


# The Importance of Hardware Security in Today's Digital World

Chu Voon Fui

Burapha University
Infineon Innovation
Launchpad

Infineon

# Agenda

1. Introduction to Infineon Hardware Security Solutions
2. Hardware vs Software Security
3. Introduction to OPTIGA Trust M and Security Use Cases
4. OPTIGA Connect IoT
5. Key Takeaway


Copyright © Infineon Technologies AG 2023. All rights reserved.

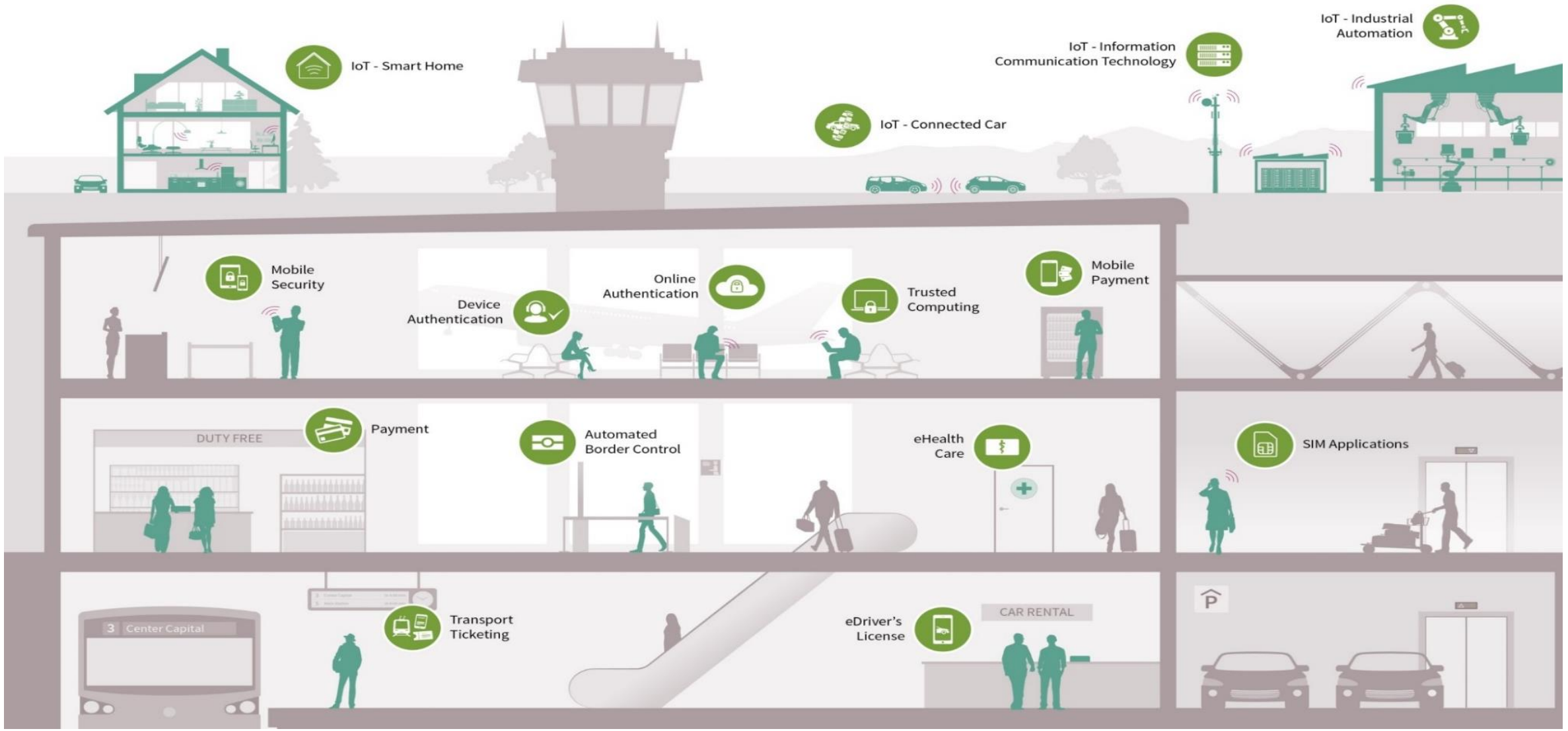
# Security is Essential





Copyright © Infineon Technologies AG 2023. All rights reserved.

# Infineon offers security for the connected world





Copyright © Infineon Technologies AG 2023. All rights reserved.

# Connected Secure Systems
## OPTIGA™ Family – Embedded Security Solutions

Burapha University Infineon Innovation Launchpad

| | OPTIGA™ Authenticate S | OPTIGA™ Trust Charge | OPTIGA™ Trust M | OPTIGA™ TPM SLB | OPTIGA™ TPM SLM/SLI | OPTIGA™ Connect |
|---|---|---|---|---|---|---|
| |  |  |  |  |  |  |
| Security Level | Basic | CC EAL 6+* | CC EAL 6+ * | CC EAL 4+ | CC EAL 4+ | CC EAL 5+ |
| Functionality | Authentication | WPC Qi 1.3<br>AEC Q100 | Connected device security | TCG standard | TCG standard<br>Automotive/industrial qualified | eSIM |
| NVM (Data) | 656 Byte | 10 kByte | 10 kByte | 6 kByte | 6 kByte | Multiple MNO-profiles |
| Cryptography<br>Private key stored in secure HW | ECC163 | ECC256 | ECC521<br>RSA2K | ECC256<br>RSA2K | ECC256<br>RSA2K | ECC, RSA |
| Type of Host System | MCU without OS / proprietary OS / RTOS | | | | | |
| | | Embedded Linux | | | | |
| | | | | Windows / Linux | | |
| Interface | I2C / SWI | SPI | I2C | I2C, SPI, LPC | SPI | ISO7816 |
| System integration | ✓ | ✓ | ✓ | Platform vendor | Platform vendor | ✓ |

* Based on certified HW


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Connected Secure Systems
## OPTIGA™ Security Functions – Use Cases



### Device Authentication
- One-way authentication
- Mutual authentication



### System integrity
- Secure Boot
- Remote platform verification



### Secure Channel
- Encrypted Communication
- Key Generation



### Lifecycle Management
- Key Backup and refurbishment
- Personalization and identities
- Supply chain tracking



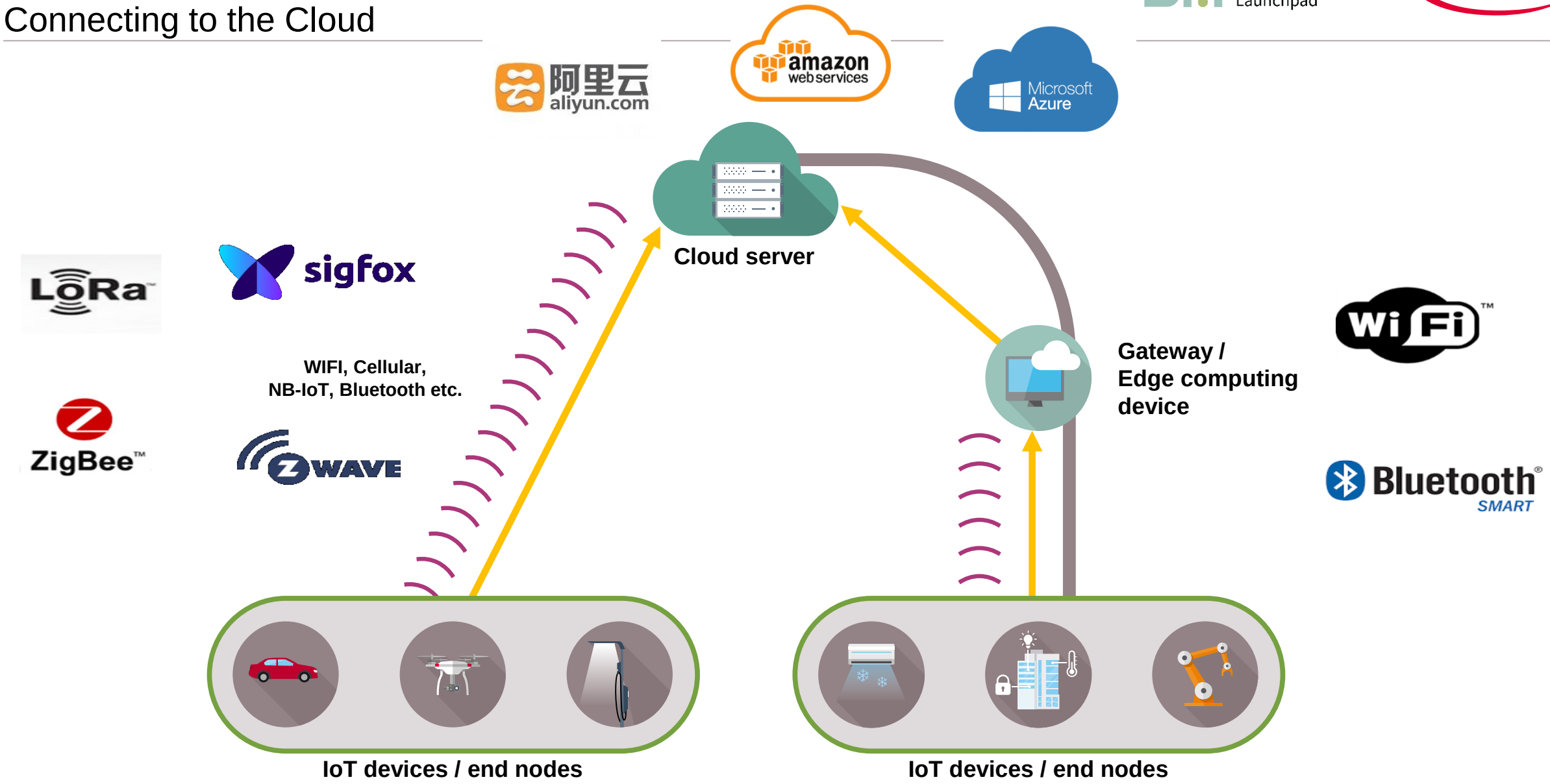
### User Management
- Password Protection
- User management and keys



