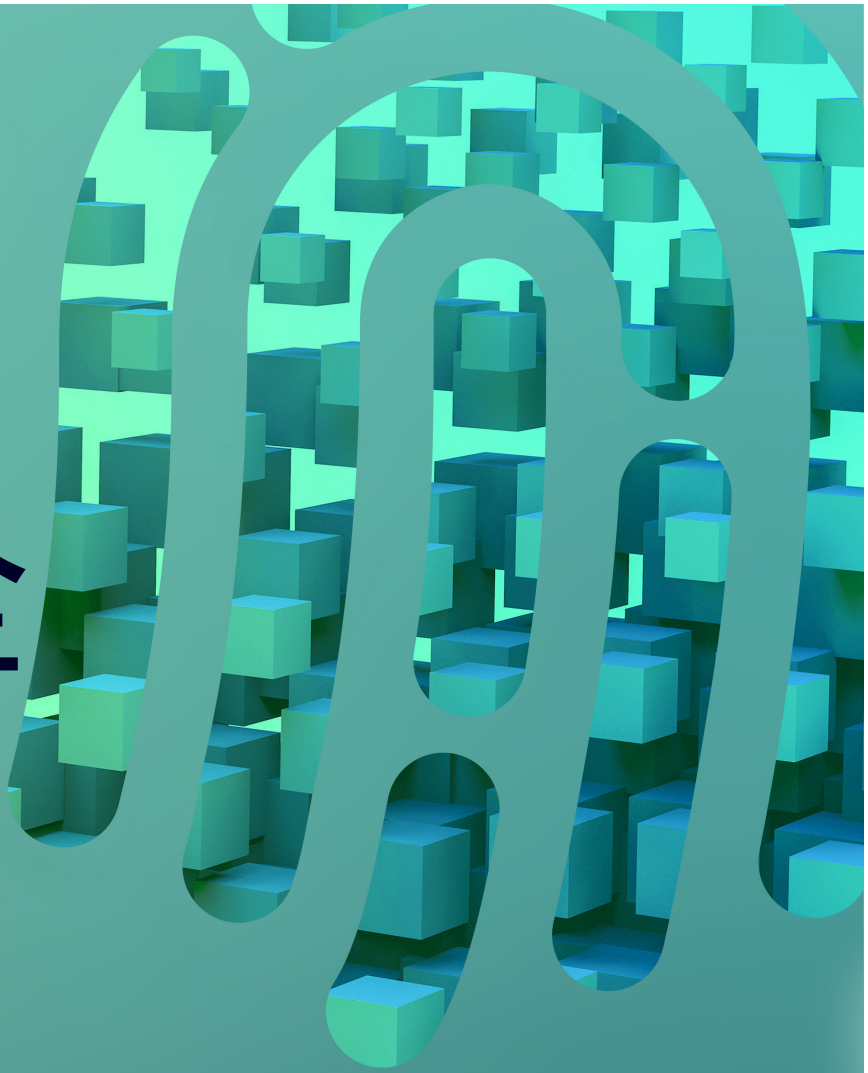
开源嵌入式安全

苏宝成 | SIEMENS DI FA



SIEMENS

目录

综述

In a glance

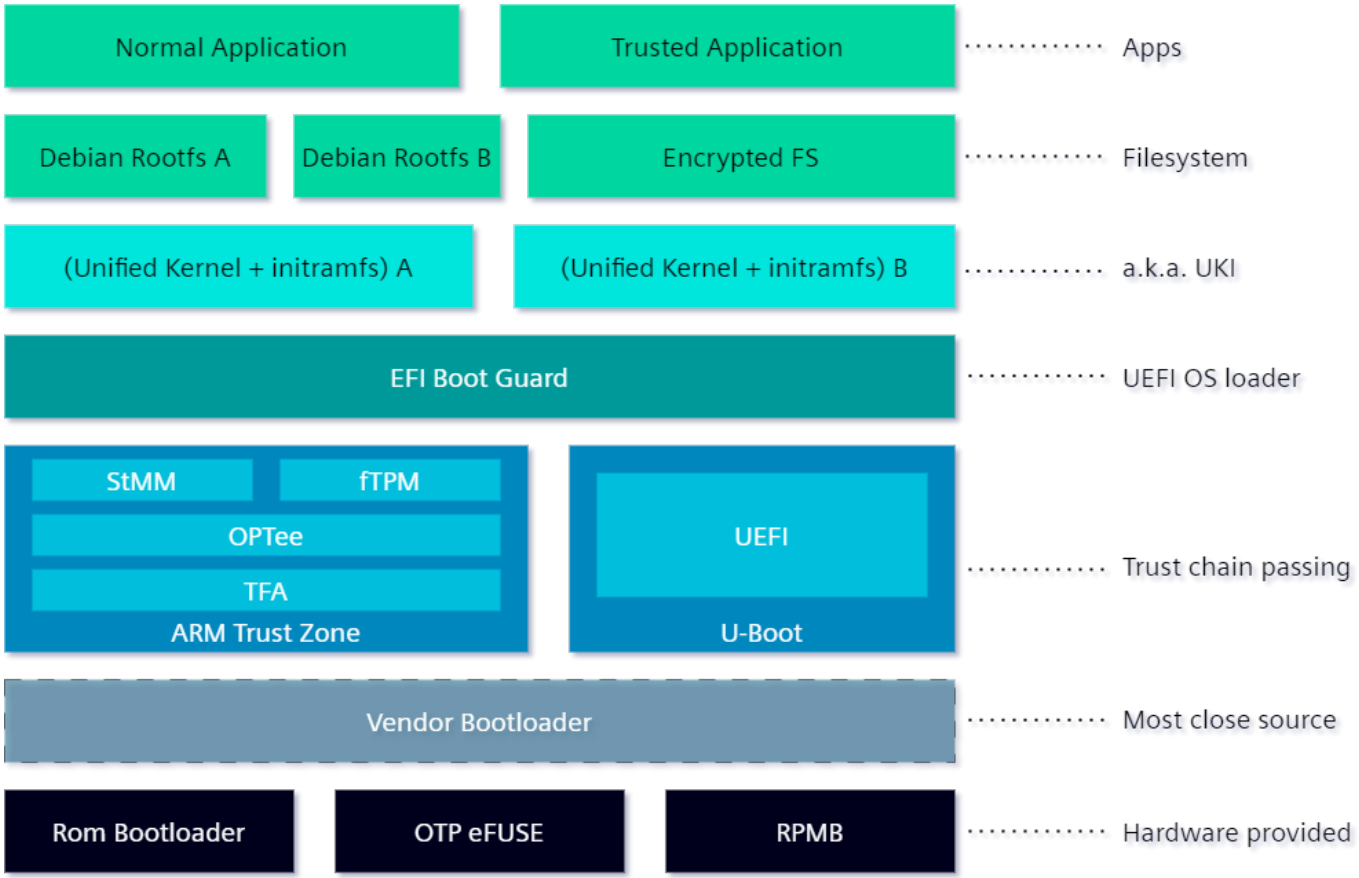
SIEMENS

赛博安全在（工业）嵌入式世界变得越来越重要

Cyber Security is becoming more and more important in industrial embedded world

SIEMENS

通用安全启动
Generic Secure Boot



SIEMENS

