Council of the European Union
General Secretariat

PUBLIC

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

Brussels, 09 May 2025

WK 5962/2025 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:	European Central Bank
To:	Working Party on Financial Services and the Banking Union (Digital Euro Package) Financial Services Attachés
Subject:	Digital euro - WP meeting on 15-16 May - ECB Note on The role of digital euro in improving resilience of euro area payments

Disclaimer: This note is a technical analysis which has not been adopted or endorsed by the decision-making bodies of the ECB and therefore any views expressed shall not, under any circumstances, be regarded as an official position of the ECB. The information transmitted is intended exclusively for the co-legislators and for the purpose of facilitating discussions in the context of the Council Working Party.

PUBLIC

7 May 2025

The role of digital euro in improving resilience of euro area payments

1. Digital euro and resilience

The Eurosystem welcomes the proposals put forward by Estonia, Finland, Latvia and Lithuania in their non-paper of January 2025 (the non-paper) to consider the role of the digital euro in improving the resilience of the euro area's payment landscape, with a view to explore how the digital euro could support continued availability of digital payments in case banks' payment services are operationally disrupted. In reaction to the specific proposals made and for the purposes of facilitating their discussion in the context of the Council Working Party, the Eurosystem has been analysing the feasibility to leverage the digital euro for national emergency solutions in case exceptional circumstances occur in individual or groups of euro area Member States.

The digital euro would strengthen the strategic autonomy and monetary sovereignty of the euro area by boosting the efficiency of the European payment ecosystem as a whole, fostering innovation and increasing its resilience to potential cyberattacks or technical disruptions, such as through the offline digital euro functionality in situations of limited internet connectivity or power outages. The resilience considerations are becoming more prominent as the European Union's general security environment is changing, as pointed out in e.g. the report on Strengthening Europe's Civilian and Military Preparedness in 2024.[1] This includes considerations as regards the need to ensure the continuity of digital payments. The digital euro can maintain sovereignty holistically over our money for all use cases, by ensuring that citizens can continue to use the euro for digital payments across the euro area. Its legal tender status would ensure that the digital euro would be widely accepted in the euro area.

The Eurosystem understands that Member States consider how the digital euro could contribute to securing daily payments when exceptional circumstances prevent the use of private payment systems. Exceptional circumstances can occur in individual Member States and require a regional response within the euro area. At the same time, it should be ensured that the digital euro can be used in the same way throughout the euro area, in accordance with the same rules and conditions and without fragmentation.

The degree to which the digital euro can improve resilience depends on the specific characteristics of the exceptional circumstances, with a significant impact on private payment systems in one or more Member States. It is important that co-legislators provide an adequate definition in the legislation, and conditions under which dedicated measures could be activated. For example, a regional loss of network connectivity due to a natural disaster in a Member State will have a different impact on the digital euro infrastructure than a cyberattack on one or more PSPs providing digital euro payment services within the Member State. Each of these scenarios will have different impacts on digital euro

[1] Niinistö (2024). Safer Together – Strengthening Europe's Civilian and Military Preparedness and Readiness. See also the Joint Communication on the European Preparedness Union Strategy (2025) and the Preparedness Union Strategy – Action Plan (2025), in particular Action No. 25.

functionalities. For example, under some exceptional circumstances the online functionality will still be available, while under others only the offline functionality would remain available.

The best way for the digital euro to provide additional resilience in payments in the euro area is to ensure its timely implementation and widespread adoption by citizens throughout the euro area. The Eurosystem is making progress with the digital euro project, while it is for the co-legislators to decide on the legislation. It will be key to ensure that the Digital Euro Regulation (DER) is adopted as soon as possible to allow market stakeholders to prepare for the launch of the digital euro. Only following the adoption of the Regulation can the ECB Governing Council take a decision to issue the digital euro and the Eurosystem work together with market participants to prepare for its issuance.

When the digital euro will be issued, the Eurosystem will support Member States in actively and clearly communicating the benefits of the digital euro to citizens. It is key that citizens are familiar with its functionalities and have sufficient digital euro holdings in a normal situation, also in the context of crisis preparedness: in order for the digital euro to be an alternative in exceptional circumstances, citizens need to know how to use the digital euro and have sufficient holdings.

