MPSoC 2019

Trusted Execution Environment (TEE) with Open Processor Cores

July 11th, 2019

Fumio Arakawa, Makoto Ikeda
The University of Tokyo
Akira Tsukamoto, Kuniyasu Suzaki
National Institute of Advanced Industrial Science and Technology (AIST)

Outline

- Background
  - Current trusted execution environment (TEE)
  - Kerckhoffs's Principle
  - RISC-V
- NEDO*) Project Overview

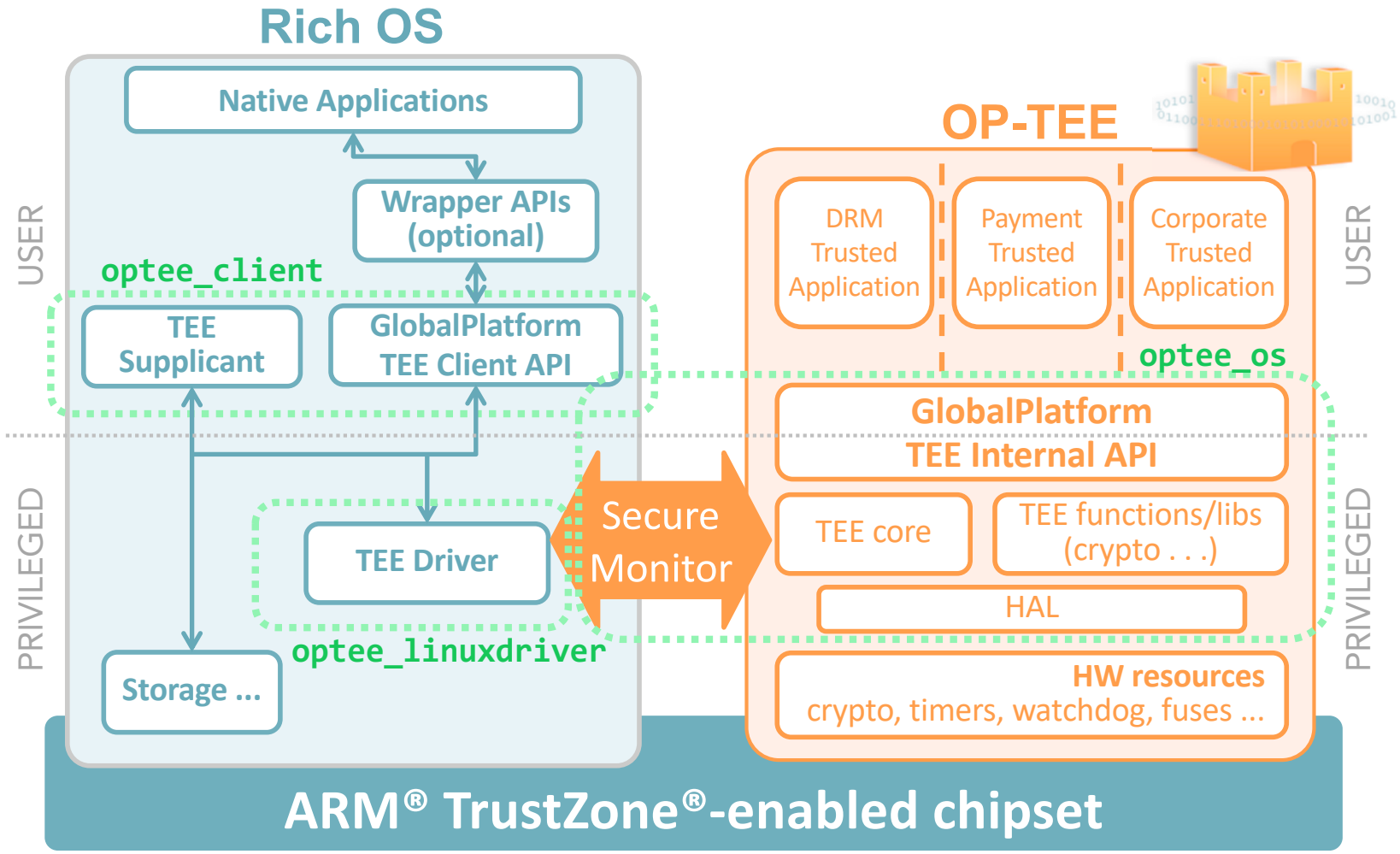
R&D of Basic Technology of Secure Open Architecture and its Application to Edge AI

