State of play on offline digital euro

11th ERPB technical session on digital euro

11 April 2024
Offline basics

Digital euro shall be used **online** and **offline**

From all the payment features offered by the digital euro, offline resembles cash the most:

- **Bearer** payment instrument
- **Instant** proximity transaction settlement
- **Proximity** payment communication

Funds must be **prefunded** and are stored locally on the end-user’s device.

**Without any third-party** involvement (subject to legislation excluding from AML monitoring).

The Eurosystem is working on all prioritised use cases (P2P, POS, e-commerce) in parallel. For offline, P2P and POS are the relevant use cases that can be used in proximity payments.
1. Use cases and form factor
## Use cases: overview

### Use cases

<table>
<thead>
<tr>
<th>Person-to-person (P2P)</th>
<th>Point-of-sale (POS)</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Mobile device</strong></td>
<td><strong>Contactless at POS terminal</strong></td>
</tr>
<tr>
<td><strong>Offline D€ wallet</strong></td>
<td></td>
</tr>
<tr>
<td><em>on the mobile phone</em></td>
<td></td>
</tr>
<tr>
<td><strong>With a bridge device for communication</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Battery powered smartcard</strong></td>
<td></td>
</tr>
<tr>
<td><strong>Offline D€ wallet</strong></td>
<td></td>
</tr>
<tr>
<td><em>on the mobile phone</em></td>
<td></td>
</tr>
<tr>
<td><strong>Contactless or contact</strong></td>
<td></td>
</tr>
<tr>
<td><strong>at POS terminal</strong></td>
<td></td>
</tr>
</tbody>
</table>

*Wallet could be integrated into the PSPs banking app or the Eurosystem’s digital euro app*

**Terminology:** [Digital euro glossary](#)
Offline P2P payment: phone

**Payer**

1. User opens his offline wallet* and selects “Transfer digital euro”
2. User specifies the amount and confirms the transfer
4. Wallet’s balance updated

**Payee**

1. User opens his offline wallet* and selects “Receive digital euro”

3. i) Payment information exchanged between devices  
ii) Payment is settled

4. Wallet’s balance updated

*Wallet could be integrated into the PSPs banking app or the Eurosystem’s digital euro app
Use case delivery challenges – mobile phone

For mobile phones, delivery timeline is conditional to access to the following components, which are currently restricted by some mobile device manufacturers:

- Near-Field Communication
- Secure element
  - Embedded Secure Element (eSE), provided by OEM*
  - Embedded Subscriber Identity Module (eSIM) or removable SIM, provided by MNO*

* OEM = Original Equipment Manufacturer; MNO = Mobile Network Operator
**Offline P2P payment: card-to-card**

1. User inserts his offline digital euro card into his bridge device and selects “Transfer digital euro”

2. User specifies the amount and confirms the transfer

3. i) Payment information exchanged between cards
   ii) Payment is settled

4. Card’s balance updated

---

**Payer**

**Payee**

1. User inserts his offline digital euro card on the payer’s bridge device for receiving funds

4. Card’s balance updated
Alternative to the mobile phone: **Smartcard option** offers more independence on the timeline but may result in poorer user experience.

**For P2P, users need to carry a bridge-device**

**Bridge device:** a pocket-sized, battery powered devices whose goal is to establish a connection channel between two non-powered smart cards, enabling a transaction to happen between them.

**Payment information exchange**

**P2P payment with smartcards**
Physical card with battery for P2P payments

**Pros**

+ More control over the secure element content
+ Allows for offline P2P
+ Might support digital financial inclusion

**Cons**

- Higher cost compared to simple smartcard
- Uncertain sustainability and reliability
- Like a simple smartcard, external connectivity (e.g. ATM) required for (de)funding and system integrity check
- Production and distribution channels would need to be set up in Europe

Preliminary assessment indicated:
Provision of digital euro offline solution

PSPs are responsible for **distributing the payment instrument** to user and for **its maintenance**.

