

GSMA IoT SAFE Applet – only for the eSIM?

Motivation



Usecase Secure Cloud Authentication

- › Establishing secure connection to AWS, Azure and Co. with TLS



High Level Overview about the GSMA IoT SAFE specification

- › A common API provided by an Java Card Applet used as a 'Root of Trust' by IoT devices



GSMA IoT SAFE for non-cellular?

- › IoT SAFE was originally intended for eSIM.



Benefits for IoT SAFE applet with Java Card™ for Infineon

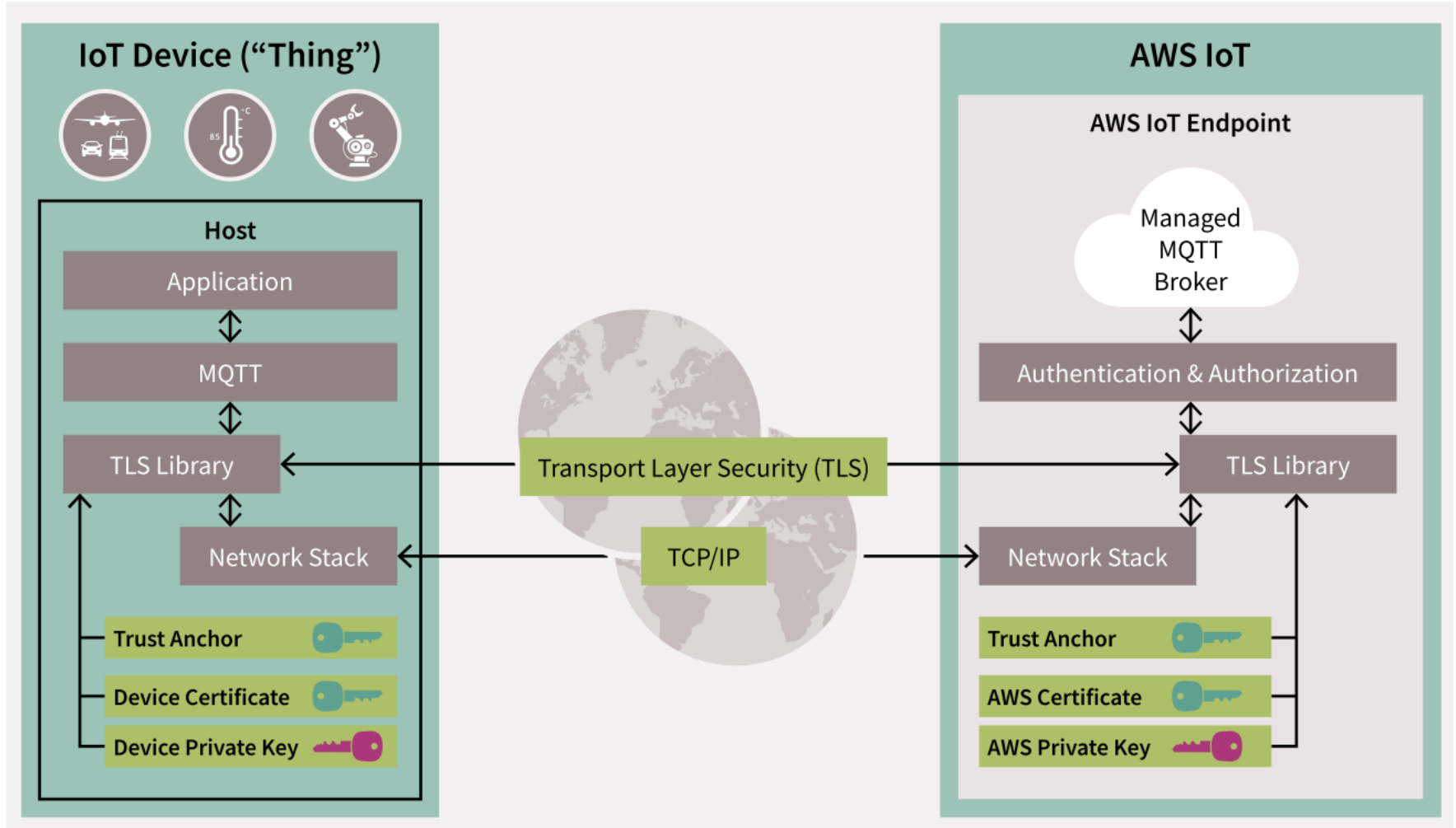
- › Java Card as the basis for Plug and Play Security.



