SIEMENS
Ingenuity for life

CIP @ Siemens Mobility
Use Cases

Siemens Mobility – Mobility Management

Benjamin Schilling, Yasin Demirci, October 2019

Agenda

SIEMENS
Ingenuity for life

1. Harmonization use case
Replacement of old Linux kernel versions

2. Maintenance use case
Benefit from long-term maintained Debian packages

3. Security use case
Create a common platform for IEC 62443 SL-3 ready products

4.-6 Security challenges
IEC 62443 SL-3 challenges and their OSS solutions

SIEMENS
Ingenuity for life

1. Harmonization use case

Replacement of old Linux kernel versions

1. Harmonization use case
Replacement of old Linux kernel versions

SIEMENS
Ingenuity for life

Rail automation specifics

- Long product life-times (20 to 30 years)
- Patching of products is not easy
- Requires safety assessment & certification
- Access to devices is difficult (e.g. no remote access)

Numerous Linux kernel versions in product portfolio

- Hard to maintain
- Even harder to keep up with vulnerability management

Solution: reduction of Linux kernel variants

- Using CIP kernel as basis for product portfolio

SIEMENS
Ingenuity for life

2. Maintenance use case

Benefit from long-term maintained Debian packages

2. Maintenance use case
Benefit from long-term maintained Debian packages

SIEMENS
Ingenuity for life

Benefits of Debian

- Packages come preconfigured (lower effort for integration, compared to „make …“)
- Easier management of Open Source Software (license compliance, vulnerability management, …)
- Reduced build times through ISAR using binary packages
- Covers all required CPU architectures

Requirement from a rail automation customer

- “The used Linux distribution shall be Debian for cybersecurity reasons”

CIP Core

- Efforts for Debian LTS maintenance are a perfect fit for this use case

3. Security use case

Create a common platform for IEC 62443 SL-3 ready products

3. Security use case
Create a common platform for IEC 62443 SL-3 ready products

SIEMENS
Ingenuity for life

CIP Security WG

- Participate in the CIP Security working group
- Provide guidelines for IEC 62443 compliance for products using the CIP

Siemens Mobility OSS contributions

- Contribute security building blocks to OSS community
- Peer review increases security
  - Security by obscurity never works!
- Increase supported hardware
- Possible increase of features through collaboration
- Increase the overall security for the industrial automation domain

SIEMENS
Ingenuity for life

4. IEC 62443 SL-3 Challenge

Certificate enrollment in closed networks

4. Challenges
Certificate enrollment in closed networks

SIEMENS
Ingenuity for life

IEC 62443 requirement for SL-3

- When a Public Key Infrastructure is used, the device shall integrate into a system which ensures that certificates are enrolled securely.

Current situation

- Most rail automation products don't use certificates
- If certificates are used they are typically self-signed
- Typically no integration with PKI possible

4. Solution
Use the Certificate Management Protocol (CMP)

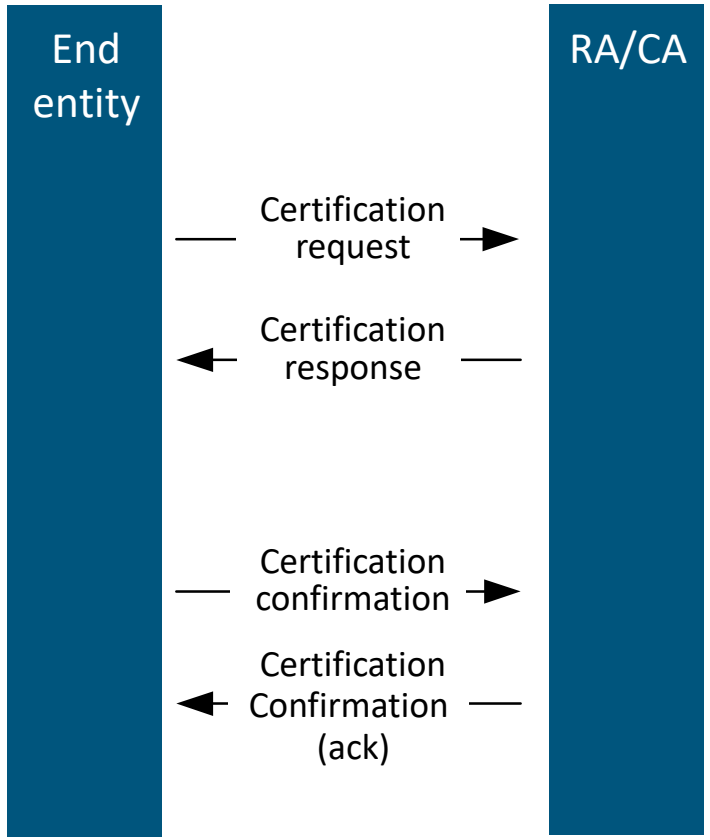
SIEMENS
Ingenuity for life

Certificate Management Protocol

- Specified in RFC4210
- Allows to enroll, renew and revoke certificates
- Can be used to distribute CRLs
- Key material is generated on the device only
- Already used in the rail automation domain (UNISIG 137 standard)

Flexible support of transport protocols

- Message exchange can be done via various protocols
- Plain TCP
- HTTP
- Using files (e.g. SCP, usb drive, …)



4. Solution
Use the Certificate Management Protocol (CMP)

SIEMENS
Ingenuity for life

Noteworthy Implementations

CMPforOpenSSL (https://github.com/mpeylo/cmpossl)

- Initially started by Nokia, Siemens joined several years ago
- Already integrated in many industrial products
- Integrated in upcoming openSSL 3.0