安全锚点

Security Anchor

SIEMENS

信任根
Root of Trust

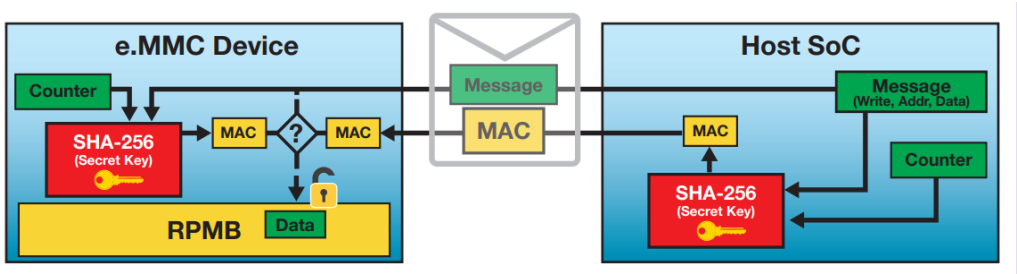
ROM 启动器 Bootloader

- 芯片厂商预先编程
- 固化到芯片内部，无法修改
- 加载和验签第一级bootloader
- **One Time Programming eFUSE 一次编程电子熔丝**
- 固化在芯片内部，外部无法接触
- 在工厂编程
- 一次编程，一旦编程无法修改
- 小容量
- 一般用于存储公钥的哈希

SIEMENS

EMMC的RPMB分区
RPMB of eMMC

