How (not) to trust your IoT device

Oneconsult Deutschland GmbH

11. February 2020

ONECONSULT AG

Holistic cyber security consultancy

- Product and vendor **independent**
- Privately owned **since 2003**
- Offices in **Switzerland** and **Germany**
- **300+** international **clients**
- **1'200+** security **projects**

ABOUT ME

- With Oneconsult since 2014, previously with a Swiss firewall manufacturer
- Work in the areas of penetration testing, malware, reverse engineering and exploit development
- Co-founder of Oneconsult Deutschland GmbH / Branch Manager in Munich
- Focus on IoT / OT Security since 2015
  - Increased focus on IoT since 2015
  - Testing of IoT environments
  - Helped set up large industrial IoT projects "from day one”
  - Research in the consumer sector (e.g. Smart TV Hacking)

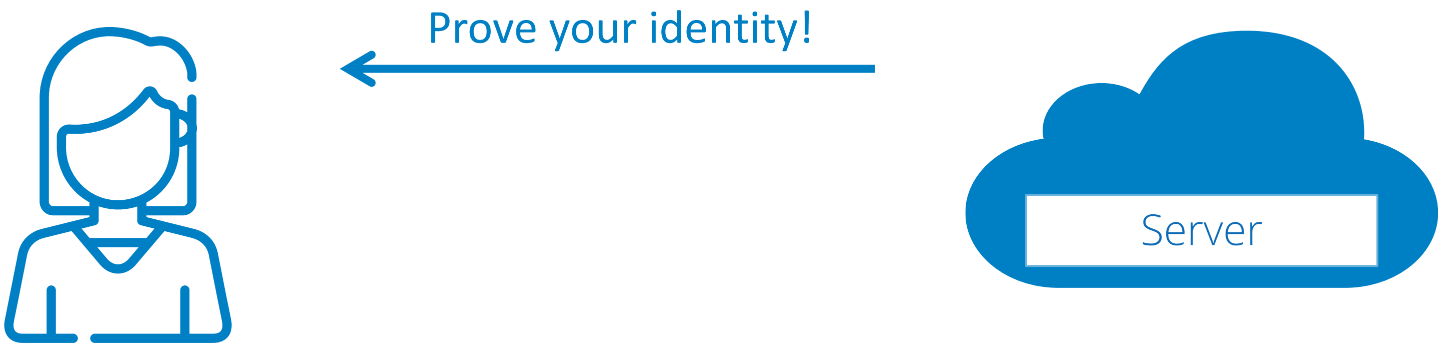
AGENDA

Basics

IoT TRUST

- Trust (here): Mutual identity trust throughout the whole communication
- Identification through **authentication**
- Trust the user vs. Trust the device

