CCP Secure-Boot Feature

What it is and how it is implemented
Open Source @ Siemens

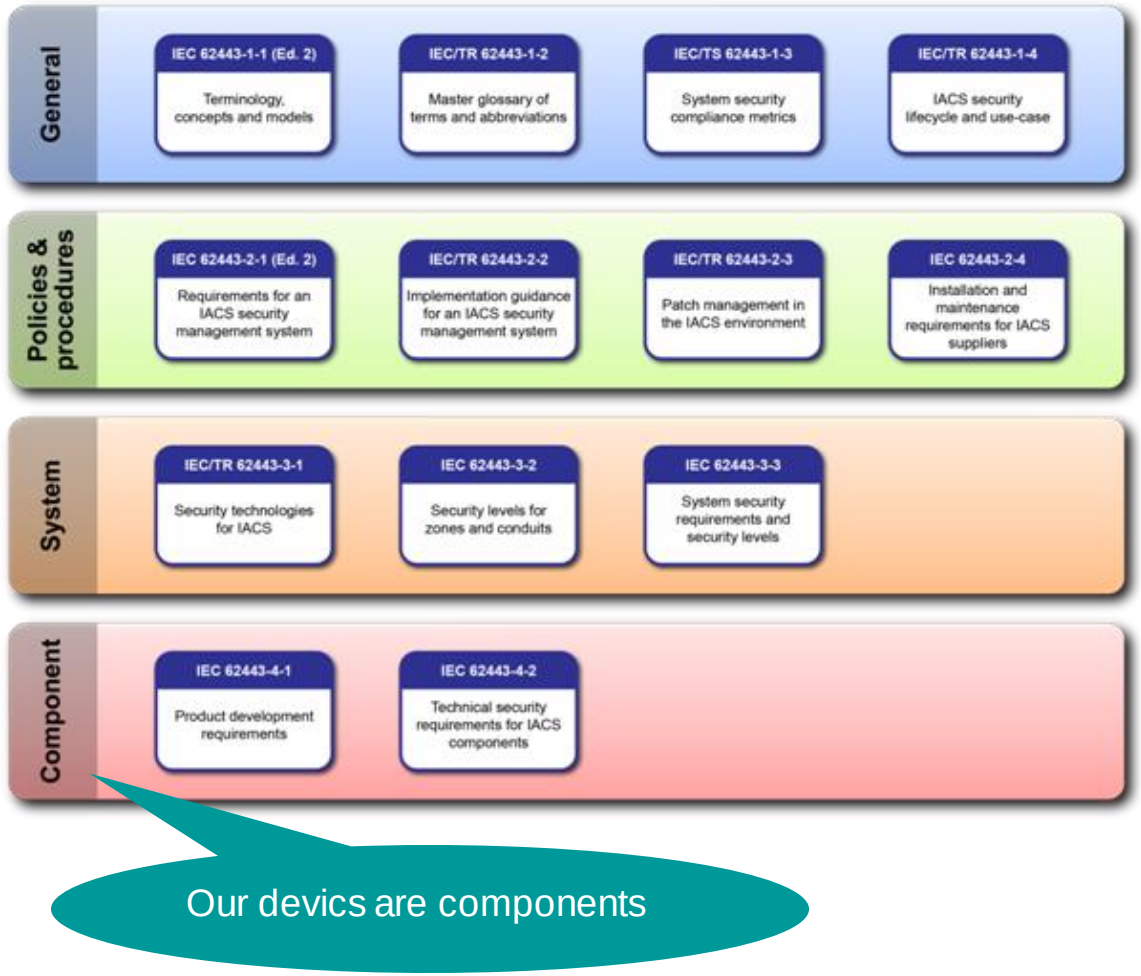
SIEMENS

Introduction
Secure-Boot

- Siemens is a **Charter of Trust** member
- **IEC 62443** is a series of standards for Industrial Automation and Control Systems (IACS)
- We have chosen **IEC 62443** as appropriate for our products in SI. The goal is to provide **capabilities** for **SL2** and possibly **SL3**

- Secure-Boot is an important security component and is mandatory for SL3 and in discussion for SL2

