Giesecke+Devrient
Creating Confidence

Digital Cash

Secure wallets for online and offline payments

Lars Hupel
Java Card Forum Webinar
2024-12-09


FINE
GOLD

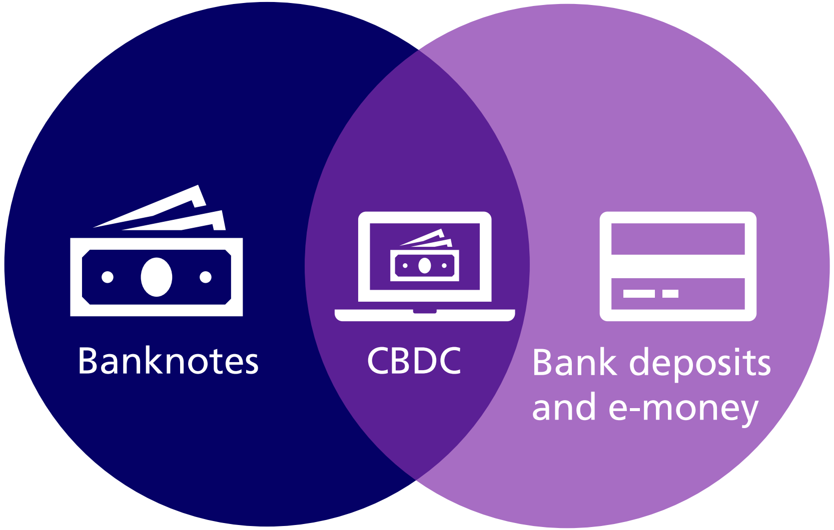

100
EURO
FEDERAL RESERVE NOTE

Digital Cash

- What is it?
- How do wallets work?
- Where is it used?
- How can I pay?