### Secure Updates
- Remote maintenance
- In-field flexibility and reaction


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Connecting to the Cloud

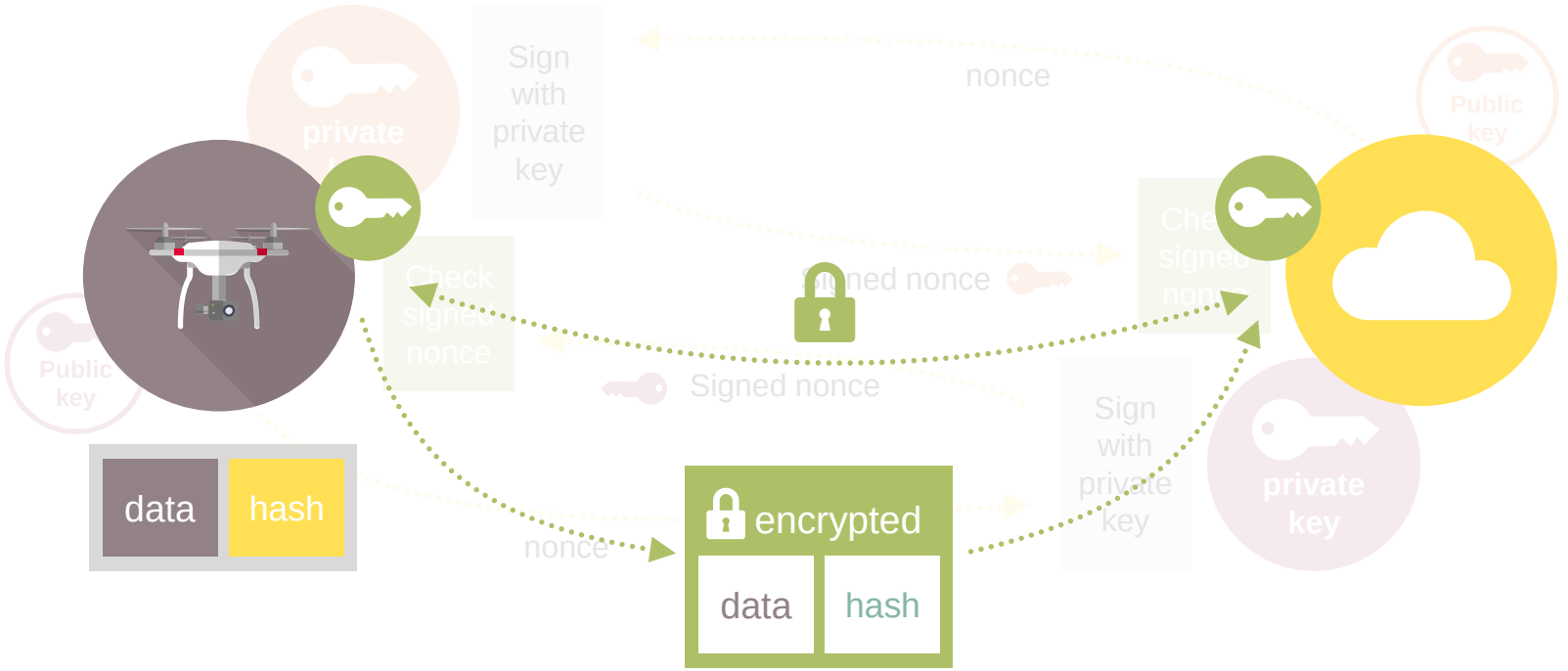




Copyright © Infineon Technologies AG 2023. All rights reserved.

# Establishing a secured communication channel: Protection of private key is essential

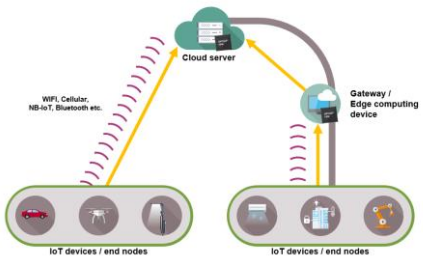
1. **Cloud authenticates** device
2. **Device authenticates** cloud
3. Generate session key
4. Encrypted & integrity **protected data transfer**

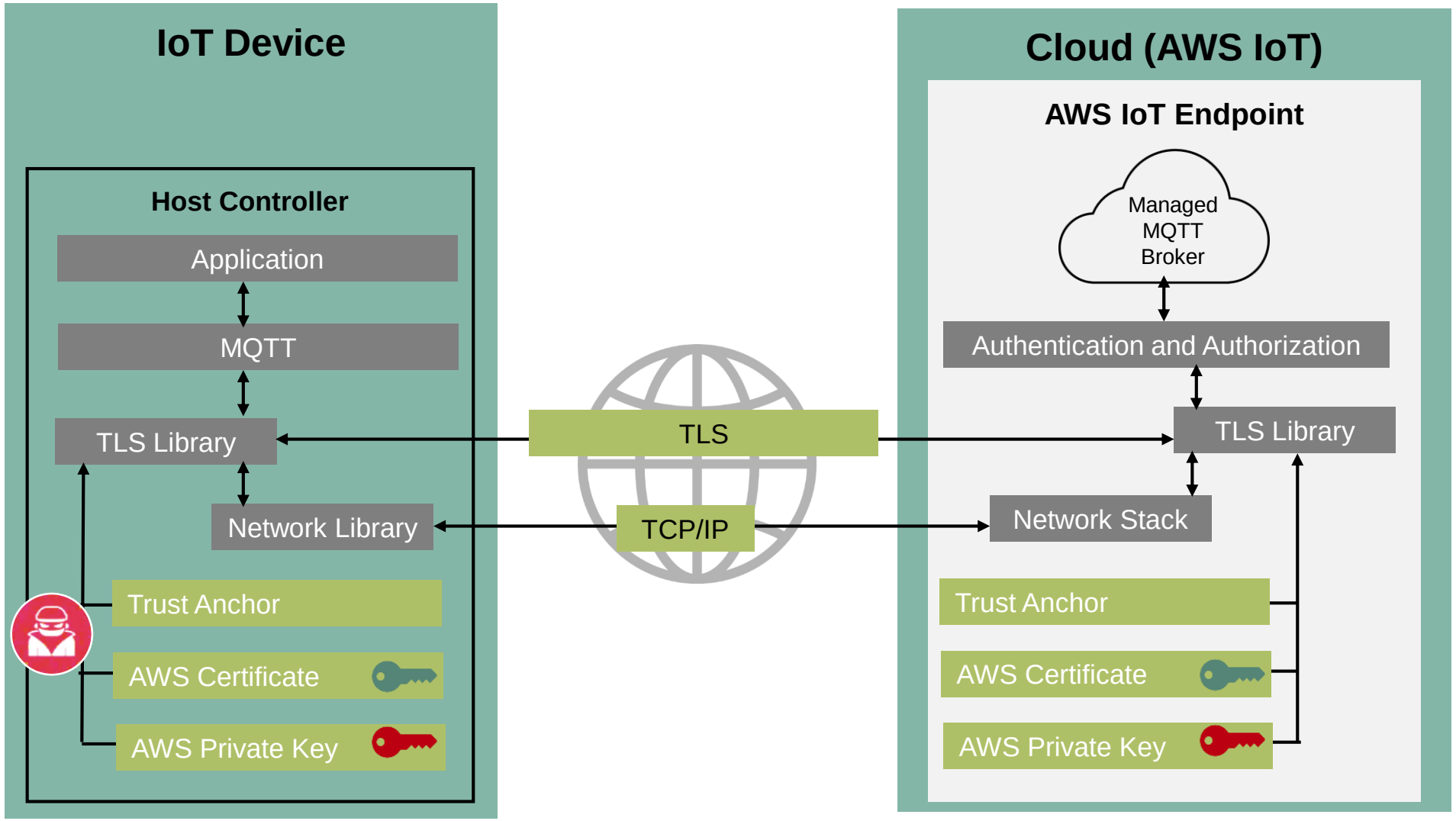



**Once the Private Keys are stolen, the devices can be Cloned.**


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Connection to Cloud with TLS
# Using Software Security Approach




