Mobile Payment Applications

- Session: Hardwarebasierte Vertrauensanker für die europäische eID Technologie
- Dr. Ullrich Martini, G+D ePayments GmbH
- Omnisecure Berlin, 22.01.2024

Mobile Payment Applications

- Branded
  - Good, UI owned by service provider
- Secure
  - Good, lab-tested and certified
- Personalized
  - Challenge, because not delivered physically
- Convenient

➢ Ready for payment applications

Vision

- Standardized
- Secure personalization
- Full branding on iOS
- Unified solution for iOS and Android

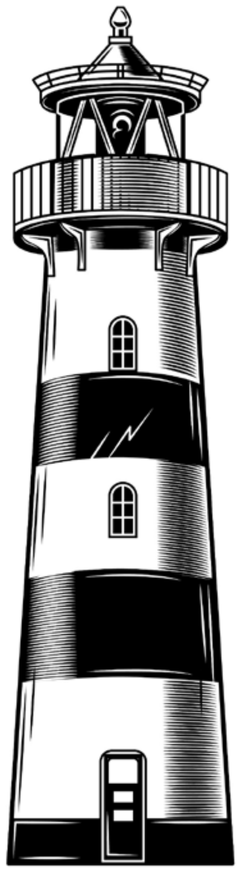


Bild von pch.vector auf Freepik

Way Forward

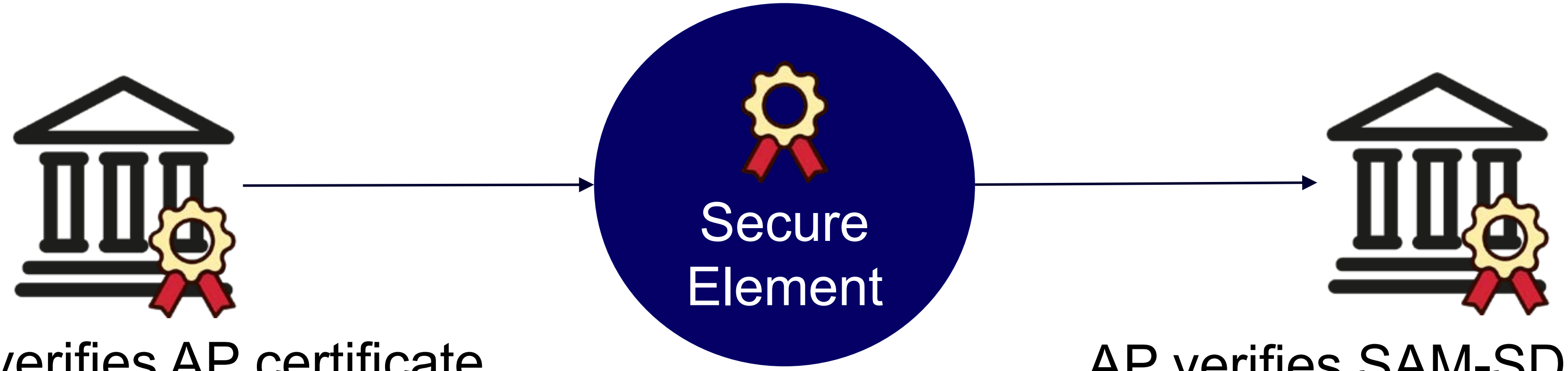
- Rely on specification: ISO, GlobalPlatform, JavaCard Forum, GSMA
- Secured Application for Mobile “SAM-SD” (GSMA specification)
  - Reliable vendor-independent end-to-end specification
  - Secure installation of applet and key material
  - Tested independently of vendors
- Will be ready for online rollout
- Requires dedicated security hardware in the device
  - Embedded SIM (eSIM)
  - Dedicated chip

Technical Basis

- JavaCard hardware and OS
  - EAL4+ or better
  - Embedded SIM
  - Other Embedded Secure Element
- Pre-personalized by silicon vendor, root of certificate chain
- GlobalPlatform SAM configuration
  - Amd A: Certificate verification; Key Generation inside Security Hardware
  - Amd F: Certificate verification; Secure Channel to Application Provider
  - Amd N: CSP; Improved internal cryptographic API inside Security Element
- Specified by GSMA