1. Secure chip architecture
2. Trusted execution environments (TEE)
3. Swift migration of industrial applications
4. Proof of concept (POC) of social implementation

- Summary

*) New Energy and Industrial Technology Development Organization

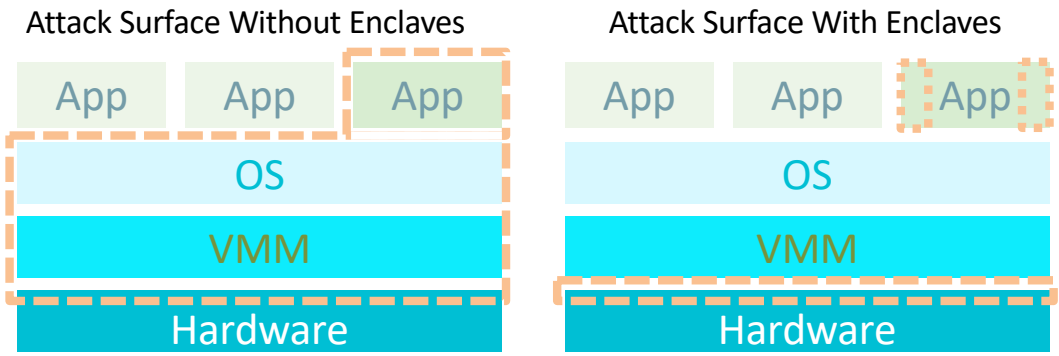
A TEE on ARM® TrustZone®

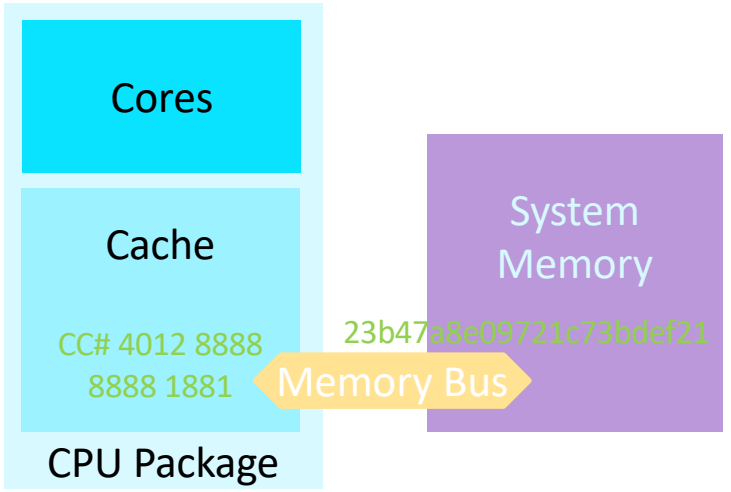


OP: Open Portable
HAL: Hardware Abstraction Layer

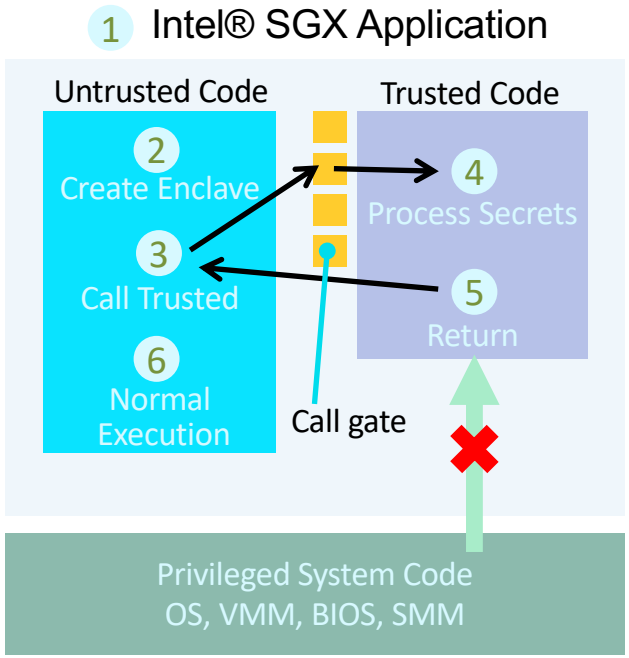
source) https://www.linaro.org/blog/op-tee-open-source-security-mass-market/