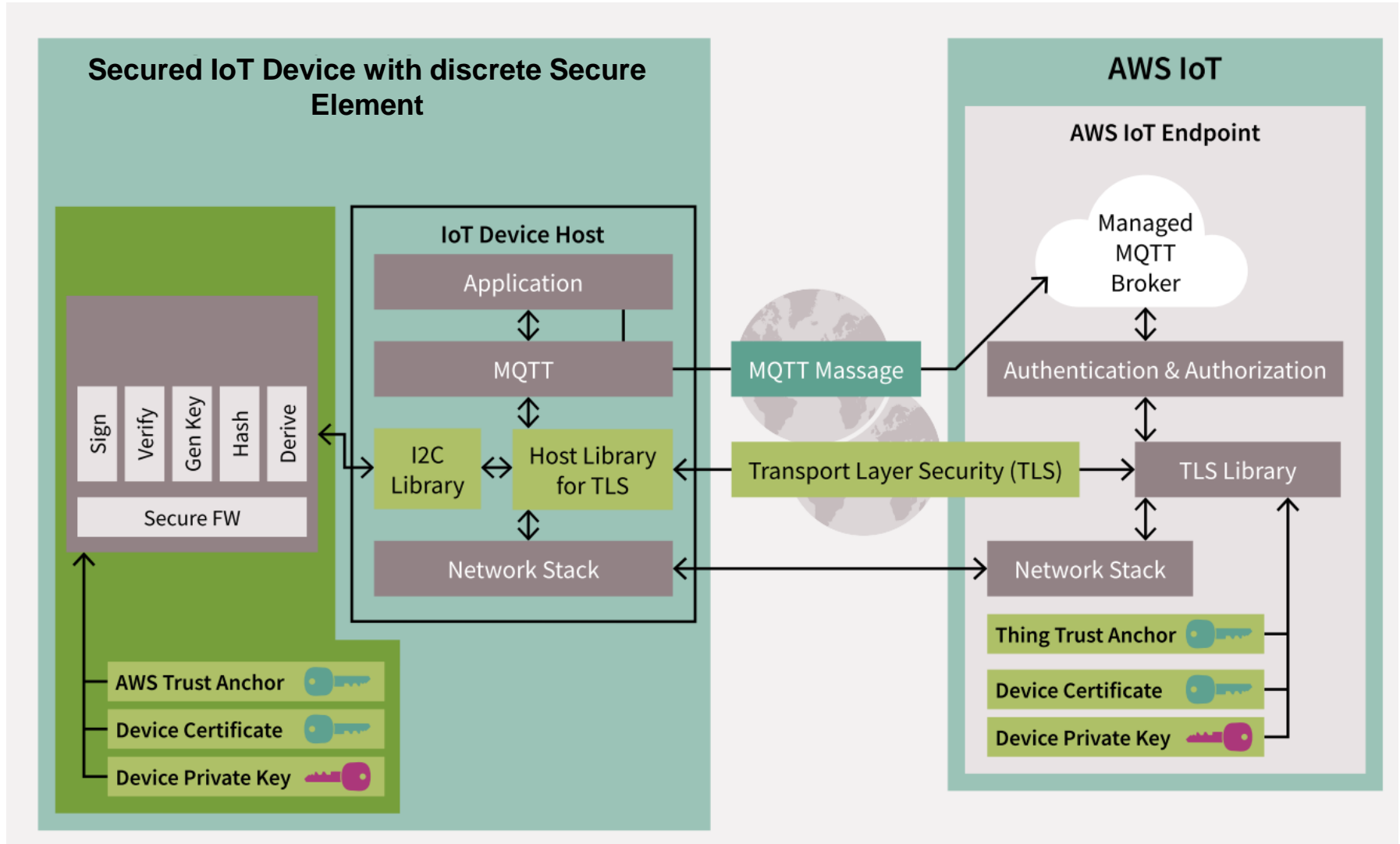
Infineon findings with a GSMA IoT SAFE applet

