ID Evolution:
The Convergence of Digital Identity, Post-Quantum Security, and Next-Generation Credentials

Fanni Vikor, Infineon Technologies AG

Mindshare, 2026

12 market shifts influencing the identity ecosystem

01 Remote identity proofing becomes mainstream

02 Convergence of physical and digital IDs

03 Travel credential digitization

04 Upgrades in physical document security and materials

05 Crypto agility and post-quantum planning

06 Mobile credential privacy and selective disclosure

07 ID infrastructure advancement

08 Document lifecycle modernization

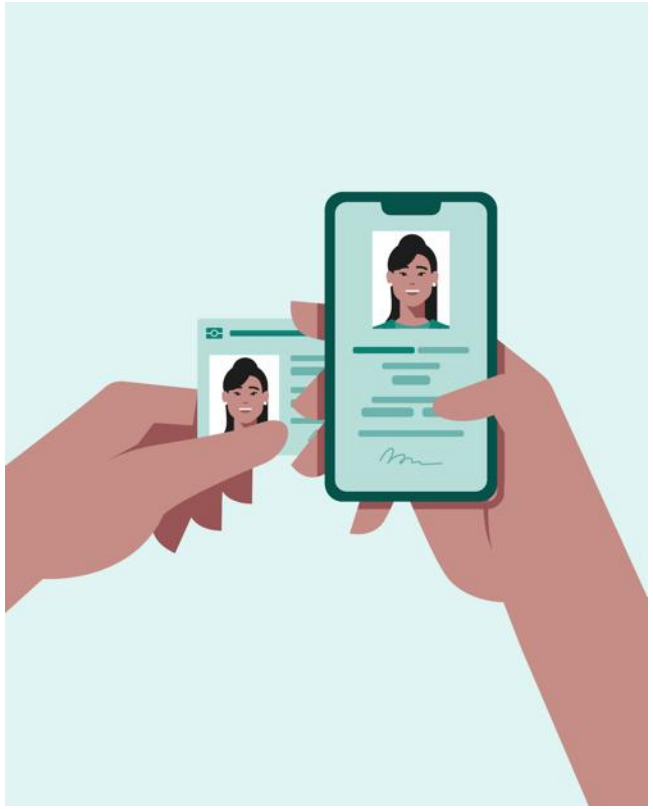
09 Biometrics everywhere

10 Standards-driven interoperability

11 Shift in revenue mix and delivery models

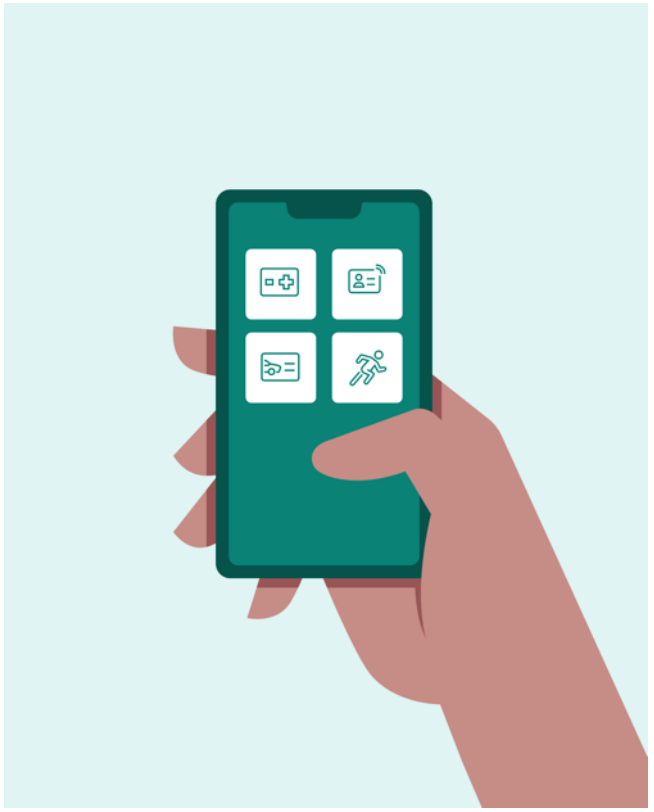
12 Growth in foundational ID programs

Digital ID, mobile ID and wallet: all related – but not the same



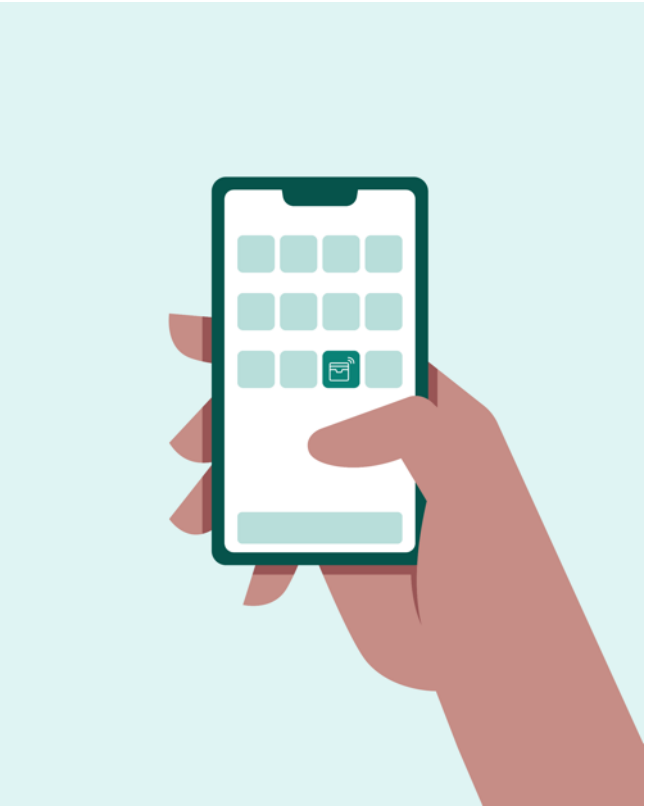
Digital ID

Refers to digital technology that can verify a person’s identity and their key credentials to enable the individual to engage in transactions.



Mobile ID

One of the different form factors of digital ID. It is mostly used for identity authentication, verification, and transactions to access private and governmental services.



Wallet

The entity that holds the virtual credentials or attributes for the holder.

Four challenges digital identity must solve to scale

Fragmentation & interoperability

Challenge
- Many issuers
- Could be limited cross-sector use
- Misaligned security requirements due to inconsistent architectures

Solutions
- Common standards
- Shared infrastructure frameworks
- Regulatory alignment

Public trust

Challenge
- Fear of data theft or misuse
- Lack of transparency
- Misinformation and missing user friendliness slow adoption

Solutions
- User control by design
- Clear data communication
- National digital education

Privacy & data minimisation

Challenge
- Full credential sharing
- More data than needed
- Unnecessary breach exposure

Solutions
- Selective disclosure
- Zero-knowledge proofs
- Strict guidelines for relying parties

High level of security

Challenge
- Ensuring that digital IDs have the same level of security as physical IDs
- Ensuring trust from citizens and verifiers

