Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0211 (COD)
2023/0212 (COD)

Brussels, 11 July 2025

WK 9764/2025 INIT

LIMITE

EF
ECOFIN
UEM
CONSOM
CODEC

This is a paper intended for a specific community of recipients. Handling and further distribution are under the sole responsibility of community members.

WORKING DOCUMENT

From:	Presidency
To:	Working Party on Financial Services and the Banking Union (Digital Euro Package) Financial Services Attachés
Subject:	Digital euro - WP meeting on 18 July 2025 - Presidency discussion note on mobile device access (Article 33)

Danish Presidency
Council of the European Union

PUBLIC

Digital euro - Presidency discussion note on mobile device access (Article 33)

Working Party on Financial Services and the Banking Union

Date: 11 July 2025

Proposal for a regulation on the establishment of the digital euro

Meeting on 18 July 2025

PUBLIC

1. Fair, reasonable and non-discriminatory access to mobile devices (Article 33)

A key feature of the digital euro is that it can be used both online and offline in a secure and inclusive way. The offline functionality is especially important in promoting financial inclusion, a high level of privacy as well as ensuring smooth continuation of payments during situations where the online payment infrastructure is interrupted. To enable this, payment service providers need access to secure environments in mobile devices, such as embedded secure elements (eSE), eSIMs, or other tamper-resistant environments.

Article 33 of the Commission proposal states that providers of front-end services and providers of European Digital Identity Wallets should have access to the necessary hardware and software features of mobile devices on fair, reasonable and non-discriminatory (FRAND) terms.

The Presidency recalls that a majority of Member States have voiced their support for having the offline functionality at the first issuance of the digital euro. **In relation to this, the Presidency notes that there is broad support among Member States for ensuring that Article 33 provides a solid legal basis for granting access to the hardware and software features** of mobile devices needed to support digital euro payments, particularly for enabling the offline functionality.

In that light, the Presidency considers it important to reflect on how to ensure an effective and affordable access for payment service providers (PSPs) to the necessary secure environments on mobile phones in order to provide digital euro offline functionality.

Against this backdrop, the Presidency invites delegations to consider targeted clarifications to Article 33, with the aim of ensuring that all PSPs have effective and affordable access to the secure environments needed for the digital euro to work offline in a safe and inclusive manner, while at the same time keeping a balanced approach in terms of incentives for Original Equipment Manufacturers (OEMs) and Mobile Network Operators (MNOs).

1.1. Access conditions

In previous Council Working Parties, Member States have generally expressed support for the objective of Article 33 and the importance of ensuring its effective implementation. At

PUBLIC

the same time, several Member States have **raised concerns that the current reference to access on fair, reasonable and non-discriminatory (FRAND) terms may lack sufficient clarity or benchmarks** to prevent discriminatory or excessive pricing and could lead to implementation uncertainties or litigation.

In this context, some practical considerations may warrant further reflection. For example, determining what constitutes "fair and reasonable" under FRAND terms could prove complex in the absence of established reference points specific to secure environments in mobile devices. Unlike in other regulatory domains, there appears to **be limited precedent for applying FRAND conditions to access to secure environments in mobile devices within the Union**, which may contribute to uncertainty in implementation and legal interpretation.

During the technical seminar in June 2025, the ECB addressed the potential uncertainty regarding whether the FRAND framework would be conducive to front-end providers being given an effective and fair access to the necessary hardware and software features in mobile devices. Furthermore, the ECB pointed out that without addressing this particular uncertainty, there are risks that such effective and fair access cannot be attained, which could have broader implications. This may include concerns regarding smaller providers or Member States with less bargaining power vis-à-vis large device manufacturers. In this regard, the requirement under Article 23 for offline functionality to be included from the first issuance of the digital euro may amplify these dynamics, as a potentially large number of PSPs would need timely and consistent access to secure environments. These considerations may have implications for market functioning, access conditions, and the overall viability of broad PSP participation.

On the other hand, the Presidency notes that other regulatory frameworks within the Union, such as the Data Act, contain provisions aimed at promoting fair contractual conditions. These include the possibility of developing model contractual clauses to promote balanced negotiations. In addition, the Presidency recalls that the Data Act further empowers the Commission to intervene where access conditions are structurally unfair or discriminatory. The Presidency notes that the Digital Markets Act may provide relevant guidance for assessing FRAND access pricing in practice, for instance by allowing comparisons across regions, user segments or similar services and use cases.

Against this background, **the Presidency invites delegations to share their views on whether article 33 should be complemented by further amendments**, such as implementing acts or other measures, with a view to specifying the economic conditions for access and supporting effective and equitable access in practice.

