Council of the European Union
General Secretariat

PUBLIC

Interinstitutional files:
2023/0212 (COD)

Brussels, 25 June 2025

WK 8739/2025 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 (VTC) technical seminar - Offline security requirements, accessibility and availability in the context of Article 33 DER

EUROPEAN CENTRAL BANK

EUROSYSTEM

CWP technical seminar

Offline security requirements, accessibility and availability in context of Article 33 DER



30 June 2025

This presentation has not been adopted or endorsed by ECB decision making bodies and therefore any views expressed shall not, under any circumstances, be regarded as an official position of the ECB. Its content is intended only for the purpose of facilitating discussions within the Council Working Party

Agenda

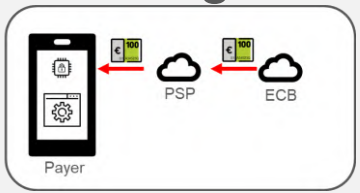
PUBLIC

1. Reminder: offline digital euro
2. Offline security
3. Accessibility
4. Availability

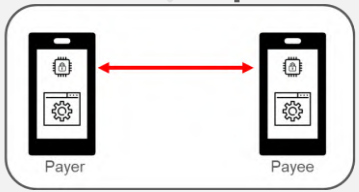
Reminder: offline digital euro

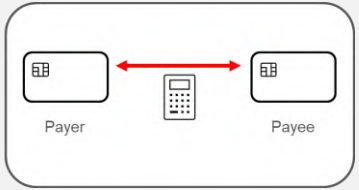
PUBLIC

Funding

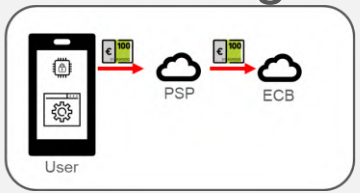


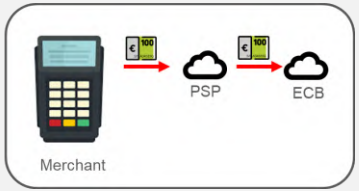
Peer-to-peer



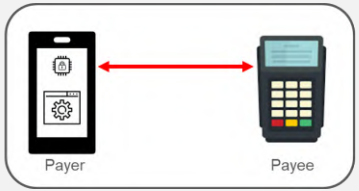


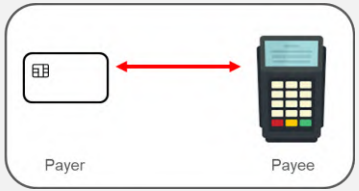
Defunding





Peer-to-merchant





www.ecb.europa.eu ©

Reminder: options to pay offline

User research shows that the best user experience is with phones on practicality, innovation and universality



Phones: best-in-class user experience



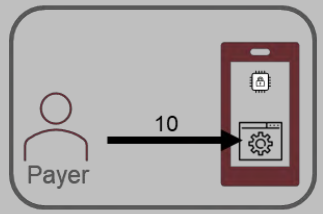
Smart cards & bridge devices: a poor user experience

A user's card cannot be used to pay to another user's phone, and a user's phone cannot be used to pay to another user's card

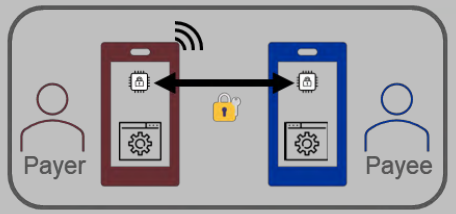
PUBLIC

www.ecb.europa.eu ©

Reminder: how an offline payment works

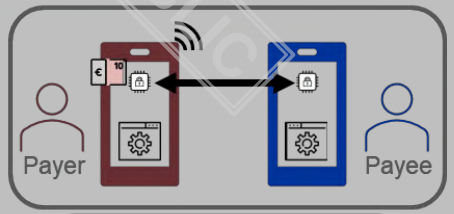


The payer unlocks phone and enters the amount

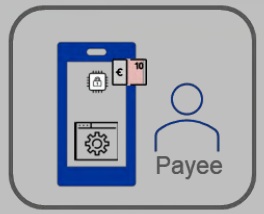


The payee taps his phone.