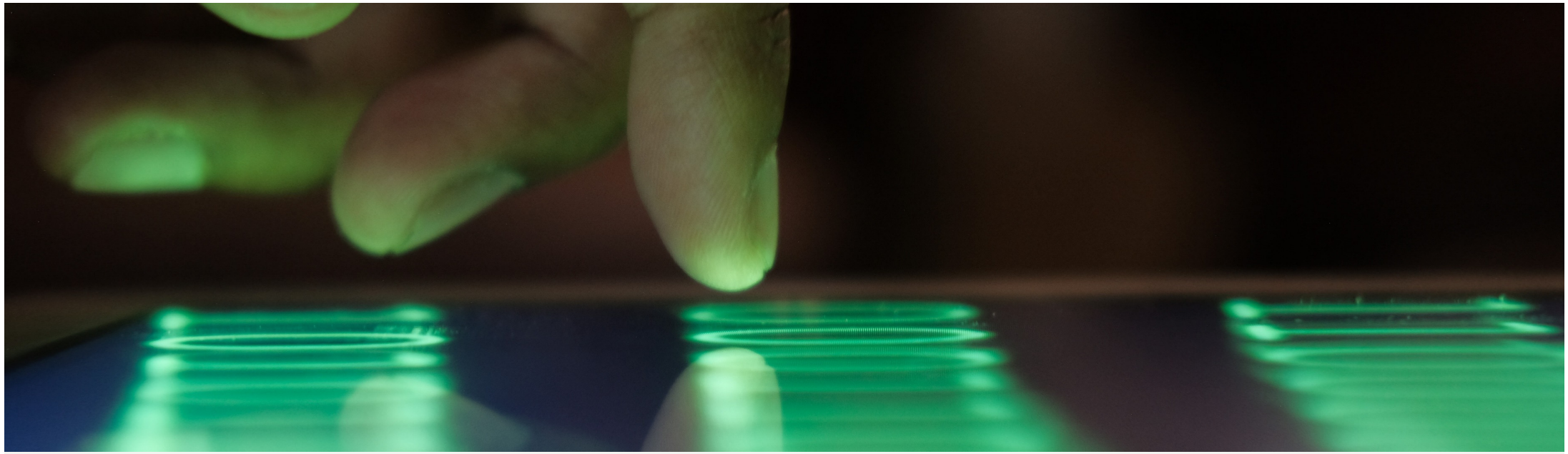
- 防篡改 – 任何写请求都需要对称加密密钥的参与
- 重放攻击保护 – a unique counter is included in each writing



典型用例: 可信执行环境TEE的安全可信任存储

1 Diagram is from https://documents.westerndigital.com/content/dam/doc-library/en_us/assets/public/western-digital/collateral/white-paper/white-paper-emmc-security.pdf

