EUROPEAN CENTRAL BANK

EUROSYSTEM

FINAL

Summary of collected inputs from MAG members:

Nov/Dec round of work

Market Advisory Group

19 January 2022

Digital euro project team

Disclaimer

The following presentation summarises findings of the contributions on the November/December round of work made individually by some digital euro MAG members; these findings need not necessarily reflect design decisions for the digital euro

Distribution

- **POS NFC-communication standards**
  - Format limitations and challenges on the creation of new ones (e.g. usage rights, governance and time-to-market).
  - New standards implemented at POS are subjected to a set of technical considerations which add complexity and time (e.g. new certification processes, third party applications compatibility).

- **Updates on POS infrastructure**
  - Time and costs depends on many factors (type of terminals, ownership and local processing structures).
  - From a technological point of view, there are several issues to consider, including diversification, technology readiness, type of connectivity and obsolescence.
  - Larger or more complex upgrades may require physical intervention.

Distribution

➢ Electronic payments form factor

- Secure e-ID solution and robust AML/fraud controls would be necessary to uphold confidence.
- QR codes might be suitable for scenarios where fast check out is not of critical importance as long as payment acceptance costs are low.

➢ PSP's integration

- Paying by digital euro should have a simple, unified experience regardless of the shopper's country, language or issuer.
- Value-added services (VASs) are possible (e.g. currency conversion, recurring transactions, account management).
- Any regulatory issues should be addressed (e.g. insolvency of supervised intermediaries).

Distribution

- **P2P payments**
  - Currently offered for free – VASs can be used as a remuneration source.
  - A link between the digital euro (if third-party validated) and commercial bank money payment accounts could represent an opportunity to expand the range of services whose remuneration could (at least partially) cover digital euro costs.

- **Account-to-account (A2A) vs card-based payment solutions**
  - The symmetric distribution of benefits for all stakeholders (consumer, merchant, intermediary) could form the foundation for the development of a successful digital euro.
  - Consumer and merchant preference might be limited on A2A payment solutions due to the lack of certain features, compared to card payments (e.g. pre-authorisation).

Design features

Offline

- Offline solution of the digital euro is needed to foster a cash-like trust in the currency.
- Current existence of barriers to offer offline functionality and trade-offs (e.g. market preference for a low cost infrastructure vs. the need for a high level of security).
- Higher level of privacy was noted as an important valuable feature that offline payments could offer.

Privacy

- Consumers in the EU are becoming more aware of the importance of privacy.
- Prepaid cards currently the electronic solution with highest level of privacy.
- Privacy-enhancing techniques (PETs) are being used by PSPs to leverage the increasing amount of personal data while ensuring personal or sensitive information stays private. No evidence of their use to guarantee higher privacy of users' data in front of their intermediary.

Design features

- **Bearer instrument**
  - The role of intermediaries is a proven way to ensure that rules of the system are enforced, including settlement finality and no unwarranted creation of digital euro. Validation without the involvement of third parties (e.g. offline) would need to ensure likewise the possibility to verify the validity of the payments and to prevent double spending.
  - The provision of VA services would be limited if intermediaries have limited roles in the transactions processing (lower data access).

- **'Bill-based' ledgers**
  - Compared to "balance-based", fixed dominated units of a digital euro represented on a "bill-based" ledger would be accompanied with additional complexity, for example in terms of privacy and AML/CTF compliance.

Thank you for your attention!