A secure session starts between phones: mutual authentication, confidentiality, integrity, anti-replay



The payer debits the balance, generates and backs-up the payment, and sends it



The payee checks the payment and credits the balance

www.ecb.europa.eu ©



PUBLIC

Offline security

The necessity of secure environments (SE)

www.ecb.europa.eu ©

Offline security: risks

PUBLIC

Technical

- Change of wallet data
- Extraction of data
- Change of executing flow of payment logic (code)



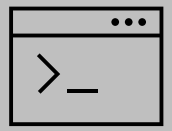
Functional: Fraudulent money creation

- Skip the balance debit when the wallet pays (“double spending”)
- Extract the wallet key used to sign a banknote change
- Change the wallet limits that force to go back online
- Re-enable a disabled wallet
- Sending again the same banknote (double spending/replay)

www.ecb.europa.eu ©

Offline security: type of attacks

Example: Sending an amount almost exceeding the valid length to obtain a huge balance value



Software attacks

Example: Injecting a power glitch at the right moment to skip the balance debit



Hardware attacks

We need to resist all plausible attacks

PUBLIC

www.ecb.europa.eu ©

Offline security: what do we need?

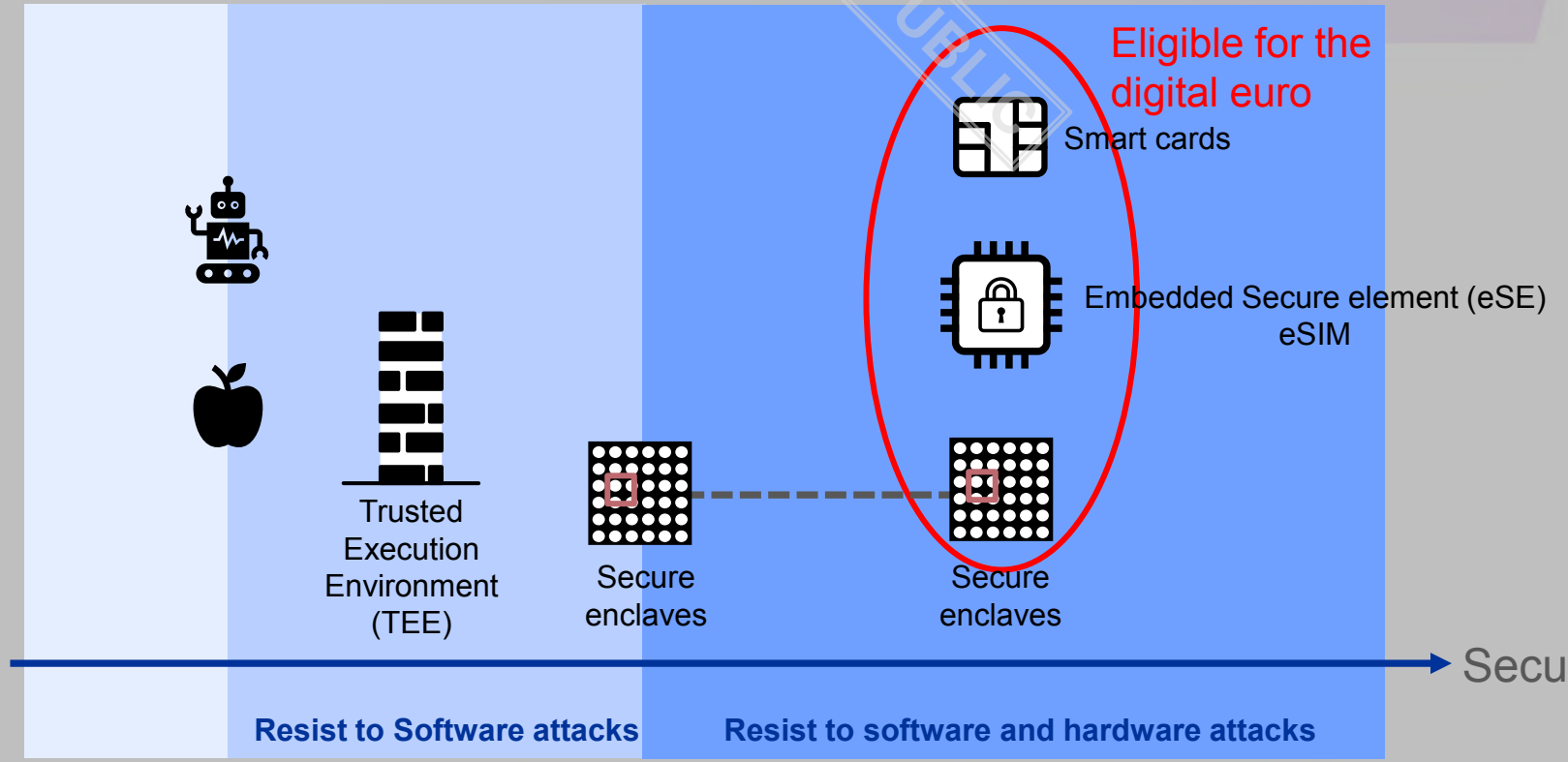
PUBLIC

We need to resist a **High Attack Potential***

Being at least as secure as market standards adopted by physical cards or Apple Pay today