SIEMENS

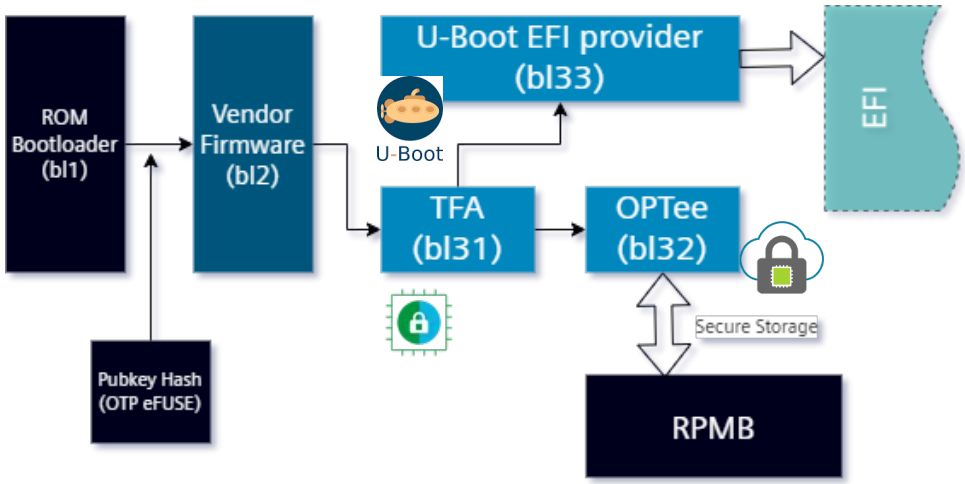


通用安全启动流程

Generic Secure Boot Flow

SIEMENS

ROM Bootloader 之后…
Just after the ROM Bootloader



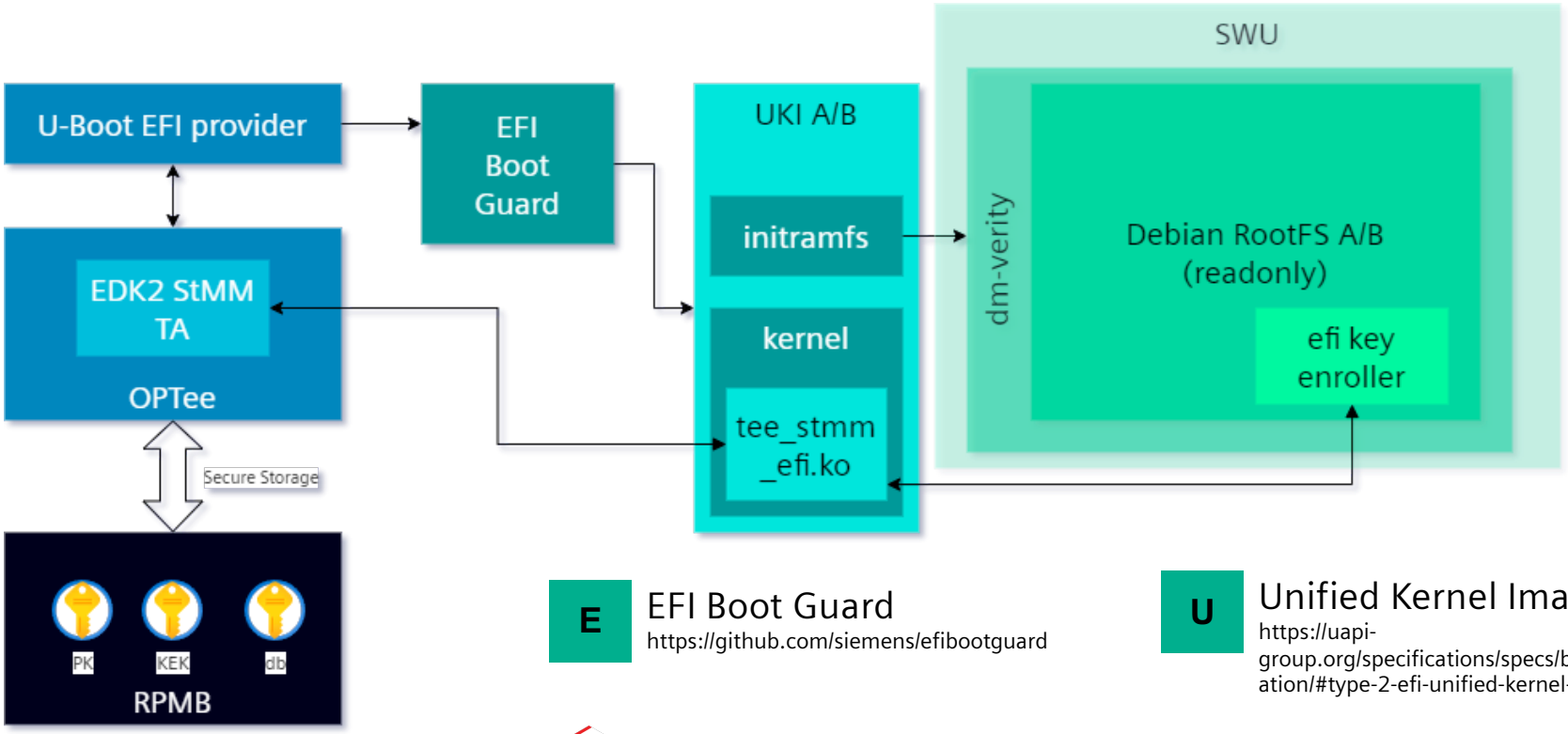
Trusted Firmware ARM
git.trustedfirmware.org/TF-A/trusted-firmware-a.git