Central Bank Digital Currency

Issued by the
central bank



Digital money

Giesecke+Devrient
Creating Confidence

The move towards CBDC is gaining momentum

94%

of central banks worldwide are actively engaged in CBDC work

54% are developing proof-of-concept technology

31% are deploying pilot projects

Source: Bank for International Settlements, 2023-24

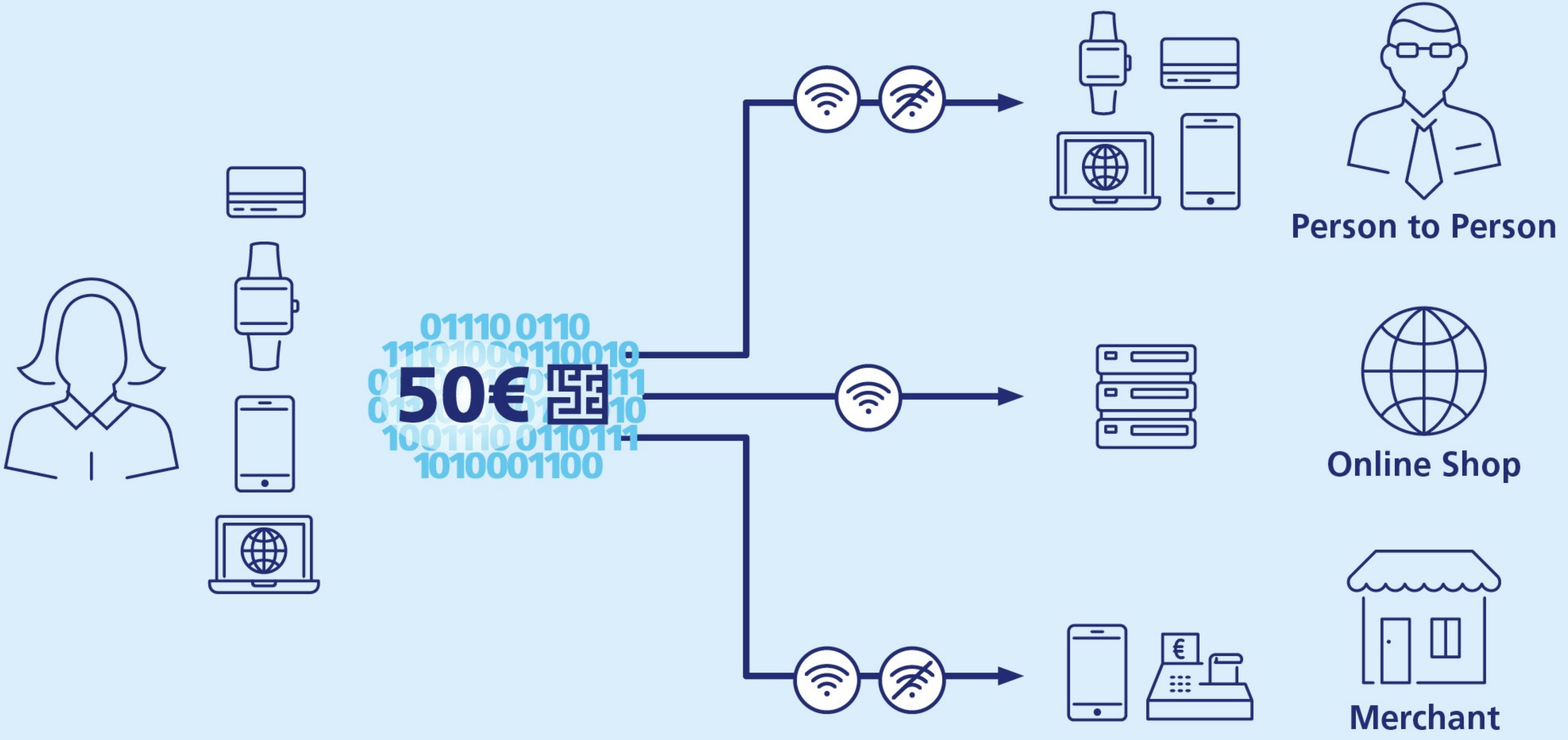
More than 13 million adults in the EU face financial exclusion