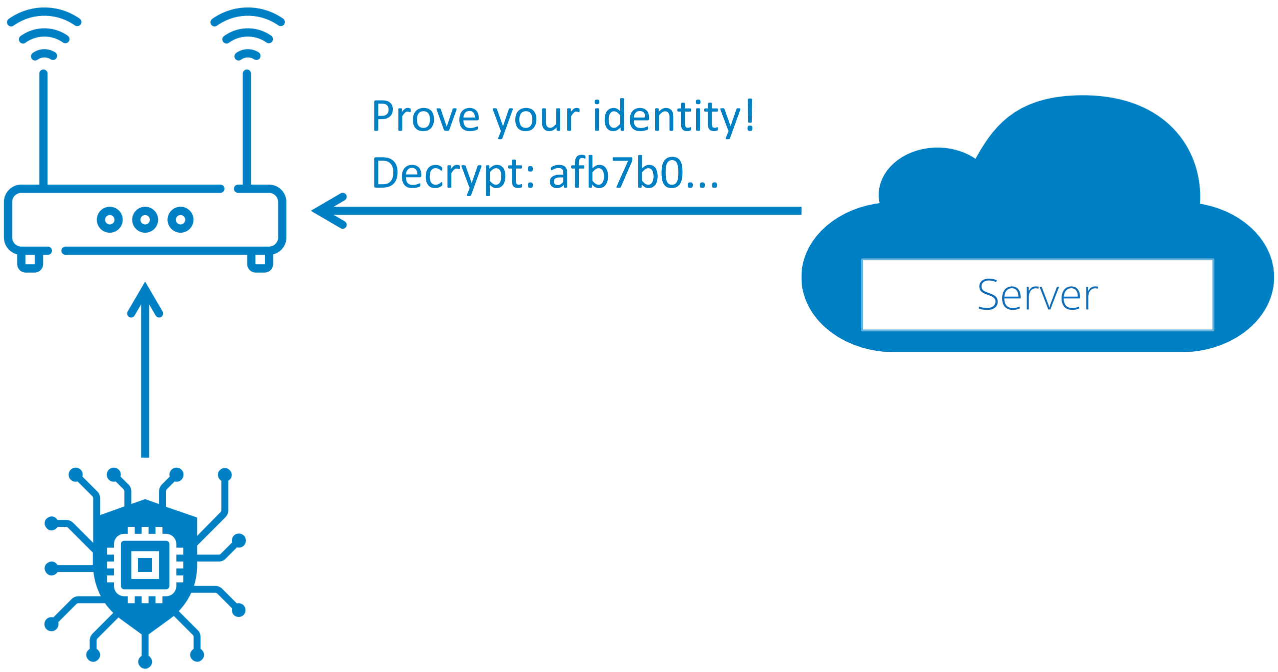
IoT TRUST - ISSUES



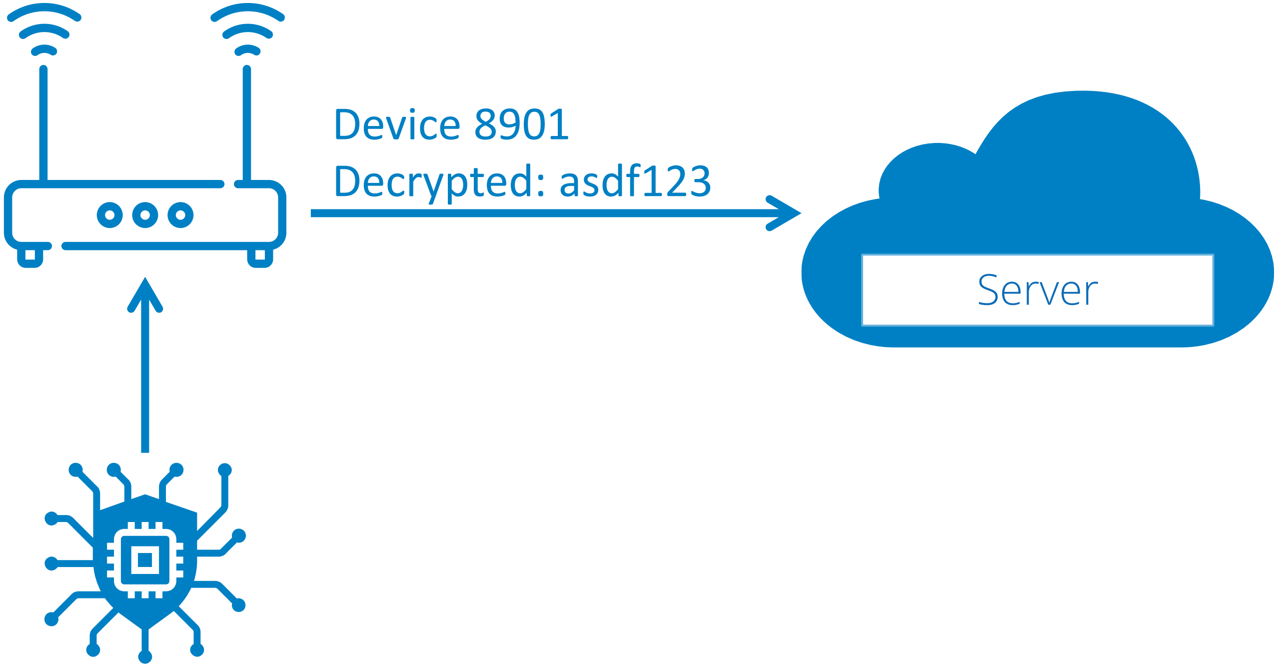
IoT TRUST - ISSUES

IoT TRUST - ISSUES

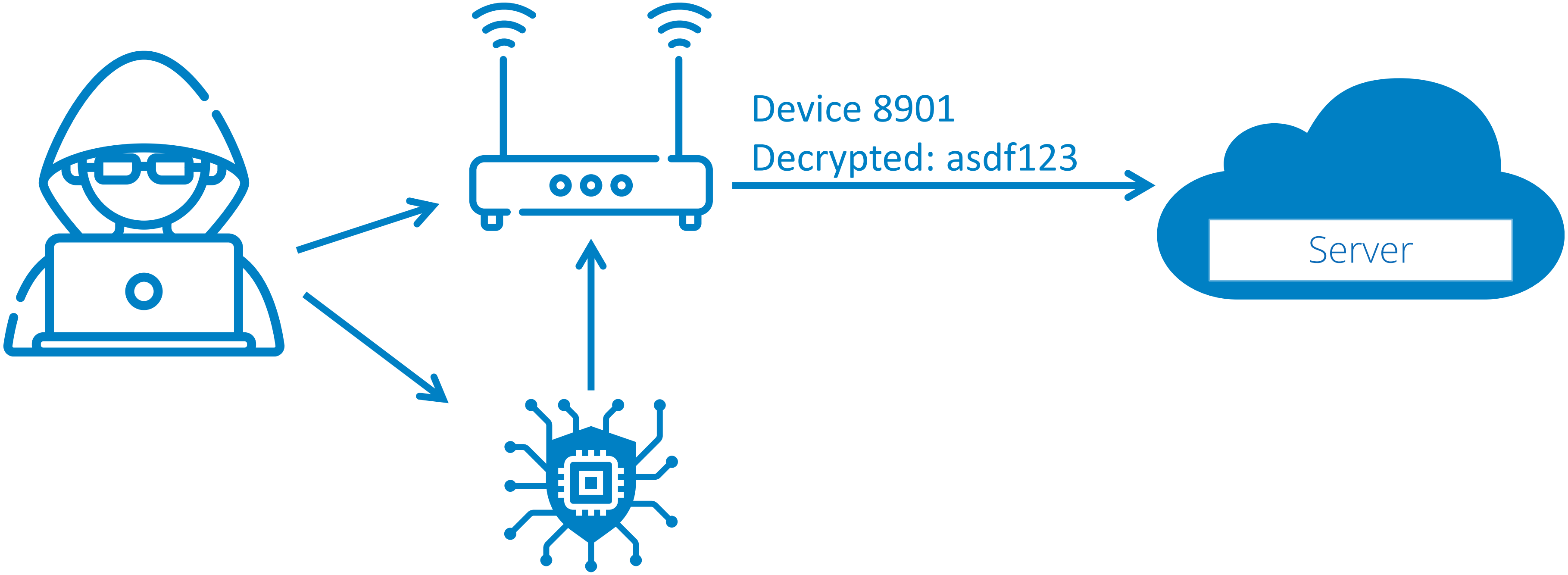
IoT TRUST - ISSUES



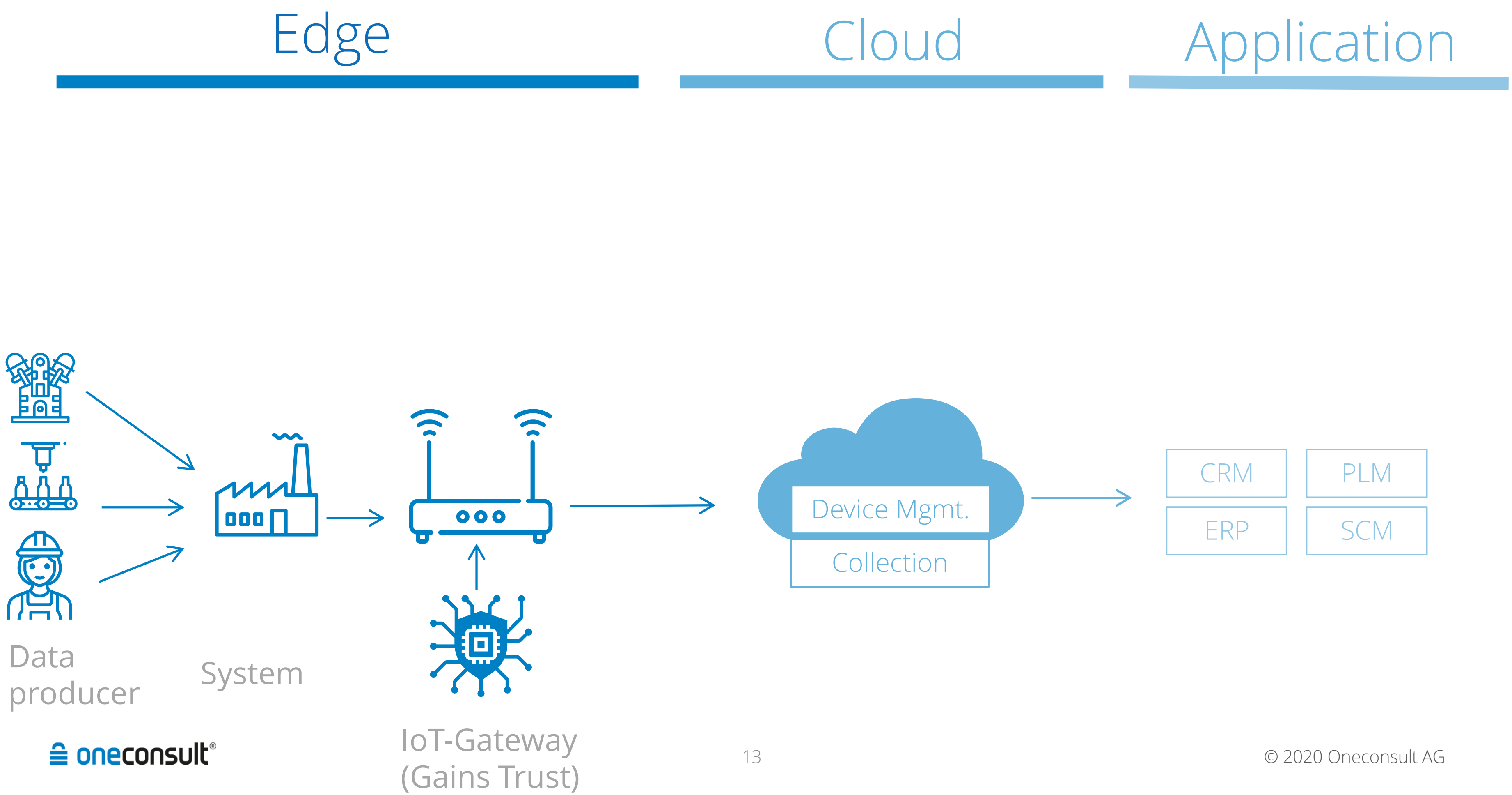
IoT TRUST - ISSUES



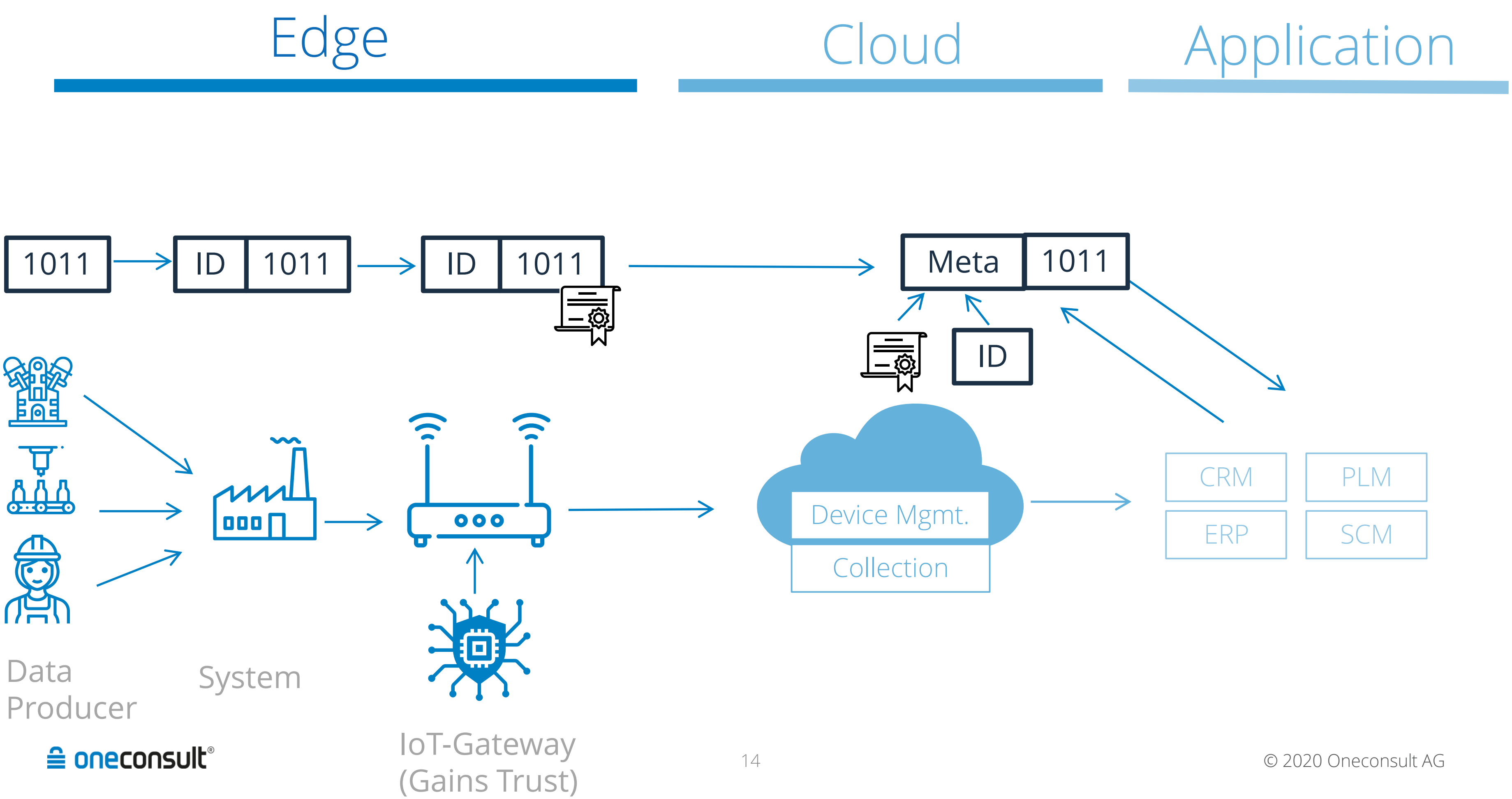
IoT TRUST - ISSUES



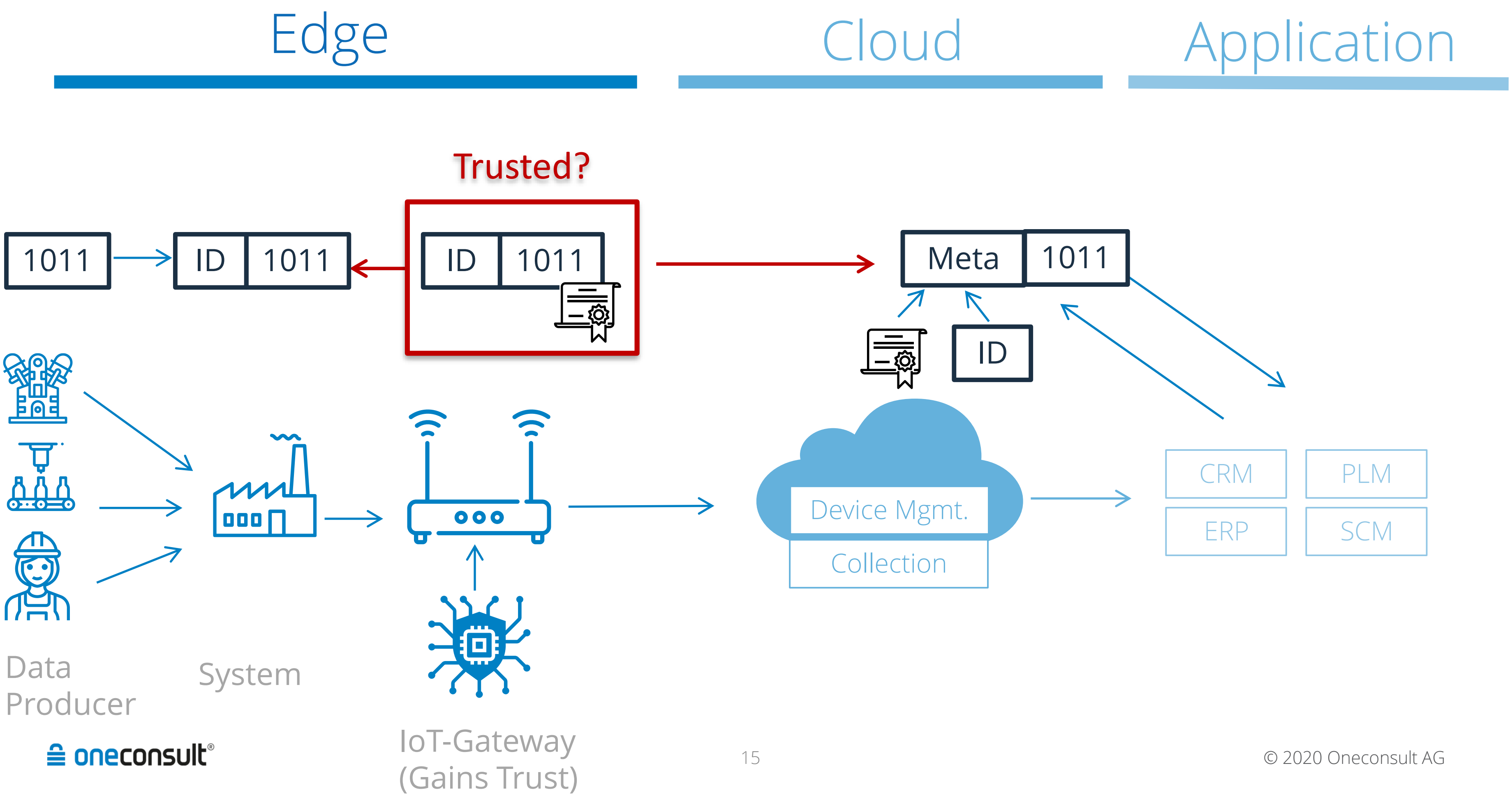
IoT TRUST - GATEWAY



IoT TRUST - GATEWAY

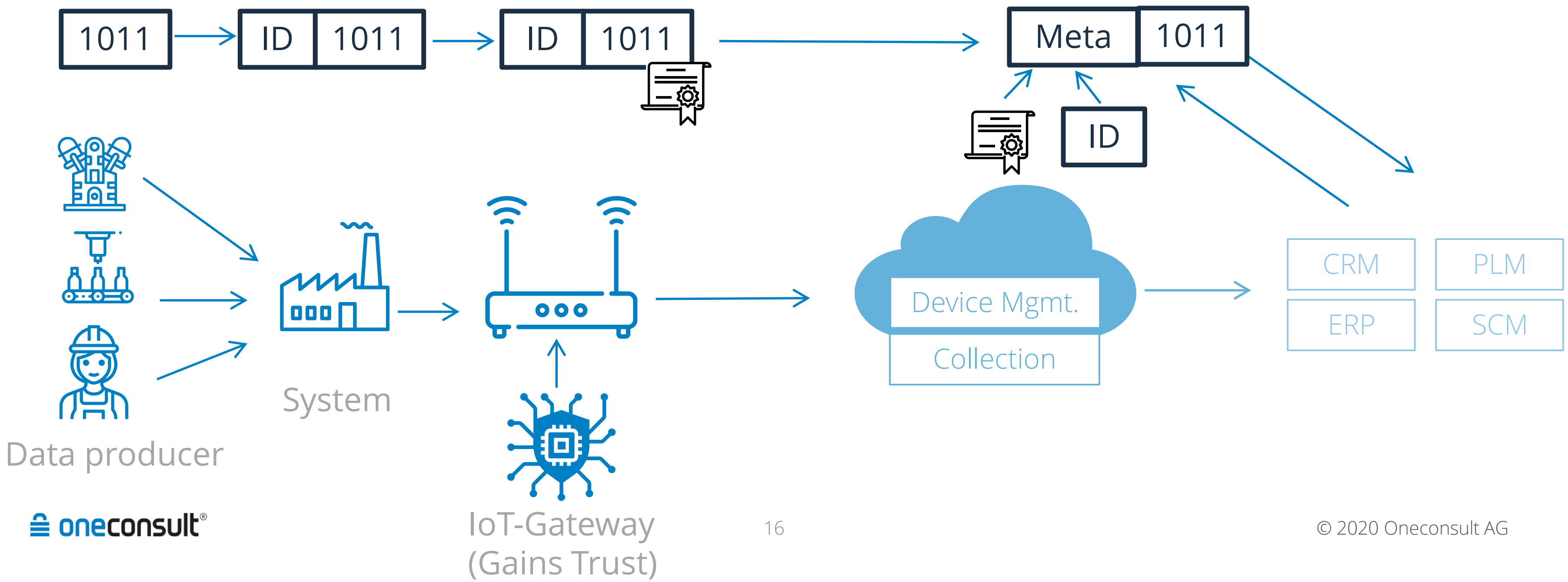


IoT TRUST - GATEWAY



IDENTITY EXTENSION

- Checked at the wrong level
  - Identity check in the cloud (e.g. VPN + API)
  - Content is not checked or only checked at the backend (e.g. serial number of the machine)



Challenges

GOALS AND RISKS

- IT Protection Goals
  - Confidentiality
  - Integrity
  - Availability