- Secure-Boot makes sure that our devices:
  - Only run software from Siemens SI (origin)
  - The software not modified (integrity)
  - It is verified at each time the device boots



SIEMENS

Secure-Boot
Trust Anchor and Chain of Trust

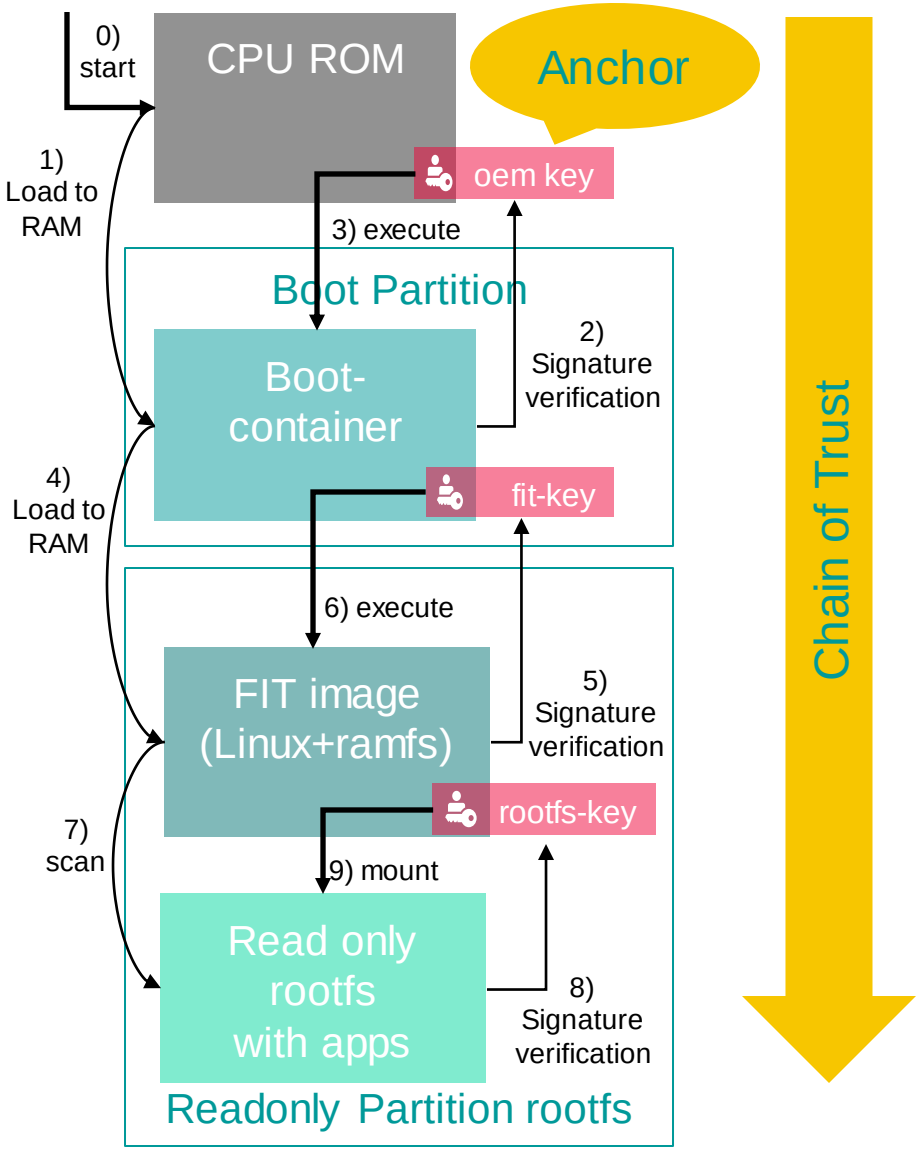
Secure-Boot needs hardware (HW) support.

The trust anchor (key) must be part of the HW.

The system only executes signed software.

