Infineon for identification and authentication

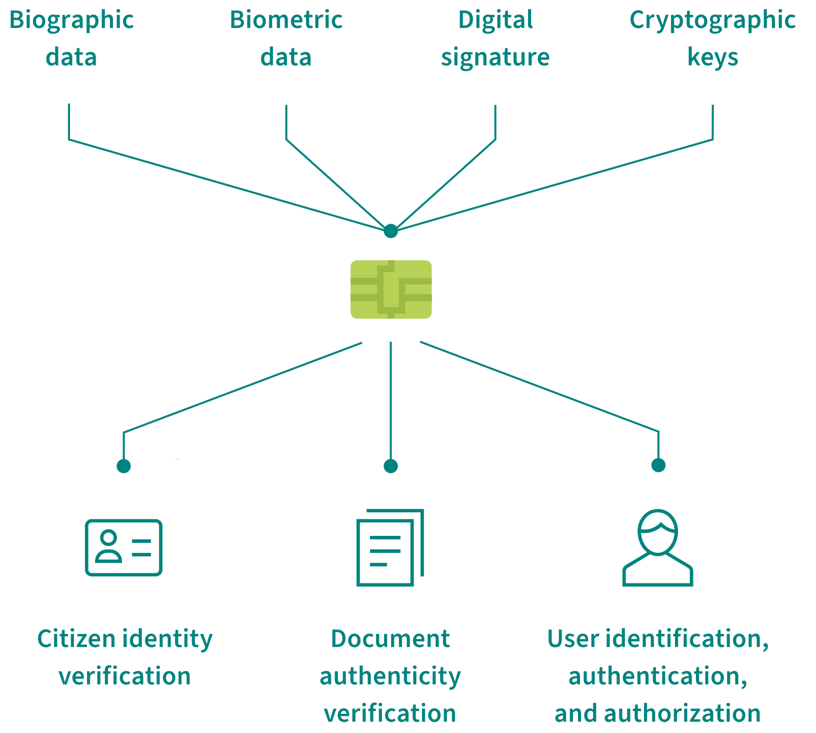
Linking identity with technology

www.infineon.com

Content

Secured identity – a lifelong journey

A secured identity gives us enormous freedom. By possessing a secured identity, we are given the freedom to access services that require proof of ID, share and receive information from trustful sources, perform legal actions, and safeguard privacy – both, in the physical and virtual world.
Whether you register the birth of your child, or sign a business contract, or authenticate on the internet – secured identity is the enabler to validate our credentials and complete all of these transactions and more through secured channels while protecting our privacy and credentials.


Biographic data

Biometric data

Digital signature

Cryptographic keys

Citizen identity verification

Document authenticity verification

User identification, authentication, and authorization

Going beyond traditional identity documents with Infineon

In addition to supporting the market for physical electronic identity documents such as eID cards, we offer smart, secured authentication solutions tailored to enterprise and access use cases. These solutions are designed to protect sensitive data and to limit access to those who are authorized. Typical applications include user authentication for biometric, physical, and logical access and NFC-based verification for various transactions.

Government ID

Application examples

- ePassport
- eID card
- eHealth card
- eDriver's license
- eResidence permit
- Digital tachograph
- Digital ID

Infineon hardware

- Most reliable security controllers for official ID applications on the market
- State-of-the-art packaging for high reliability at a competitive price

Infineon solution

A complete solution spanning security controller, packaging, operating system, and applets:

- Native operating system for optimized cost and performance
- Java Card™ Platform operating system for maximum flexibility

Authentication and access

Application examples

- Logical access incl. secured web access
- Secured data storage and encryption
- Digital signatures
- Physical access
- Biometric authentication
- Cold wallet
- Software monetization and protection

Infineon hardware

- For USB and USB/NFC applications: Easy-to-use dual-chip SMD package with integrated security controller, USB, and NFC interface
- For smart card applications: Security controller in contact-based, contactless (NFC), and dual-interface packages

Infineon solution

- A complete solution based on SECORA™ ID platform (chip, OS, packaging), plus applets
- Applets for both PKI-based and FIDO2 device-bound passkey use cases

Meeting highest security requirements

Our products and solutions are designed to meet strictest requirements of our customers and international regulatory authorities, and are fully certified in accordance with international security standards.