Attackers' focus:
- Key material (keys, certificates, …)
- Security functions (e.g. cryptographic signature functions)


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Possible Ways to Steal Keys and Credentials from IoT Device

Agent Tesla malware receives module for stealing Wi-Fi passwords

By Sead Fadilpašić 5 days ago

Besides Wi-Fi profiles, the malware can also collect data about the target system.

Major rise in password-stealing malware detected

By Anthony Spadafora July 23, 2019

60 percent increase in users hit by password stealers in the last year

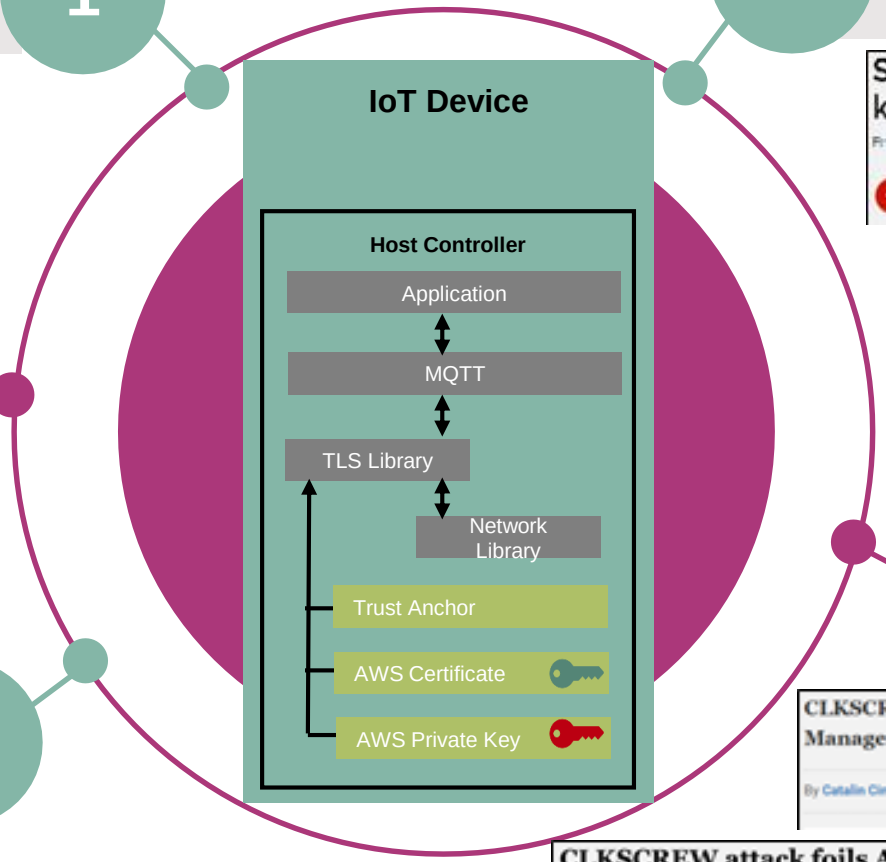
## 1 Malware

## 2 Software Bugs

#cloudbleed

## 3 Hardware Bugs

MELTDOWN SPECTRE FORESHADOW




## 4 SW Security Flaws

Security flaw lets attackers recover private keys from Qualcomm chips

TrustZone Downgrade Attack Opens Android Devices to Old Vulnerabilities

By Catalin Cimpanu

## 5 Cyber-Physical Attacks

CLKSCREW Attack Can Hack Modern Chipsets via Their Power Management Features

By Catalin Cimpanu

CLKSCREW attack foils ARM TrustZone component

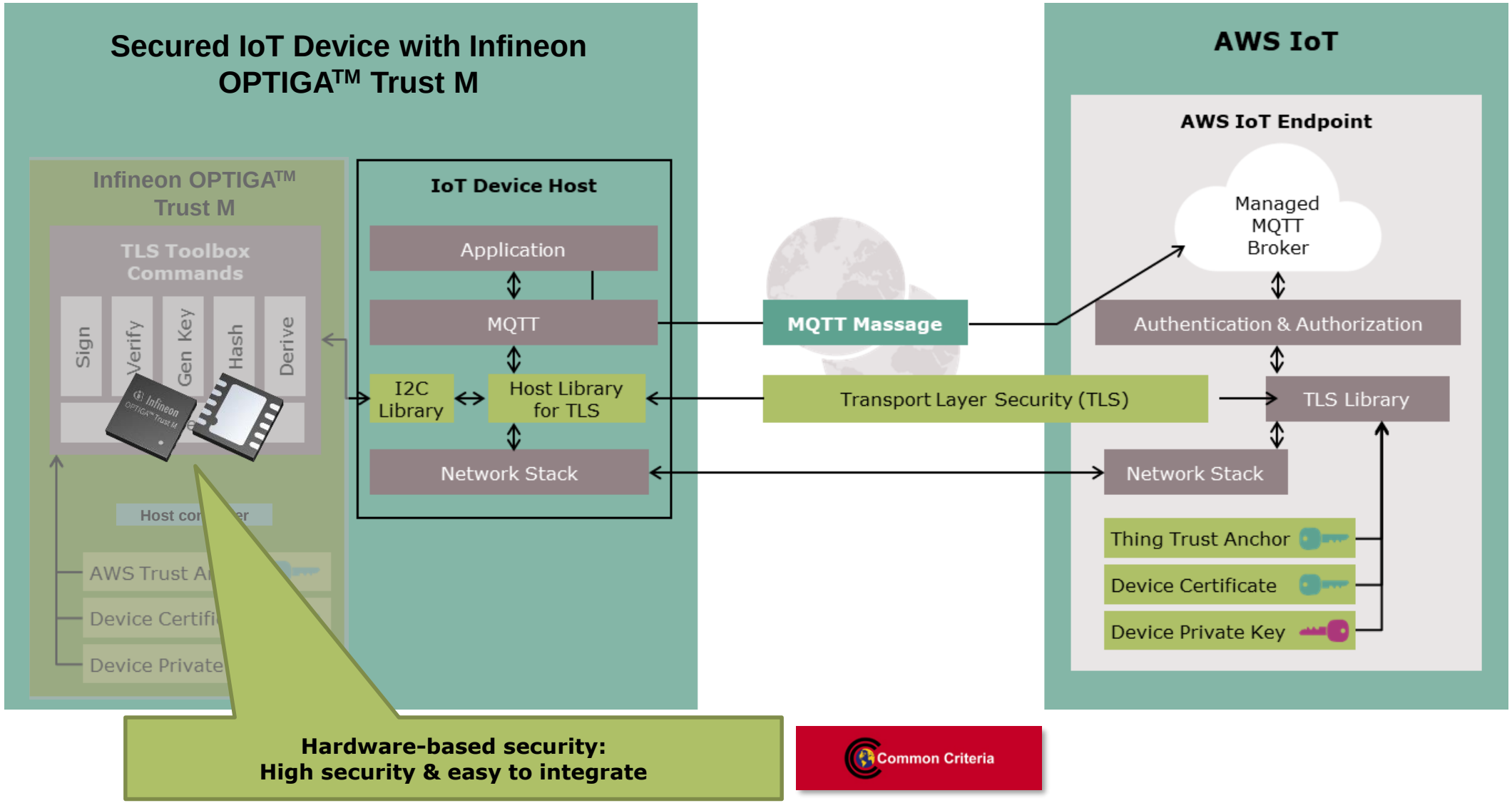
In a research paper, the Columbia team explains how it used CLKSCREW to attack ARM TrustZone, a separate chip included mobile CPUs on Android devices, and which handles secure and cryptographic operations on behalf of the main operating system

Researchers use Rowhammer bit flips to steal 2048-bit crypto key

RAMBleed side-channel attack works even when DRAM is protected by error-correcting code.