PRESS RELEASE

ECB publishes second progress report on the digital euro preparation phase

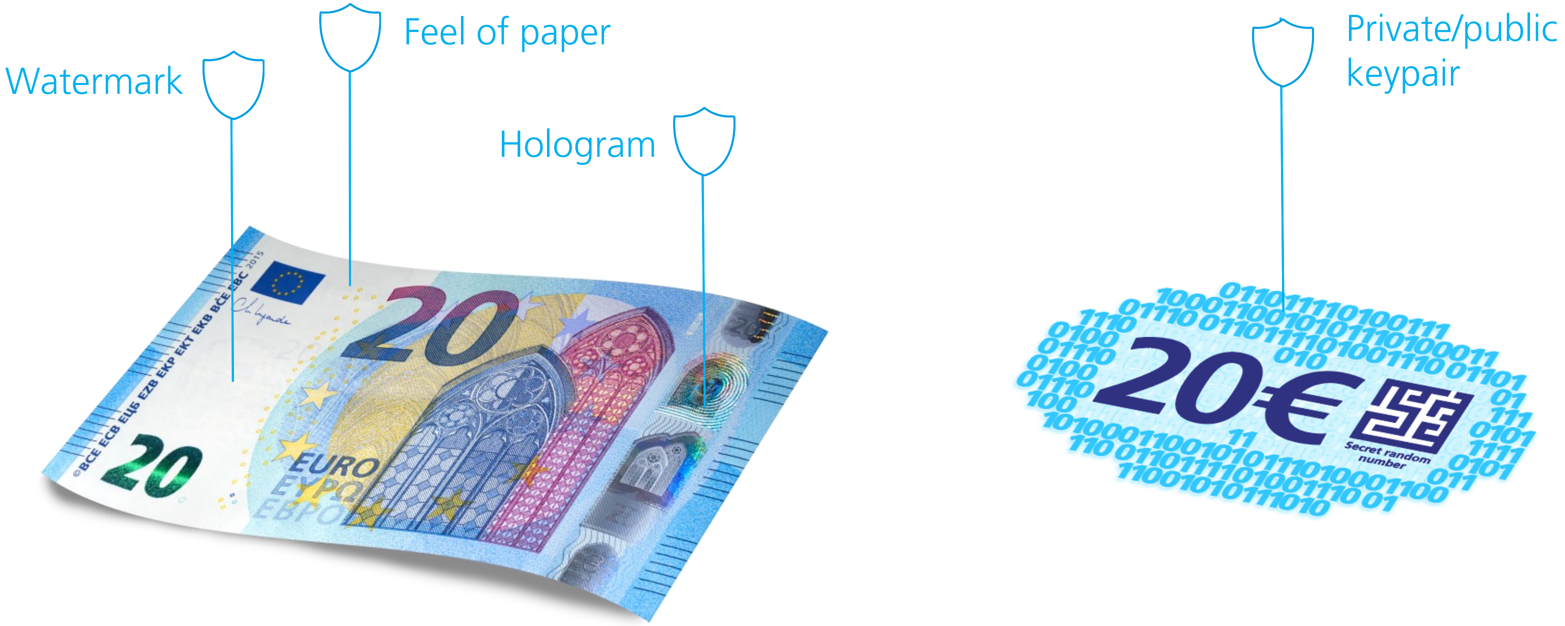
2 December 2024

- ECB updates digital euro rulebook following joint review with consumers, retailers and payment service providers
- ECB concludes call for applications to select potential external providers and publishes invitation to tender
- ECB launches new research to incorporate users’ digital euro design preferences
- Stakeholder engagement across euro area remains key priority to support ongoing legislative deliberations

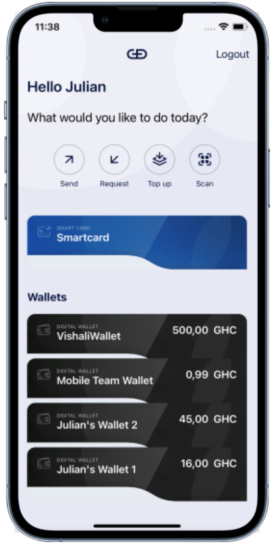


50€
Person to Person
Online Shop
Merchant

Modelling digital cash after physical cash



Wallet form factors



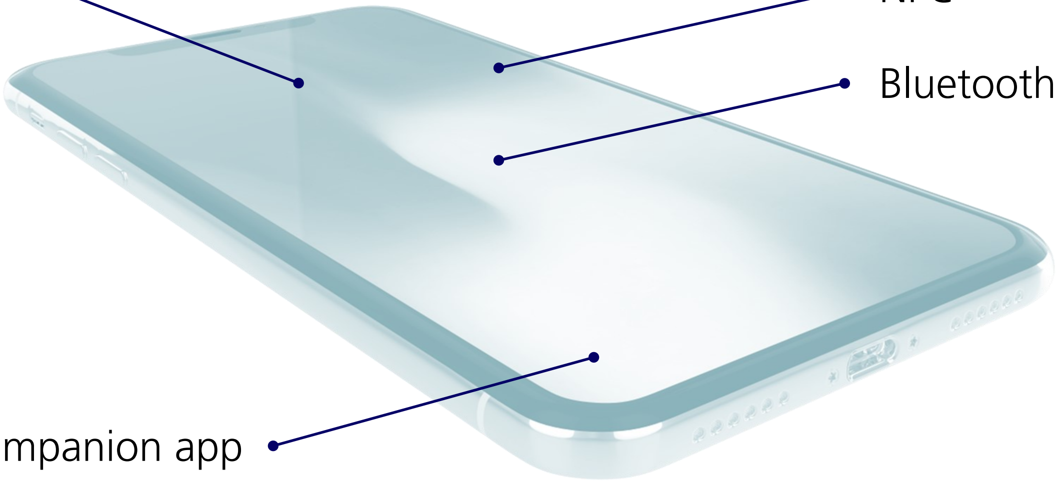
Now, where is my money?