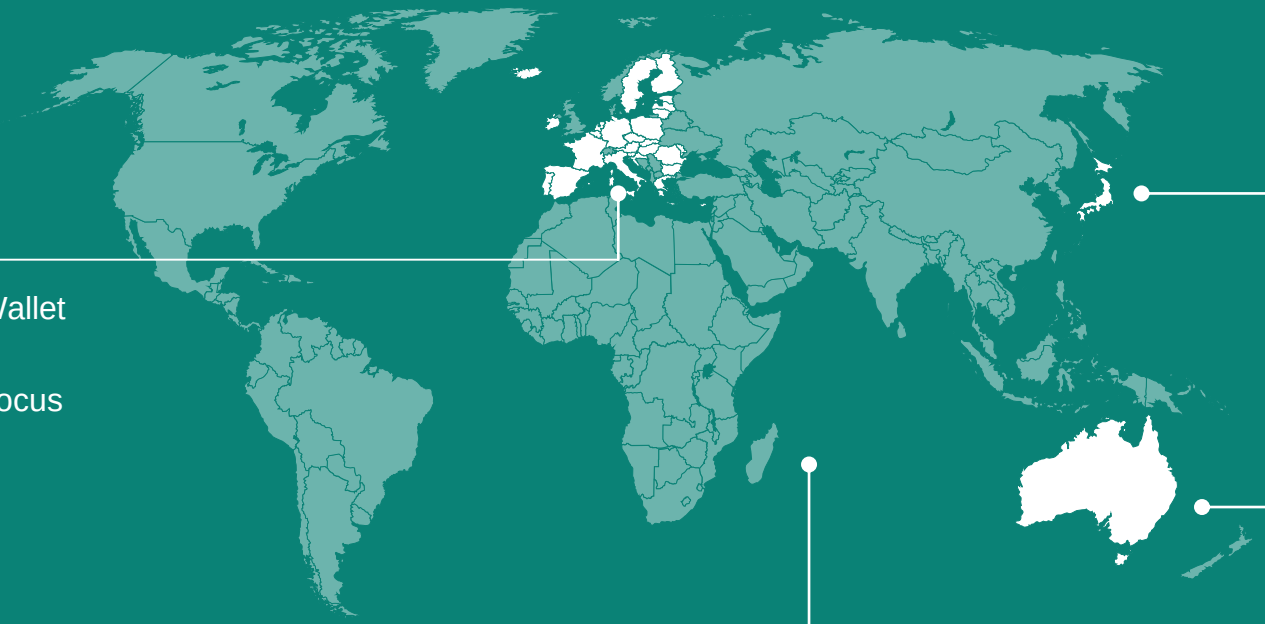
Solutions
- Secured hardware with high security requirements
- Cryptographic trust chains
- Certification

Physical and digital IDs are converging globally

Hybrid / twin models to stay
Citizens keep physical credentials while digital wallets and mobile IDs expand.

Global examples
Regions and countries are piloting or deploying digital identity models with different levels of assurance, security architecture and root of trust.

Physical and digital IDs are converging globally



European Union
- European Digital Identity Wallet
- eIDAS 2.0 framework
- Interoperability + security focus

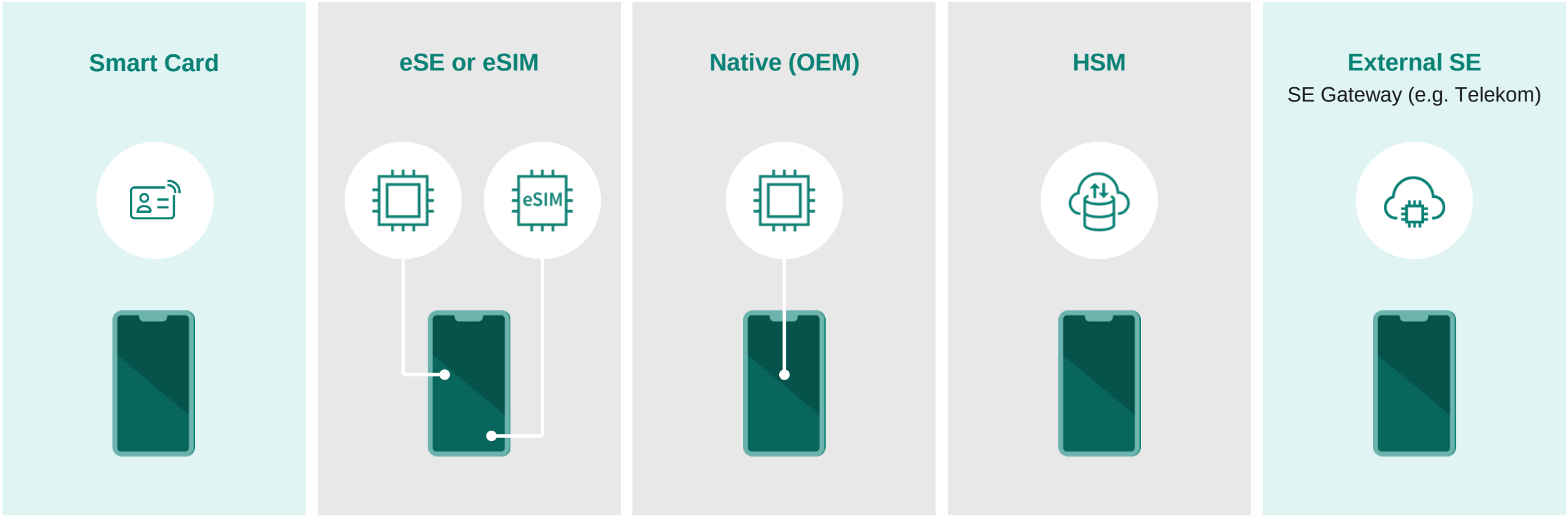
Japan
- My Number Card in Apple Wallet
- Online + in-person presentation
- Physical card as trust anchor