* High Attack Potential, as defined by the Common Criteria methodology with the vulnerability assessment AVA.VAN 5 over identified protection profiles, as accepted by the payment market

Offline security: secure environments (SE) necessary



PUBLIC



PUBLIC

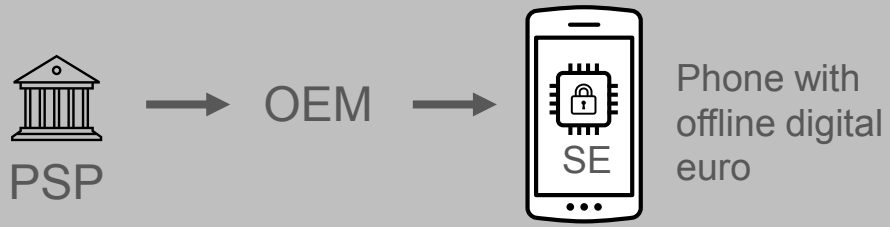
Accessibility

Access to the phone’s secure environment is critical

www.ecb.europa.eu ©

Accessibility: definitions

- ✓ **OEMs** = Original Equipment Manufacturers; owner of the SE.
- ✓ **FRAND** = fair, reasonable and non-discriminatory terms for access to the SE of OEM phones to allow for offline digital euro.
- ✓ **DMA** = Digital Markets Act which notes that the gatekeeper shall provide free-of-charge access to the same hardware and software features that it accesses or controls



The offline functionality of the digital euro relies on a secure environment embedded in users' smartphones to prevent counterfeiting. However, accessing this secure environment is expected to come at a cost as OEMs are likely to charge fees.

www.ecb.europa.eu ©

Accessibility: DMA and FRAND

- DMA covers 27% of shipments
- Majority (73%) of OEMs can charge for SE access
- The biggest OEM (34%) is not under DMA



Shipments of mobile phones

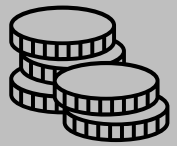
Canalys market analysis data (2024)

PUBLIC

Accessibility: secure environments and the D€

PUBLIC

Expectation



Majority of **OEMs start charging** for third-party access to the secure environment on top of the sales price of the mobile device.