Electronic document integrity

- Secured storage for large amounts of sensitive data
- High level of resistance to identity fraud and personal data manipulation
- Fast contactless processing performance – essential for multi-application schemes
- Ten-year lifecycle for physical documents

Interoperability and standardization

- Global, regional, and local interoperability
- Physical and digital document co-existence
- Compatibility with international security standards
- Complete certification for components and OS
- Middleware offering

User experience

- Ease of implementation and reduced design-in effort
- Enhanced user experience for program administrators and verifying authorities
- Fast verification, authentication, and identification
- Increased administrative efficiency and return on investment
- Solutions fitting into legacy systems

Reliable supplier with customers support

- Reliable supply thanks to different manufacturing sites and foundries
- Continuous technological advances through steady investment in and development of future manufacturing capabilities
- Outstanding customer support and expert services

Why do customers choose Infineon?

Features with proven track record

Integrity Guard

Integrity Guard is Infineon's proprietary and widely acclaimed security architecture, comprising error detection/correction codes and a self-contained and self-checking dual-CPU system. This feature makes it extremely difficult to manipulate the chip and provides the most robust protection against potential attacks to the chip.

VHBR

Our mega memory sizes, combined with very high bit rates (VHBR), deliver the highest contactless performance levels, also supporting the latest ICAO standards such as LDS 2.0. Mega memory is thus ideal for evolving data-intensive applications such as eVisa.

SOLID FLASH™

Our SOLID FLASH™ memory technology is suited to multi-application identification schemes. It offers maximum convenience and supports post-issuance of new applications, dramatically accelerating software development times (by more than 50%) by eliminating ROM processing times and enabling speedy application field updates.

System-on-chip

As multi-application devices grow in popularity, they are driving the need for enhanced security on the device itself. Elements such as keyboards, displays, and fingerprint sensors can now be incorporated into such devices. Infineon provides a range of Secure Elements (SE) that act as the central component in such systems, with system-on-chip optimized solutions that include power management and interfaces for full sensor management.

CoM (Coil on Module)

Infineon's innovative CoM packaging technology uses a radio frequency link instead of the mechanical/electrical connection used between the card antenna and the module. This improves the robustness and long-term reliability of smart card and ID products, while simplifying the manufacturing process. The universal card antenna supports all chip technologies, reducing the need for different antennas. Additionally, the use of FCOS™ (flip chip on substrate) technology reduces module thickness by 20%, contributing to a more efficient design. These advancements result in lower production costs, increased yield, and fewer quality issues.

Innovative technologies addressing new market trends

TEGRION™ – The next level of security, efficiency and performance

TEGRION™ is Infineon's most powerful security controller family in 28 nm technology, offering ease of implementation, fast design-in and time-to-market, while supporting long product lifecycles. It integrates the new Integrity Guard 32 security architecture and an advanced Arm® v8-M instruction set for enhanced device performance. It allows design-for-security conditions that are critical to sustainable success of today's and tomorrow's connected applications. The broad portfolio of TEGRION™ security controllers is designed to support a wide range of applications from smart home, smart mobility and smart industry to payment, identity and lifestyle.

Scan QR code and find out
more about TEGRION™

Smart antenna customization for local requirements

Infineon offers an easily customizable antenna design for smart cards that allows displays, keyboards, LEDs, and biometric sensors to be added to the smart card.