A TEE on Intel® SGX (Software Guard Extensions)





1. Security perimeter is the CPU package boundary
2. Data unencrypted inside the CPU package only
3. Externally, memory reads and bus snooping attacks see only encrypted data



1. App is built with trusted and untrusted parts
2. App runs and creates the enclave, which is placed in trusted memory
3. Trusted function is called, and execution is transitioned to the enclave
4. Enclave sees all process data in the clear; external access to the enclave data is denied
5. Function returns; enclave data remains in trusted memory
6. Normal execution resumes

Source) https://software.intel.com/en-us/articles/intel-software-guard-extensions-tutorial-part-1-foundation

Kerckhoffs's Principle and RISC-V

- **Kerckhoff's Principle**
  - "The design of a system should not require **secrecy**."
  - "A crypto system should be **secure** even if **everything** about the system, **except the key**, is **public knowledge**."

- Current major systems are based on **proprietary** architecture (x86 or ARM)
- We cannot check such systems whether they **comply the principle** or not.

- **RISC-V**
  - **Free** and **Open ISA**
  - **Open** or Proprietary Implementation
  - Rapidly growing **Eco System**
  - **RISC-V Foundation**: More than 250 members in 28 countries

- **Secure system** complying **Kerckhoff's principle** based on the **RISC-V**

RISC-V: Free and Open RISC ISA

What's Different about RISC-V?

- ***Simple***
  - *Far smaller than other commercial ISAs*
- ***Clean-slate design***
  - *Clear separation between user and privileged ISA*
  - *Avoids μarchitecture or technology-dependent features*
- ***A modular ISA***
  - *Small standard base ISA*
  - *Multiple standard extensions*
- ***Designed for extensibility/specialization***
  - *Variable-length instruction encoding*
  - *Vast opcode space available for instruction-set extensions*
- ***Stable***
  - *Base and standard extensions are frozen*
  - *Additions via optional extensions, not new versions*