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Principal #1
# Hardware Separation





Copyright © Infineon Technologies AG 2023. All rights reserved.

# Principal #2
# Tamper-Resistant Means Protection Against Physical Attacks



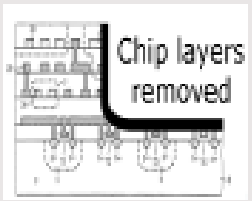
## Manipulating Attacks



Manipulating station



Probing Needles

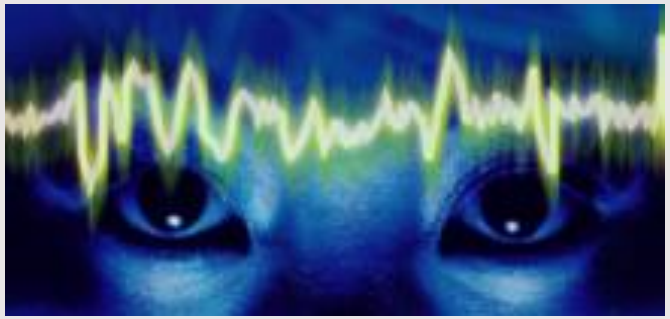



Reverse Engineering

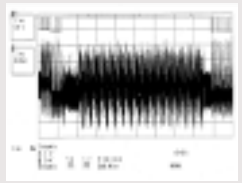


Focused Ion Beam

**Physical manipulation of chip to gain access to secrets**



## Observing Attacks



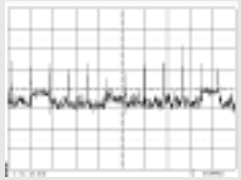
Simple Power Analysis



Differential Power Analysis



Electromagnetic Analysis



Timing Analysis

**Monitor operation parameters of chip to deduce secrets**



## Semi-Invasive Attacks



Spike/Glitch Attacks



Optical Fault Induction



Electromagnetic Induction



Alpha Radiation Attack

**Induce error in the chip to alter the operation flow**


Copyright © Infineon Technologies AG 2023. All rights reserved.

# In-depth Security Comparison
# TEE and Dedicated Security Chip

Burapha University
Infineon Innovation
Launchpad

## TEE Security on SoC




- TEE security depends on various modules of the SoC
  - Achieved security depends on the quality of this SoC integration
  - Integration typically NOT done by security experts
- Huge complexity for security evaluation

## Dedicated Security Element




Common Criteria

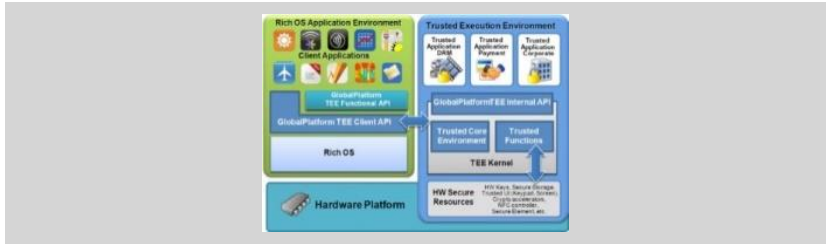
- Security as primary focus
  - Secure development and manufacturing environments
  - Design and implementation done by security experts
- Evaluated by third party
  - Common Criteria
    EAL6+ (High) Evaluated Security Controller

Graphics Source: UL White paper - HCE security implications, analyzing the security aspects of HCE (Jan 8, 2014); Infineon


Copyright © Infineon Technologies AG 2023. All rights reserved.

# IoT Devices
# Leveraging on Hardware Trust Anchors









| | | |
|---|---|---|
| Crypto functionality | ✓ | ✓ |
| Strong isolation | - | ✓ |
| Pre-Provisioning of Keys | - | ✓ |
| Prevent Key Extraction | - | ✓ |
| Prevent IP Theft | - | ✓ |
| Platform Integrity Protection | - | ✓ |


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Hardware Security offers faster Time-to-Market

Time to market

WHY **HW security**

**Customer challenge**

Achieving a fast time to market for their secured system

**SOLUTION**

Average time to do a secured implementation of a functionality on a microcontroller

**2 years***

*vs.*

Average time to implement same functionality with a turnkey hardware based product

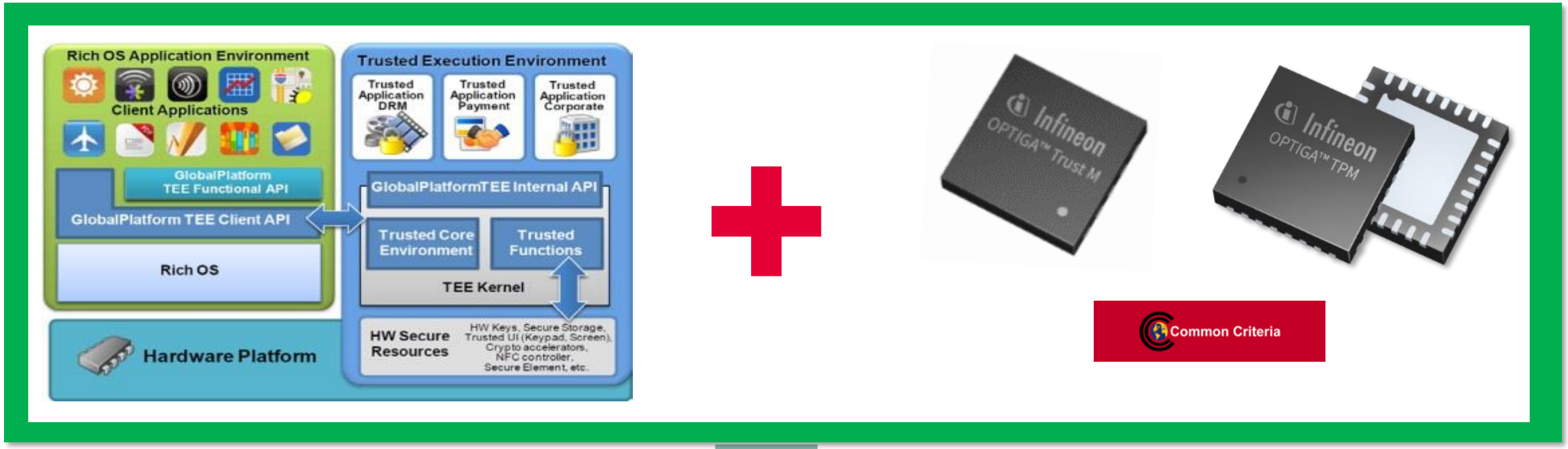
**2-4 months****

*(Infineon estimation based on implementation of product functionalities)

**(Infineon estimation based on customer feedback for OPTIGA™ family)


Copyright © Infineon Technologies AG 2023. All rights reserved.

# TEE + Secure Element
## Achieving Hardware Separation and Tamper-Resistant




**Idea**

Protection against SW and logical attacks using the TEE

+

Protection against HW attacks using Secure Elements
- Tamper-resistant
- Well-protected keys
- Common Criteria Certified


Copyright © Infineon Technologies AG 2023. All rights reserved.

Burapha University
Infineon Innovation
Launchpad

# OPTIGA™ Trust M

# Optiga Trust M - Protecting against Known and Future Attack

Zero-touch cloud provisioning

Easy integration

Future-proof security

High performance




USON-10 (3x3mm)

## Key Features

- High-end CC EAL6+ (high) certified security controller
- Turnkey solution
- Up to 10kB user memory
- I2C interface with Shielded Connection
- Cryptographic support:
  - ECC : NIST curves up to P-521, Brainpool r1 curve up to 512,
  - RSA® up to 2048,
  - AES key up to 256 , HMAC up to SHA512,
  - TLS v1.2 PRF and HKDF up to SHA512
- Crypto ToolBox commands for SHA-256, ECC and RSA® Feature, AES, HMAC and Key derivation
- Hibernate for zero power consumption
- Temperature: -25°C to 85°C and -40 to 105°C
- Lifetime of up to 20 years for enterprise and industrial applications


Copyright © Infineon Technologies AG 2023. All rights reserved.