  - (+ Safety) ...
- Other Vectors
  - Physical Attacks
  - Device Lifecycle
  - HW Limitations
  - ...
- Different Environments
  - Industrial IoT
    - ICS / SCADA
    - Manufacturing
  - Enterprise IoT
    - Cars
    - Digital Twins
  - End-User IoT
    - Smart TV
    - Coffee Machines
    - Wearables

GOALS AND RISKS

Challenges

Hardware
OEMs
Software
Enrollment
Supply chains

Vectors

Hacker
Competitors
Customers
Partners

Protective Measures

HW / SW
TPM
TrustZones
Encryption

Security requirements

Assets

Intellectual property
Safety
Protocols
Know-how

GOALS AND RISKS

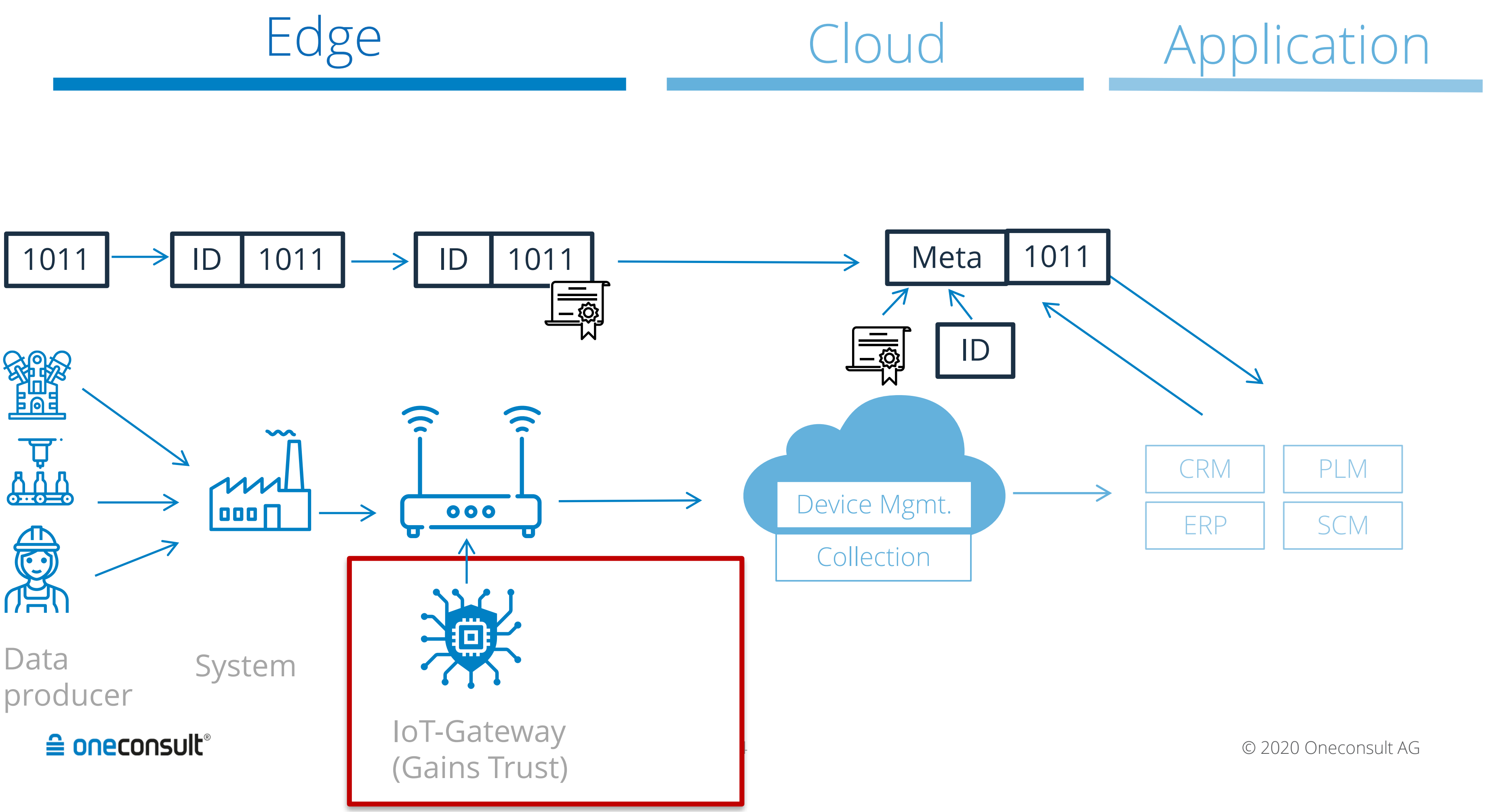
- More subject areas and more attack vectors require more protective measures than with conventional IT
  - What should be protected?
  - Against which attacks?