2. Specific observations

This section offers specific observations in reaction to the proposals put forward in the non-paper as to how the digital euro can strengthen the resilience and preparedness of the European retail payment landscape. The observations are made mainly from the perspective of technical feasibility. For instance, certain proposals in the non-paper and certain solutions proposed in the response would require some degree of flexibility in applying anti-money laundering and countering the financing of terrorism (AML/CFT) legal obligations, including for the onboarding of new digital euro users.

2.1. A designated entity for providing services in exceptional circumstances

Non-paper proposal: The non-paper outlines that if under exceptional circumstances in a Member State critical PSPs become unavailable and the emergency switching as foreseen under Article 31(2) of the DER to another PSP is not possible, Member States might want to have the tools to ensure the continued availability of the digital euro to ensure that citizens continue to have access to a digital means of payment. The non-paper proposes allowing Member States to develop an emergency backup solution to enable continued use of the digital euro, by allowing the Member State to stand in for the systemically important intermediary bank until its recovery or emergency switching. The non-paper also proposes that, if needed, the Member State could temporarily distribute pre-paid digital euro cards/wallets and facilitate the top-up of offline digital euro balances by users.

Observations and comments: The objective of ensuring the continued availability of digital euro payment services to support daily payments under exceptional circumstances that result in the wide unavailability of PSPs in one or more Member States could be reached by using and extending a set-up that is currently already foreseen in Article 14 of the DER, which provides a basis for Member States to designate authorities (Member States or their regional or local authorities when not acting in their capacity as public authorities) or post office giro institutions to provide digital euro payment services to natural persons, under normal circumstances. Article 14 foresees that these entities can contribute to digital financial inclusion by allowing citizens to access digital euro payment services without being clients of PSPs, and to provide support to vulnerable groups. The population that would benefit from the support services outlined in Article 14(3) would be broad and would include those with no access to formal financial products; those using a very limited range of products; inexperienced, newly

included consumers; users with a low level of financial literacy; users with disabilities or functional limitations; and the elderly.

Synergies can be created by adding a provision that would provide a resilience mandate to these entities in Article 14. This could (i) ease the implementation of the public approach as the scope of the article is broader and not purely focused on inclusion; and (ii) provide the option for Member States to enable the entity already designated for digital financial inclusion purposes to also support resilience features of the digital euro. Given the expansion of the mandate, co-legislators could also decide to expand the types of entities that could be designated. For example, they could also include private entities. The entity would need to be allowed to provide payments services under law and could already be part of the digital euro scheme in normal circumstances when the entity would fulfil its tasks related to financial inclusion as described in Article 14 (i.e. providing access to the digital euro by vulnerable groups or currently financially underserved populations). This would also help ensure that the entity is well-prepared to step up under exceptional circumstances and take on an extended role. [2]

The proposal to temporarily distribute pre-paid digital euro cards/wallets is not consistent with the AML Regulation[3] which effectively bans prepaid cards in case of non-identified users. In line with the principles underlying the design of the digital euro, users need to be identified before being able to use the digital euro and offline payments can only be made through devices that are linked to an identified user.

Assessment and recommendations: Under exceptional circumstances the designated entity under Article 14(3) of the draft Regulation could take on an extended role and become an 'entity of last resort', to which citizens can switch their accounts in case PSPs become unavailable (see also section 2.2). Once users have switched to the entity, it could provide digital euro payment services to these users that are necessary from a resilience and preparedness perspective. This could also include providing an offline payment instrument in case users do not have one yet or have lost their device. Users could then fund their offline wallets from their digital euro payment account via the entity of last resort. This approach would ensure that the offline payment instrument provided by the entity could be associated with a digital euro user, which would be in line with the processes foreseen for facilitating offline payments under normal circumstances. The entity could support continued circulation of the digital euro and facilitate (de)funding of offline digital euro holdings by users. One NCB pointed out that Member States may want to explore temporarily paying out social benefits and welfare payments in digital euro in a situation where the services of PSPs are operationally unavailable and citizens would not have access to their commercial bank funds. In this case, the 'entity of last resort' could facilitate payments by Member states directly to online digital euro accounts or to users' offline wallets. The co-legislators could consider how to apply appropriate AML/CFT risk controls to facilitate the onboarding of users (via switching) and the provision of online and offline digital euro services by the entity under exceptional circumstances.