# OPTIGA™ Trust M
# Secured cloud service provisioning – the easy way!

Burapha University
Infineon Innovation
Launchpad

Infineon

### Easy to Integrate
- Full turnkey solution
- Customer specific certificate  provided for zero-touch provisioning
- Host code with abstraction layer
- Evaluation kit

### Premium Security
- Based on CC EAL 6+ (high) certified security controller
- X.509 certificate supported
- TRNG AIS-31 certified
- OPTIGA™ Shielded Connection
- CA certificate in-field update

### Cryptographic ToolBox
- TLS/DTLS implementation
- Arbitrary security schemes

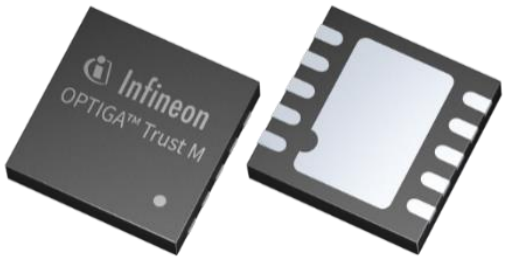
### Extensive Set of Use Cases
- Mutual Authentication
- Secure Communication
- Data Store Protection
- Lifecycle Management
- Power Management
- Secure Update

### Endurance
- Up to 1.6 M write cycles



### Product Details

| | | | |
|---|---|---|---|
| Temperature range | -40 to +105°C | Interface | I2C |
| Data Store | 10kB | Interface Speed | 1 Mbit/sec |
| Cryptography | ECC, RSA, AES, SHA | Package | USON-10 |
| Available | Avaliable | Size | 3 x 3 mm |





Copyright © Infineon Technologies AG 2023. All rights reserved.

# Extensive set of use cases



Use cases

**Authentication**
- One-way ECC/ RSA based

**Secure Communication**
- DTLS Client
- Toolbox
- Shielded Connection

**Secure Update**
- SoC/MCU FW

**Key Provisioning**
- Customer specific PKI

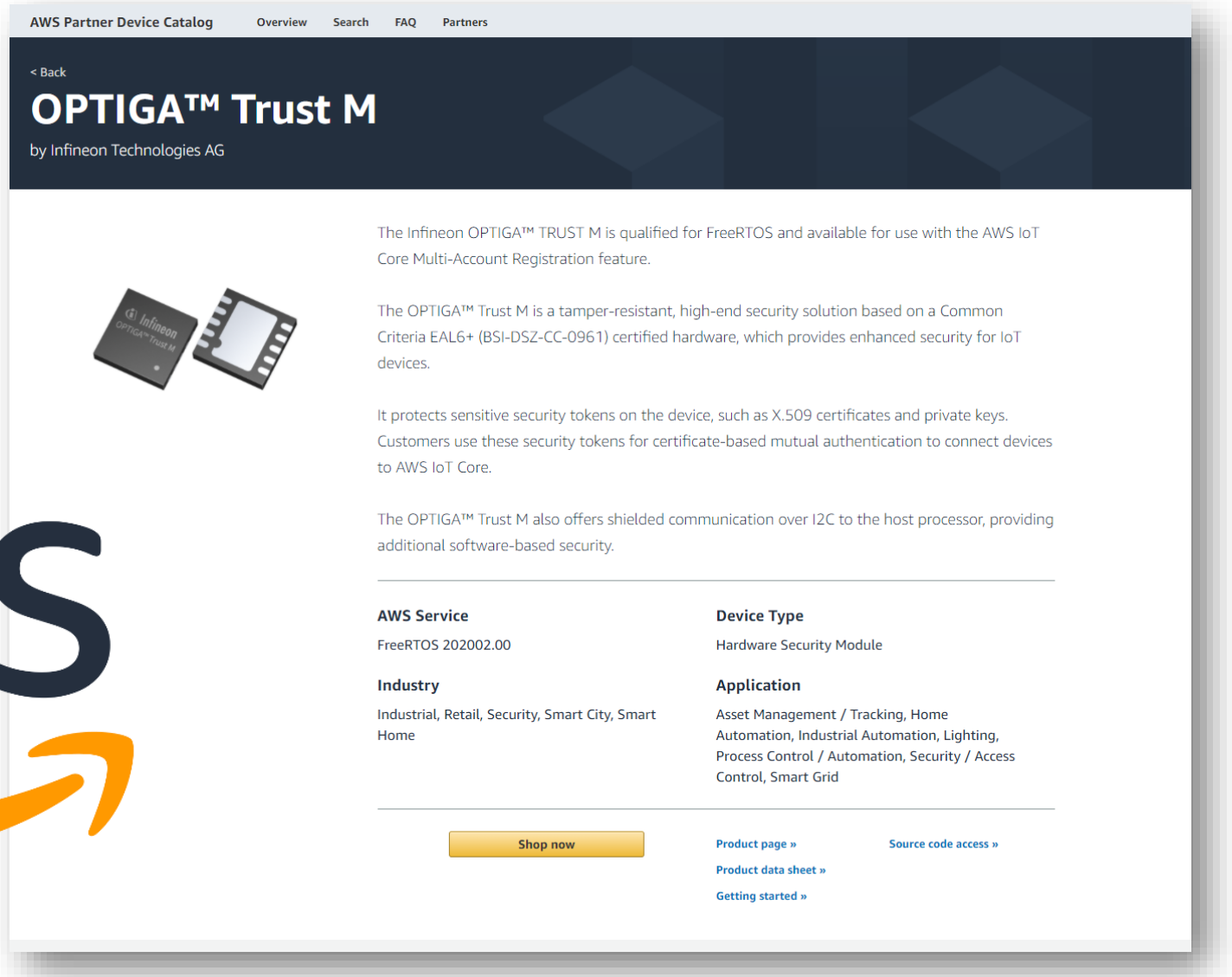
**Lifecycle Management**
- Lifecycle State Management

**Data Store Protection**
- Protection by Lifecycle & Runtime State
- Protected Data Object Update

**Power Management**
- Max. Power and Sleep
- Hibernate


Copyright © Infineon Technologies AG 2023. All rights reserved.

# OPTIGA™ Trust M , AWS Qualified





Copyright © Infineon Technologies AG 2023. All rights reserved.

Less effort, more transparent licensing, more convenience

OPTIGA™ Trust M host software is Open Source, and available on GitHub together with the product documentation

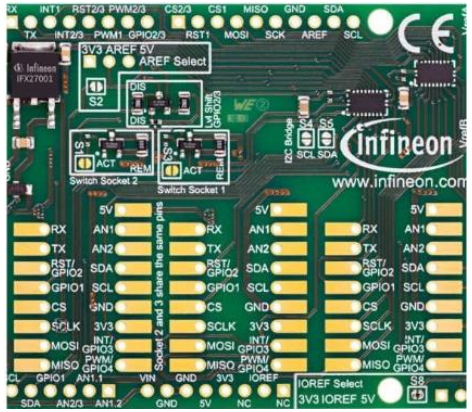
https://github.com/Infineon/optiga-trust-m



# Evaluation boards OPTIGA Trust M







Copyright © Infineon Technologies AG 2023. All rights reserved.

# How It Works: Manifest file from Cirrent Cloud ID to Private Cloud

1. Device ships with built-in Device Certificate prepopulated in Cirrent Cloud ID service

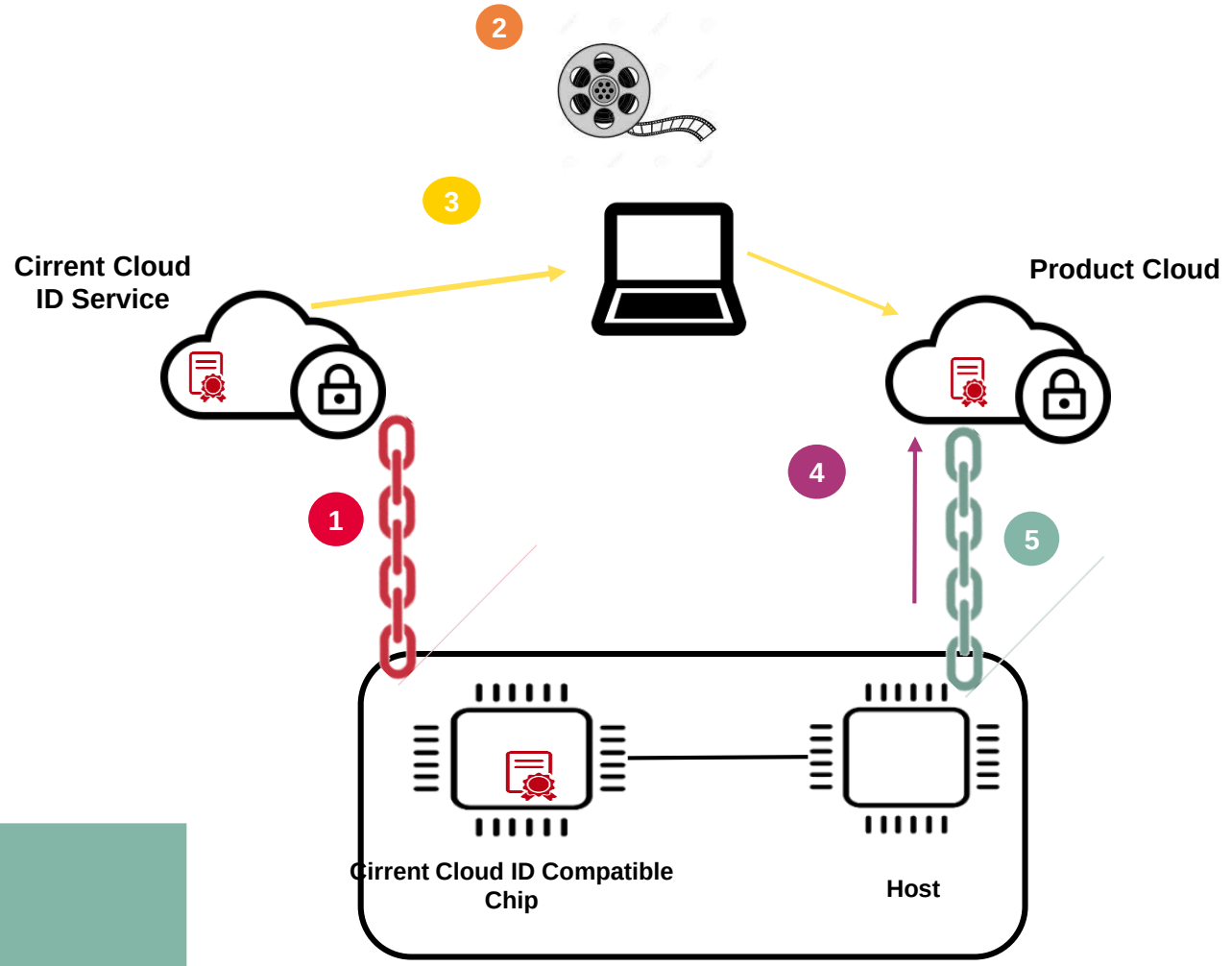
2. Log onto the Cirrent Console and enter in the unique reel code to bind ownership.