Security requirements and threat models are essential!

Identity Protection

Core Root of Trust

IDENTITY PROTECTION



IDENTITY PROTECTION ON THE DEVICE

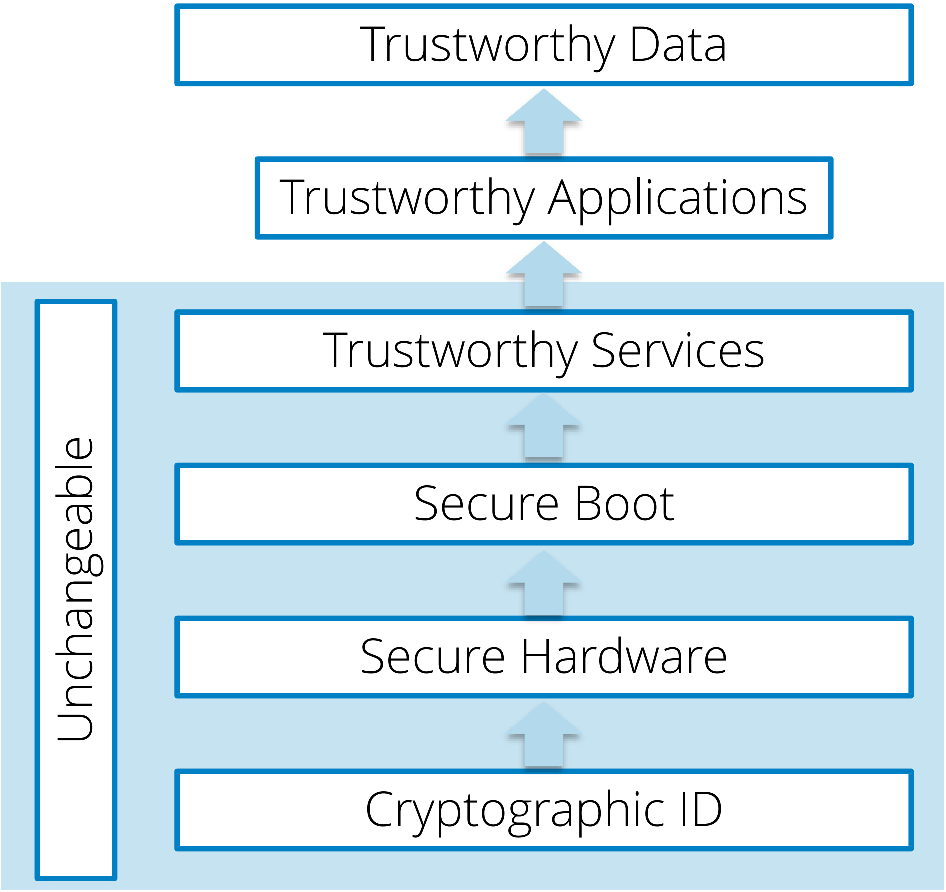
- Device Identity should not:
  - Be able to be manipulated
  - Be able to be stolen via:
    - Software
    - Physical attacks
  - Be able to be duplicated

- Protection of identity possible without protection against physical attacks?
- Is usually created by a "Core Root of Trust”
  - Expression coined by TCG

CORE ROOT OF TRUST

→ Core Root Of Trust (CROT)
  - TCG / TPM coined term
  - Secure identity
  - Mostly based on PKI principles

→ Further information:
  - Root of Trust Definitions and Requirements - GlobalPlatform



Identity Protection

Technology

WHAT ARE THE COMMON REQUIREMENTS?

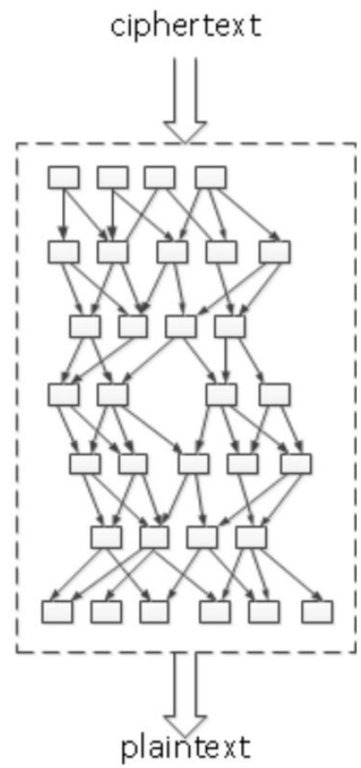
- We must know what we need!
- Protection from HW attacks
  - Protecting the secure storage
  - Protecting the whole system / important parts of it
- Protection from SW attacks
  - Attacker has access to the environment at runtime
    - Protection from stealing / exporting the identity
    - Protection from performing actions with the identity
- Enrollment and management capabilities
  - Can provide an identity issued by a 3rd party
  - Allows traceability and auditing

DEVICE IDENTITY – WITHOUT HW PROTECTION

- Certificate and PK on the device
- Simple protection against manipulation via SW using RO-Memory
- **Each device identity must be unique!**
- Advantages
  - Affordable
  - Manipulation of the identity is not possible
- Disadvantages
  - Little to no protection against attacks with physical access
  - Export or theft of the identity is possible
  - Unique identity before enrollment only with additional measures

OBFUSCATION

- Protection of identity and intellectual property even if the memory can be read
- Very difficult with IoT because of side-channels and vector diversity
- Supplementary measure
- Use when no alternative exists
- Examples:
  - White-Box Crypto for Keys
  - Hiding protocols



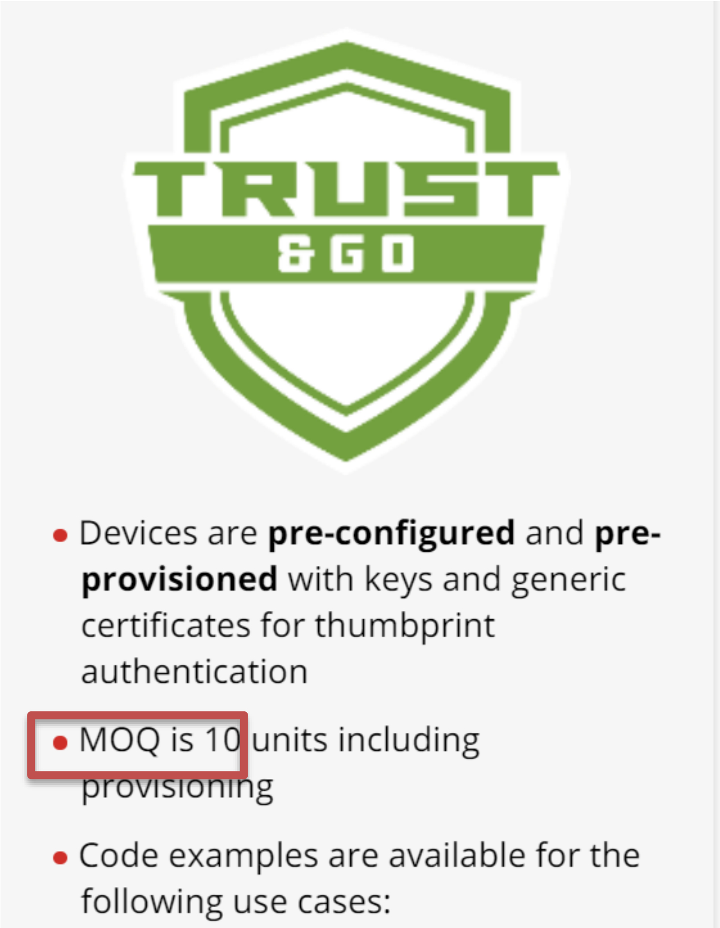
Hardware Modules

MICROCONTROLLER - RDP

- Microcontroller or CPU with integrated Memory
- Read out Protection /deactivation of debug-interfaces
  - Integrated memory can often be protected
  - Protected Core Root of Trust possible
  - Enrollment / Flashing critical
- Mass of production in recent years
  - Microchips
  - ST
  - NXP
  - ....
  - (Microsoft / Azure)

MICROCONTROLLER - RDP

- → Everyone does the same thing, but differently
- → Implementation is not as simple as it seems
- → Check further information carefully with the manufacturers
  - Creating a Root of Trust to protect the Internet of Things (IoT) - Mark Patrick, Mouser Electronics
  - Example ST: Introduction to STM32 microcontrollers security
- → Security as good as the chip
  - → Attacks known (examples STM32)
  - → Read Out Services