Custodial wallet

Bearer wallet


NETFLIX

Hardware wallet requirements



A simple payment

Token transported via E2E-encrypted channel (SCP)

Public Key: `0xCAFE`
Amount: 20 €

Public key (without metadata) for integrity check

Date: 2024-11-06
Time: 10:15 CET
Payer: me
Payee: `023ab5`
Amount: 20 €

Wallet ID = pseudonym; KYC managed by intermediary

Metadata kept in both wallets; shared on demand

Date: 2024-11-06
Time: 10:15 CET
Payer: `014ca3`
Payee: me
Amount: 20 €


Ownership
Payer identity
Payee identity
Authenticity

Security requirements of (digital) money

Payer identity
Payee identity

Non-repudiation

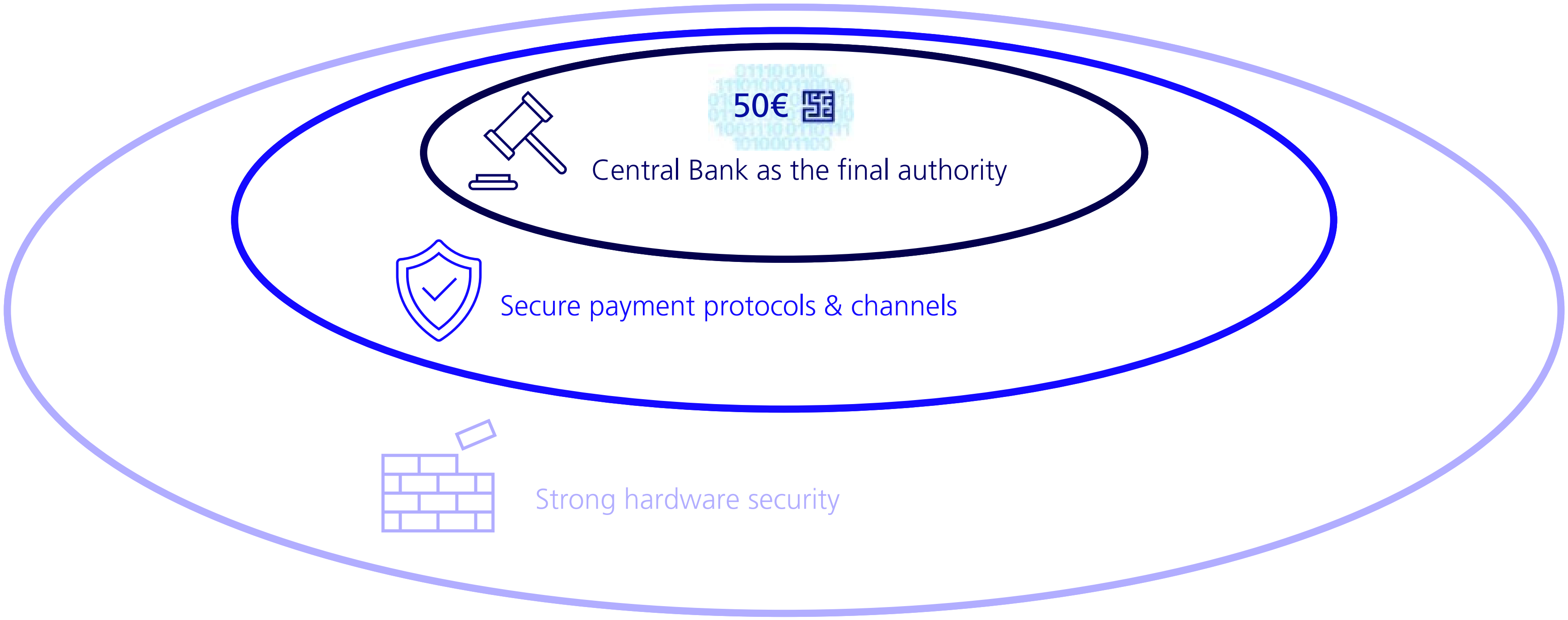
Authenticity

No double spending

Ownership

No tracing

A security architecture with three lines of defence



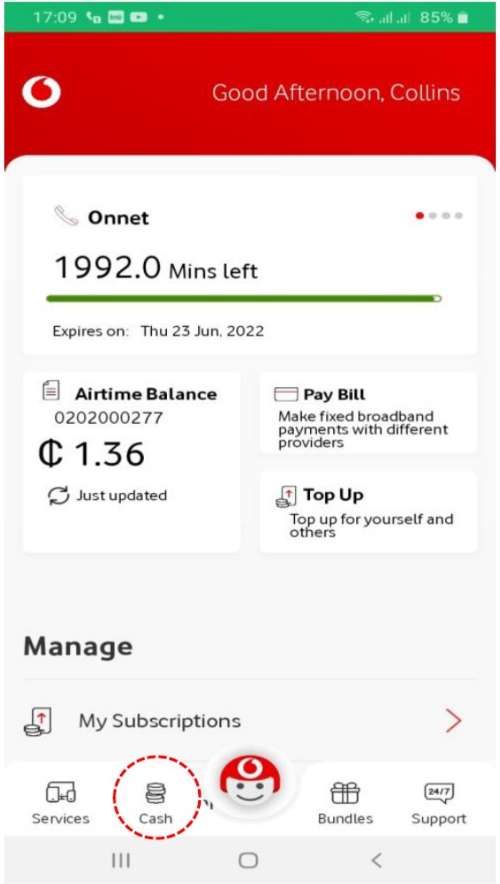
Designs that create confidence

Reference projects

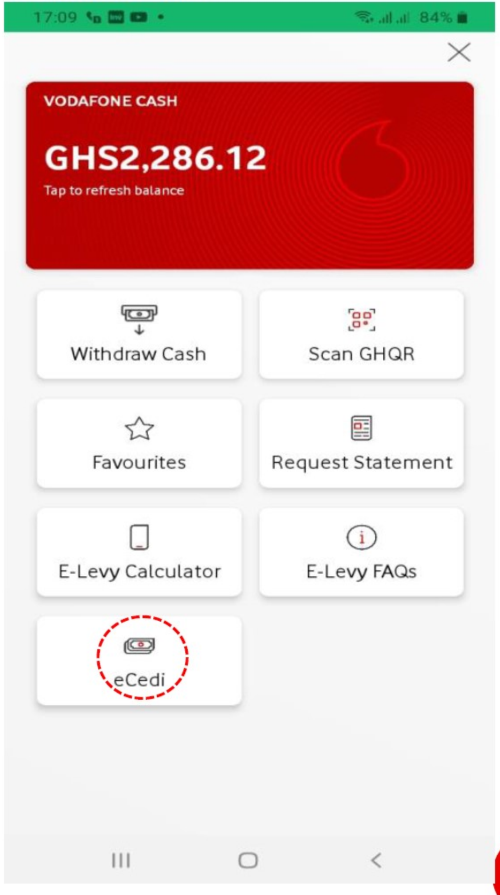
Giesecke+Devrient
Creating Confidence

Mobile app integration

Select Cash



Select e-cedi




Logout
Hello
Fleamarket-ehkd-user-002,
What would you like to do today?
Send
Request
Top up
Scan
standard chartered
Wallets
eHKD Wallet
500.00 HK$
standard chartered
hypothetical
e-HKD