At system boot:

- Boot has multiple steps starting in CPU ROM
- In each step software is loaded and verified
- Verification works with public keys and digital signatures
- The next step is executed when the verification was successful; otherwise reboot



https://ccp.code.siemens.io/meta-siemens/device-security/hw-security/

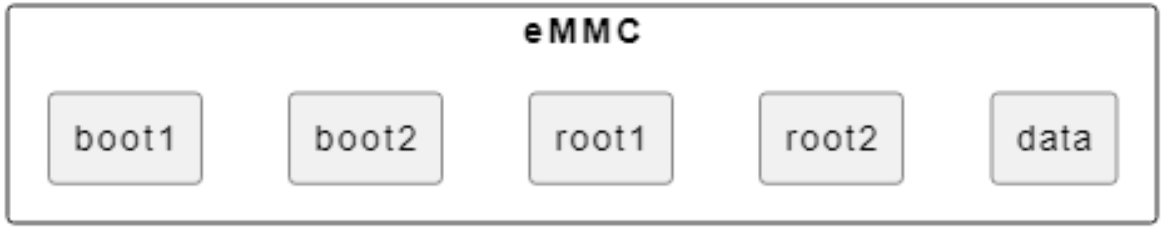
SIEMENS

Common controller platform
Capricorn module

Capricorn modules offer a secure-boot option using eFuses. (NXP i.MX8X)
The “oem-keys” are burned in the factory (eFuse) and cannot be changed anymore.
All other keys can be changed later in the field by software-update.

item	**key name**	**algorithms**
boot-container	oem-key	ec521+sha512
fitImage	fit-key	rsa2048+sha256
root-fs	rootfs-key	ec521+sha256
swupdate	*swu-key*	*ec521+sha256*

For redundancy there are two boot partitions and two root partitions on the eMMC. The current secure-boot setup is compatible with the existing Capricorn eMMC partitioning schema.



SIEMENS

Development and Release signing

Development

- For developers, each image is signed with the developer keys in the CI pipeline.
- These keys are less secure because of the exposure in the CI pipeline.
- Only **developer devices** accept these images.
- We want to test Secure-Boot already during development.
- Development images cannot be installed in the field.