In order to stay within the boundaries of the Treaty, the privacy framework foreseen for the digital euro and the exclusion of a contractual relationship between the Eurosystem and the digital euro end-

[2] Alternatively, Member States could designate an entity that would only be activated However, it would not rule out the option of creating the national emergency solution only to be activated and used in case of exceptional circumstances, to temporarily provide basic digital euro services. This may require detailing specific rules in the digital euro rulebook for the entity.

[3] Regulation (EU) 1624/2024, on the prevention of the use of the financial system for the purposes of money laundering or terrorist financing.

users foreseen in the DER, it is important that the designated entity is not the ECB or a national central bank. The Eurosystem cannot directly provide accounts to citizens and should not be able to directly identify users.

Lastly, the entity could decide to cease its provision of digital euro payment services related to exceptional circumstances once the situation in a Member State has returned to normal. It would continue its digital euro services for digital financial inclusion. Users would then be able to use the regular switching process to switch to the digital euro payment services of a PSP of their choice. This could be the PSP from which they originated, or any other PSP.

2.2. Emergency switching to a designated entity and availability of front-end services

Non-paper proposal: Based on the proposal for a designated entity in section 2.1, the non-paper proposes that Member States can enable emergency switching of users to that entity providing the emergency backup solution with the possibility to deviate from the standard KYC and AML/CFT procedures, while still applying appropriate safeguards to contain ML/TF risks.

The non-paper also suggests facilitating front-end solutions that are independent from intermediating banks' digital channels, such as the digital euro app, for resilience purposes.

Observations and comments: From a technical perspective, the current design of the digital euro would already allow for users to switch their digital euro payment accounts in a situation in which their PSP has become operationally unavailable. Via this switching facility users could also be offered the option to switch their digital euro payment accounts to the entity (see section 2.1) in exceptional circumstances. The ECB has always made clear that it should have no discretion as regards the decision to activate emergency switching: the legal framework should provide objective and clear parameters for activating emergency switching in exceptional circumstances and for which PSPs in a given Member State. It should also define when emergency switching under exceptional circumstances should be deactivated. Lastly, it is important that co-legislators consider a mechanism that ensures that the digital euro can be used in the same way, in accordance with the same rules and conditions without fragmentation, throughout the euro area.

Assessment and recommendations: The draft Regulation could foresee the option for a Member State to request the ECB and national central banks to activate emergency switching in case of exceptional circumstances. Two considerations become relevant in exceptional circumstances:

First, it is plausible that in such circumstances the front-end services of many, if not all, PSPs in the affected Member State or region would not be accessible to users. Both the DER and the design of the digital euro already foresee a common digital euro app developed by the Eurosystem which can be used for this purpose and, which would be essential to ensure that users would have access to the emergency switching procedure. It would be an independent front-end service and an efficient solution as no independent solutions would need to be developed at national level. The digital euro app would therefore be a cost-efficient way for PSPs to ensure that their front-end services are accessible to users via multiple apps. Member States could propagate the use of the common digital euro app as part of their crisis preparedness campaigns. In case digital euro is used by the PSPs' customers via the digital euro app developed by the Eurosystem, the entities of last resort could easily become the temporary distributor of digital euro services and provide it to new customers where necessary.

Second, users need to provide a 'technical proof'[4] to activate emergency switching. This technical proof is provided to the user by the PSP upon the creation of a digital euro payment account. From a technical perspective, Member States could consider offering their citizens a public repository where they can voluntarily store these technical proofs. The repository should be subject to strict privacy and security requirements, including public communication thereof, and could in any case not be accessible to the ECB and/or national central banks.