Risk

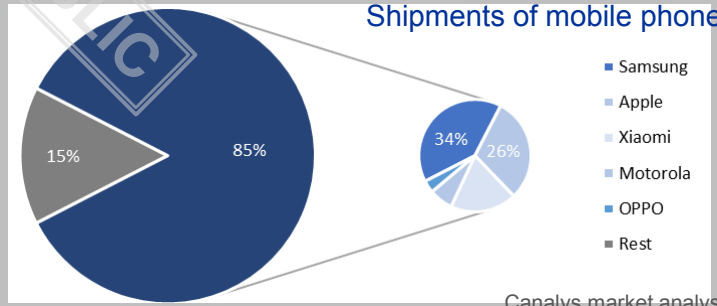


Substantial costs for providers of digital euro front-end services, including **banks.**

www.ecb.europa.eu ©

Accessibility: secure environments – market status quo

Secure environments are **controlled by OEMs**. The top 5 OEMs (85% shipments) are all non-EU.



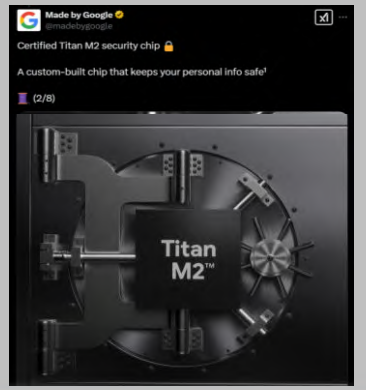
~90%

Canalys market analysis data (2024)

Secure environments are marketed as a reason for why consumers should buy the mobile device.







www.ecb.europa.eu ©

Accessibility: ECB concerns with FRAND terms

PUBLIC

Unclarity of the fee level

- Free security yesterday may no longer be free in the context of the digital euro
- European PSPs could face substantial charges from largely non-EU OEMs

Timeline uncertainties

- Risk of strategic non-compliance and lengthy + expensive court cases to determine FRAND rate
- PSPs have little experience with litigation on technology access compared to OEMs

www.ecb.europa.eu ©



PUBLIC

Availability

Towards a secure offline digital euro for all

www.ecb.europa.eu ©

Availability: security in future EU smartphones

PUBLIC

- ✓ Purpose: ensure that the only pan-European offline payment solution, the offline digital euro, is **widely availability and secure** for euro area citizens
- ✓ Method: a **SE is essential** to ensure security and this needs to be available on EU smartphones
- ✓ Effectiveness: security level and attack potential of SE could be defined and evaluated by mature methodology, **certified by accredited third parties**, already adopted by safe payment means (payment cards, Apple pay)
- ✓ Choice: **OEMs could choose how to implement the SE** – technology neutral (not mandating hardware or a specific form factor like eSIM, iSIM, secure enclave, eSE, iSE, pure software)

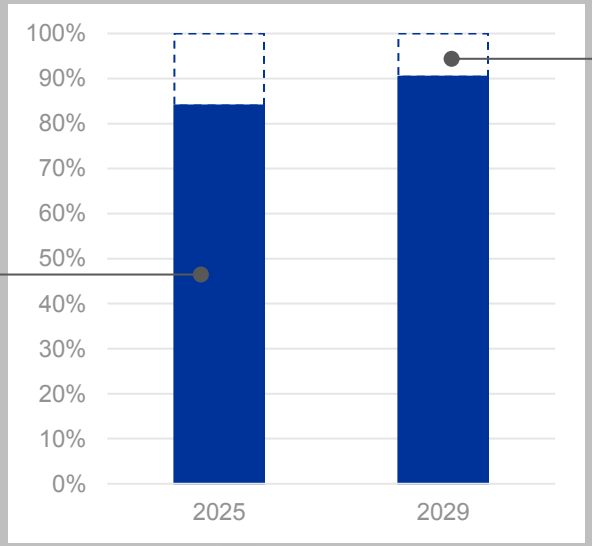
www.ecb.europa.eu ©

Availability: by 2029, approx. 10% of major OEMs phones are not secure enough

PUBLIC

Expected shipments of mobile phones with high security

In % share of expected mobile phones shipments in EU by top 5 vendors*



- Potentially eligible SE

- Approx. 4 Million phones would not be compatible with the offline digital euro
- These phones tend to be cheaper and provide a benefit to end-users on low incomes