Australia
- Queensland Digital Identity
- Assurance levels by use case
- Application-based trust model

Mauritius
- ISO-compliant Digital ID Wallet
- Chip-based eID + companion app
- Hybrid credential model

Selected examples

Root of Trust – different security architectures – EUDI example



Local WSCD — **Remote WSCD**

Hybrid versions between remote WSCDs and local WSCDs are also possible

WSCD: Wallet Security Cryptographic Device, CC: Common Criteria, eSIM: electronic SIM, eSE: embedded Secure Element

Value of an external Smart Card for mobile ID

Smart Card

What the Smart Card enables

- Card issuance with mobile applet (ISO 18013-5)
- Secured authentication for critical transactions (e.g., paying large amounts, privacy topics,…)
- Issuance of person attributes (PID) to mobile phone
- Regular update of PID after expiry of data on phone
- In-field update of OS, applet or data
- Local signature with own key on card
- High level of assurance

Value of an external Smart Card for mobile ID

Field-proven security solution

Future-proof through PQC readiness

Easy deployment and high reach

High level of assurance

Offline and online usage

Government sovereignty over the card infrastructure

What the Smart Card enables

- Card issuance with mobile applet (ISO 18013-5)
- Secured authentication for critical transactions (e.g., paying large amounts, privacy topics,…)
- Issuance of person attributes (PID) to mobile phone
- Regular update of PID after expiry of data on phone
- In-field update of OS, applet or data
- Local signature with own key on card
- High level of assurance

Value of an external SE / SE gateway for mobile ID

External SE

SE Gateway (e.g. Telekom)

What the external SE / SE gateway enables

- Use SE Gateway for issuance of credentials
- Secured authentication for critical transactions (e.g., paying large amounts, privacy topics,…)
- Issuance of person attributes (PID) to mobile phone
- Regular update of PID after expiry of data on phone
- On-site update of OS, applet or data
- Remote signature with own key on card
- High level of assurance

Value of an external SE / SE gateway for mobile ID

Field-proven security solution

Future-proof through PQC readiness

Easy deployment and high reach

High level of assurance

Online usage

Optional government sovereignty over the trust infrastructure

What the external SE / SE gateway enables

- Use SE Gateway for issuance of credentials
- Secured authentication for critical transactions (e.g., paying large amounts, privacy topics,…)
- Issuance of person attributes (PID) to mobile phone
- Regular update of PID after expiry of data on phone
- On-site update of OS, applet or data
- Remote signature with own key on card
- High level of assurance

Key takeaways: digital identity builds on physical trust

Digital ID complements electronic physical documents – the hybrid model

Trusted credentials move into mobile and online use cases while electronic documents remain the root of trust.

Mobile ID adoption is gaining momentum

Mobile ID is already being adopted in several countries, while EUDI and eIDAS 2.0 are accelerating standardization and infrastructure development. Some non-EU countries may also align with emerging wallet infrastructures (i.e. Canada, US, UK).

Hardware security remains essential

Secure Elements provide the root of trust and help ensure that digital ID can reach the assurance level of today’s electronic documents.

Infineon enables next-generation ID

Security-certified hardware for physical, digital and hybrid credentials.