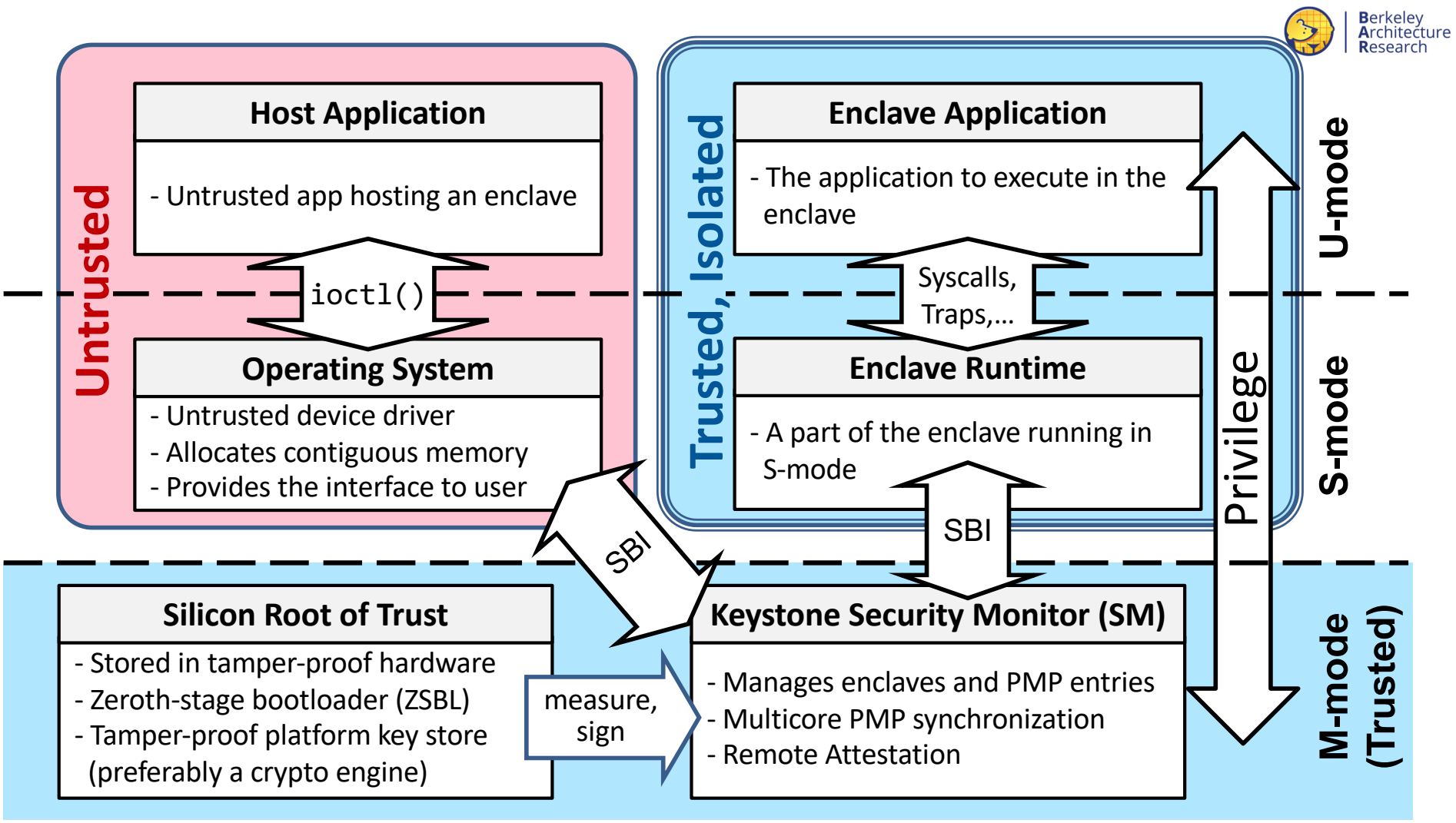
source) *https://content.riscv.org/wp-content/uploads/2018/12/Welcome-RISC-V-ISA-Foundation-Overview-Rick-OConnor.pdf*

RISC-V Foundation Members

- More than **250** members in 28 countries (as of May 2019)

source) https://content.riscv.org/wp-content/uploads/2019/06/RISC-V-Foundation-Calista-Redmond-06-18-2019.pdf