OPTee-OS
https://github.com/OP-TEE/optee_os

Das U-Boot
https://source.denx.de/u-boot/u-boot.git

SIEMENS

UEFI 安全启动
UEFI Secure Boot



E EFI Boot Guard
https://github.com/siemens/efibootguard

U Unified Kernel Image
https://uapi-group.org/specifications/specs/boot_loader_specification/#type-2-efi-unified-kernel-images

EDK2 StMM
https://github.com/tianocore/edk2/tree/master/StandaloneMmPkg

SWUpdate
https://github.com/sbabic/swupdate

SIEMENS

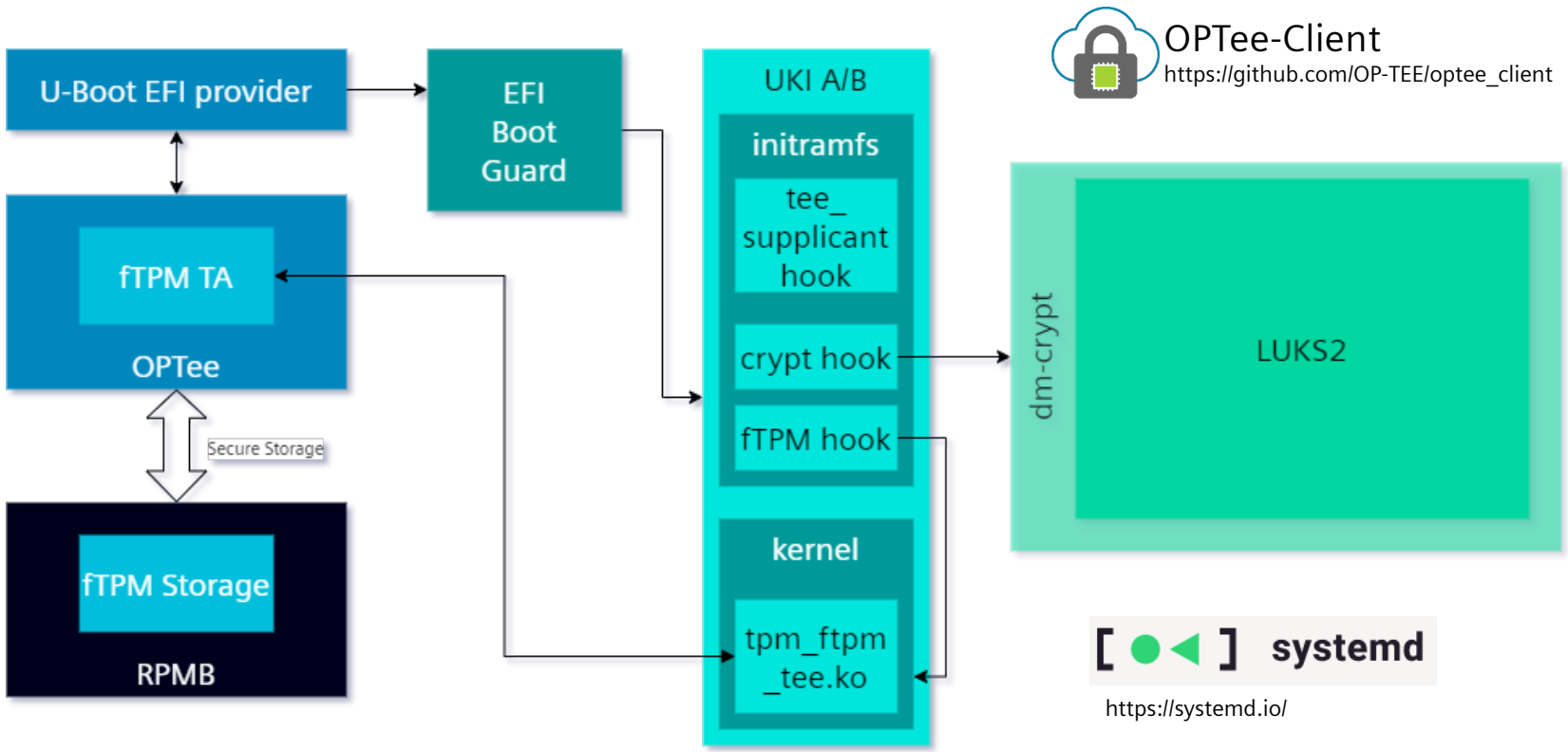
固件TPM
Firmware TPM

Official Complete TPM 2.0 Reference Implementation (by Microsoft)

- Provide a TEE Trusted application
- Use RPMB as the secure storage
- No hardware chips required -> cost efficient
- Upgradable

https://github.com/microsoft/ms-tpm-20-ref

磁盘加密
Disk Encryption – Protect Data-at-rest



SIEMENS

集成

Integration

SIEMENS

ISAR
Integration System for Automated Root filesystem generation

Isar is a set of scripts for building software packages and repeatable generation of Debian-based root filesystems with customizations

Integrated components:

- trusted-firmware-a
