital euro being used with waterfall mechanism to different bank accounts or is this not planned to be supported? "

The limitation relates to the number of accounts an end user can have; the end user can still use this account on different devices. It is not envisaged that the Onboarding Repository will have a role in supporting digital euro accounts/wallets and commercial bank account linking. This linking should be performed by intermediaries instead. Requirements for account linking, including the possibility of linking more than one commercial bank account to a digital euro account/wallet or linking a commercial bank account operated by another intermediary, are still being analysed.

Question 3

If the end-user changes her intermediary institution (or if the latter does not exist anymore - bankrupt or closed by authorities), then there will be a need for data migration within the onboarding repository. As you write "The Onboarding Repository consisting of interoperable databases managed by multiple operationally independent entities. would be preferred over a centralised implementation." do you envisage these "interopable databases" existing only at national level?

Regardless of the suggested implementation of the Onboarding Repository (either interoperable (national) databases managed by multiple operationally independent entities or centralised implementation), the operator of the Onboarding Repository should be able to access all the data. Therefore, the implementation approach with multiple interoperable databases should not in any way limit the functionality of the repository (for example, by only allowing national checks on the existing digital euro accounts/wallets of an end user). If an end user decides to port a digital euro account/wallet to another intermediary, the intermediary identifier linked to the digital euro identifier of the end user will be updated in the Onboarding Repository.

Question 4

Are nationally-segregated onboarding repositories, designed to avoid a centralized pan-European database of citizen identities, deemed to satisfy ECB's requirements?

Data segregation (multiple databases, for example at national level) would be desirable to improve the resilience and management of operational and cyber risks of the Onboarding Repository. However, we still expect interoperability between databases, e.g. the databases should still enable an existing digital euro account/wallet to check on a pan-European basis. The segregation, therefore, should not affect the functionality of the Onboarding Repository.

Question 5

What existing databases (§6.10, p. 66) are considered to be in scope to reuse for the shared onboarding repository?

Through the market research we would like to understand whether there are any existing databases that respondents could reuse to provide the Onboarding Repository.

Question 6

Which national or pan-European national identity system is applicable to the shared onboarding repository?

The decision which national or pan-European identity system to use is not of the primary importance for the purpose of the market research, since the Onboarding Repository only receives hashed information. However, we would welcome respondents' proposals concerning which national or pan-European identity system would be most suitable to differentiate between end users. Please be informed that we are particularly interested in identity systems related to natural persons and refer to the answer to the following question to learn more about criteria to be used for the selection of an appropriate identifier.

Question 7

What is the threat model regarding the shared onboarding repository? Please clarify how hashing contributes to threat protection, given that national tax identity numbers are not necessarily secret.

Applicable threats include potential abuse by a legitimate intermediary, in terms of violation of the intended data integrity: e.g., maliciously inserting new records to prevent legitimate end users to open digital euro accounts/wallets with competing intermediaries. This may also include an unwanted "bulk load" of data records. These types of threats can be mitigated by applying proper auditing, rate-limiting and anti-abuse technical measures, ensuring the accountability of the involved intermediaries.

Internal threats (e.g., direct access by the repository operator to data) can be similarly mitigated by technical and organisational controls to prevent unauthorised or undue access to the (hashed) end user data.

In extreme scenarios, like a possible massive exfiltration of the data, the hashing is only useful in avoiding a direct exposure of personal identifiable information. An adversary with access to an individual’s unique national personal identifier could only infer if the citizen is actually listed in the Onboarding Repository and is therefore a digital euro end user.

The decision which national identifier would be used has not been taken yet. If tax identity number (which is publicly available in some countries) or other national identifier is used, will be based on different criteria, e.g., privacy considerations, identifier’s power to differentiate between end users, identifier’s adoption rate – if it is assigned automatically by country to all end users or easily obtainable, identifier’s use in the onboarding processes for existing financial services.