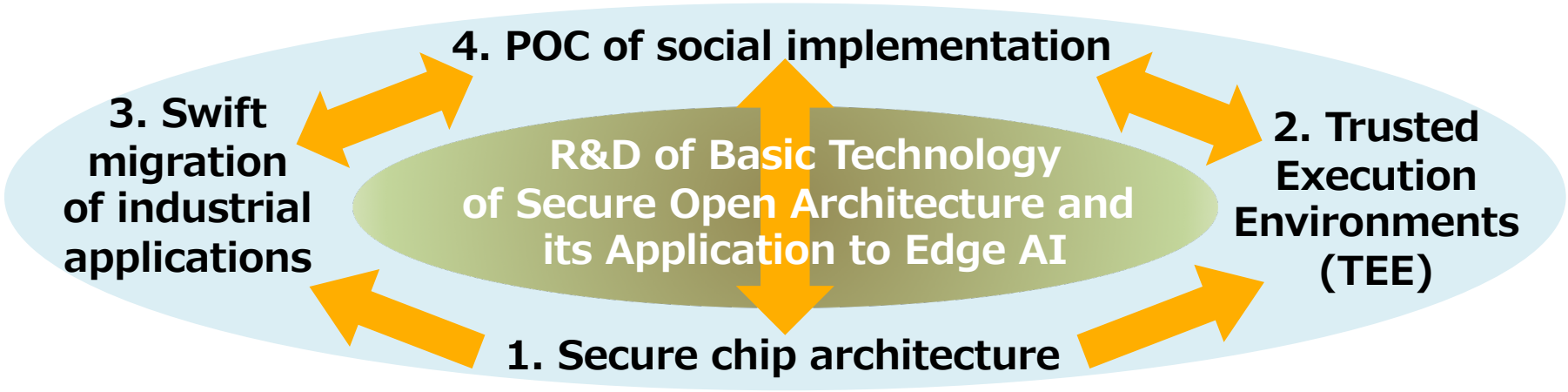
Keystone: A TEE on RISC-V



source) https://content.riscv.org/wp-content/uploads/2018/12/Keystone-Enclave-An-Open-Source-Secure-Enclave-for-RISC-V.pdf

NEDO Project Overview

- PJ theme & 4 sub-themes

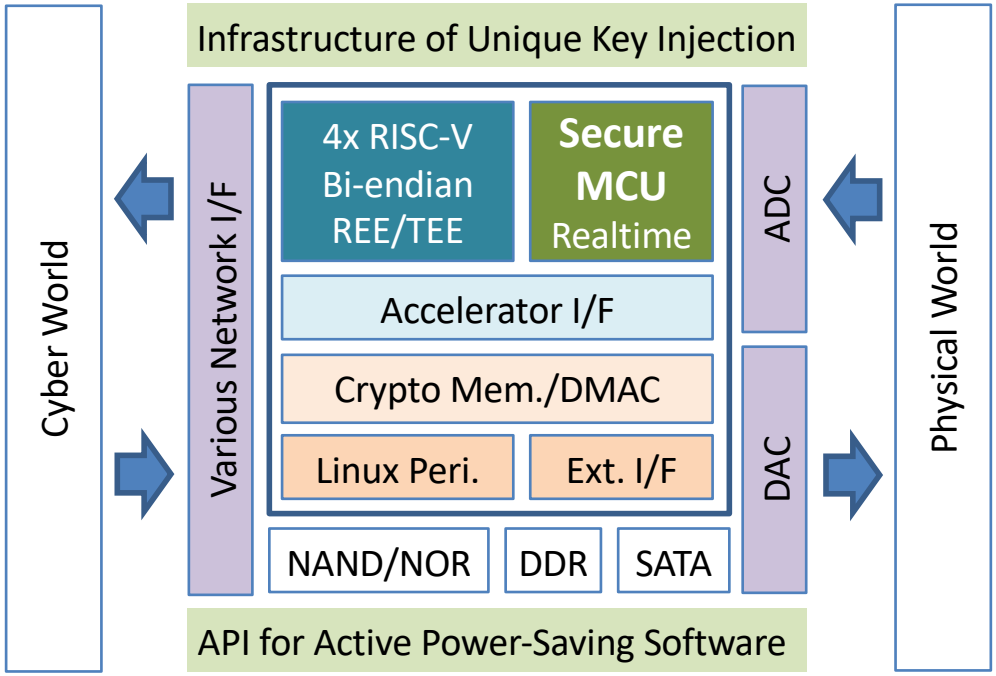


- PJ targets
  - **White box** approach of edge-AI devices for **security** throughout supply chains
  - Trusted execution environments (**TEE**) based on **RISC-V open architecture**
  - Architecture **extension** for swift migration of **industrial** applications
  - **Secure chip** architecture and efficient method to assign a **unique key** to each chip
  - **Management** technology of the unique keys for **services**
  - Proof of concept (**POC**) of social implementation with industrial use case of edge AI

- Commissioned members: AIST, Keio Univ., Hitachi
  Re-commissioned members: SECOM, SHC, UEC, Univ. of Tokyo

1. Secure chip architecture

- Targets
  - Developing **secure chip architecture** and providing it to sub-themes 2 to 4
  - Developing **secure MCU** based on **RISC-V** and basic **software stack**