Source: Microchip Trust Platform for the CryptoAuthentication™ Family

MICROCONTROLLER – READ OUT SERVICES

Focus on the reverse development of various electronic products and equipment prototypes at home and abroad

It has the most professional reverse technology R & D team in China, focusing on the research of copy (clone) technology of various electronic products and equipment prototypes at home and abroad, and the technology is leading in the country. Provide PCB copy board, chip decryption, program secondary development, SMT chip foundry, and other services. Tel: 0755-28289770 —24-hour hotline: 13717069599 (Same as WeChat)

Case Show | Contact Us

Location: Home › success case ›

26 2019-10
Strength crack M30260F3AGP chip decryption program extraction
M30260F3AGP chip decryption, contact phone: 13717069599 0755-28289770 audio, camera, office equipment, communication equipment, portable equipment, household appliances

26 2019-10
STM32F417IEH6 chip decryption / SCM decryption / STM32 crack
Shenzhen Weidong Zhixin Technology provides STM32F405 415 407 417 chip decryption MCU decryption IC chip decryption model: STM32F405RGT6, STM32F415RGT6, STM32F407VET6, STM32F41

21 2019-10
2F TSOC6 DALLAS custom version chip decryption
This chip is a customized version, which is used in beauty equipment consumables. Now it has successfully obtained the password area. If you need it, please contact us for cooperation and negotiation. Note: Thi

21 2019-10
Nuvoton N76E003AT20 Fast Decryption Fascia Gun Control Board Decryption
Since its establishment, Shenzhen Weidong Zhixin Technology has been focusing on decryption technology services. Integrity first, quality assurance, core service! Welcome to inquire. Nuvoton N76E003AT20 Qu

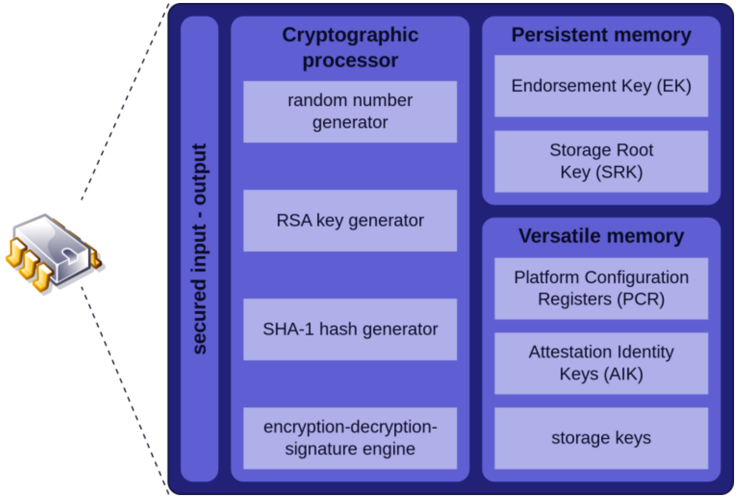
16 2019-10
STM32F417IGT6 chip decryption technology breakthrough
Exclusive release! STM32F407 STM32F417, 32-bit flash microcontroller with Cortex-M4 core can finally be cracked. STM32F407 STM32F417, chip decryption phone: 13717069599. Shenzhen

Recommended information

- Strength crack M30260F3AGP chip decryption program extraction
- STM32F417IEH6 chip decryption / SCM decryption / STM32 crack
- 2F TSOC6 DALLAS custom version chip decryption
- Nuvoton N76E003AT20 Fast Decryption Fascia Gun Control Board Decryption
- STM32F417IGT6 chip decryption technology breakthrough
- OB1800 chip decryption DALLAS custom chip beauty instrument crack
- Fascia relaxation gun motor control board PCBA development N76E003
- Renesas R5F full series of chip decryption success stories
- Micro font printer reverse PCB copy board prototype clone

TRUSTED PLATFORM MODULE

- Trusted Platform Module (TPM)
- Standard for secure crypto co-processors
- Chip is protected against physical access and anti-hammering attacks
- Endorsement Key (EK)
  - Private key cannot be exported
  - TPM key attestation
  - List of public keys usually available
- Secure storage for keys
- Remote attestation



[https://en.wikipedia.org/wiki/Trusted_Platform_Module]

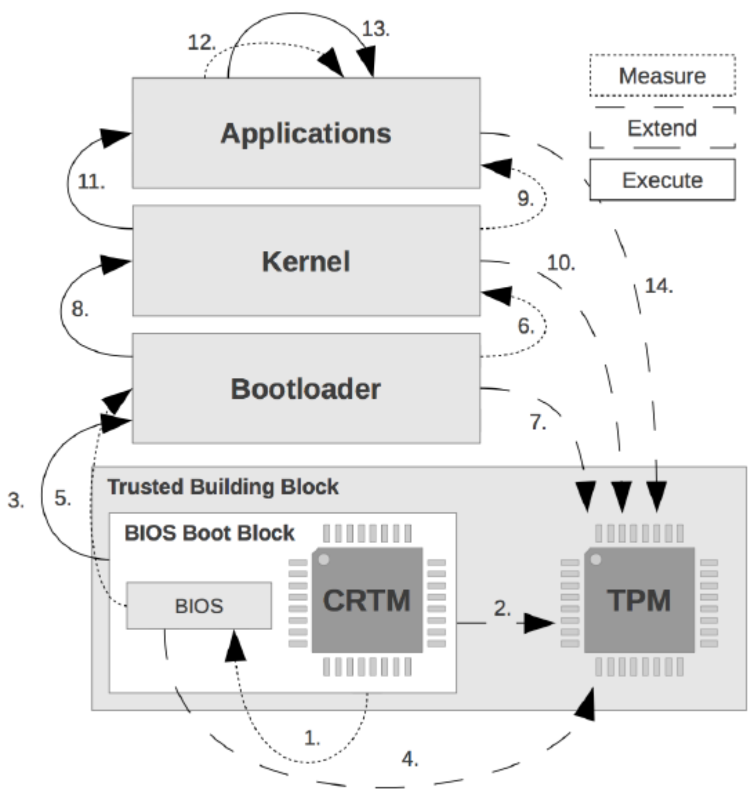
TRUSTED PLATFORM MODULE - PCR

- 24 Registers (20-Bytes)
- Secrets can be bound to PCR-Registers (Sealing / Unsealing)
- Used primarily to store system measurements
- Can only be extended (e.g. SHA1 of old + new value)

TRUSTED PLATFORM MODULE - SRTM

- Static Root of Trust for Measurements (SRTM)
- SRTM sets the PCRs to the right state during boot
- 0-7 during boot, 8-15 for OS
- Unseal / Seal possible if PCRs correct

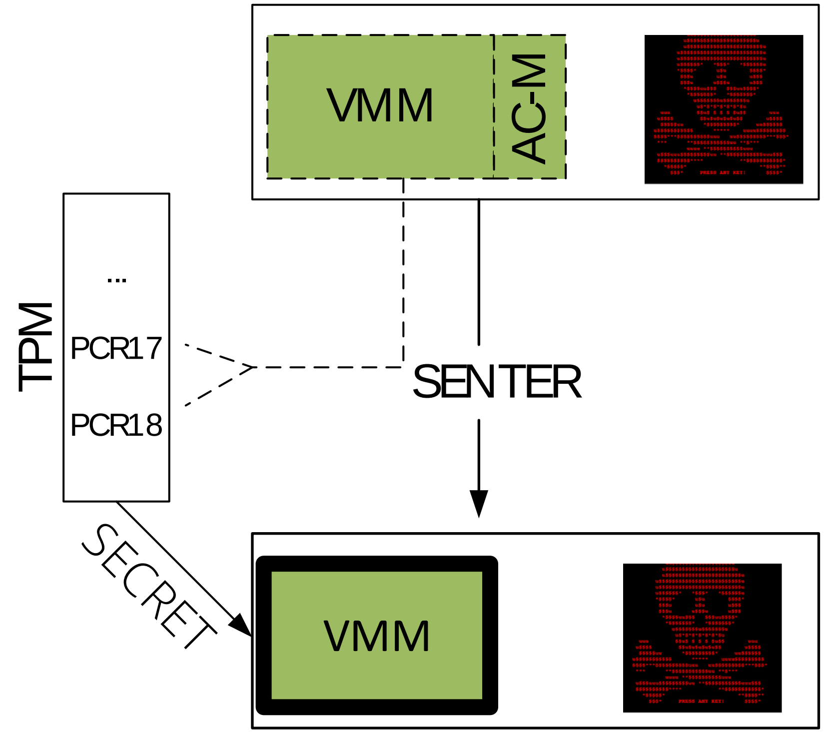
- Issues:
  - **Completeness** required
  - Scalability an issue because of that



[Armin Simma – Trusting Your Cloud Provider.]

TRUSTED PLATFORM MODULE - DRTM

- Dynamic Root of Trust for Measurements (SRTM)
- Intel Trusted Execution Technology (TXT) / AMDs Secure Virtual Machine (SVM)
- Example with Intel
  - SENTER instruction (simplified)
  - All co-processors are informed
  - VMM hash into PCR18
  - VMM completely isolated by CPU
  - Secret sealed to PCR18
- Implemented by TBOOT



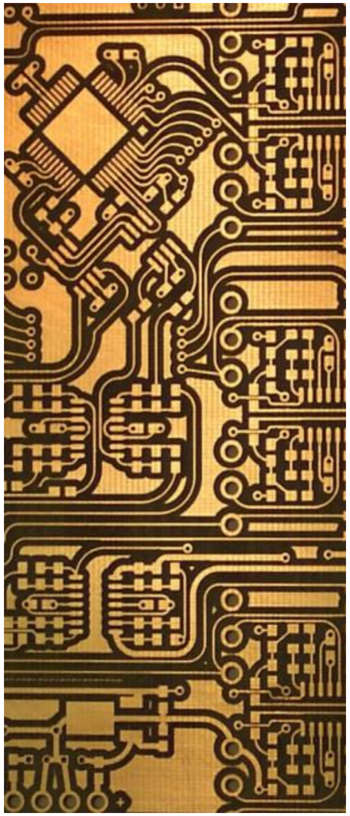
[Armin Simma – Trusting Your Cloud Provider.]