- › Performance and Feature proposals

Usecase Secure Cloud Authentication: System Integration Perspective **Without** Hardware Security



Usecase Secure Cloud Authentication: System Integration Perspective with Hardware Security



Main drivers why customers decide on discrete SecureElements for Cloud Authentication



Secure Trust Provisioning decoupled from the Main MCU Firmware

- › Cloud authentication keys is security sensitive data
- › Device OEM treating this very carefully and try to separate this from standard firmware loading for the MCU
- › SE components provide a secure storage for this sensitive data
- › This sensitive data shall only be handled by highly secure and trusted personalization sites.

Physical Tamper Resistance

- › mitigation against strong adversaries, e.g. against cold boot memory attacks or hardware bugs such as Spectre/Meltdown Rowhammer , or Clkscrew
- › the main application processor will always have a significantly larger attack surface than dedicated secure hardware

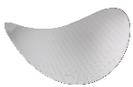


Certification and Regulations

- › Some cloud products require a certified Secure Element today e.g. AliCloud
- › Preparing long term
- › Proofing "state of the art security" by using a certified product

Persistent Storage for flashless SoC

- › Application Processors with their extremely small technology nodes today (<10nm) cannot efficiently accommodate NVM anymore
- › Monotonic values for countermeasures need to reside in NVM
 - Retry counter for the PIN
 - Session counter in Secure Protocols Replay Attack Prevention
 - Values have to be persistent (atomic and tearing-safe)



Flexible, fast and costefficient personalization options

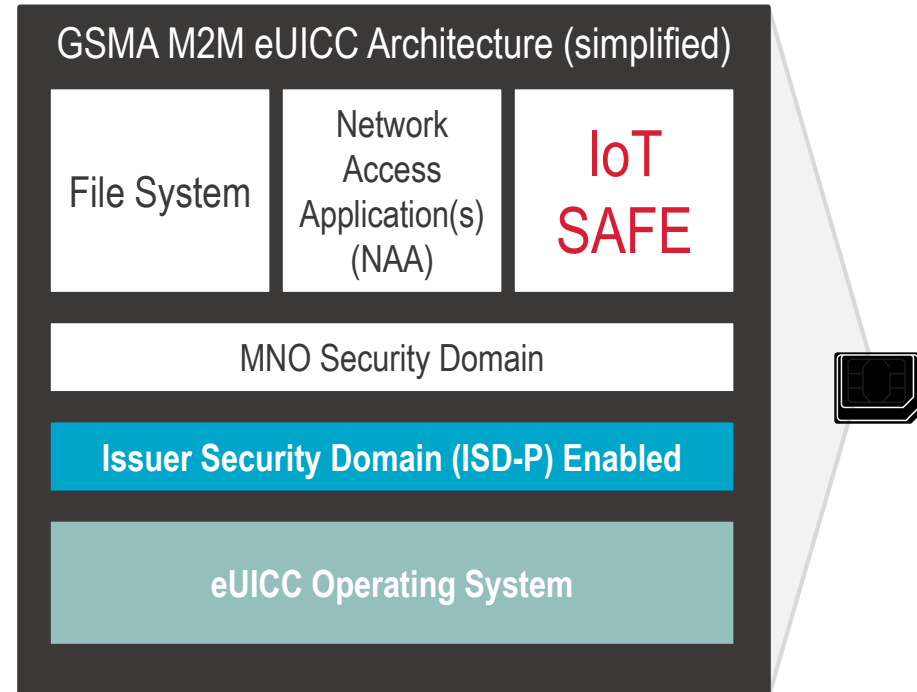
- › Loading of customer specific and chip unique credentials during the wafer test
- › Wireless of the inbuild low cost contactless interface on each chip (for some products)

GSMA IoT SAFE

IoT SIM Applet For Secure End-to-End Communication

IoT SAFE:

- › Uses the SIM as a mini 'crypto-safe' inside the device to securely establish a (D)TLS session with a corresponding application cloud/server
- › Is compatible with all SIM form factors (e.g. SIM, eSIM, iSIM)
- › Provides a common API for the highly secure SIM to be used as a hardware 'Root of Trust' by IoT devices
- › Helps solve the challenge of provisioning millions of IoT devices



- Standardized approach for a TLS Root of Trust in form of an Java Card Applet
- Another important step towards real Plug and Play Security
- Eases the integration efforts with middleware ecosystems eg. openSSL

GSMA IoT SAFE Supporting Documents

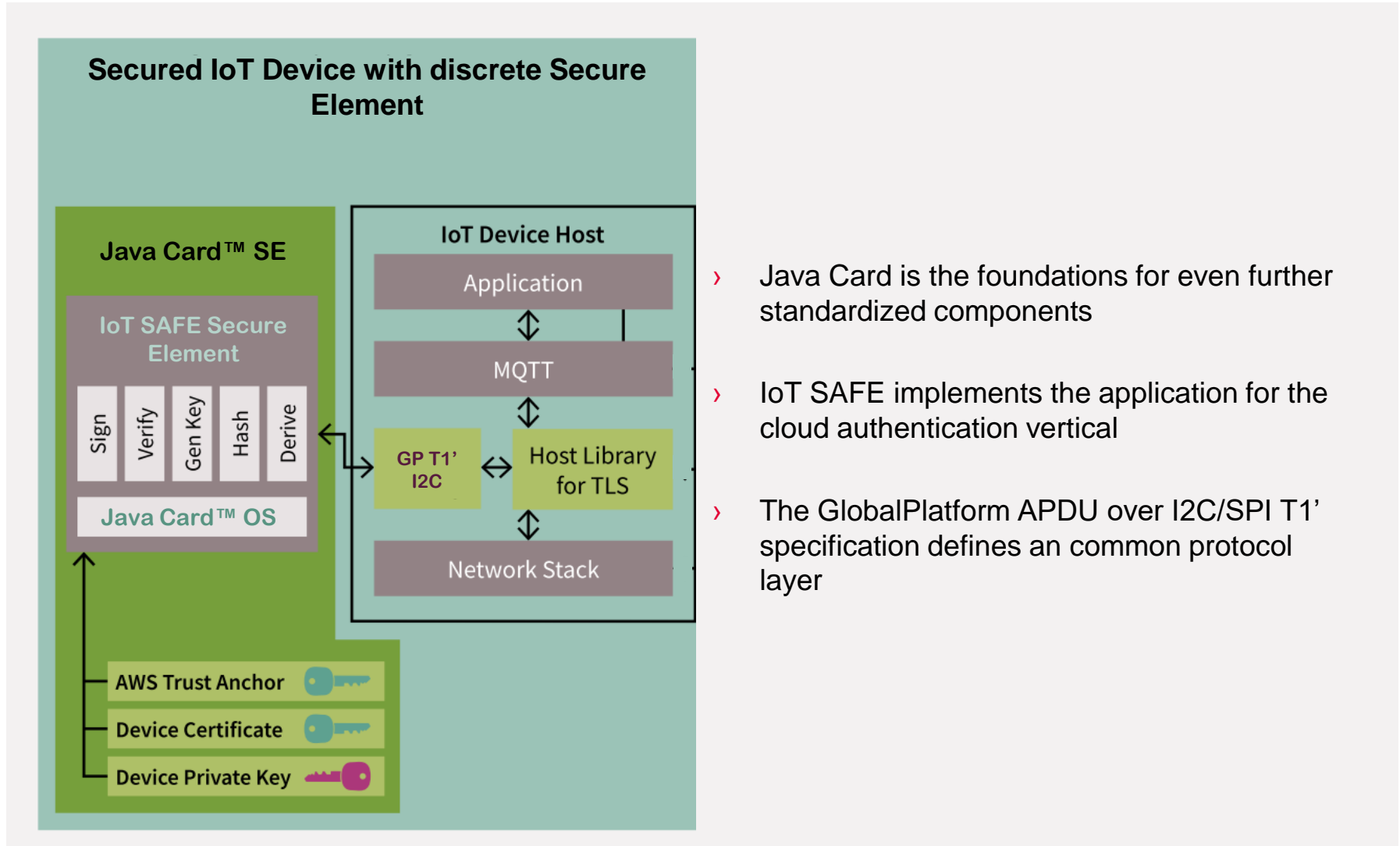


Download from [here](#)