Post-quantum cryptography (PQC)

PQC refers to new cryptographic algorithms which are set to protect against attacks using quantum computers. Infineon is conducting comprehensive research and development in the field of PQC to enable a smooth transition once the appropriate standards are in place. Security experts at Infineon have made a breakthrough in this field by implementing a post-quantum key exchange scheme on a commercially available contactless smart card chip used for eID documents.

Scan QR code and find out
more about PQC

Reference projects in ID

Status November 2023

> 200

projects across all government ID applications in > 110 countries representing 77 % of the world's population

> 75 %

of all eID projects in Europe

> 75 %

of all ePassport projects in APAC

SecurITy made in Germany

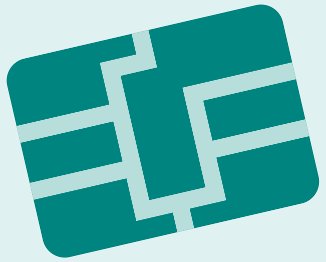
Trust Seal www.teletrust.de/itsmig

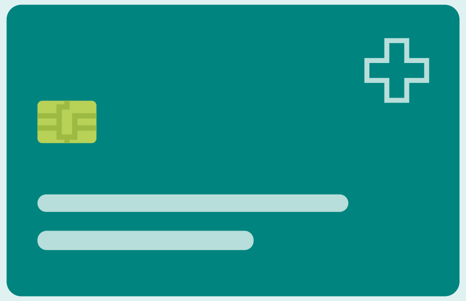
Only IC company

to supply key ePassport components to the world's 5 biggest countries

> 3 billion

chips shipped for government identity projects since 2010





60 %

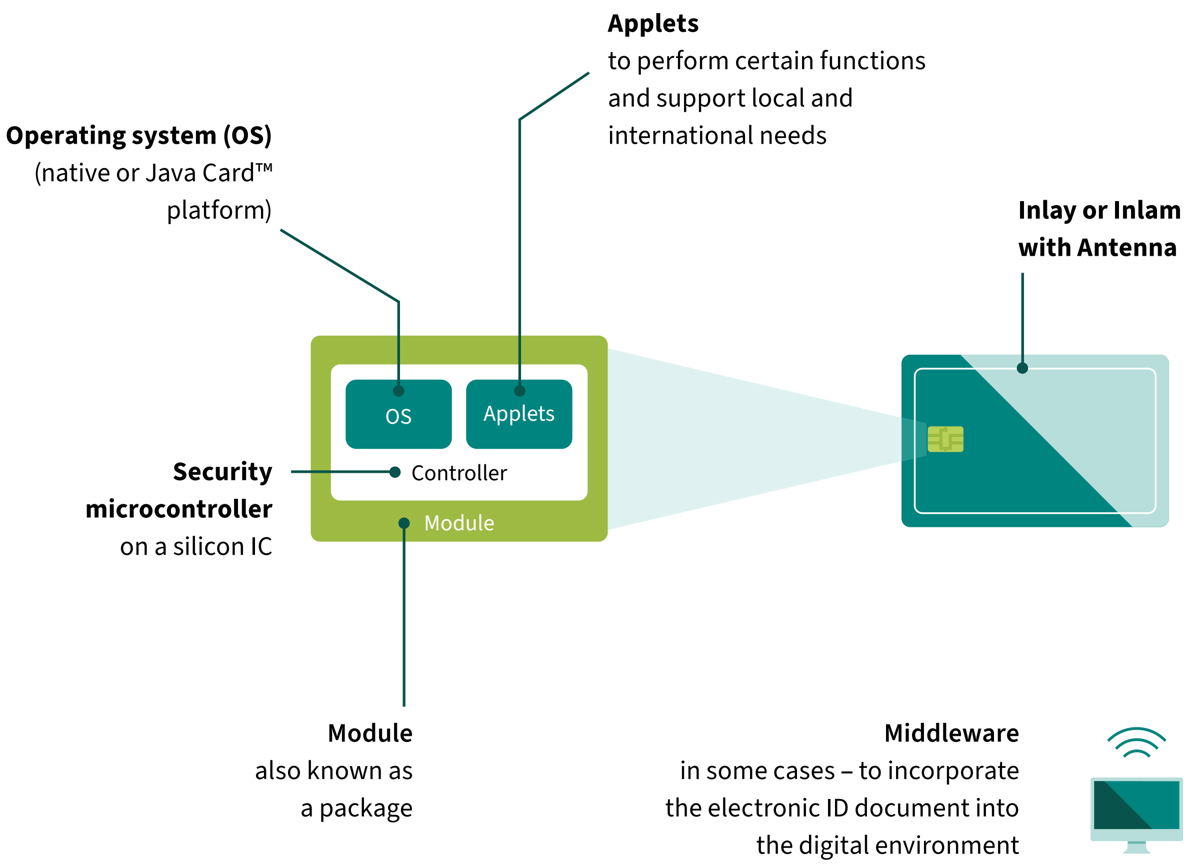
of all smart healthcare cards worldwide

Our solutions for government ID

Potential use-cases

- ePassport
- eID card
- eHealth card
- eDriver's license
- eResidence permit
- Digital tachograph
- Digital ID

To deploy an efficient and highly secured electronic identity document, components of the highest quality must be selected. In addition to the conventional document components, such as cover and data page, the following are also required:



Applets
to perform certain functions and support local and international needs

Operating system (OS)
(native or Java Card™ platform)

Inlay or Inlam with Antenna

Security microcontroller
on a silicon IC

Module
also known as a package

Middleware
in some cases – to incorporate the electronic ID document into the digital environment

All these components are part of Infineon's product portfolio for government ID. We also offer inlays, a key element in the physical document structure.

Security microcontroller