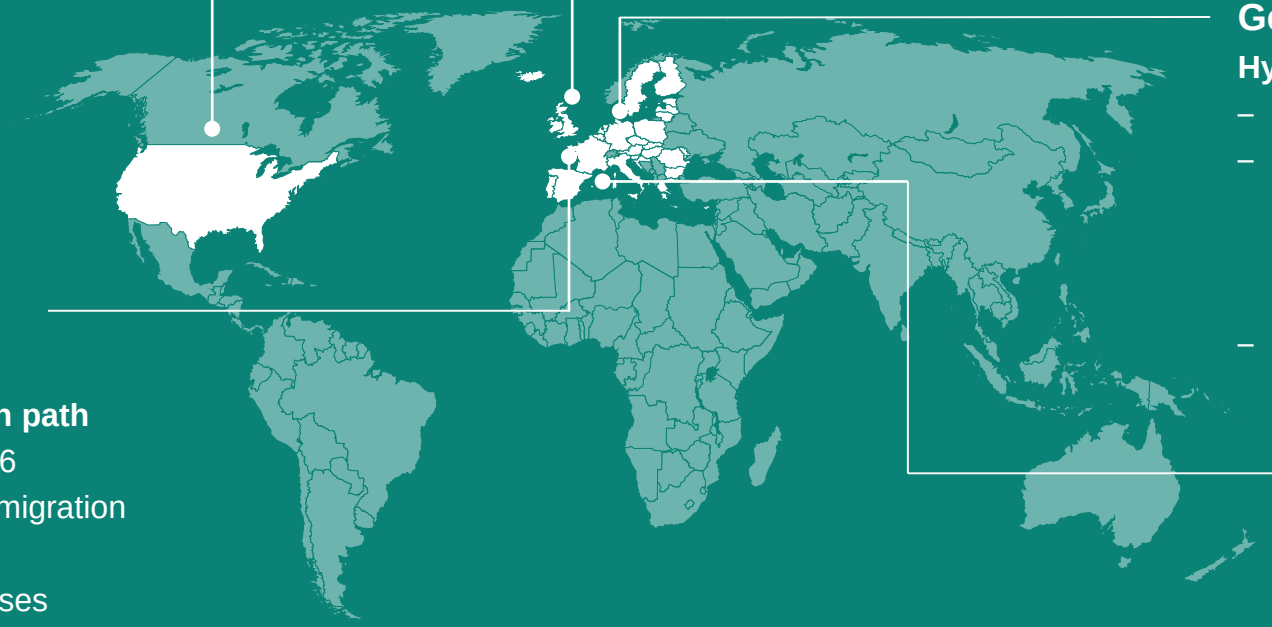
Don’t wait for quantum to start preparing

“Quantum computers are not here yet – so why act now?”

Because sensitive data is already being collected, while ID systems take years to change.

Problem	Solution	Your benefit
– Data stolen today may be decrypted tomorrow – ID documents and infrastructures have long lifecycles – Late migration creates cost, pressure and disruption	– Deploy PQC-ready secure hardware today – Keep cryptographic algorithms updateable – Build a migration path for future standards	– Protect long-term identity data – Extend the value of today’s infrastructure – Stay secured, compliant and trusted over time

PQC global transition plan



USA / NIST

Legacy crypto phase-out

- Deprecated after 2030
- Disallowed after 2035

UK

National PQC roadmap

- Key milestone definition by 2028
- Highest-priority migration by 2031
- Full migration by 2035

Germany / BSI

Hybrid transition recommended

- Classical-only algorithms only until 2031
- Hybrid implementations after 2031 -> Signatures based on RSA with a key length of at least. 3000 bit are recommended to be used until 2035
- Migration completed by 2035

European Union / ENISA / NIS

Risk-based transition path

- Initial phase by 2026
- High-risk use case migration completion by 2030
- Medium risk use cases migration completion by 2035

France / ANSSI

Early migration mandate

- Hybrid implementation
- 2027: mandatory PQC for qualification entry

Who is ready? Infineon is ready.
Worlds first CC certificate for PQC

Certification in December 2024

- **World's first CC-certificate for ML-KEM** on an Infineon security controller
- **Common press release** with German Federal Office for Information Security (BSI)

Bundesamt für Sicherheit in der Informationstechnik

Deutsches IT-Sicherheitszertifikat

erteilt vom Bundesamt für Sicherheit in der Informationstechnik

BSI-DSZ-CC-1249-2024 (*)