Question 8

In order to control the number of offline wallets/accounts than an end user can hold, it is not clear in the requirements if the Onboarding Repository should also store end users’ id for which an intermediary provided an offline wallet/account.

If this is the case, can it be assumed that the Onboarding Repository' requirement/limit of the Annex 1, ""one digital euro account/wallet per end user is envisaged"", could be read as one “online account” and one “offline account” per end user? (apart from merchants, for which it is explicitly said in page. 47 that they can hold more than one offline wallet/account).

Your understanding is correct.

Component 11: Dispute Management

Question 1

"The settlement process for financial disputes will be similar to the process for usual digital euro payments and marked as dispute-related to facilitate identification." Could you please clarify what do you mean by "financial disputes", in reference to usual payment-related disputes?

The statement above indicates that any credit or debit transaction resulting from the dispute process is not expected to be managed by the Dispute Management component. Depending on the solution design and dispute process definition, the dispute Management component should either trigger/initiate any financial transactions (e.g. refund to the payer for a successfully disputed transaction) via the Settlement component or only report the result to the intermediary which would initiate the financial transaction directly via the regular settlement process. In any case, the dispute solution needs to record the outcome of the dispute resolution.

Question 2

"The component should be capable of managing user access rights". Which users are you referring to, please? If the component only transmits messages between the intermediaries (diagram on p.68), then the users can only be those authorized employees of intermediaries who can add documentation to a forwarded message, so with access rights already granted by intermediaries. Which other "users" do you mean, please? Arbitrators, perhaps?

For the purpose of the market research, the main users ware connected intermediaries. An Arbitrator is an example of another potential additional user other than intermediaries.

Question 3

"The (pre-)dispute API should support the provision of documentation together with the (pre-)dispute response" Such documentation is "dispute-related data" which will have to be stored. Should this store be made available to other components as well (e.g., for operational support and quality assurance purposes)?

The storage of any documentation is considered as not in scope as it might contain personal data which should not be visible to the Eurosystem.

Question 4

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

How would this functionality be expected to work if it’s not possible to track the individual transactions?

Avoiding tracking individual transactions of a user does not necessarily imply there will be no transaction records available. These transaction records might have unique transaction IDs to identify them without allowing them to be linked to individual users.

Component 12: Fraud and Risk Management

Question 1

We understand from your specifications that this component will have dual functionality: 1) intercepting fraudulent transactions before being recorded in the central ledger, 2) analyzing transactions post-fraud to discover fraud patterns and update its own rules. Are we correct?

Yes, the understanding is correct. Both functions are considered, identification of fraudulent activities before settlement is recorded and post-fraud analysis.

Question 2

If this component must indeed intercept fraudulent transactions before they are recorded in the central ledger, then are we correct in expecting that it not will allow them to be written in the central ledger, but will return them to the intermediary with appropriate messages? Or it will still allow them through with an indication "possibly fraudulent"?

Both should be possible. A "'fraud rule'' should be able to trigger a settlement verification rejection of a payment request or just indicate possible fraud to the intermediary.

Question 3

We assume that for the purposes of post-fraud pattern detection, this component will have to scan several transactions of different end-users. Is that correct? If so, will it have to have its own analytical datastore, or will it be allowed to search directly in the central ledger?

The current assumption is an own analytical data store which should not interfere with any other components or processes.

Question 4

"Fraud and Risk Management should support the provision of fraud-related reporting". Also for historical fraud cases? That would pre-suppose the persistence of fraudulent-transaction data and metadata in an own data repository. Or do you mean only for the "online validation" fraud detection functionality?

Yes, also for historical fraud cases.

Question 5

Fraud patterns are sometimes linked to specific end-users. Should this component be saving internally the identifiers of said end-users (e.g. in a manner not visible outside the component, but still accessible to country-level law authorities)?

The fraud component should be able to store any data element of the transaction record and apply fraud rules to any of them. Through the market research we would like to receive respondents' proposals on fraud solutions without storing specific end-user identifiers.