Infineon offers different security microcontroller families to meet individual customer needs. The latest addition to this offering is our 28 nm TEGRION™ family of controllers.

Operating system

Broad solution offering based on Java Card™ or native OS to meet the varied and complex requirements of our customers:
- SECORA™ ID: Infineon's solution based on proprietary Java Card™ OS, security chip and applets for a maximum flexibility.
- Infineon eID-OS: Performance- and size-optimized solution based on native OS offering the simplest solution for introducing new eID documents.
- MaskTech MTCOS: Solution based on native OS with Infineon hardware.

Applets

Based on the chosen OS, various ready-to-use applets are available: eMRTD, ePKI, FIDO2, ISO7816 File System, eDL, etc.

Middleware

Middleware serves as a bridge between a smart card and applications on a PC. We use SCinterface middleware, which supports ePasslet Suite from cryptovision and applet collection from MaskTech.

Module/package

We offer smart card modules for security ICs supporting all communication interfaces (contactless, dual-interface, and contact-based). A highlight is our innovative Coil on Module contactless chip packaging which is designed to increase the durability and robustness of smart cards.

Inlay, inlam or cover page

Together with our partners, we provide antenna inlays which can be designed and customized to meet specific customer requests (for example, a document with a clear window element).

Infineon SECORA™ ID – Java Card™ solution

Most flexible and complete security solution for Java Card™ applications

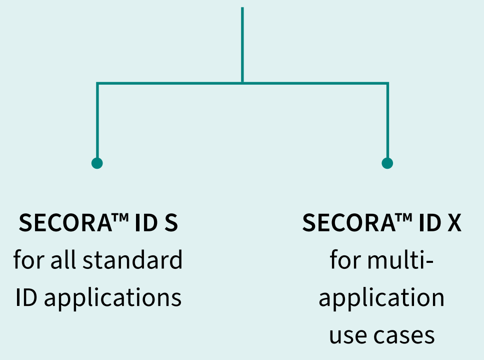
SECORA™ is Infineon's family of one-stop solutions at the heart of security. It is the most flexible and complete security solution portfolio for JavaCard™ applications.
With multiple flavors and a wide range of applets targeted at existing and emerging use cases, SECORA™ covers the broadest application spectrum from smart device and wearable payments through identification and access control to asset and brand protection based on blockchain technology.