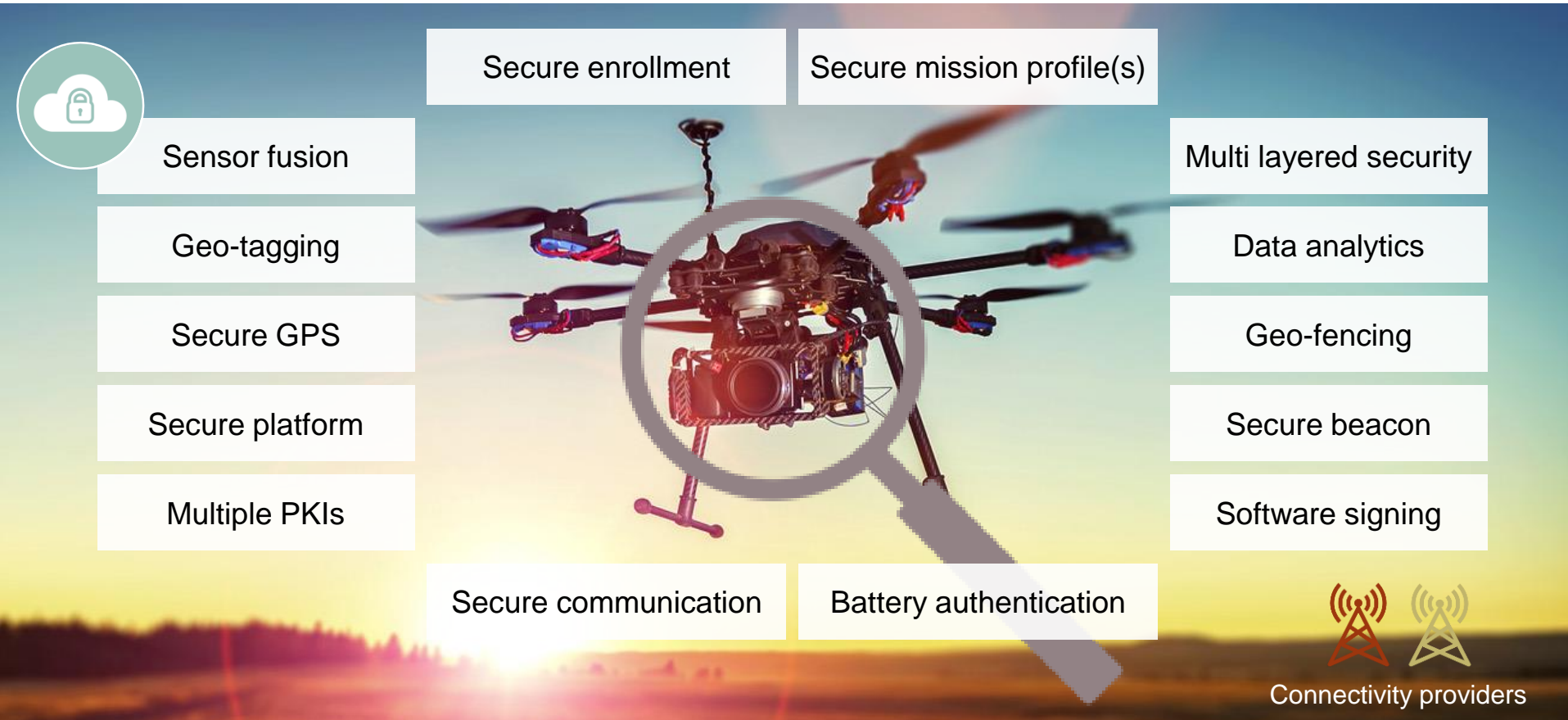


Download from [here](#)