Lifecycle of a SAM-SD

- Silicon vendor pre-personalizes the SAM-SD with keys and certificates
- Application Provider performs Mutual Authentication with SAM-SD
  - Secure Channel between SAM-SD and Application Provider
- Application Provider (AP) installs and personalizes its own Security Domain (APSD)
  - Secure Channel between APSD and Application Provider

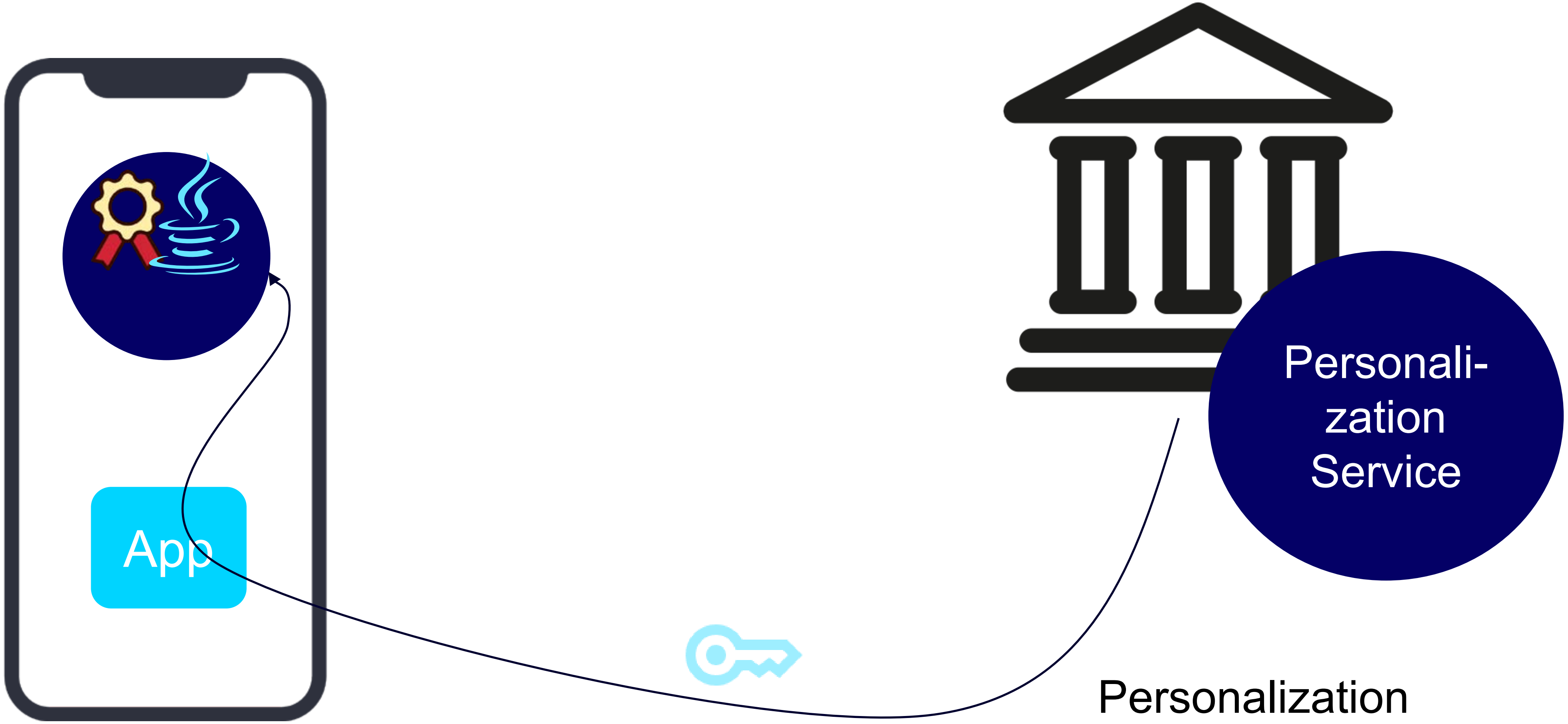


Secure Element

SAM-SD verifies AP certificate