PUBLIC

Question 1-3 to Member States:

Q1. Do Member States consider that the current FRAND-based framework in Article 33 provides sufficient legal clarity and guarantees to ensure effective and equitable access to secure environments for digital euro services?

Q2. Do Member States support further specification or adjustment of the economic conditions for access to mobile devices under Article 33, with a view to ensuring legal clarity, proportionality and practical enforceability?

Q3. Would Member States agree with empowering the Commission with the possibility to introduce guidance on what may constitute FRAND terms, similar to Article 41 of the Data Act?

1.2. Scope of access and technical requirements

As highlighted above, the Presidency notes that there is broad support among Member States for ensuring that Article 33 provides a solid legal basis for granting access to the hardware and software features of mobile devices needed to support digital euro payments, particularly for enabling the offline functionality. **At the same time, several Member States have requested further clarification on the scope of the provision** and to ensure that the provision adequately reflects the technical requirements.

In particular, a number of delegations have pointed out that the current wording, which refers to access for the purpose of **"storing and transferring data," may not fully capture the functional and security requirements necessary for offline digital euro payments**. These requirements include, specifically, the ability to securely execute operations such as transaction signing and balance updates, which rely on access to secure environments.

The Presidency aims to facilitate a constructive discussion on how the security and functional requirements for offline digital euro on mobile devices (see box 1), as outlined in a recent presentation by the ECB in a technical seminar, are appropriately reflected in the legislative text. In that regard, questions have been raised as to how access for digital euro front-end providers can be ensured in a manner that upholds a high level of security, taking into account the digital euro's status as central bank money and its offline functionality.

PUBLIC

Box 1: ECB security requirements for offline digital euro

According to the ECB's current assessment, for mobile payments with offline digital euro, access to one or more updatable and programmable[1] tamper-resistant secure executing environments, with the capacity of executing a sequence of instructions atomically, is crucial because it provides the highest level of security in the face of attackers. For security, it should reference the *Common Criteria* Methodology *(CC),* stating that the executing environment should be able to resist attackers with a high attack potential, corresponding to vulnerability assessment AVA.VAN.5.[2] This would exclude, for example, Trusted Exchange Environments (TEEs) as adequate environments.

As recognised in the recitals of the Commission proposal, the task of maintaining the security and integrity of the digital euro infrastructure is considered as a task of public interest, essential to protect users and ensuring the stability of the financial system.

Given this context, the Presidency notes that certain security requirements are necessary to support the offline functionality of the digital euro on mobile devices, particularly in light of its legal tender status and role as central bank money. To this end, the Presidency considers that the adherence to certain security requirements by OEMs and MNOs, when granting access to mobile devices for digital euro front-end providers, plays an important role in ensuring the secure use of the digital euro.

In this context, **the Presidency invites delegations to consider whether the current reference in Article 33(1) to "storing and transferring data" sufficiently captures the functional and security requirements** linked to the offline use of the digital euro. To ensure consistency with the underlying technical needs, two possible clarifications could be explored.

First, the Presidency suggest that Article 33 should avoid limiting or contradicting what may be required in terms of hardware and software features to support offline digital euro transactions. In this regard, **the Presidency proposes including a broader formulation in**

[1] This would be further specified in reference to certain standards, e.g., JavaCard and GlobalPlatform standards.

[2] This standard Common Criteria (CC) ISO 15408:2022 and Evaluation Methodology ISO/IEC 18045:2022 are complemented by *Application of Attack Potential to Smartcards and Similar Devices, see https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3.2.1.pdf*. It is applied with the protection profiles *BSI-CC-PP-0084-2014* or *BSI-CC-PP-0117-V2-2023,* depending on the form factor, see https://www.commoncriteriaportal.org/files/ppfiles/pp0084b_pdf.pdf and https://www.bsi.bund.de/SharedDocs/Zertifikate_CC/PP/aktuell/PP_0117.html.

PUBLIC

order to cover a wider range of requirements. This suggestion implies an addition of "*storing and transferring data … transactions, including the storage and transfer of data*"**.** This would aim at allowing for the execution of atomic operations, such as transaction signing and balance updates, which goes beyond the scope of simple data transfer or storage.

Second, the Presidency invites Member States to share their views on whether, and eventually where, further elaborations of functional and security requirements for mobile devices could be warranted. This should be considered in light of the recent technical input during the dedicated seminar on mobile device access, which highlighted the challenges and limitations regarding mobile device security and the need to ensure adaptability over time. The Presidency notes that additional elaboration could be considered, for example, through specific guidance from the Commission or from competent authorities. Such an approach would aim at ensuring the future-proofing of the regulation in light of evolving threats and technological developments.