3. From the Cirrent Console download the manifest file and upload it into your cloud to add your devices to the product Access Control List. This is the whitelisting process. The device is pre-registered with the product cloud

4. The Device is born and connects to your cloud and presents it's public key

5. **Chain of Trust is established between Product & Product Cloud**
   All ongoing communications is direct between Host & Product Company Cloud

- Can use a default OPTIGA Trust M SKU
- Simpler order to product to device birth
- Provides Cryptographically secure device authentication
- Unique Cloud ID prevents device spoofing





Copyright © Infineon Technologies AG 2023. All rights reserved.

Burapha University
Infineon Innovation
Launchpad

# Security Use Cases

# How do we overcome Key Provisioning problem

**How can we inject the keys securely into the blank device?**





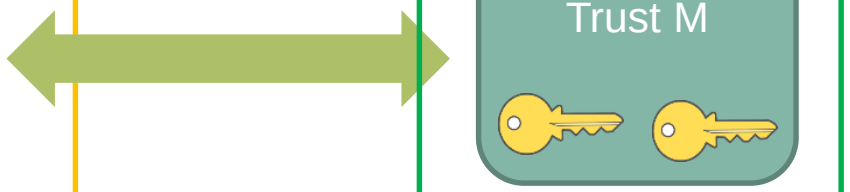
Keys generated externally



**1st Key pair injection will always be in clear as the device is blank**

Host MCU

- Application
- Crypto Library
- OPTIGA™ Services




**1st Key Pairs are pre-provisioned in Trust M**

**More key pairs can be generated securely by Trust M**

**High Security Environment**




Copyright © Infineon Technologies AG 2023. All rights reserved.

# How do we prevent Identity Theft



Cloud server



**Physically remove the chip and solder to another PCB**

**Host ID**

**Crypt ID**

Host MCU

- Application
- Crypto Library
- OPTIGA™ Services




STOP!

Fake Host

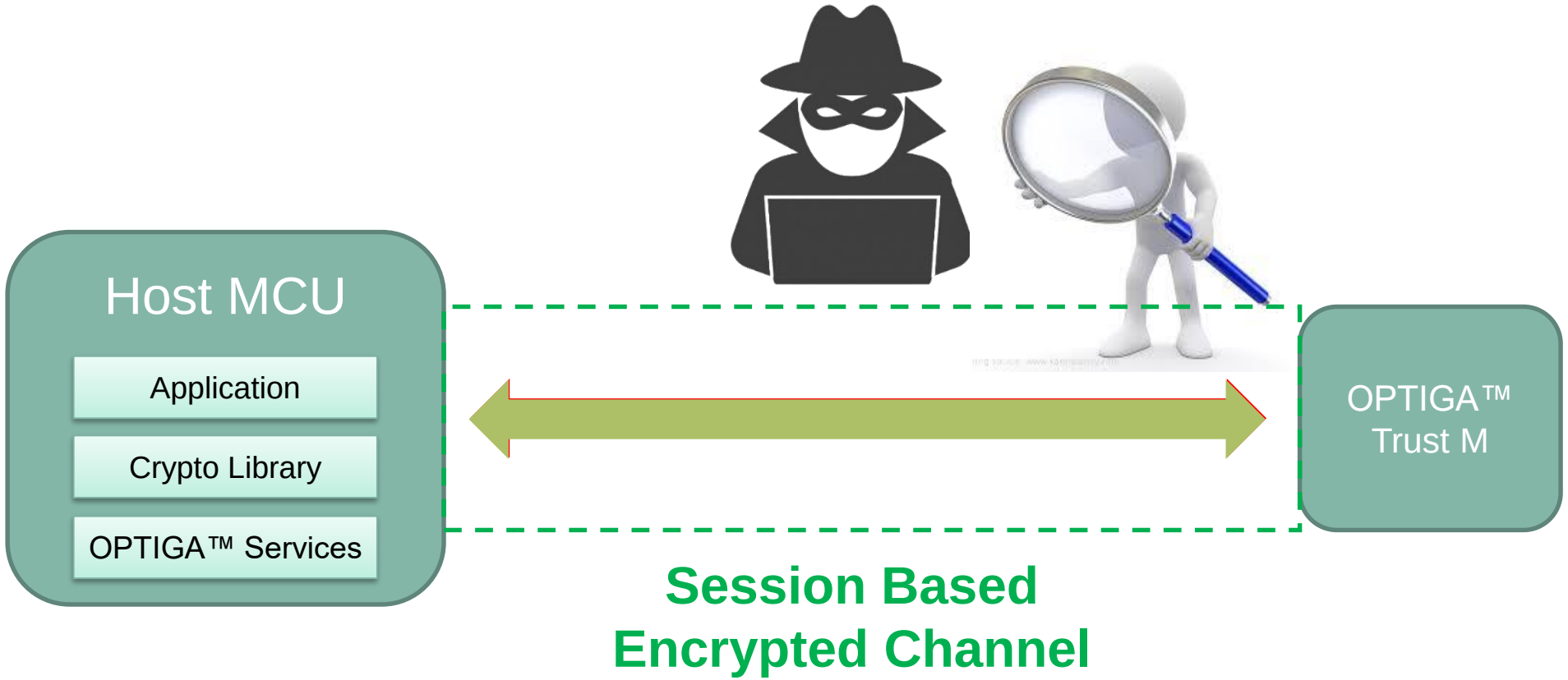
- Application
- Crypto Library
- OPTIGA™ Services

**Trust M can be cryptographically bound to the Host MCU**

**Trust M will deny security functions if original host is absent**


Copyright © Infineon Technologies AG 2023. All rights reserved.