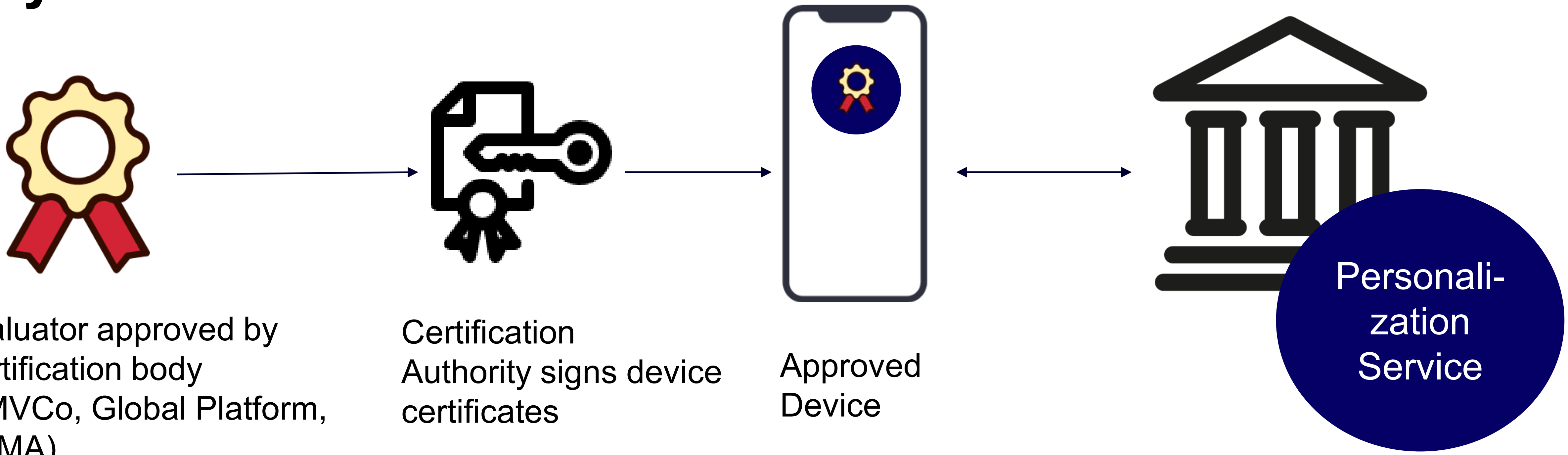
AP verifies SAM-SD certificates

Personalization



Personalization
Requires Mutual Trust
between Service and Device

Why Is It Secure?



Personali-zation Service

Evaluator approved by Certification body (EMVCo, Global Platform, GSMA)

Certification Authority signs device certificates

Approved Device

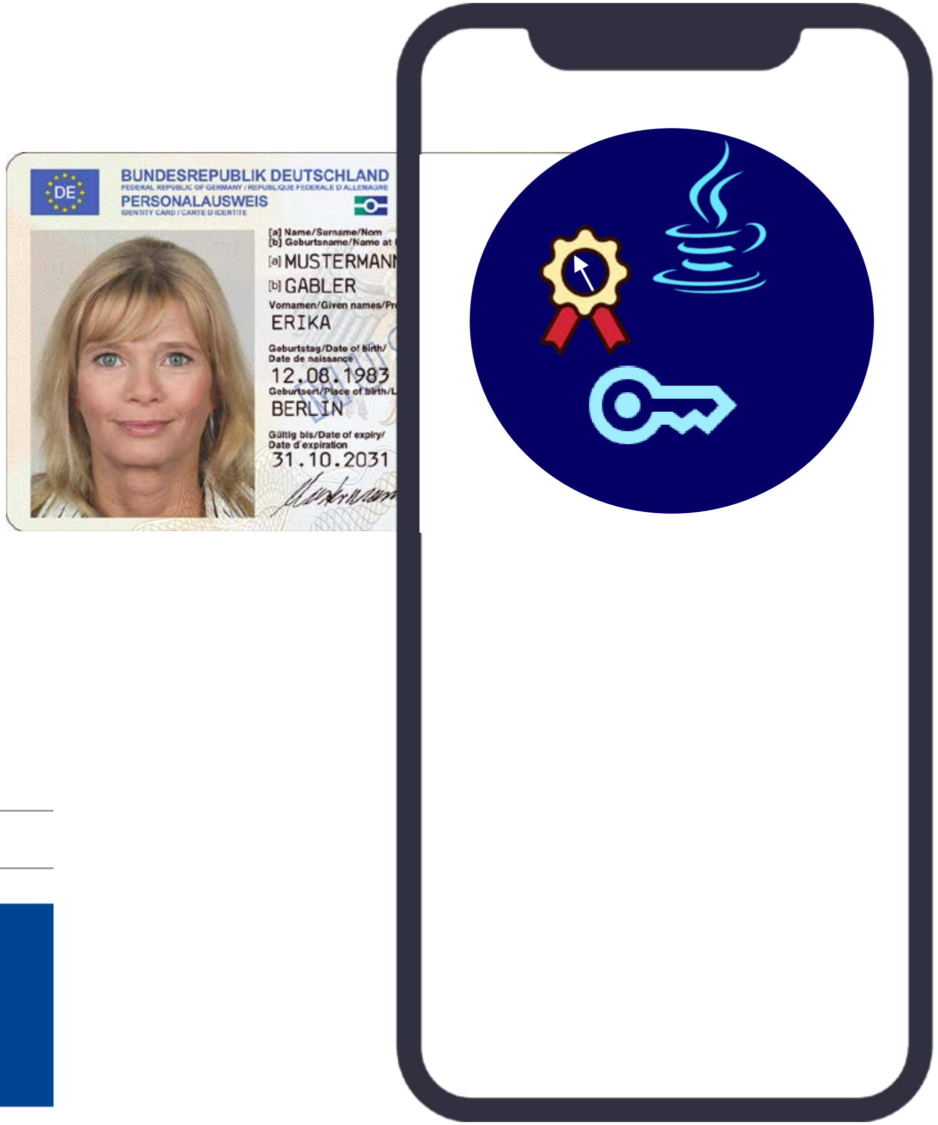
Bank issues digital payment card if certificates are correct