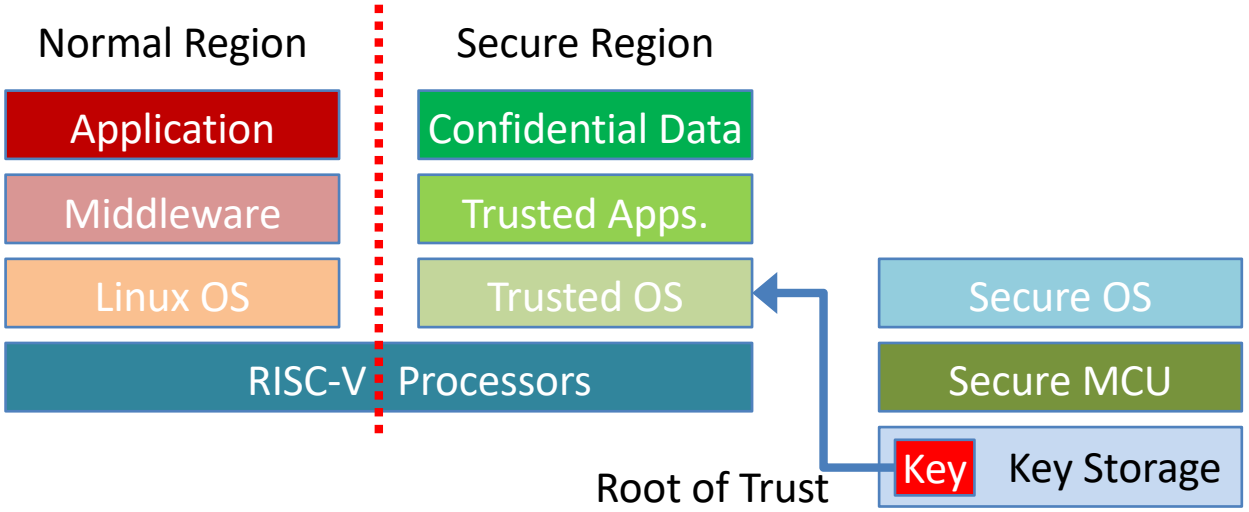


secure chip architecture

REE: Rich Execution Environment

2. Trusted execution environments (TEE)

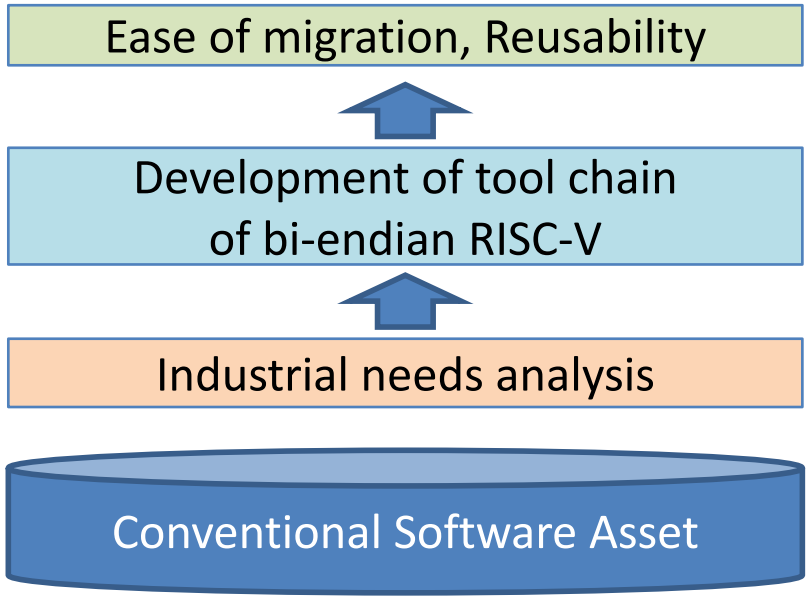
- Research Targets
  - **White box** implementation of TEE based on **RISC-V open architecture**
  - **Trusted OS** and **Trusted applications** for **industrial** use cases of edge AI
  - Providing TEE to sub-theme 4 (POC of social implementation)