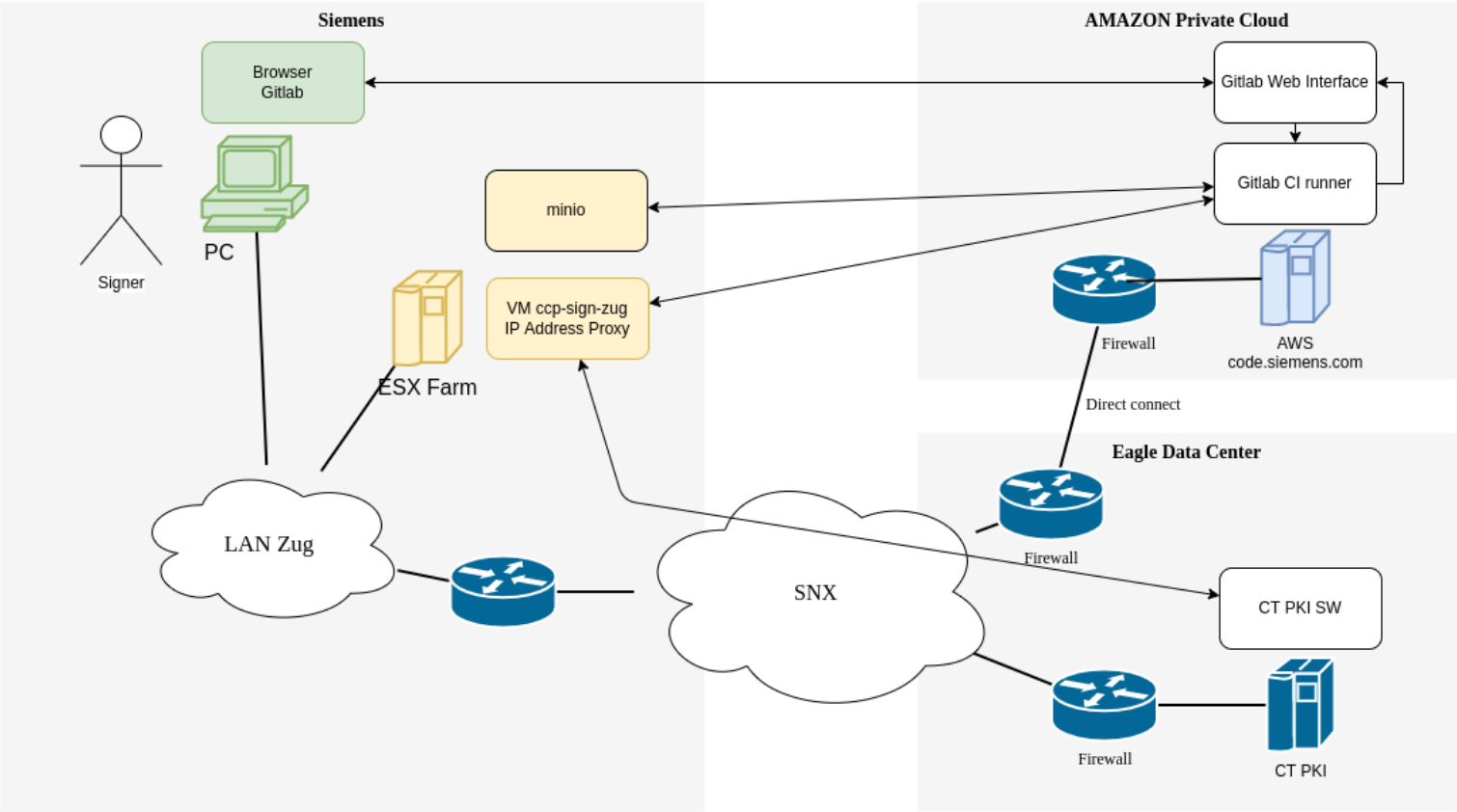
Release

- Official image are signed with the release keys.
- The private keys are stored on the Product-PKI.
- **Field devices** (that we sell) only accept images signed with release keys.
- We have established a CI pipeline to replace all signatures in a development image with production signatures.
- The Capricorn module can store 4 keys in eFuses. We can **revoke** up to 3 keys if necessary.
- The factory must **lock the eFuses**.

Debugging in the field with Secure-Boot may become more complicated!

SIEMENS

Production signing for FS30i using Product PKI (PPKI)



Why PPKI?

- Well protected keys (ACP 3-3-3)

Why re-sign an existing image?

- Only the signatures are replaced; everything else remains **binary equal**
- System test can be made with developer images
- Only well tested images shall be signed with the release key
- Only few people are authorized for signing with the release key

SIEMENS

Secure-Boot and Open-Source

We use Yocto Linux on our controllers.

- Secure-boot locks down a device
- Standards like IEC62443 require secure-boot on a certain level and we need it to pass certification
- Open-Source enthusiasts do not like locked devices
- Be careful when choosing components, avoid licenses like GPLv3

Customers are increasingly security aware. We do not expect complaints on secure-boot.

Controller

- We use the mechanism provided by the chip vendor for the trust anchor
- eFuses are integrated in U-Boot
- Only the boot-container uses closed source blobs
- All other steps are implemented with open-source components

Signing pipeline

- PPKI uses commercial HW and SW
- PPKI has a hardware security module
- Pipeline is on GitLab using open-source components
- We modified tools to interface with the PPKI

Secure-Boot summary

- All products that are using CCP **Capricorn** modules can use Secure-Boot if desired.
- **FS30i**, a fire detection system, is our first product featuring Secure-Boot.
- Competition is offering products with Secure-Boot too.
- More of our products are considered.
- The new Aries modules will offer Secure-Boot.

We underestimated the complexity of Secure-Boot

- Integration into build scripts
- Hardening
- Adaption of external tools to PPKI
- eMMC partitions backwards compatible

In the future vendor specific secure-boot may be replaced with standard mechanism like TPM or fTPM.

CCP is ready for Secure-Boot! Are you?

SIEMENS

Contact

Published by Siemens 2023

Walter Schweizer
Common Controller Platform security architect, PSSE
SI BP R&D ZG FW CCP
Theilerstrasse 1a
6300 Zug
Switzerland

E-mail walter.schweizer@siemens.com

SIEMENS