SECORA™ is based on the Java Card™ operating system, providing an efficient path to fast and agile implementations. The complete portfolio of SECORA™ products are certified to highest security standards.

Scan QR code and
find out more

SECORA™ ID for electronic ID documents – tailored to your needs

SECORA™ ID is the ready-to-go Java Card™ solution portfolio optimized for electronic ID use cases. It accelerates time-to-market, while enabling easy and efficient customization to support local eID and multi-application schemes. Combined with a dedicated tool, the SECORA ID™ platform also gives the highest amount of flexibility to applet developers to write their own customized applications. Based on our best-in-class security controllers, SECORA™ ID comes with a lean operating system certified to the highest security standards, along with standardized applets and innovative packages.



SECORA™ ID S
for all standard
ID applications

SECORA™ ID X
for multi-
application
use cases

Infineon eID-OS – Native solution

Infineon eID-OS – a fast and highly secured solution – ready to use

The native operating system is optimized for TEGRION™ hardware which results in an impressively short transaction time as well as personalization time.

The combination of software, hardware and certifications, such as Common Criteria and Qualification Renforcée, and a high degree of compliance with international standards enable highest compatibility and security.

This solution comes with applets for ePass, eID, eDL, eHC, and ePKI use cases.

A secured, fully certified chain of trust in combination with advanced features enables simple and cost-efficient personalization by local municipalities.

Our standard solution is ready to support your successful rollout quickly.

The fastest and most cost-efficient way to introduce a state-of-the-art eID solution

Infineon eID-OS is a native OS-based ID solution operating on the latest TEGRION™ security controller family from Infineon. It provides high security and low cost of ownership, paired with easy introduction, rollout, and maintenance in the target country.

Low cost of ownership thanks to contactless Coil on Module (COM-CL) packaging

Infineon eID-OS solutions are offered in our COM-CL package, which enables thin data pages in passports. In addition to an attractive look and feel, thin data pages also save money and carbon emissions as less polycarbonate is needed in the manufacturing process. Infineon's CoM inductive coupling technology greatly simplifies the production flow and improves reliability.

Scan QR code and
find out more

Our solutions for authentication and access

Potential use-cases

- Logical access incl. secured web access
- Secured data storage and encryption
- Digital signatures
- Physical access
- Biometric authentication
- Cold wallet
- Software monetization and protection

Infineon’s ID Key product family offers a variety of solutions for securing all types of digital assets and physical locations. Our products are available in USB, USB/NFC token, smart card and key fob form factors, enabling many different application scenarios.

By implementing cryptographic algorithms that are built on hardware certified to Common Criteria standards, this product family protects enterprise, government, and other institutional users against a vast variety of attacks like data manipulation or identity fraud.

Our product offering fulfills different authentication and access token and smart card use cases. Our ID Key products are available as hardware-only options for customers or system integrators that develop their own OS and applets. Our SECORA™ ID Key products are available as Java Card™-based turnkey solutions that are customizable with proprietary and/or with pre-loaded Infineon FIDO and ePKI applets. The complete portfolio is certified to highest security standards.

Infineon's ID Key product offering for:

USB tokens & key fobs

Infineon ID Key USB hardware-only product and full SECORA™ ID Key USB ready-to-go Java Card™ solution for all types of USB and NFC tokens and PKI and FIDO security keys.

Smart cards

Infineon ID Key Card hardware-only product and full SECORA™ ID Key Card ready-to-go Java Card™ solution for all types of authentication and access smart card use cases.