Giesecke+Devrient
Creating Confidence

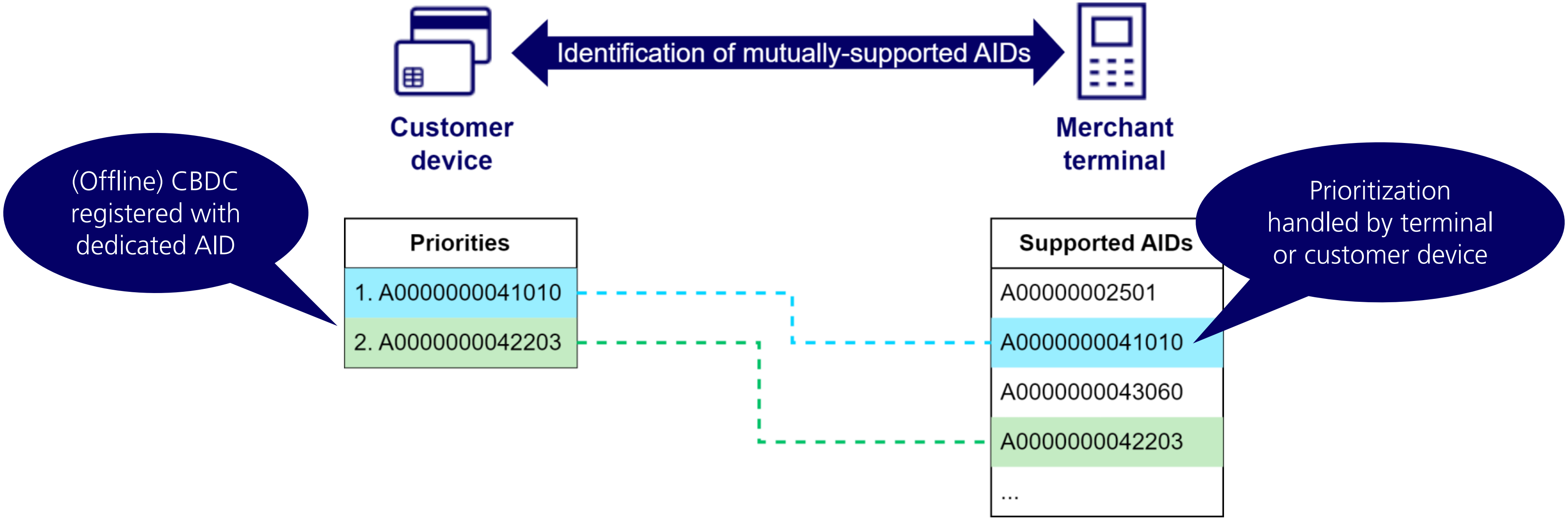
How would payments work in practice?