Plug and Play Trust Anchor Secure Element



Flying with Security ease – paradigm of flying IoT



Multiple certification and PKI in action



No-fly zone – e.g. airport



Special permit to enter no-fly zones –
e.g. to inspect critical infrastructure

Issuance of certificates and keys to the drone



PKI service
PKI hierarchy



 PrimeKey

Permission is granted via personalization of certificates and keys

Permission is managed by PKI system provided by PrimeKey

Certificates are used to authenticate the drone to a Air Traffic Control Center using LTE

Secure Drone Demo

Supporting Material

Securing the commercial use of multicopters - whitepaper



PKI in Action

Securing the commercial use of multicopters

www.infineon.com



[Home](#) > [Applications](#) > [Consumer](#) > [Multicopters and drones](#)

Multicopters and drones

- Overview
- Products
- Boards
- Tools & Software
- Simulation
- Documents
- Highlights
- Videos
- Training
- Support

Personal electronics solutions by Cypress

Cypress Semiconductor has become part of Infineon Technologies: Its product range is a perfect match. Infineon now offers the industry's most comprehensive portfolio for linking the real with the digital world – comprising an unparalleled range of hardware, software and security solutions for the connected age.

Strengthening the link between the real and the digital world



Infineon brings ready-to-use drone solutions to a high-potential, emerging market. As a leading semiconductor company, we offer a complete system solution that includes every essential semiconductor, from power electronics, to controllers, to securities, to authentication, to sensors.

For drones and multicopters, flying is the most critical application in terms of performance, efficiency and control. At Infineon, we cover all relevant aspects and address your precise needs, allowing you to design a highly-efficient multicopter capable of what counts most for consumers: long airtime. Here, the control is the soul of the system and our cutting-edge technologies and portfolio let you achieve a higher degree of innovation and differentiation. Additionally, our state-of-the-art security solutions can help establish a brand's identity and help ensure brand protection.

Drone and multicopter solutions from Infineon

In Infineon's comprehensive portfolio of high quality products, you'll find the widest spectrum of drone and multicopter components on the market. We offer everything from controllers like AURIX™ and XMC™, to IMotion motor control, to XENSIV™ sensors such as pressure, radar and magnetic and more – with the exception of one commodity, an IMU (inertial measurement units) for existing solutions. Take a moment to discover our game changing products.

As a key player in leading-edge projects towards autonomous flying vehicles solutions, we at Infineon offer game changing products, such as our XENSIV™ sensor portfolio of 3D time of flight sensors, radar sensors, barometric pressure sensors, and 3D magnetic sensors. Our AURIX™ microcontrollers are the controllers of choice in the automotive industry towards autonomous driving applications. With CoolGaN™ we have the technology of choice in our portfolio, that will deliver cutting edge efficiency in driving motors of drones/multicopters.

Infineon Multicopters and Drones - website

1

- > Applet Development
- > Verification
- > Documentation

External Sourcing because of
Java Card API and IoT SAFE



1

GSMA IoT SAFE Java Card™
Applet

Cellular eSIM portfolio

non-cellular SE portfolio

4

Java Card™



OPTIGA™ Connect IoT

Java Card™



OPTIGA™ Connect Consumer

Java Card™



OPTIGA™ Trust
non-cellular IoT

Java Card™



Secora™ Connect
for wearables

Findings in our IoT SAFE implementation

Performance Improvements

- Extended APDU vs Chaining support
- Combination of commands into oneShot operations