2.3. Facilitating online and offline use of digital euro in exceptional circumstances

Non-paper proposal: The non-paper proposes to allow for the flexibility to temporarily increase the limits and online use of digital euro services, as well as to ensure (by default) a sufficient offline limit for purchases of necessities during exceptional circumstances.

Observations and comments: As regards the overall holding limit and the online functionality of the digital euro, the DER foresees limits for digital euro holdings to limit the use of the digital euro as a store of value. The methodology for setting the holding limit is designed to balance usability and financial stability considerations in normal circumstances. The Eurosystem's work on the calibration of holding limits is based on these principles and focuses on normal circumstances. As it is important to ensure predictability and stability of the holding limits, any legal provision enabling a change in the holding limits in exceptional circumstances should come with adequate conditions under which the provision can be activated and for which period of time. This should avoid any arbitrary use of the provision.

Furthermore, temporarily increasing online holding limits would only benefit the user in case the increase is performed before the PSP funding a digital euro account becomes unavailable, as it would allow the user to increase digital euro holdings. It would also require the continued availability of PSPs to provide online digital euro services, which will not always be guaranteed in exceptional circumstances: as the design of the digital euro foresees making use of existing standards to achieve cost efficiency, PSPs would likely not separate their digital euro services from their core (banking) system. It would therefore be expected that under exceptional circumstances the offline functionality would play a main role to ensure resilience.[5]

The DER empowers the European Commission to set the limits for offline holdings and transactions. These limits are a mitigant to money laundering/terrorism financing risks, taking into account the derogatory regime for offline payments under the DER. In order to both maintain these risk controls and allow increased holdings of offline digital euro under exceptional circumstances, the regulatory framework could provide for the possibility for Member States or the Commission to request to temporarily raise offline holding limits to a level that is still within the overall holding limit. Also in this case, the legislation should provide provisions on when holding limits should revert to their original levels after a return to normal circumstances.

Assessment and recommendations: While increasing online holding limits will likely not contribute much to support the continued use of digital euro under exceptional circumstances, increasing offline holding limits under exceptional circumstances (and within the overall holding limit) would support

[4] A technical proof is a cryptographic proof or authority over entries (holdings) or identity in the digital euro settlement infrastructure. Please see the slide deck for the technical seminar on switching, as provided by the ECB to the CWP on 22 March 2024.

[5] The process for the selection of the provider for the digital euro offline services component takes into account the security requirements for this component.

users making payments in proximity with digital euro in situations without connectivity, resembling the functions of cash in exceptional circumstances. From a technical perspective, offline holding limits and transaction limits would need to be altered on the offline devices of users themselves. This can be done at any moment when an offline device connects online, which it needs to do regularly e.g. to (de)fund holdings. It would not only allow the temporary raising of the limits on devices, but also the subsequent lowering of the holding limit after a return to normal circumstances. Implementing the technical ability to change the offline limits while devices are offline would require a change to vendor requirements and in addition would come with high development efforts and major coordination and communication aspects. The coordination and communication aspects have not been evaluated or scoped at this point. A last consideration on the use of offline digital euro is that offline devices' batteries will need to be recharged; the intervals differ depending on the device used, e.g. a mobile phone will require more power than a smartcard. A way to address this need for power could be that the payee's device could be powered up by the payer's device, which would still allow it to receive payments.

2.4. Queueing incoming payments until the waterfall functionality becomes available again and/or emergency switching is performed

Non-paper proposal: The non-paper proposes allowing private individuals and merchants to 'pile up' incoming online digital euro payments in the digital euro account and in their payment terminals in case the waterfall account is unavailable. This would require technically exceeding the "store of value" holding limits for private individuals and merchants until the waterfall functionality becomes available and excess funds would be automatically transferred to commercial bank accounts.

Observations and comments: It could be expected that in exceptional circumstances, commercial bank accounts linked to digital euro payment accounts are no longer available, which would also render the (reverse) waterfall and manual/automated funding functionalities unavailable. Individual users might still have their existing online digital euro holdings and are certain to have offline digital euro holdings available to both make and receive digital euro payment transactions. However, the Eurosystem foresees that merchants would be subject to a zero holding limit and would under normal circumstances immediately convert payments received in digital euro into commercial bank money via the waterfall mechanism.