2021

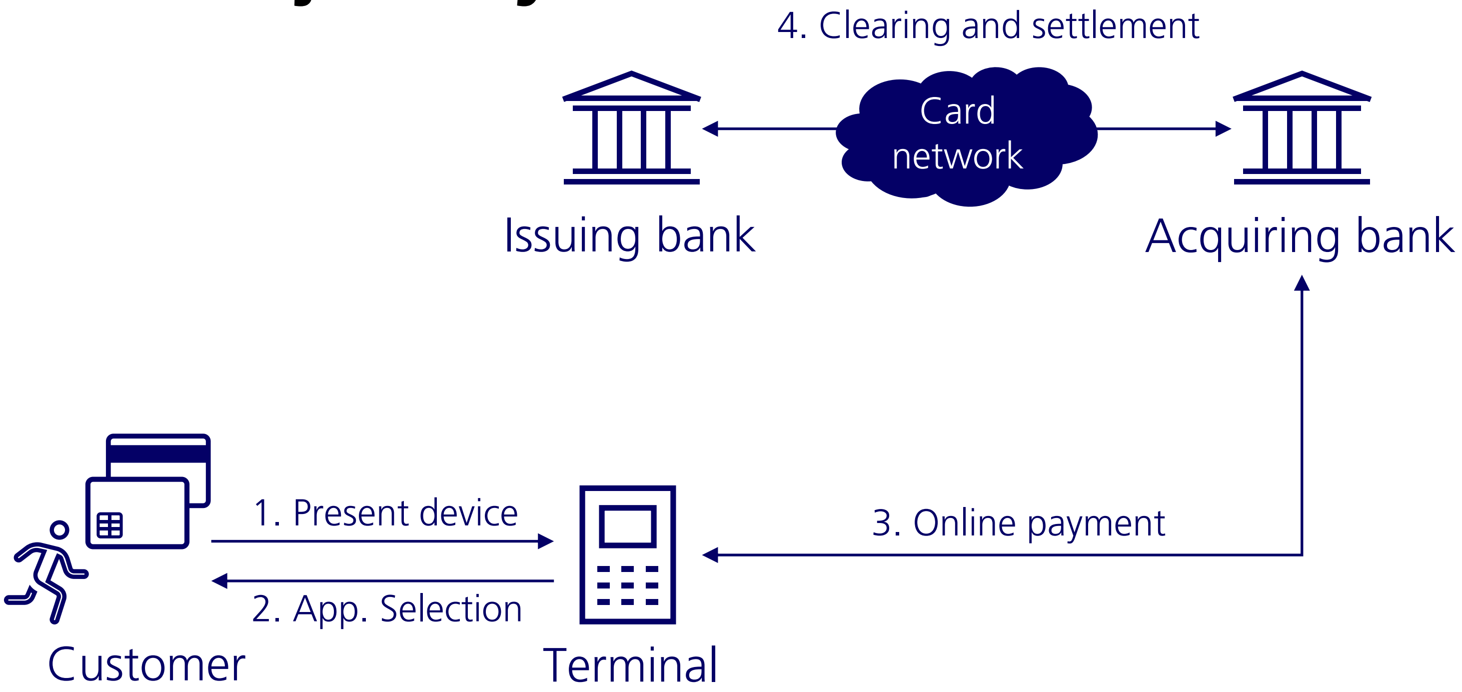

EXIT

“The EMV applications on the smart cards **were not appropriate for storing offline balances** … Therefore, we developed a new application that could store offline balances on the smart cards. This new application was **not based on EMV standards so we also needed to deploy a new kernel** …”