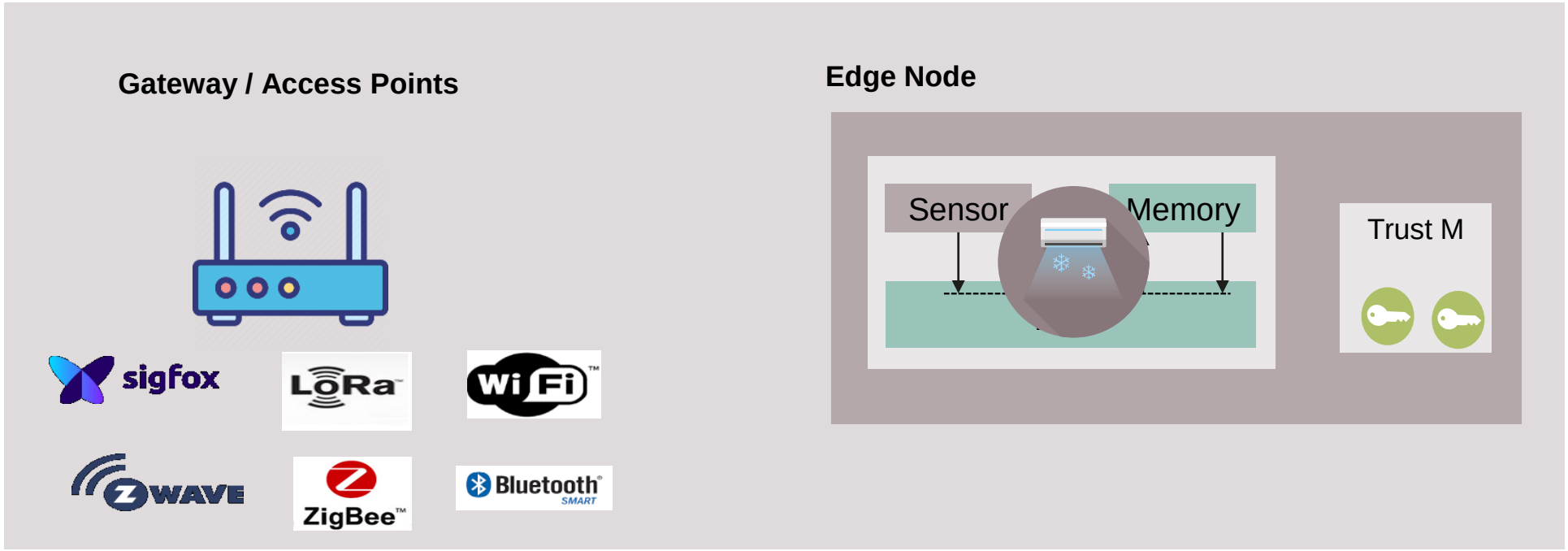
# How can we prevent Spying of the I2C bus





Copyright © Infineon Technologies AG 2023. All rights reserved.

# How can we Protect Network Credentials



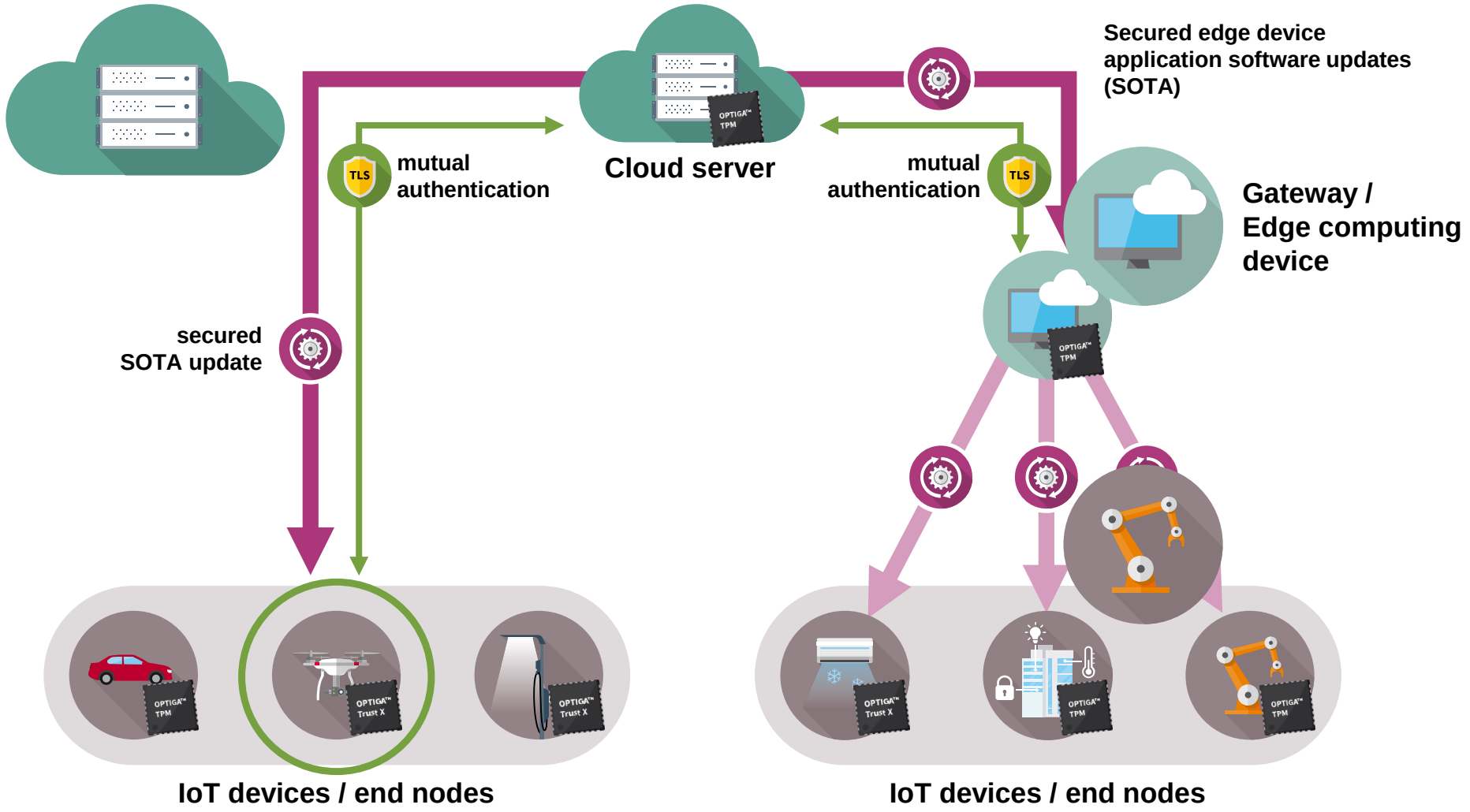

## Securing Network Credentials

Infineon´s OPTIGA™ hardware security not only provides a **secured storage for network keys, usernames and passwords**.

This **Defense-in-Depth** concept provides a **longer lasting protection** for credentials in the event that the Host controller is compromised by cyber-attacks.


Copyright © Infineon Technologies AG 2023. All rights reserved.

# Use case: Secured Software Update (SOTA)




## Secured Software Updates (SOTA) on devices

Infineon´s OPTIGA™ hardware security not only provides a secured device identity by secured key generation on chip but **maintains and manages** this device identity **securely along the lifecycle** of Edge and IoT Endpoint devices by, for example, securing the transmission of over-the-air software updates.


Copyright © Infineon Technologies AG 2023. All rights reserved.

Burapha University
Infineon Innovation
Launchpad

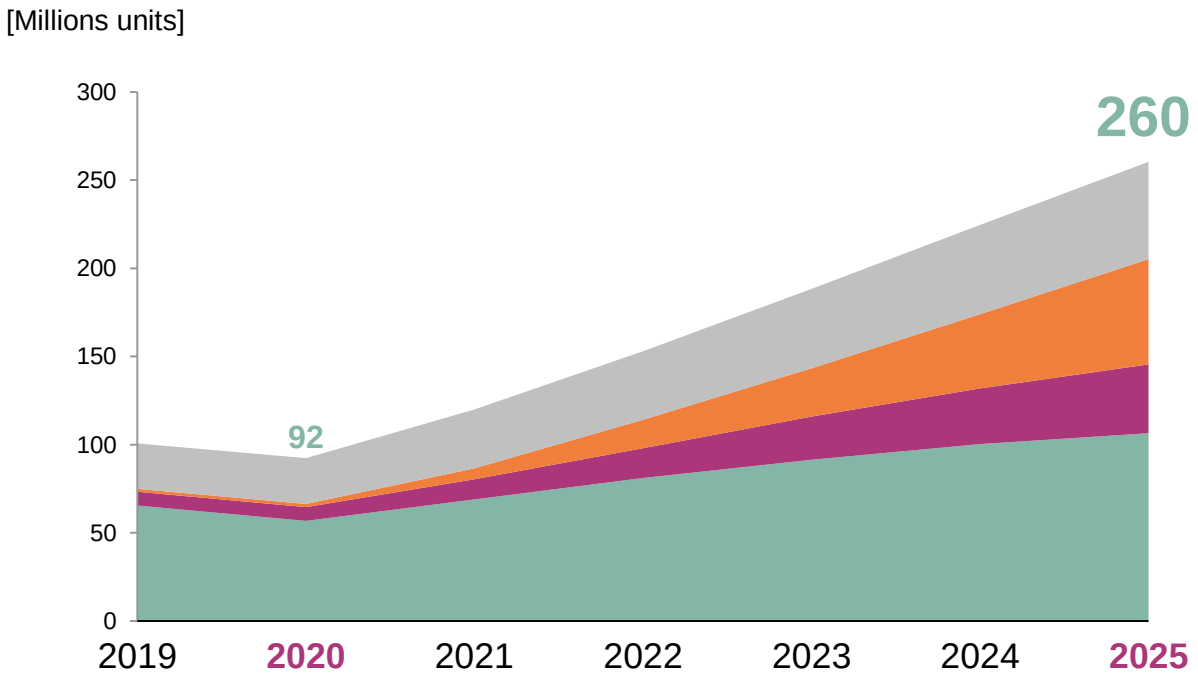
# OPTIGA Connect IoT

# eSIM provides new opportunities for IoT applications

## M2M / IoT

- Safety & Automotive
- Energy Management
- Track & Trace
- Others

## M2M / IoT eSIM Enabled Device Shipments




Source: ABI Research, https://go.abiresearch.com/lp-the-true-value-proposition-of-the-esim; ABI Research, eSIM in the Consumer and M2M Markets Q3-2020