TRUSTED PLATFORM MODULE

- Advantages
  - Unique identity before enrollment
  - Identity theft not possible
  - Reduced dependence on chip / board manufacturer
  - Measured Boot
- Disadvantages
  - Costs
  - Communication CPU / TPM chip difficult to protect against attacks with physical access
  - Implementation errors
  - Initialization usually necessary during the manufacturing lane after mounting the TPMs

SECURE ELEMENTS

- Tamper resistant secret store
- Like TPMs but SEs are:
  - generally cheaper
  - smaller
  - less possibilities
  - not standardized
  - sometimes removable
- Used for
  - Authentication / attestation
  - Digital signature
  - Mobile payments
  - Lyfecycle management



TRUSTED EXECUTION ENVIRONMENTS

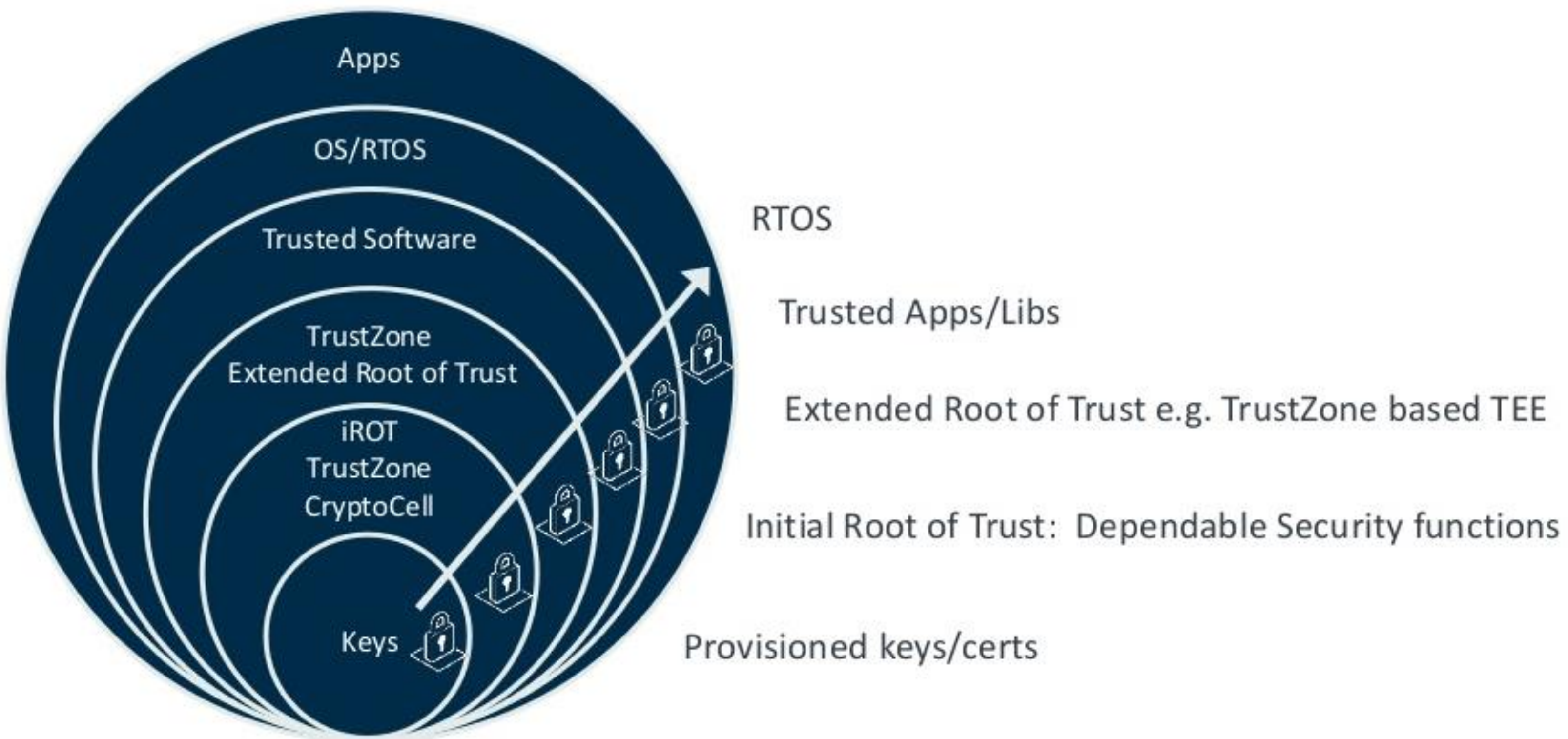
TEE

TRUSTED EXECUTION ENVIRONMENTS

Rich environments are not secure!

TRUSTZONE

→ Pushes the TPM into the chip / SOC

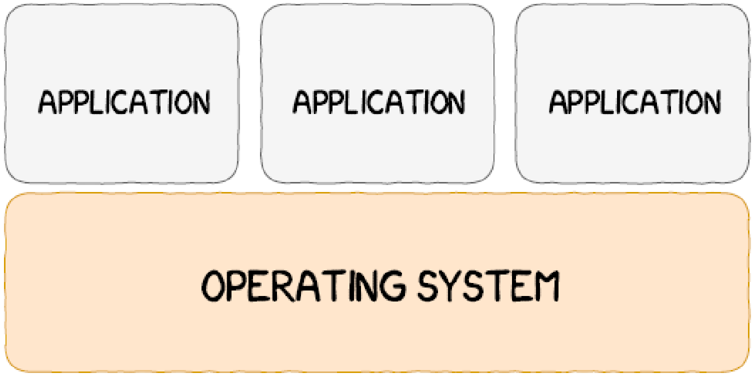


[Source: ARM - Demystifying Security Root of Trust Approaches for IoT/Embedded - SFO17-304]

TRUSTZONE

- Pushes the TPM into the chip / SOC
- Enables safe boot
  - Chain of Trust starts with Initial Boot Block (IBB)
  - "Boots" a safe and insecure space
  - Communication via a monitor
- More than just a Core Root of Trust
  - Trusted Execution Environment (TEE)
  - Protection of critical applications
  - Extensive TEE environments e.g. OP-TEE, Samsung TIMA

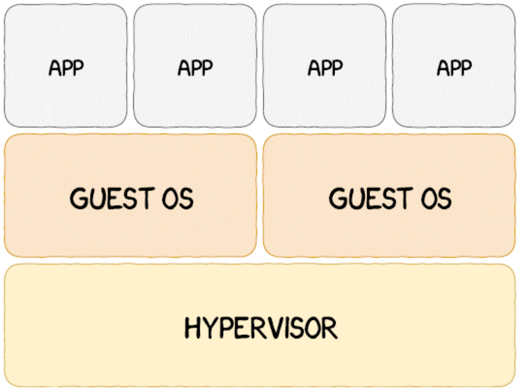
TRUSTZONE



[Source: Quarkslab - Attacking ARM TrustZones]

- → Security traditionally relied on kernel mechanisms
- → The kernel was considered «secure»....

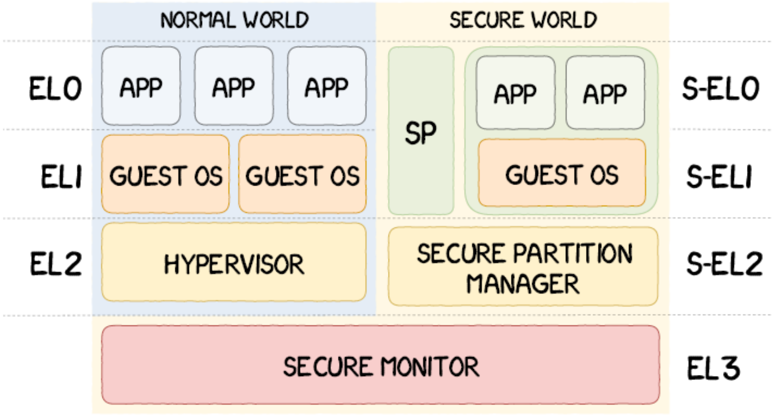
TRUSTZONE



[Source: Quarkslab - Attacking ARM TrustZones]

- Virtualization technology allows to run insecure Apps and secure Apps on the same HW
- Resource heavy
- VM escapes and hypervisor attacks possible