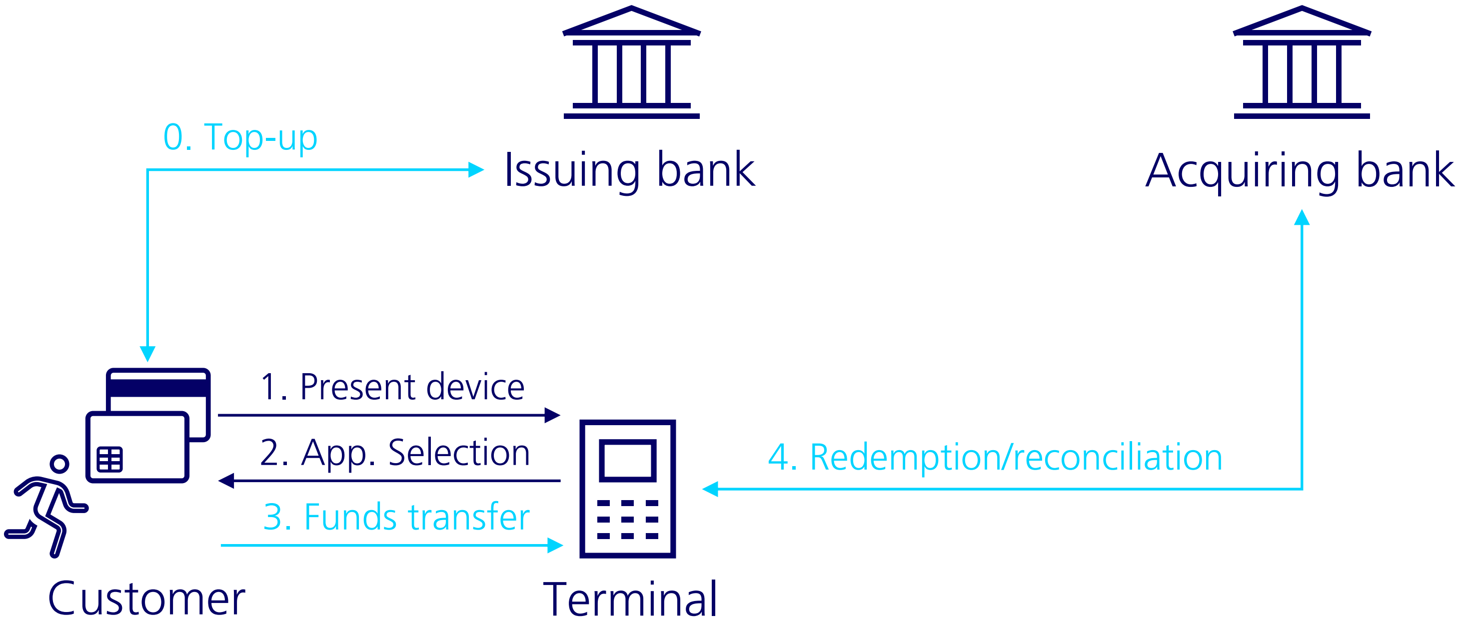
Application selection



Traditional user journey



Offline user journey



Application Selection

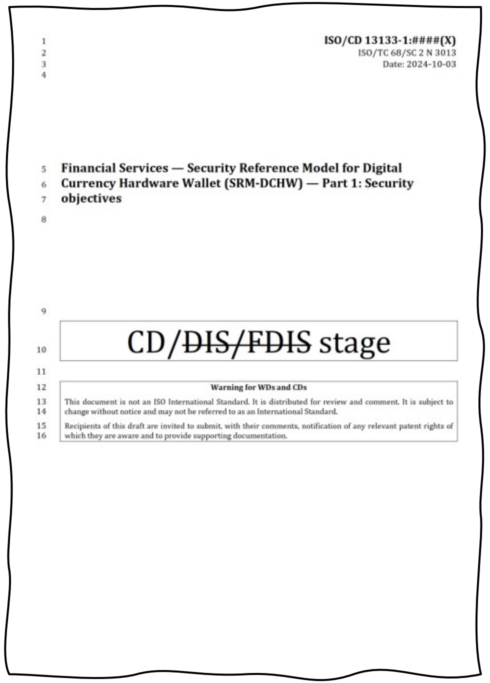
↓

Offline transfer of funds

↓

Reconciliation

Giesecke+Devrient
Creating Confidence


ISO/CD 13133-1:####(X)
ISO/TC 68/SC 2 N 3013
Date: 2024-10-03

Financial Services — Security Reference Model for Digital Currency Hardware Wallet (SRM-DCHW) — Part 1: Security objectives

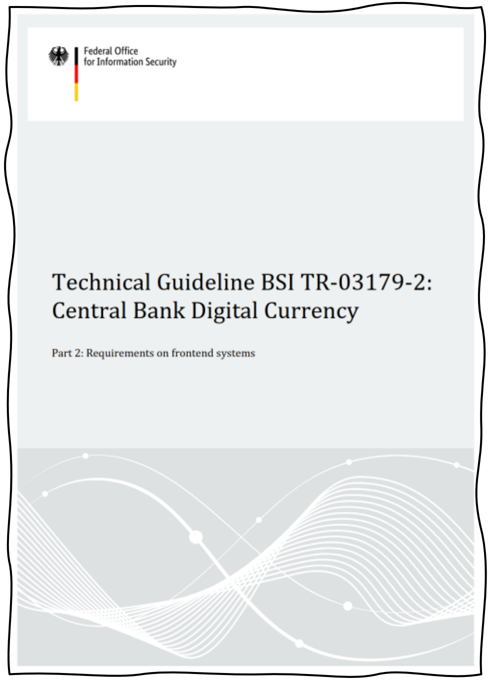
CD/~~DIS/FDIS~~ stage

Warning for WDs and CDs

This document is not an ISO International Standard. It is distributed for review and comment. It is subject to change without notice and may not be referred to as an International Standard.

Recipients of this draft are invited to submit, with their comments, notification of any relevant patent rights of which they are aware and to provide supporting documentation.

TC 68/SC 2/WG 13
ISO/CD 13133


Federal Office
for Information Security

Technical Guideline BSI TR-03179-2: Central Bank Digital Currency

Part 2: Requirements on frontend systems

BSI
TR-03179-2

Questions?
Answers!

Lars Hupel

https://lars.hupel.info

lars.hupel@gi-de.com