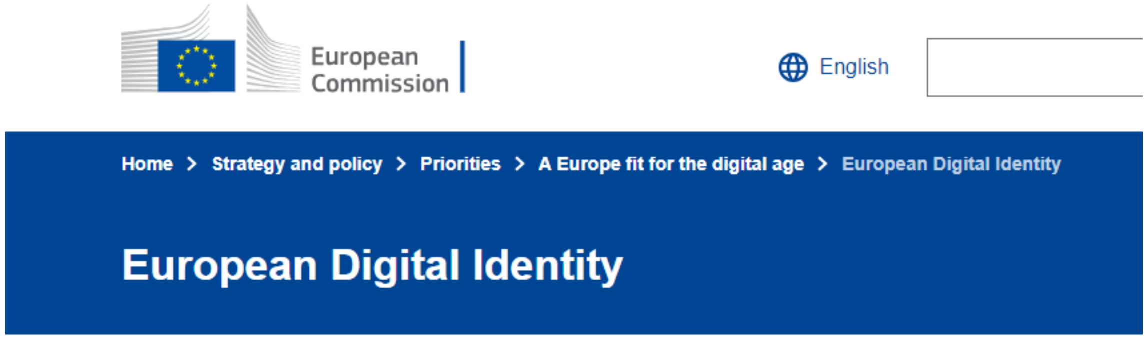
Identification Challenge

- Need to connect the pseudonymous internet user to a banking customer
- Customers cannot be asked to visit a branch office
- Need internet-native solution

European Digital Identity

- Identity established by the local government
- Requires interaction between application backend and eID provider


DE
BUNDESREPUBLIK DEUTSCHLAND
FEDERAL REPUBLIC OF GERMANY / REPUBLIQUE FEDERALE D'ALLEMAGNE
PERSONALAUSWEIS
IDENTITY CARD / CARTE D'IDENTITE
[a] Name/Surname/Nom
[b] Geburtsname/Name at
[a] MUSTERMANN
[b] GABLER
Vornamen/Given names/Pr
ERIKA
Geburtstag/Date of birth/
Date de naissance
12.08.1983
Geburtsort/Place of birth/L
BERLIN
Gültig bis/Date of expiry/
Date d'expiration
31.10.2031



European Commission

English

Home > Strategy and policy > Priorities > A Europe fit for the digital age > European Digital Identity

European Digital Identity

Vielen Dank für Ihre Aufmerksamkeit!

Kontakt

Dr. Ullrich Martini

ullrich.martini@gi-de.com

Giesecke+Devrient ePayments GmbH

Prinzregentenstraße 161
81677 München, Germany