* Standard dev 9% - Based on external data provider MRU Market Research Update

www.ecb.europa.eu ©



PUBLIC

Conclusion

www.ecb.europa.eu ©

Conclusion

PUBLIC

SE accessibility

- Potentially expensive for PSPs/end-users at the benefit of non-EU OEMs

SE availability

- By 2029, approx. 10% of newly shipped smartphones in EU from major vendors would not be eligible for the digital euro

www.ecb.europa.eu ©



PUBLIC

Annex

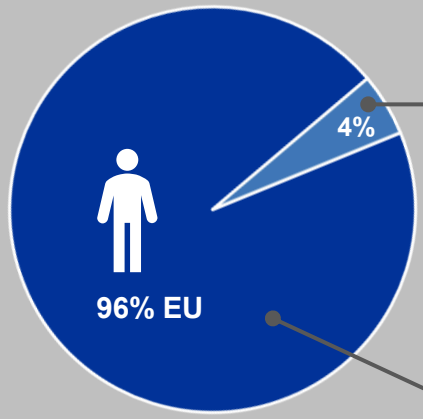
www.ecb.europa.eu ©

PUBLIC

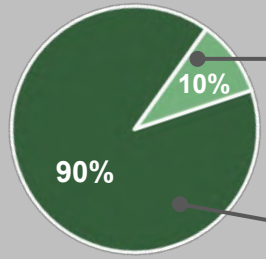


Although available data is limited, it indicates that at least one of the top three smartphone vendors in three European countries sells devices that lack a compatible secure environment necessary for supporting the offline digital euro.

www.ecb.europa.eu ©



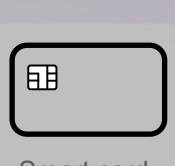
Newly shipped phones by top EU vendors 2029



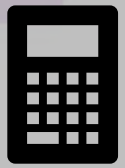
Additional cost for D€



No Phone



Smart card



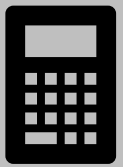
Bridge device

Phone without SE

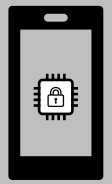




Smart card



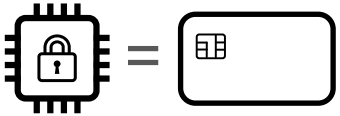
Bridge device



Phone with SE



Least expensive



Similar production cost

www.ecb.europa.eu ©

References & credits

PUBLIC

- **JIL: Application of Attack Potential to Smartcards and similar devices**

https://www.sogis.eu/documents/cc/domains/sc/JIL-Application-of-Attack-Potential-to-Smartcards-v3.2.1.pdf

- **Common Criteria (CC)**

https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/Zertifizierung-und-Anerkennung/Zertifizierung-von-Produkten/Zertifizierung-nach-CC/IT-Sicherheitskriterien/CommonCriteria_2022_ISO/commoncriteria_2022_ISO.html

- **Eurobarometer: Europeans' use and views of electronic communications in the EU**

https://digital-strategy.ec.europa.eu/en/news/eurobarometer-europeans-use-and-views-electronic-communications-eu#:~:text=The%20survey%20results%20show%20that,%25%2C%20households%20have%20internet%20access.

- **Smartphone Shipments in 2024**

https://www.canalys.com/newsroom/europe-smartphone-market-q4-2024

- **Total number of unique mobile subscribers 2022-2030**

https://www.gsma.com/solutions-and-impact/connectivity-for-good/mobile-economy/wp-content/uploads/2023/11/GSMA-Mobile-Economy-Europe-2023.pdf

- **Common charger (USB-C)**

https://commission.europa.eu/news/eu-common-charger-rules-power-all-your-devices-single-charger-2024-12-28_en

https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32022L2380

- **Picture credits**

CC: https://www.svgrepo.com/svg/312116/euro-banknote

www.ecb.europa.eu ©