Assessment and recommendations: Discussions with market stakeholders have raised the question how the zero holding limit for merchants should be enforced. Technically, defunding could be done in a way that every payment would immediately be defunded into private money. It could also be done on an end-of-day basis, where defunding would take place at the end of each day. This would be comparable to merchants depositing cash from their cash registers at the bank at the end of a business day. From a resilience perspective, the end-of-day approach to defunding would ensure that the option to pay merchants with digital euro would remain available, also in a situation where the online digital euro is functioning, but payments with commercial bank money are unavailable.

As an alternative, and taking into account the considerations in section 2.3, it is possible from a technical perspective for merchants to hold offline digital euro, which would be stored in their payment terminals until connectivity is restored.

2.5. Providing digital euro payment services to an extended range of users

Non-paper proposal: The non-paper proposes exploring the possibility of extending the requirement to accept digital euro payments to additional users under exceptional circumstances. It proposes doing this by allowing for Member States to limit the exceptions to the obligation to accept digital euro in exceptional circumstances.

Observations and comments: This proposal will be difficult to implement from a technical perspective. While technically feasible, it might be challenging to provide the necessary technical equipment to those users who could be covered by the existing design but have chosen not to accept digital euro payments (for example merchants who do not accept any form of digital payment) when exceptional circumstances occur.

Assessment and recommendations: For this purpose, it would be better to ensure that (potential) users are prepared and accept digital euro payment under normal circumstances, while keeping the number of exceptions to the mandatory acceptance requirement in Article 9 of the DER limited.

3. Conclusions

The Eurosystem and co-legislators could explore the possibility to further strengthen the contribution of the digital euro to payment resilience in Europe. The best way for the digital euro to provide additional resilience in payments in the euro area is to ensure its timely implementation and widespread adoption by citizens throughout the euro area. From an operational perspective, it is key to ensure the preparedness of users and all other stakeholders in the digital euro eco-system: users should be aware of all functionalities and be willing to use digital euro so that they are incentivised to have a sufficient level of both online and offline digital euro holdings under normal circumstances.

The feasibility analysis shows there are some ways to explore an enhanced contribution of the digital euro to ensuring the resilience of the European payment landscape, in particular as regards the following elements:

- As proposed in the non-paper, Member States can designate an ‘entity of last resort’ to which citizens can switch their accounts in case PSPs become unavailable. Under normal circumstances, this entity could carry out the financial inclusion-related tasks that are already included in Article 14 of the draft Regulation; this, however, does not rule out its use only in times of crisis. Once users have switched to the entity under exceptional circumstances, it could provide digital euro payment services to these users that are necessary from a resilience and preparedness perspective. The entity could decide to cease its provision of digital euro payment services once the situation in a Member State has returned to normal. Users would then be able to use the regular switching process to switch to the digital euro payment services of a PSP of their choice. The draft Regulation could set requirements for the extraordinary circumstances to ensure harmonised implementation across Member States.
- The draft Regulation could foresee the option for a Member States to request the ECB and national central banks to activate emergency switching in case of exceptional circumstances. This would allow users to switch their digital euro services to an alternative PSP, including the ‘entity of last resort’. As users need to provide a ‘technical proof’ to activate emergency switching, Member States could offer their citizens a public repository where they can store these technical proofs, and which could be managed by the designated entity.
- The entities of last resort could also make use of the digital euro app developed by the Eurosystem, as long as they have the required license, according to the DER, to distribute

digital euro. The digital euro app would therefore be a cost-efficient way for PSPs to ensure that their front-end services are accessible to users via multiple apps.

- Increasing offline holding limits under exceptional circumstances (and within the overall holding limit) would support users making payments in proximity with digital euro in situations without connectivity. It is also possible from a technical perspective for merchants to hold offline digital euro, which would be stored in their payment terminals until connectivity is restored. This can be done at any moment when an offline device connects online, which it needs to do regularly e.g. to (de)fund holdings. Implementing the technical ability to change the offline limits while devices are offline would require a change to vendor requirements and in addition would come with high development efforts and major coordination and communication aspects.