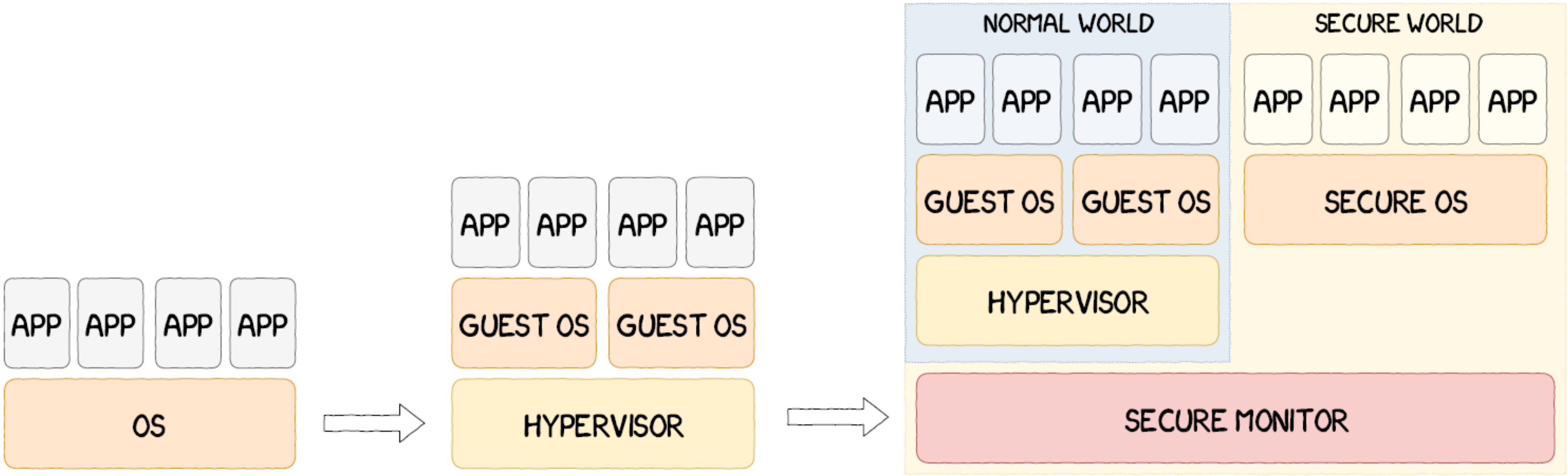
TRUSTZONE



[Source: Quarkslab - Attacking ARM TrustZones]

→ Hardware based separation for trusted secure world and distributed normal world

TRUSTZONE



[Source: Quarkslab - Attacking ARM TrustZones]

TRUSTEZONE - VERSATILITY

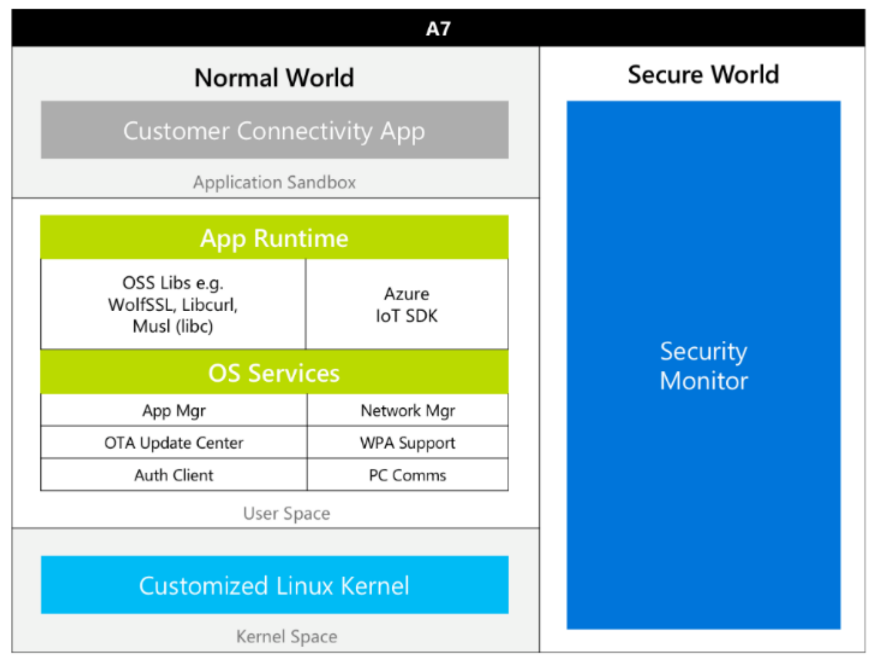
- Trustonic's TEE-OS
  - 32-bit micro-kernel developed by Trustonic and called **Kinibi**
  - Integrated in Samsung's TrustZone as its trusted OS
  - Uses the **ARM Trusted Firmware** monitor implementation
  - Loads and executes small programs, called Trusted Applications, to add functionalities
- Qualcomm's TEE-OS
  - Completely custom and closed source TEE written by Qualcomm and named Qualcomm Secure Execution Environment (QSEE)
  - 32-bit and 64-bit
  - Monolithic kernel called Qualcomm Secure Environment OS (**QSEOS**)

TRUSTEZONE - VERSATILITY

→ OP-TEE TEE-OS
  - Open-source TEE-OS implementation
  - Monolithic kernel
  - Allows to loads signed trusted applications

TRUSTEZONE - VERSATILITY

- Azure Sphere SoC
  - Cortex A7 with integrated cloud connectivity over the secure world
  - Secure World as ROM / extremely small



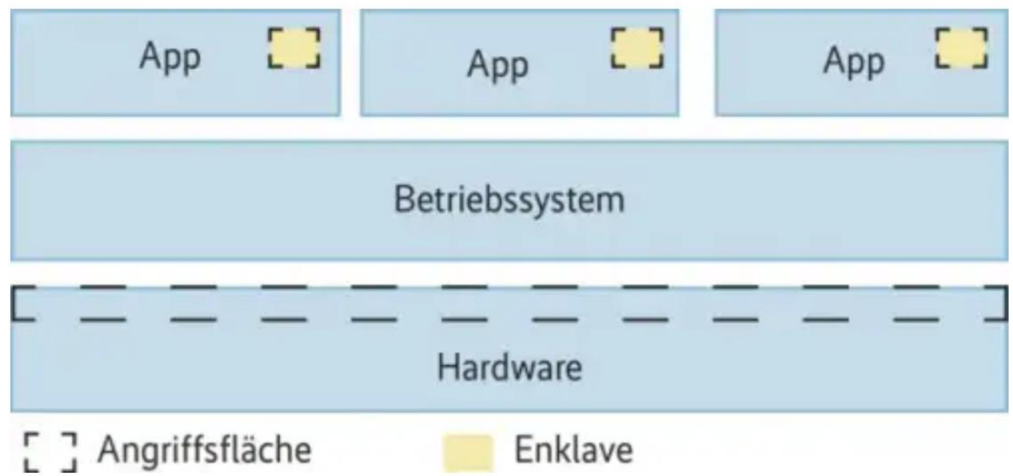
[Source: Avnet Silica / Konferenz Internet of Things 2019]

TRUSTZONE

- Advantages:
  - Protection against physical attacks
  - Protection still possible if the OS has been compromised
  - Protection when the user is not trusted (e.g. when third-party applications are loaded)
- Disadvantages:
  - Cost
  - Implementation very different and can be difficult
  - Many possibilities = large attack surface (e.g. attacks against trusted apps)

INTEL – SOFTWARE GUARD EXTENSION (SGX)

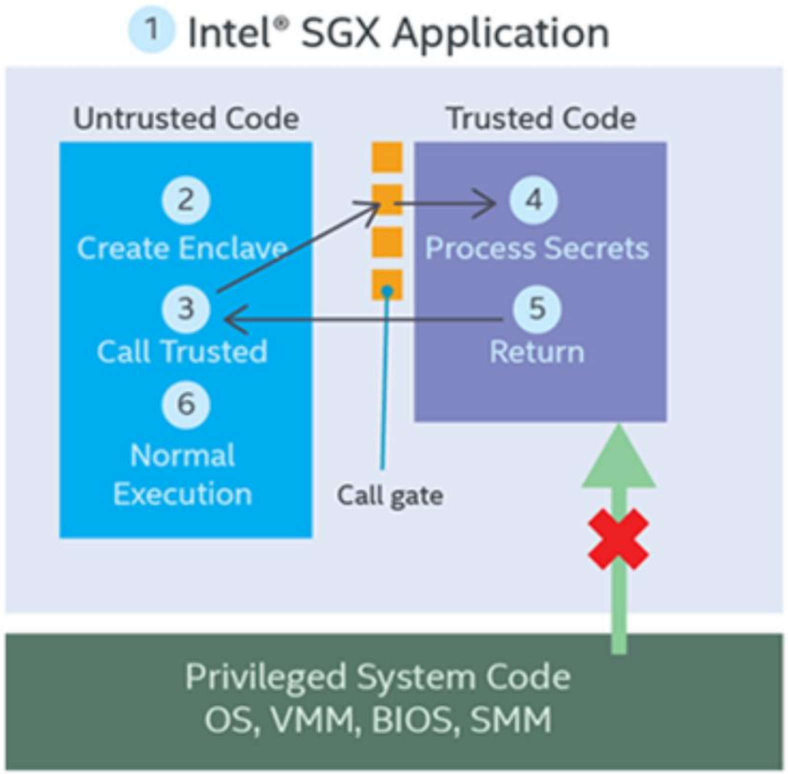
- A TEE within the application
- Set of CPU instructions
- Reduces attack surface
- Enclave page cache
- Encryption of memory for trusted code



[Source: iX – 1/2018 – P100]

INTEL – SOFTWARE GUARD EXTENSION (SGX)

- App built with trusted and untrusted parts
- App runs and creates the enclave which is placed in trusted memory
- Trusted function is called and execution is transitioned to the enclave
- Enclave sees all process data in the clear; external access to enclave is denied
- Function returns



[Source: Intel - software.intel.com]

TECHNOLOGIES – EXAMPLE

No protection / obfuscation	CROT unprotected	- Unique ID - Enrollment critical
Read Out Protection / MCU	+ CROT protected against SW & HW manipulation + IP protected against HW attacks + Secure Boot	- Cooperation with Manufacturers is important - HW
Trustzone / TEE	+ Protection from untustworthy SW and users	- HW - Implementation is complex / own OS
Trusted Platform Module	+ Identity comes from a trustworthy 3rd party + CROT protected against SW & HW manipulation	- HW - No protection of the IP, or against HW attacks against the device