Software Stack of Secure Edge-AI Devices

3. Swift migration of industrial applications

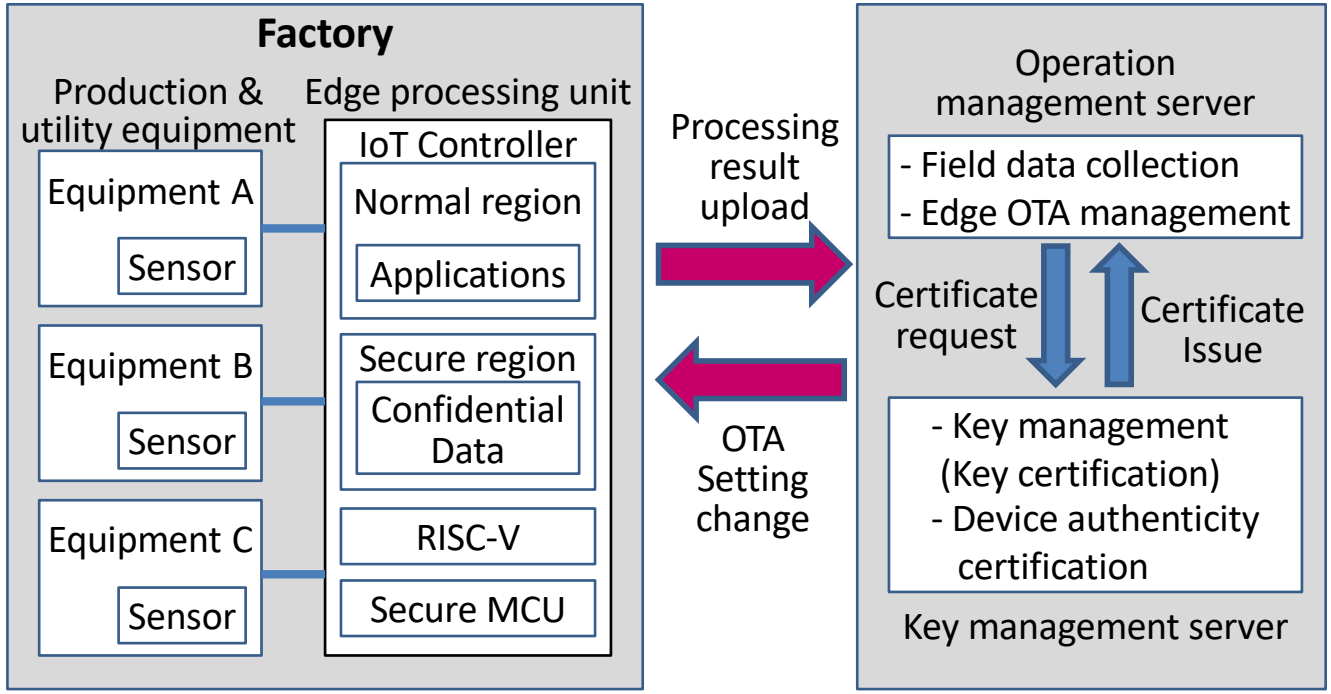
- Targets
  - Extension of RISC-V architecture and tool-chain from little-endian to **bi-endian**
  - Evaluation and Verification of Reuse Environment of Conventional Software Assets
  - Providing the extension to sub-theme 4 (POC of social implementation)



Development flow

4. POC of social implementation

- Targets
  - Field POC of Secure Industrial IoT
  - POC simulation of application life cycle of Secure Edge AI (Next slide)
  - Feedback to sub-themes 1 to 3