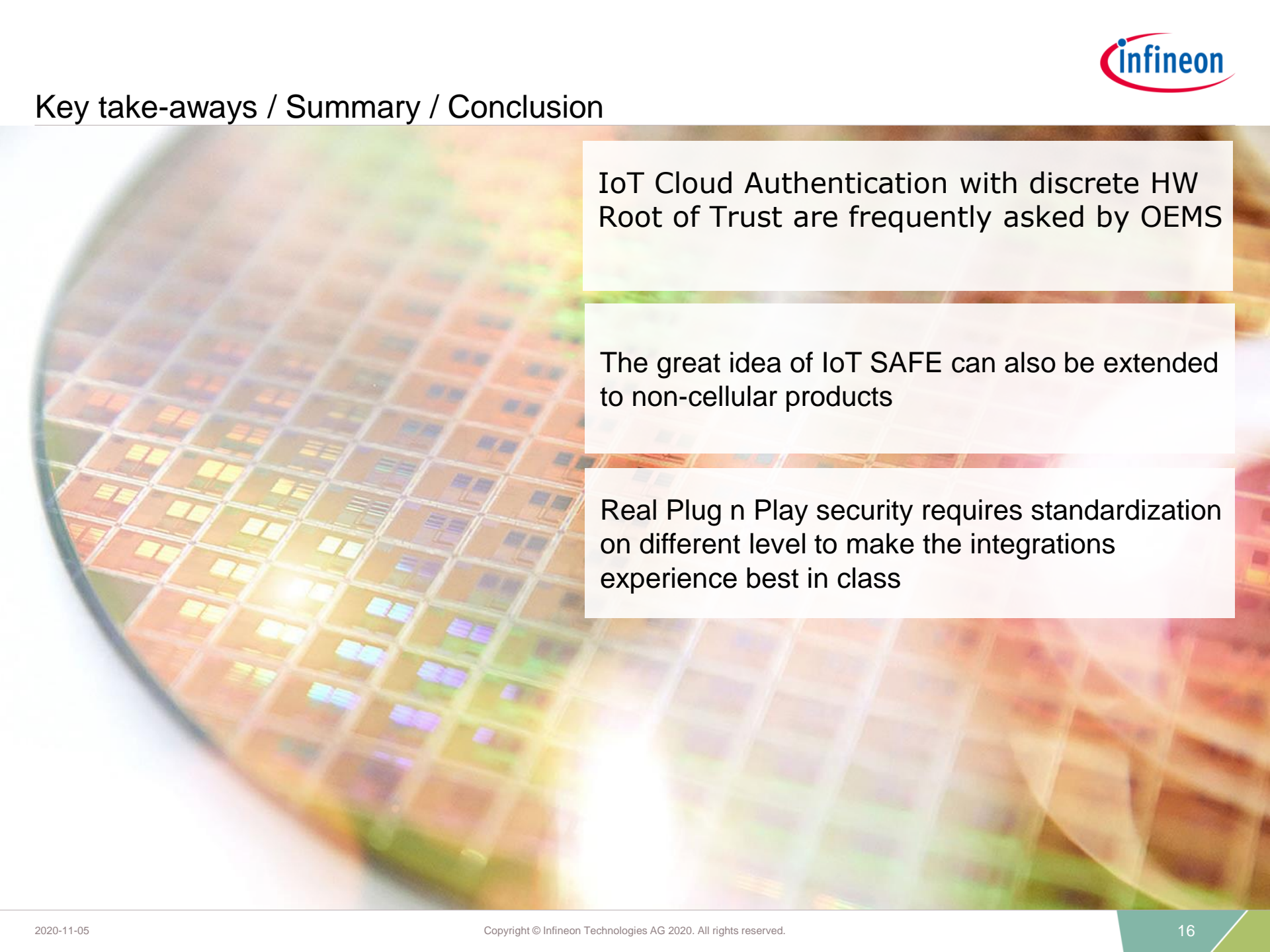
Feature Improvements

- Configurable Access Policies
- Creation of generic data objects
- Creation of referenced key object
- More algorithm supported e.g. ED25519 and NIST p384/521

ALI ID2 support

- AES encryption schemes(ECB)

Key take-aways / Summary / Conclusion

A close-up, slightly blurred image of a circular microchip or wafer, showing a grid of small, colorful square components in shades of orange, yellow, and blue.

IoT Cloud Authentication with discrete HW
Root of Trust are frequently asked by OEMS

The great idea of IoT SAFE can also be extended
to non-cellular products

Real Plug n Play security requires standardization
on different level to make the integrations
experience best in class



Part of your life. Part of tomorrow.