Question 6

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."

Will the system be able infer the end user? For fraud detection/management purposes will it be possible to aggregate data on the end user level?

The fraud component should be able to store any data element of the transaction record and apply fraud rules to any of them. Through the market research we would like to receive respondents' proposals on fraud solutions without storing specific end-user identifiers.

Question 7

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

Who will be responsible for the upkeep / maintenance of the rules that are implemented?

The solution is expected to include the maintenance of the rules to be implemented.

Question 8

"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."

Why is this the responsibility of the fraud and risk management component? Is it not a systemic requirement and all usage of data will follow the same paradigm and data values?

Support of privacy-protecting techniques is indeed a general systemic requirement across all components and the solution design. It is explicitly stated in the context of this component as fraud and risk management could require specific considerations for privacy purposes.

Question 9

The descriptions and requirements of the Fraud and Risk Management component (detailed on pages 26 and 72-72 of Annex 1) only references Fraud Management. Could you please confirm that fraud is the only risk to be included in the Fraud and Risk Management component?

Yes, prevention of fraud during the payment process and ex-post detection and identification of fraud patterns in the case of fraud that was not prevented are currently the only risks to be managed in the Fraud and Risk Management component. However, as indicated in the market research document, respondents are encouraged to provide additional solutions.

Question 10

The component should interact with intermediaries during payment validation, providing a transaction risk profile assessment result in the validation message.

What is the validation message? This is only mentioned on this page in the fraud section.

As indicated on page 19 of Annex 1 in the payer- and payee-initiated flows there are validations performed by both intermediaries. It is during these validations that the transaction risk profile will be assessed.

Question 11

The fraud-related data and/or fraud management results required for subsequent processes (e.g. for statistical/reporting purposes) should be stored.

Does this mean that the supplier has to store the confirmed fraud attacks or payments? How will the fraud be confirmed? Who confirms the fraud?

Fraud management results need to be stored. Fraud-related reporting (e.g. absolute number of fraud cases) can be done either in the Fraud and Risk Management component locally or in a central Data Warehouse. Please describe the options supported by the solution proposed.

Question 12

The data from the component should be accessible via user-to-application (U2A) and application-to-application (A2A) interfaces.

What data? The fraud solution will output a risk score. Should the risk score be visible for the payer in order to not initiate or reject the payment?

The risk score should be visible to the payer's or payee's intermediary only and not to the end users. The Fraud and Risk Management component should support fraud-related reporting and statistics. In addition, it is assumed that new fraud rules can be set up and existing ones can be managed and that different user profiles might apply.

Question 13

The component should be capable of managing user access rights.

Does this mean that the fraud solution will be used for authentication in the app?

No, the fraud solution will not be used for authentication in the app. Depending on the solution proposed, user access rights related to the fraud functions could be managed either centrally or locally by the Fraud and Risk Management component.

Question 14

Within the Market Research, there are 2 kinds of requirements which are in contradiction.

First the very strong requirement regarding the privacy implying globally that ESY cannot access to the holdings of the end-users, track their transactions history or even infer their payments pattern.

However, Fraud & risk management is supposed to be dedicate to cross-intermediaries context and to be feed with the data available within the Dataware component. This component only gathers the data of the ESY D€ component thus no information related to end-users payments patterns for instance.

Should the data, really limited to the D€ components scope, Fraud & Risk component (and DWH in a lesser magnitude) won't be able to provide accurate results if privacy requirements are ensured.

What would be your preferred way forward on this topic: reduce the privacy requirements so to allow an accurate processing by Fraud & Risk management and DWH in particular for Remuneration part; OR allow ESY D€ components to work on a confidential way on data owned and provided by intermediaries?

The solution design and data model still need to be defined. Indeed, an appropriate balance between maximum possible privacy and sufficient availability of data for fraud and risk management has to be achieved.