SECORA™ Blockchain – Java Card™ solution

SECORA™ Blockchain is a fast, easy-to-use Java Card™ solution supporting best-in-class security for blockchain system integration. This security solution can be used to generate and manage private keys which enable users to access blockchains securely. Java Card™ solutions are available in different form factors for blockchain applications requiring secured access to the physical world, allowing for easier blockchain design and integration into a wide range of goods. By providing a protected "vault" for user credentials, Infineon's SECORA™ Blockchain security solutions can reduce the end user's commercial risk and help to increase trust in the blockchain system.

Why is security so important for Blockchain applications?

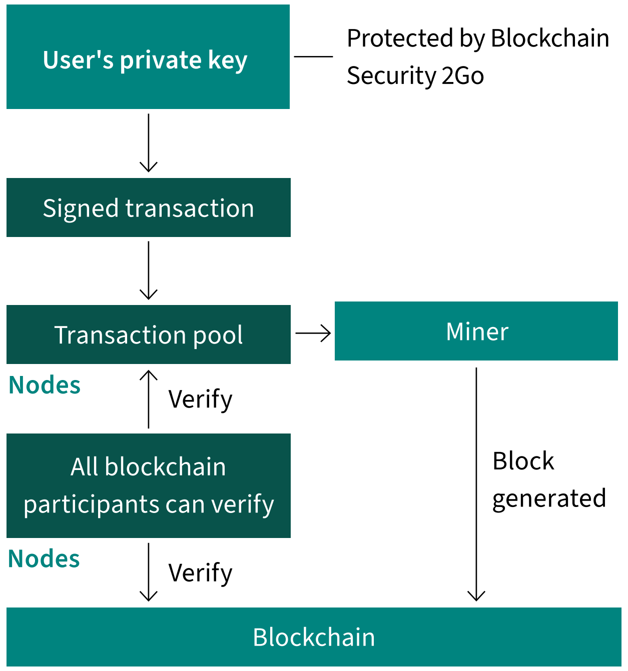
The private key of a user plays a critical role. If the private key is lost, usually all assets are lost. Moreover, if the private key is stolen, the attacker has full access to assets which allows the creation of seemingly valid transactions.

Private key storage requires best possible protection!

Hardware-based security tokens are the most effective way against attacks and unauthorized access.

Infineon's Blockchain Security 2Go starter kit

Our starter kit is an easy and efficient tool for system designers to quickly build-in security into block chain system designs for many different kinds of block chain technologies. It features hardware-based protection mechanisms to generate and store private keys in a secured way. The starter kit contains 5 ready-to-use NFC cards, on-card software, as well as an access to open source example application code.


User's private key
Protected by Blockchain Security 2Go
Signed transaction
Transaction pool
Miner
Nodes
Verify
All blockchain participants can verify
Block generated
Nodes
Verify
Blockchain

Scan QR code
and find out more

About Infineon

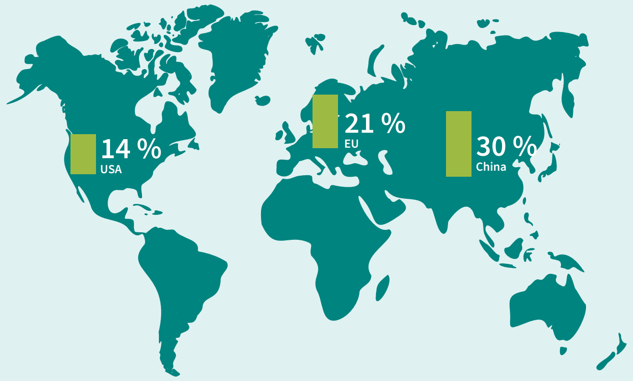
Status February 2023

Global semiconductor leader

in power systems and IoT, enabling game-changing solutions for green and efficient energy, clean and safe mobility, as well as smart and secure IoT.

R&D and manufacturing locations

in Americas, EMEA, and APAC



> 56,000

employees worldwide

Headquarters in

Munich, Germany

Published by
Infineon Technologies AG
Am Campeon 1-15, 85579 Neubiberg
Germany

Public

Version: V1.0_EN
Date: 04/2024