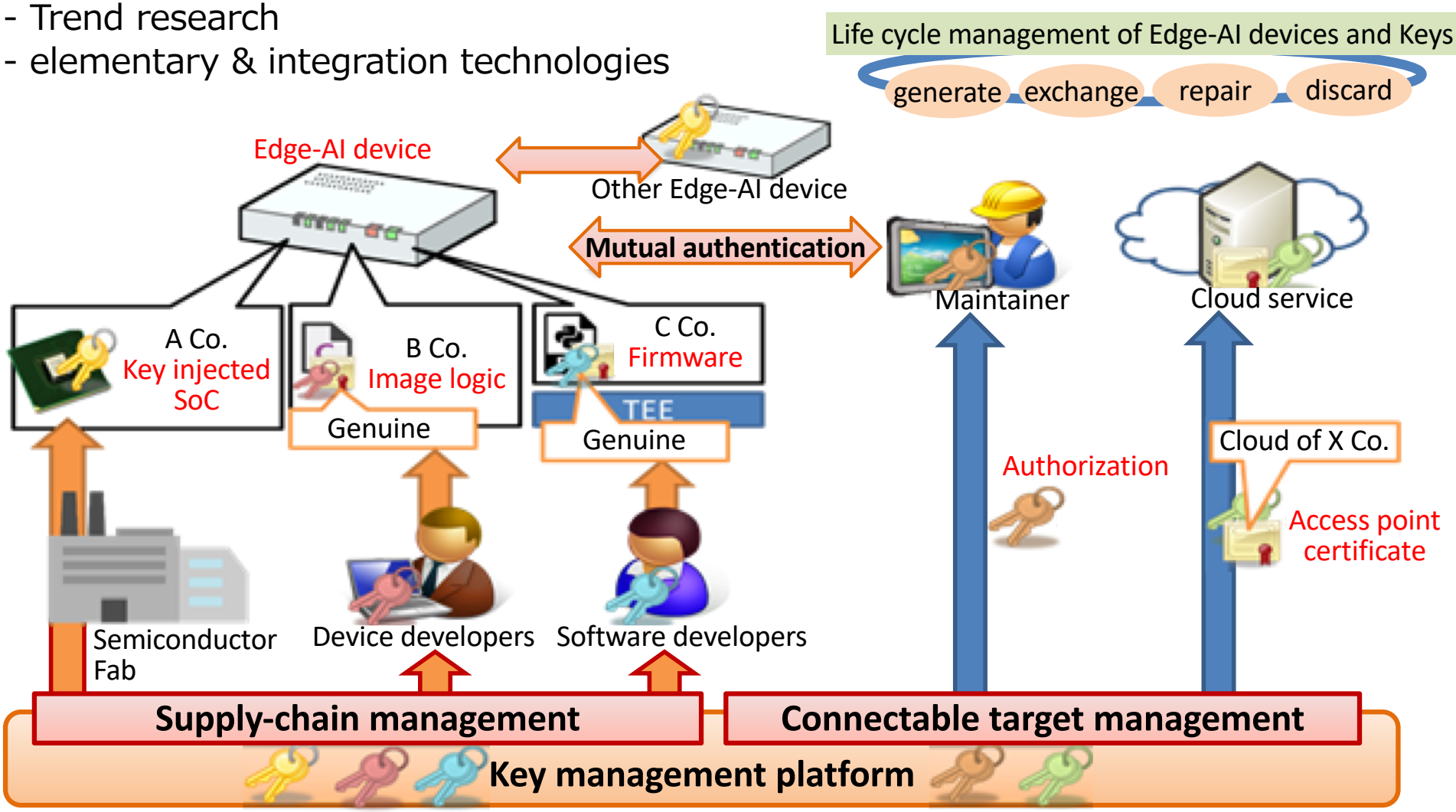


Rough image of secure factory IoT

Research and POC of supply chain of secure-chip-embedded products

4. POC of social implementation

- Trend research
- elementary & integration technologies



POC simulation of application life cycle of Secure Edge AI

Summary

- **Kerckhoff's Principle**
  - "The design of a system should not require **secrecy**."
- Current major systems are based on **proprietary** architecture (x86 or ARM)
- **RISC-V**
  - **Free** and **Open ISA**; **Open** or Proprietary Implementation
  - Rapidly growing **Eco System**; More than **250** Members of **RISC-V Foundation**
- NEDO Project
  - Developing the **TEE** and **secure MCU** with the **RISC-V**
  - **Bi-endian** support for swift migration of industrial applications
  - **POC** of social implementation with **Secure chip** architecture

Acknowledgement

- This presentation is based on results obtained from a project commissioned by the New Energy and Industrial Technology Development Organization (NEDO).

Thank you !!