FINAL

# Summary of collected inputs from MAG members:

Jan/Feb round of work

Market Advisory Group

**9 March 2022**
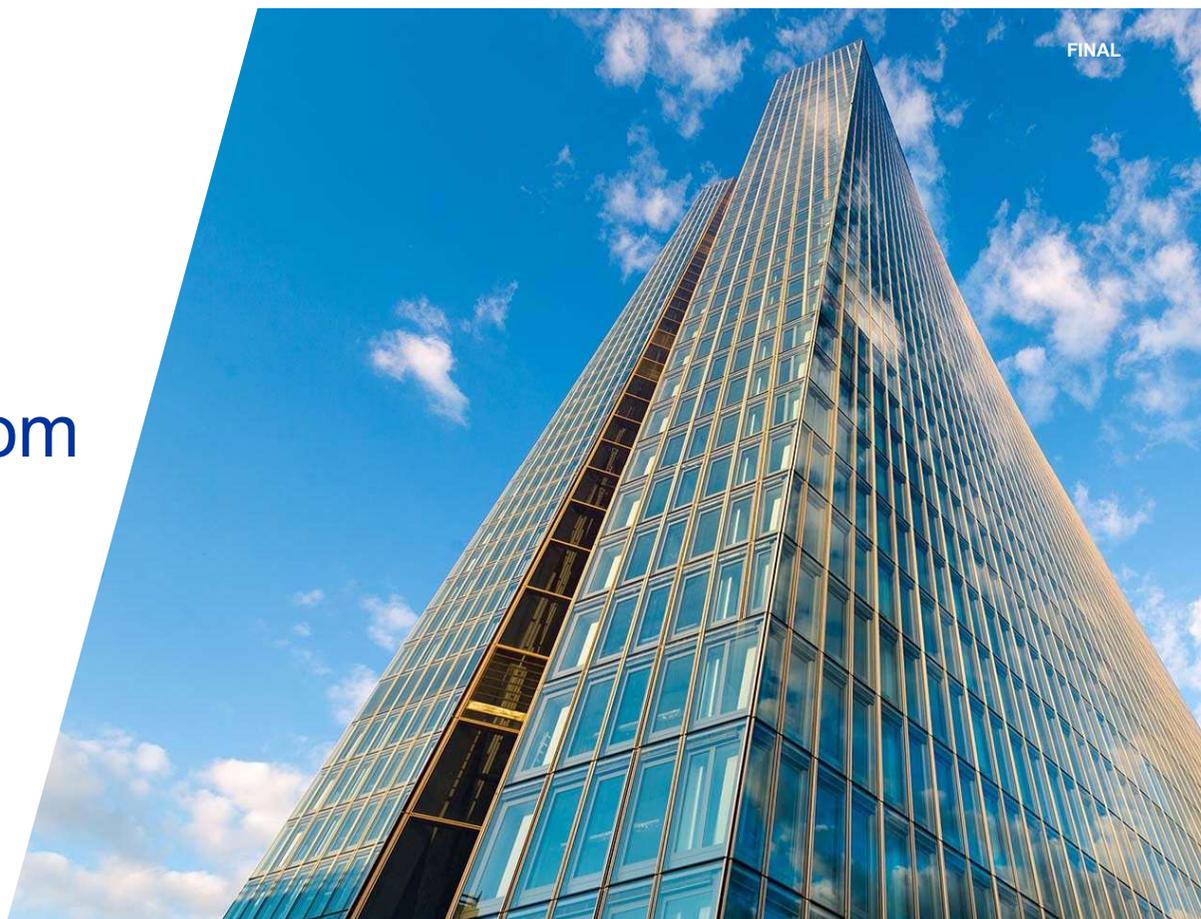
**Digital euro project team**

# Disclaimer

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

# Distribution & business models

➤ Alternative rails (e.g. SCT Inst) to processing card-initiated payments could be feasible, but would require changes to the current infrastructure on issuers, acquirers and processors to a greater or lesser extent. Likely need for a central infrastructure acting as a convergence switch (e.g. data exchange for payment initiation, data reconciliation).