- **Digital euro offline smart card**: Delivered physically (proximity / mail)
- **Digital euro offline mobile solution**: Installed on Secure Element of mobile device

On mobile devices, the offline solution offers instant installation without delivery wait, but involves technical complexity.
Online operations: (De)funding and integrity check
Funding and defunding of digital euro offline wallet

Possible sources:
- Cash
- Private money
- Online digital euro

Possible funding methods:
- ATM
- Bank branch
- POS terminal

Depending on the user’s form factor:
- Using the same device
- Via a secondary device providing physical connectivity (e.g. mobile phone, ATM, POS terminal)
AML and forgery check during (de)funding operation

Offline payments do not involve sharing transaction data with PSPs, the Eurosystem or any potential providers of supporting services, except for what may be required to avoid forgery of digital euro.

The draft legislation provides for a high level of privacy for low-value offline payments, which are treated as cash-like proximity payment.

Anti-money laundering check seeing:
- Amount (de)funded
- Identifier local storage device
- The date and hour of the (de)funding transaction;
- Accounts number of online account used for funding
- or defunding

System security and integrity check
To make sure that the funds recirculating back to the digital euro system are genuine and to detect possible double spending and fraudulent currency, Eurosystem to receive the minimum amount of data* compatible with the need to detect forgery.

Offline payments do not involve sharing transaction data with PSPs, the Eurosystem or any potential providers of supporting services, except for what may be required to avoid forgery of digital euro.

The draft legislation provides for a high level of privacy for low-value offline payments, which are treated as cash-like proximity payment.

*This data would not enable Eurosystem to identify individuals

End-user

Intermediary channels crediting message to offline device

Requests funding

Intermediary

Requests offline issuance

Eurosystem
Online Reconciliation

Eurosystem must maintain **ownership** and ensure **integrity** of its **balance sheet**

SE on the device: tamper-resistant features protect the information stored on the device and allow mutual device authenticity checks

Online reconciliation: provides ultimate line of defence as the authenticity of defunded offline digital euro is checked

Some data is needed to perform double spending and anti-forgery checks, while it should not be data which allows the direct identification of individuals by the Eurosystem. Data elements depend on the technical solution **which will evolve** with the state-of-the-art of anti-forgery checks.
Delivery considerations
Speeding up the delivery: Single vendor approach

In a multiple vendor approach, offline P2P **delivery time** is impacted by:

- Development of different solutions which are based on interoperability standards and a certification framework, first to be provided by the Eurosystem.
- Integration time and effort of the intermediaries.

To reduce the delivery time, a **single vendor** approach was chosen.

**Single vendor** will provide:

- (Open) Technical design and the development of a production-ready solution, to be made available to intermediaries by the Eurosystem** for integration and usage, aiming to reduce their integration time and investment.

Tender procedures will test and confirm market interest in this approach.

**Eurosystem with the selected vendor, would need to ensure a sufficient level of technical and operational assistance for the intermediaries to ensure smooth operations.**
4 POS strategy
Complex ecosystem of POS terminals

Offline digital euro needs to be accepted at multiple various different POS terminals across the euro area:
- Market for terminals has many competing providers (different sets of implementation specifications)
- Interoperability hinges on active collaboration among industry stakeholders

Eurosystem: Defines functional & security requirements

Specification providers / technical bodies:
- Define specs for level 2 kernel and terminal app
- Develop certification processes
- Degree of Eurosystem involvement still to be explored

Terminal vendors:
- Implement level 2 kernel and terminal app;
- Run certification processes

Offline digital euro acceptance, due to its status as legal tender, should be facilitated at point-of-sale (POS) terminals across the euro area. This implies the following:
- The rulebook may need to contain market-compatible specifications, as a single application won’t fit all terminal types. Some very old terminals might require replacement.
- A strong industry collaboration and backing is needed

Project team is further investigating how to leverage tender procedures to deliver offline POS payments

*: European Payment Stakeholders Group (EPSG) book of requirements
Thank you

Additional supporting materials:
- Updated digital euro FAQ
- Report: A stocktake on the digital euro
- ECB opinion on the EU Commission’s digital euro legislative proposal
- Digital euro one-pager
- Digital euro booklet
- Digital euro LinkedIn page