Drafting suggestions

BE Presidency drafting suggestions in black
DK Presidency drafting suggestion in red

Article 33

1. Without prejudice to Article 6 paragraph (7) of Regulation (EU) 2022/1925 of the European Parliament and of the Council of 14 September 2022 on contestable and fair markets in the digital sector and amending Directives (EU) 2019/1937 and (EU) 2020/1828, original equipment manufacturers of mobile devices and providers of electronic communication services within the meaning of Article 2 (1) Directive (EU) 2018/1972 shall allow providers of front end ~~services~~ **solutions,** ~~and~~ providers of European Digital Identity Wallets **and third-party technical support providers acting on their behalf** effective interoperability with, and access for the purposes of interoperability to, the hardware features and software features necessary for ~~storing and transferring data~~ **securely processing (/executing)** ~~to process~~ online or offline digital euro **payment** transactions, **including the storage and transfer of data,** on fair, reasonable and non-discriminatory terms**. The terms of access shall not depend on the services offered by original equipment manufacturers of mobile devices and providers of electronic communication services.**

PUBLIC

Question 4-5 to Member States:

Q4. Do Member States support the proposed clarifications to Article 33, in particular the inclusion of "securely processing/executing … transactions", to better reflect the functional and security requirements of the offline digital euro?

Q5. Do Member States consider that the formulation of Article 33 is sufficient to ensure effective interoperability with the hardware and software features of mobile devices, notably in the case of offline transactions?

If not, should the following options be pursued:

- *5.a Clarify the necessary functional and security requirements in the text of the Regulation, e.g., in an Annex.*
- *5.b Define those requirements in specific guidelines that would be issued by competent authorities.*
- *5.c Other options.*

PUBLIC

1.3 Availability

As noted above, the offline functionality of the digital euro is expected to rely on secure environments embedded in end-user devices, in particular smartphones. At the technical seminar in June 2025, the ECB explained that it is estimated that, by 2029, an average of 90% of smartphones from the top five European vendors will be equipped with a secure environment compatible with the offline functionality of the digital euro. This means that the remaining **10% of smartphones in 2029, primarily in the lower-cost segment, may not support the offline digital euro**. This raises concerns about whether additional measures might be needed to ensure that the offline functionality can be deployed effectively and at scale.

The Presidency notes that while alternative form factors such as smartcards combined with bridge devices may also meet the required security standards, they could offer a less effective user experience compared to smartphones. To support inclusion as well as ensure that all users across the EU can access the digital euro as legal tender, it may be necessary to ensure that secure environments are available across the full range of commonly used devices.

To support equal access across the Union, the Presidency considers that it may be relevant to **explore whether additional measures are needed to ensure that secure environments are available** across the full range of commonly used devices. These considerations should inform future reflections on how to ensure that the digital euro remains accessible to all users, including those relying on lower-cost devices.

Question 6 to Member States:

Q6. Do Member States find the envisioned accessibility level of the smartphones form factor to be sufficient in light of the inclusiveness objectives of the digital euro?

PUBLIC

1.4 Enforcement and governance

The Presidency notes that several Member States have questioned whether the current drafting of Article 33 provides sufficient **clarity on monitoring and enforcement mechanisms**. In particular, some Member States have highlighted that entities such as OEMs and MNOs are not traditionally supervised by financial services competent authorities. These entities are also not governed by the digital euro scheme rulebook and thus are not subject to the enforcement of the rulebook.

Moreover, as stated by the ECB and in accordance with available data[3], over 70% of mobile devices currently used in the EU are not subject to obligations under the Digital Markets Act (DMA), and may therefore fall outside the scope of mechanisms that support monitoring and enforcement to ensure appropriate access to secure environments required for supporting offline digital euro payments under the Digital Euro Regulation.

In light of these considerations, the Presidency invites delegations to reflect on **whether additional mechanisms may be needed to ensure the effective and consistent application of Article 33** across the relevant Member States. This includes the question of whether a dedicated supervisory framework should be considered, particularly given the cross-sectoral nature of the stakeholders involved.

Question 7 to Member States:

Q7. Should a specific supervisory framework be introduced to ensure compliance with Article 33, for example involving competent authorities designated under Article 6 in the digital euro regulation? If so, how should coordination at EU level be ensured?

[3] Canalys, 2025: Europe's smartphone market grew 5% in 2024, as vendors adjust ahead of a disruptive 2025 (link)