- optee-os & optee-ftpm & optee-client
- u-boot & kernel customization base
- initramfs-tee-ftpm-hook
- initramfs-tee-supplicant-hook, etc.

https://github.com/ilbers/isar

isar-cip-core

ISAR layer to provide CIP Core (Generic Profile) package set

Responsible for developing, testing and maintaining tools to generate CIP Core reference file system images

Integrated components:

- edk2-standalonemm-rpmb
- efibootguard
- swupdate
- initramfs-crypt-hook, initramfs-verity-hook, etc.

https://www.cip-project.org/
https://gitlab.com/cip-project/cip-core/isar-cip-core

示例

Example

SIEMENS

Example: SIMATIC IOT2050 & meta-iot2050

连接数字化世界 – 支持工业边缘计算和云连接的智能网关。

Meta-iot2050: ISAR layer contains recipes, configuration and other artifacts that are specific to Debian-based IOT2050 product.

- ./kas-container build kas-iot2050-boot-pg2.yml:kas/opt/secure-boot.yml
- ./kas-container build kas-iot2050-swupdate.yml:kas/opt/secure-boot.yml

https://github.com/siemens/meta-iot2050

SIEMENS

Contact

Su Bao Cheng

Siemens DI FA

E-mail baocheng.su@siemens.com

SIEMENS