Smartcard Controller

IFX_CCI_000068h, IFX_CCI_000080h design step G12 with firmware version 80.505.04.1, optional PQ Crypto Suite v5.00.012, optional HSL v04.05.0040, optional UMSLC v02.01.0040 and user guidance documents

from	Infineon Technologies AG
PP Conformance:	Security IC Platform Protection Profile with Augmentation Packages Version 1.0, 13 January 2014, BSI-CC-PP-0084-2014
Functionality:	PP conformant plus product specific extensions Common Criteria Part 2 extended
Assurance:	Common Criteria Part 3 conformant EAL 6 augmented by ALC_FLR.1
valid until:	16 December 2029

The IT Product identified in this certificate has been evaluated at an approved evaluation facility using the Common Methodology for IT Security Evaluation (CEM), Version 3.1 extended by Scheme Interpretations, by advice of the Certification Body for components beyond EAL 5 and CC Supporting Documents as listed in the Certification Report for conformance to the Common Criteria for IT Security Evaluation (CC), Version 3.1. CC and CEM are also published as ISO/IEC 15408 and ISO/IEC 18045.

(*) This certificate applies only to the specific version and release of the product in its evaluated configuration and in conjunction with the complete Certification Report and Notification. For details on the validity see Certification Report part A chapter 5.

The evaluation has been conducted in accordance with the provisions of the certification scheme of the German Federal Office for Information Security (BSI) and the conclusions of the evaluation facility in the evaluation technical report are consistent with the evidence adduced.

This certificate is not an endorsement of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, and no warranty of the IT Product by the Federal Office for Information Security or any other organisation that recognises or gives effect to this certificate, is either expressed or implied.

Bonn, 17 December 2024

For the Federal Office for Information Security

Sandro Amendola
Director-General

L.S.

Bundesamt für Sicherheit in der Informationstechnik
Godesberger Allee 185-189 - D-53175 Bonn - Postfach 20 03 63 - D-53133 Bonn
Phone +49 (0)228 99 9582-0 - Fax +49 (0)228 9582-5477 - Infoline +49 (0)228 99 9582-111

SOGIS Recognition Agreement

Common Criteria Recognition Arrangement recognition for components up to EAL 2 and ALC_FLR only

DAkkS Deutsche Akkreditierungsstelle D-ZE-19615-01-00

Who is ready? Infineon is ready.
Worlds first CC certificate for PQC

Demonstration model of a quantum-secured ID card
Source: Bundesdruckerei GmbH

- Bundesdruckerei, Giesecke+Devrient, BSI, and Infineon developed new security technology for **Germany's next-generation ID cards with quantum-resistant chips.**
- The solution uses BSI's recommendations: hybrid cryptography combining classical methods with ML-KEM and ML-DSA (post-quantum algorithms).
- Infineon's new chip design enables fast, side-channel-resistant implementation of post-quantum cryptography.
- **Early adoption is important, as ID cards are valid for ten years.**

Paper documents need a digital trust layer – Chip-in-Paper

Many high-value documents will remain paper-based – but their authenticity must become easier, faster and more reliable to verify.

- **Fraud risks in paper-based documents**
  - Forgery & counterfeiting
  - Physical vulnerability
  - Limited traceability
  - Manual verification gaps
- **The solution: Chip-in-Paper**
  - Ultra-thin security chip embedded in paper
  - NFC/RFID-based verification
  - Cryptographic authenticity + integrity
  - Tamper resistance + clone detection
- **Potential use cases**
  - Land deed and land lease certificates
  - Birth certificates
  - University diplomas
  - High-value tickets or documents

Future-proof document security – enabled by Infineon

Certified security
- High Security Controller
- Common Criteria EAL6+
- NFC interface

Implementation expertise
- Proven security track record
- Integration support
- Accelerated go-to-market

Multiple integration options
- Ultra-thin module for seamless integration
- Embedded in substrate
- Sticker implementation option

Long lifetime options
- Different lifetime possibilities
- Suitable for different document types
- Suitable for high-value credentials

Aligned with global standards for trusted digital verification

Proof of concept: Chip-in-Paper

Banknote of the future

16 May 2024: Bundesdruckerei wins Industry Award

Award-winning concept for the Banknote of the Future

Infineon security controller built into the cavity of a half-window

NFC-enabled chip connects the physical banknote to digital services

Opens new possibilities for central banks and high-value documents

Fanni Vikor

Infineon Technologies AG

Business Development and Innovation Manager

Fanni.Vikor@infineon.com


Infineon