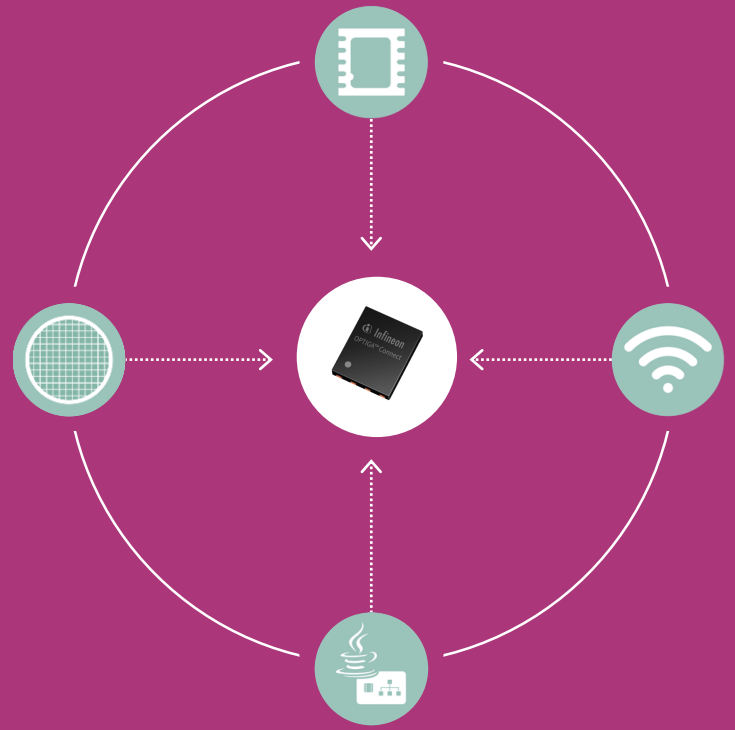

Copyright © Infineon Technologies AG 2023. All rights reserved.

# OPTIGA™ Connect IoT
## Combining key components to provide a turnkey eSIM solution

Burapha University
Infineon Innovation
Launchpad

**Packaging**
Standardized form factors

**Technology**
State-of-the-art security controller technology



**Connectivity**
Global coverage & Easy management

**TATA**

**Operating system**
Performance,
**Security & GSMA compliance**





Copyright © Infineon Technologies AG 2023. All rights reserved.



# OPTIGA™ Connect IoT
## Shaping the New cellular technology

Burapha University Infineon Innovation Launchpad

### Minimize Logistic Nightmare

- One **SKU** can be used all over the world
- Can hold multiple MNO Profiles.
- Interoperability, Security
- Offers an increased Life Span

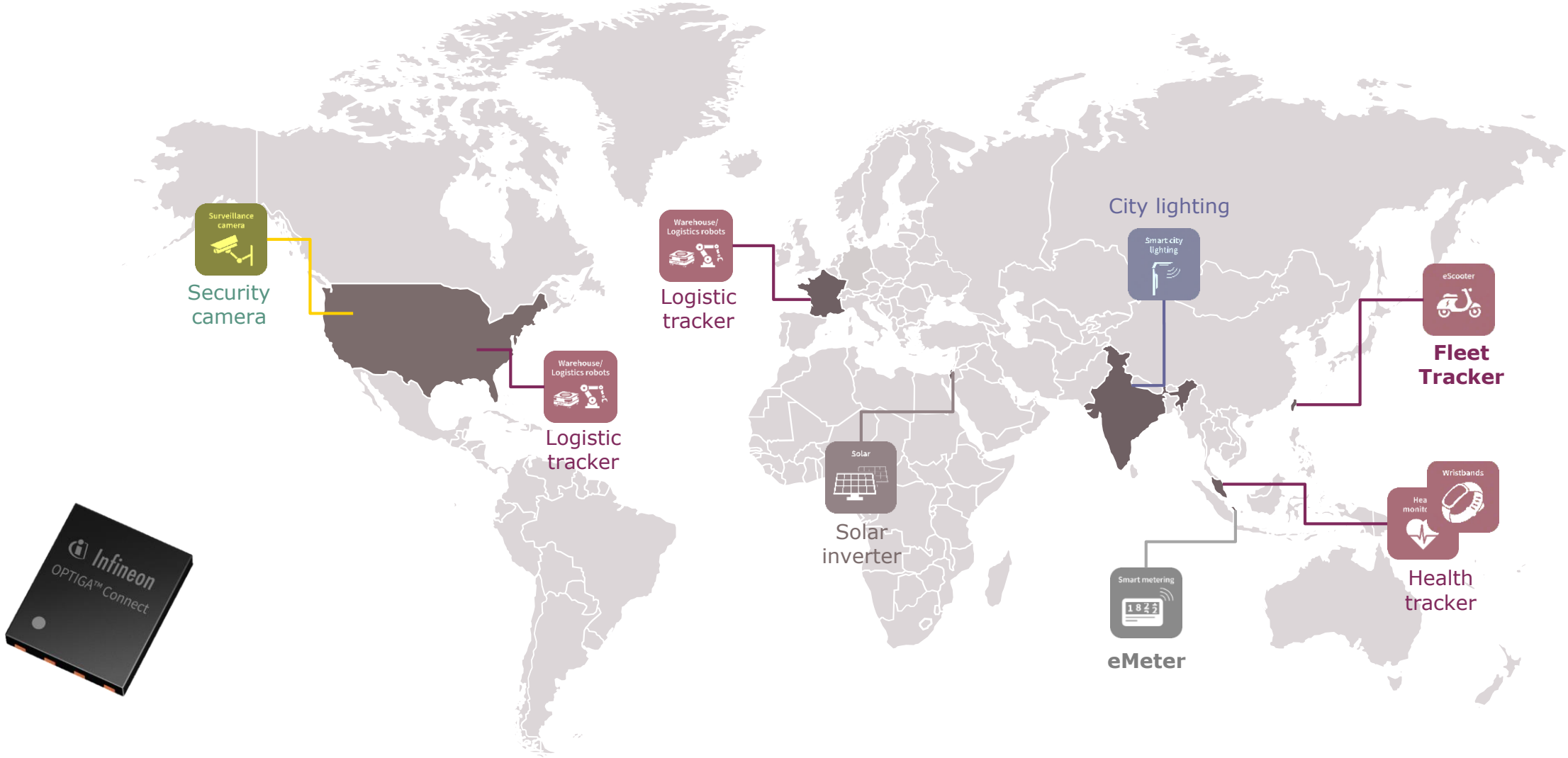



### Remote SIM Provisioning

- Remote Provisioning Over The Air through a subscription management portal
- **GSMA Standard**
- **2G/3G/4G/LPWA/5G Compliant**
- Removable or solderable


Copyright © Infineon Technologies AG 2023. All rights reserved.

# OPTIGA™ Connect IoT use case examples





Copyright © Infineon Technologies AG 2023. All rights reserved.

# We have some amazing Success Stories from Asia Pacific

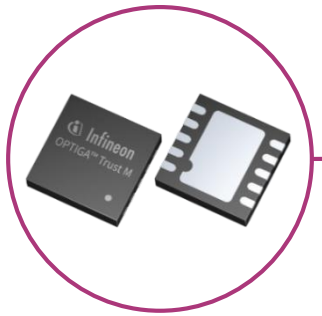



**Smart Meter**

**People Tracking Device**

**Telematics in 2 & 3 Wheelers**

# Key Takeaway




**Hardware separation provides a long-lasting and effective countermeasure against various cyber-attacks**

**Tamper-resistant HW security in IoT devices is vital for protecting the digital identity and credentials**

**Infineon OPTIGA™ security controllers enable a secured, trusted communication between the cloud and the edge/IoT devices.**

**Infineon OPTIGA™ security controllers enables highly secured device enrollment for edge devices and platforms.**


Copyright © Infineon Technologies AG 2023. All rights reserved.




Part of your life. Part of tomorrow.