➤ On onboarding processes, end-to-end automatization will help to generate efficiencies. A harmonised provision of these services across Europe should require harmonisation on regulatory and implementation frameworks, data standardisation and controls minimisation.

➤ Different approaches for the provision of mobile payment applications (app) to end-users were identified (e.g. universal or bank-specific standalone app, bank integrated app, hybrid, third party wallets). Experience reveals some reluctancy to download a new app in addition to the bank's own app.

➤ Some new pricing trends identified on acquiring services are monthly subscription fees for small/medium size merchants.

# Design features & functionalities

➢ Some examples given on services that could be provided by intermediaries are onboarding, the management and administration of the wallets/accounts (including funding and defunding), payment services, payment processing and value-added services. The provision of those services would require access to some personal and transaction data attributes.

➢ Several functionalities were identified to foster innovation and competitiveness of a digital euro payments solution, including: (i) programmability (a first tier linked to governance decisions and a second tier enabling the provision of innovative services by PSPs); (ii) offline as a temporary backup functionality; (iii) applications for corporates; (iv) cross-border payments; (v) single identification tool fully interoperable and accepted among Member States.

➢ On offline payment functionality, the trade-off between fast-tracking certification of the hardware/software components and ensuring security was highlighted. Furthermore, the link between certification and its effects on the business case for merchants was noted (the more components a device is certified with, the more expensive it will be to implement and maintain it for the merchant). Some examples on features that may drive consumer adoption but require online functionality were provided (e.g. digital receipts provision).

# Design features & technical considerations (I)

➢ On privacy perception by end users, it was mentioned that finding the correct balance between trust and control on the one hand, and transparency obligations and concerns on the other hand, would be key in designing a digital euro.

➢ Some reasons cited why initiatives of bearer instruments are not being successfully deployed were the diminishing cost advantage over other payment methods such as electronic payment cards and increasing internet penetration that facilitated other payment methods.

➢ Examples on potential added-value technical features/capabilities that the digital euro could provide to enable faster evolution in retail payments are the provision of APIs and its integration with identity services.

➢ There is more than one way to present the difference between central bank money and commercial bank money to the user in one interface. Attention should also be paid to contexts where users can choose between different pockets (e.g. POI).

# Design features & technical considerations (II)

➢ Some relevant areas on security standards are the protection of the value of money, personal data protection, operational resilience and IT security. Intermediaries need to have access to transaction data for security, operational and fraud prevention reasons.

➢ User experience is not a primary differentiating factor, but a supporting condition for a positive value proposition to succeed. Competition based on value-added services is key.
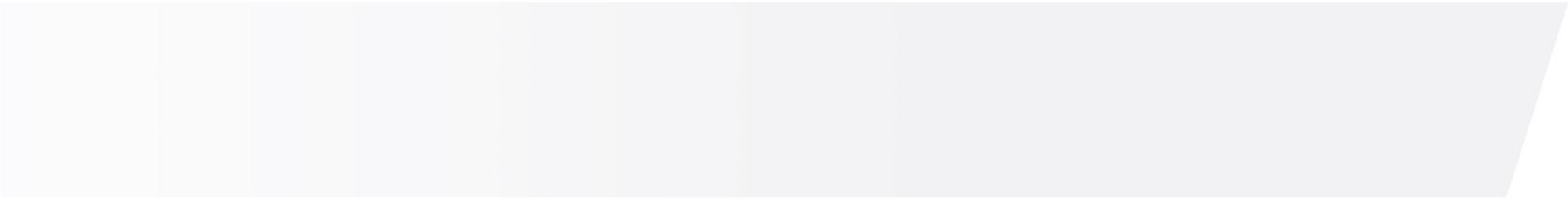
# Thank you for your attention!