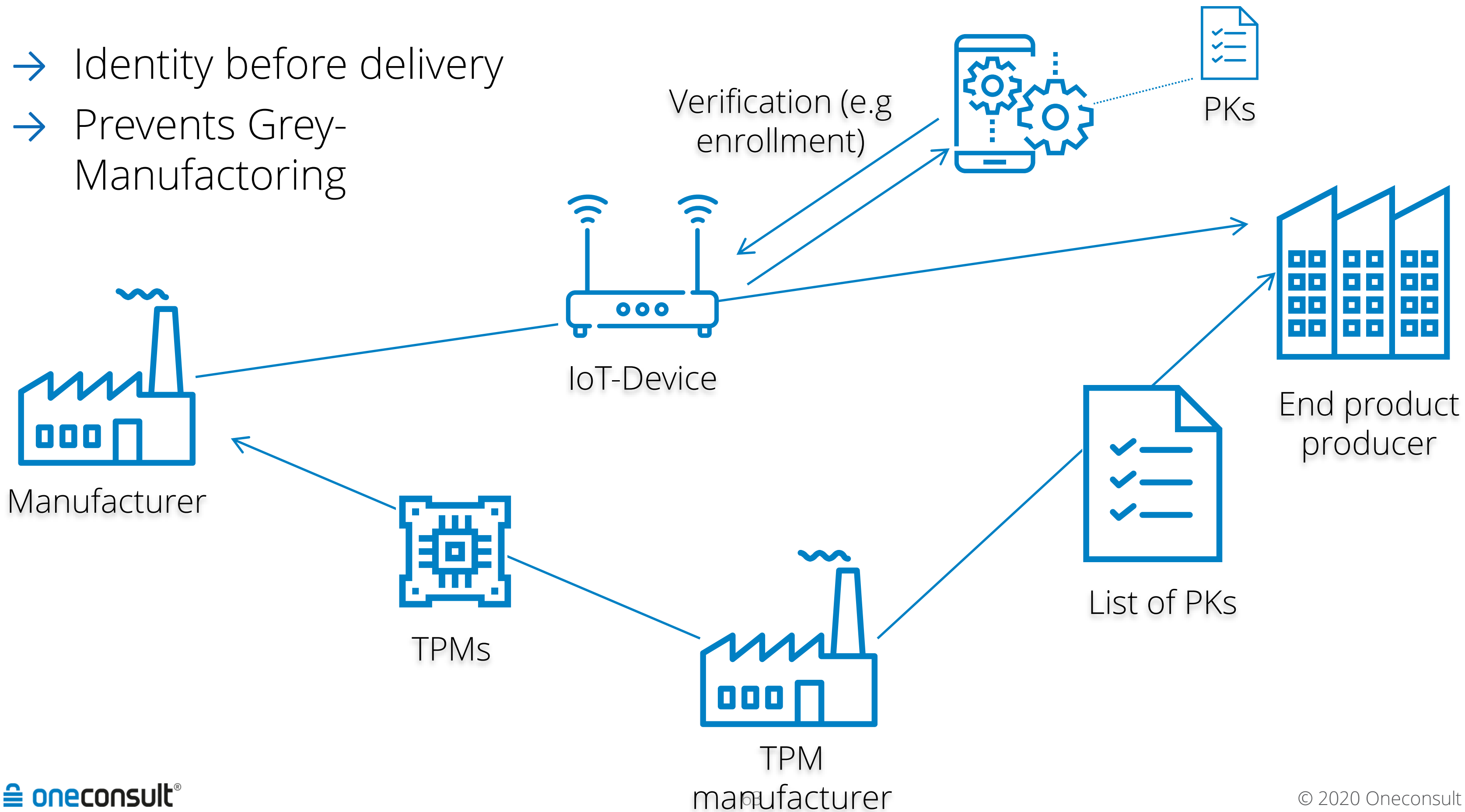
ENROLLMENT & PARTNER

ENROLLMENT

- Enrollment before delivery
- Enrollment through authenticated end customers
  - All devices "equal"
  - E.g. Smart-Watch
- Independent enrollment / by untrustworthy persons
  - Device requires an identity before delivery
  - Self-registration without identity is problematic
  - Cooperation with manufacturers is necessary
- Many solutions also exist for small environments
  - e.g. microchips

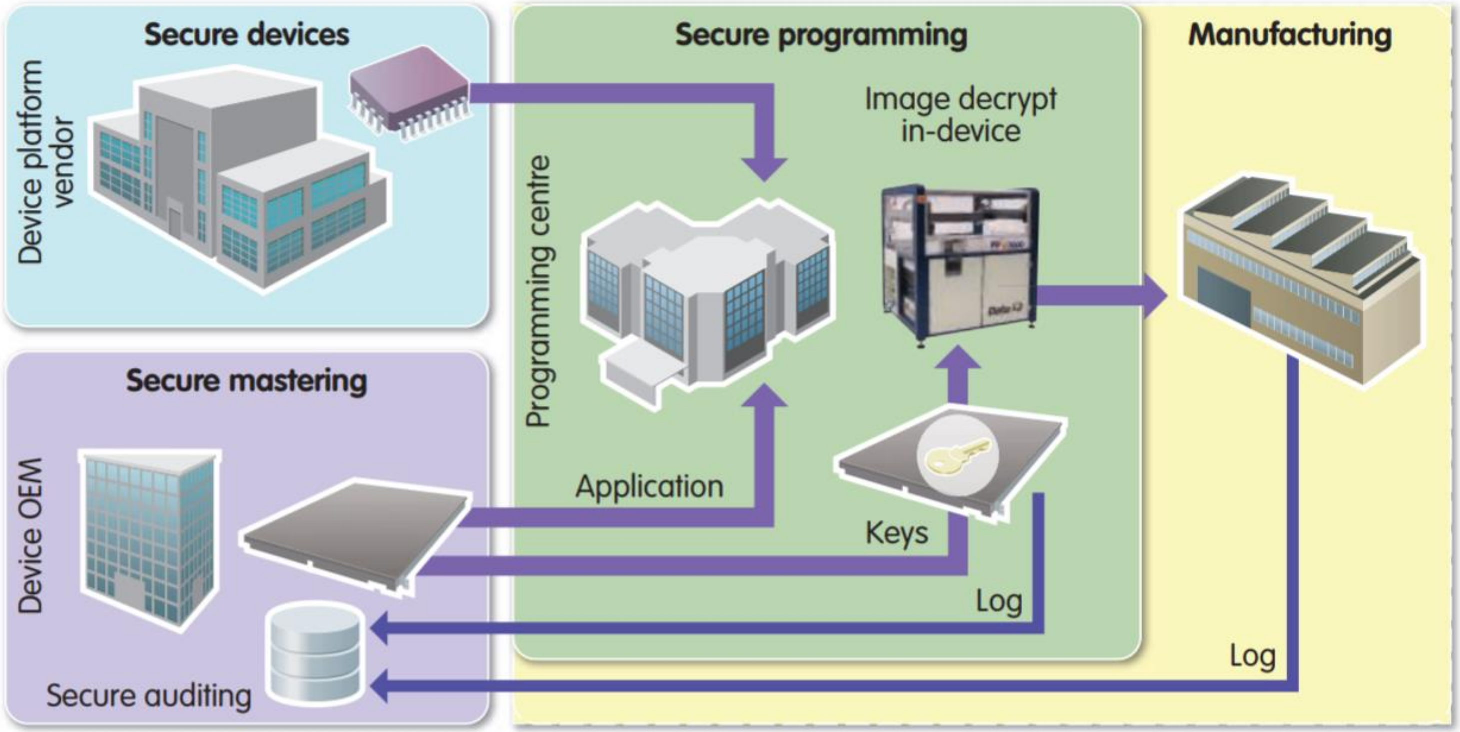
ENROLLMENT WITH TPM

- Identity before delivery
- Prevents Grey-Manufactoring



SUPPLIERS & PARTNERS

→ Supply Chain of Trust by Haydn Povey



SUPPLIERS & PARTNERS

- Supply Chain of Trust
  - ROT as explained
  - Encrypt applications before suppliers / producers
  - Deliver critical IP only after enrolment
- IoT Security Compliance Framework
  - Review and audit
  - Supply of security reports and documentation of the components
- Do not trust software and repositories per se
  - Risk / Expense Estimation

SUPPLIERS & PARTNERS

→ Cooperation with partners – e.g. Cloud
  - Proactive management of partner trust
  - Avoid the unnecessary
  - Determine who is entrusted with which data
  - End-to-end encryption
  - Partners can also be hacked by third-parties

Q & A

Thank you for your attention!

CONTACT US

Switzerland

Oneconsult AG
Schuetzenstrasse 1
8800 Thalwil

Tel +41 43 377 22 22
info@oneconsult.com

Oneconsult AG
Baerenplatz 7
3011 Bern

Tel +41 31 327 15 15
info@oneconsult.com

Germany

Oneconsult Deutschland GmbH
Agnes-Pockels-Bogen 1
80992 Munich

Tel +49 89 248820 600
info@oneconsult.de

RECOMMENDED RESOURCES

- Core Root of Trust
  - GlobalPlatform Technology - **Root of Trust Definitions and Requirements** - Version 1.1
  - Thomas Müller - **Trusted Computing Systeme, Konzepte und Anforderungen** – Springer 2008 (!!)
- IoT Security
  - IoT Security Foundation – **IoT Security Compliance Framework** – Release 2 December 2018
- Supply Chain
  - Haydn Povey – **A supply chain of trust** - NewElectronics 28.02.2017
- Hardware Security
  - Enisa OPSEC - **Hardware Threat Landscape and Good Practice Guide** – Enisa January 2017

RECOMMENDED RESOURCES

- TrustZone
  - arm - **TrustZone Technology for the Armv8-M Architecture** – v2.1 2018
  - ARM Security Technology - **Building a Secure System using TrustZone® Technology –** ARM 2009
- Intel SGX
  - Heise – **Programmieren mit Intels Trusted Execution SGX** - iX 1/2018 S. 100