CMP in memory constrained environments

- mbedCMP (https://github.com/siemens/mbedCMP)
- CMPclient-embedded-lib (https://github.com/nokia/CMPclient-embedded-lib)

For less constrained environments

- Bouncy Castle (https://www.bouncycastle.org/)

SIEMENS
Ingenuity for life

5. IEC 62443 SL-3 Challenge

OSS has to access credentials in a secure way

5. Challenge
OSS has to access credentials in a secure way

SIEMENS
Ingenuity for life

IEC 62443 requirement for SL-3

- Credentials which are used by the component shall be protected by hardware means

Typical OSS components load credentials from files

- Usually the password for the private key is stored in plain text in a configuration file

Many available hardware key store implementations

- Different functionality
- Different software interfaces

5. Solution
The Trust Anchor API

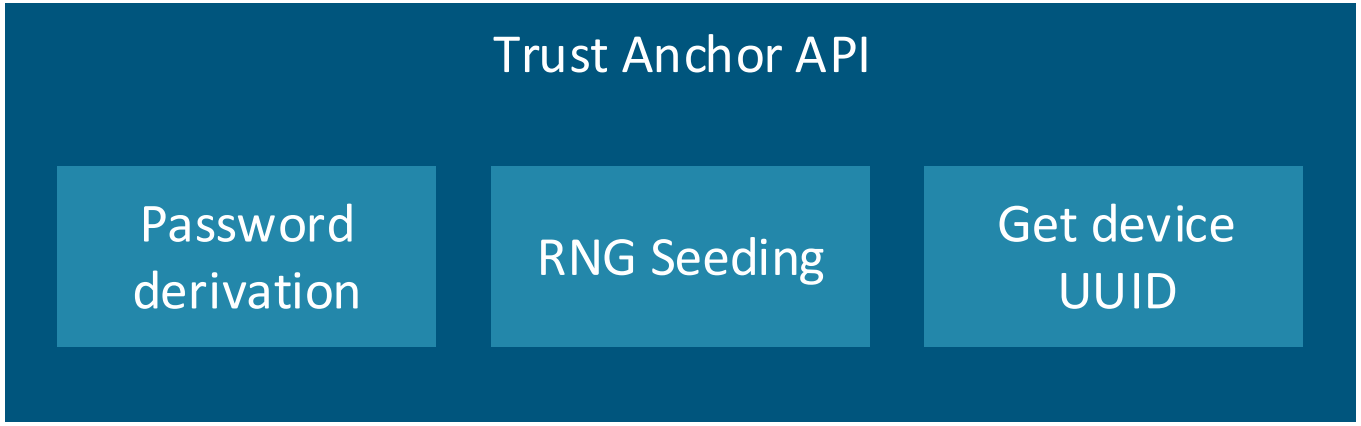
SIEMENS
Ingenuity for life

Trust Anchor functionality

- Derive individual passwords for each device
- Seed the random number generator (esp. for devices with low entropy)
- Get an UUID identifying the device

Derive hardware-specific passwords

- Allows applications to use these passwords to protect its credentials
- E.g. by an OpenSSL engine



5. Solution
The Trust Anchor API

SIEMENS
Ingenuity for life

Bound to the hardware

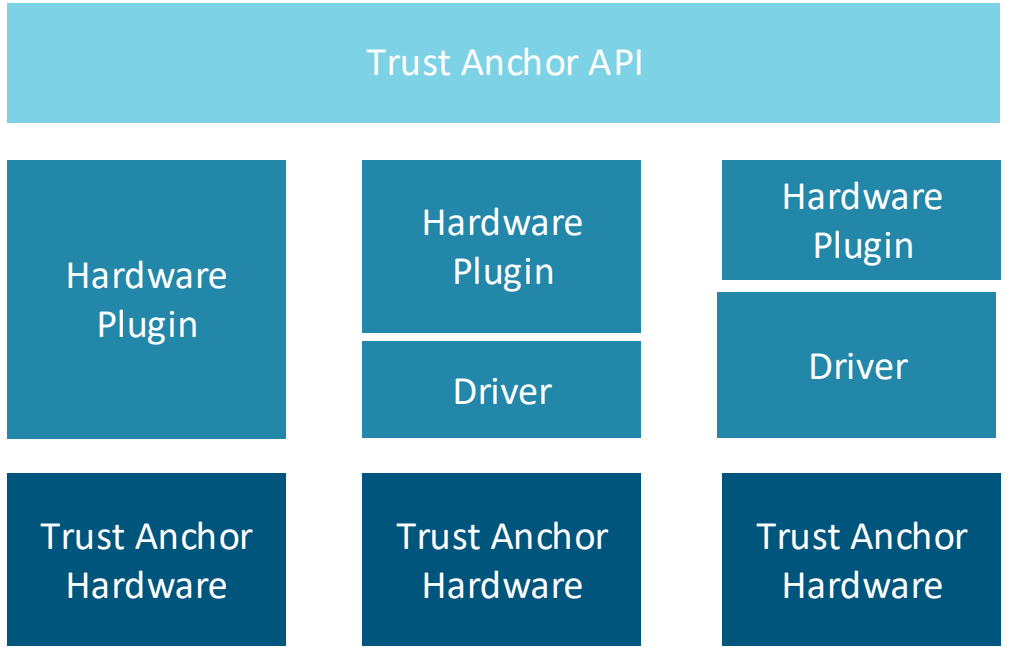
- Requires live OS access to get the password
- Reading the flash/stealing the HDD does not reveal the credentials

Designed for embedded systems

- Limited feature set allows to use various kinds of embedded hardware (no TPM required)

Plugin architecture

- Hardware specific implementation of the trust anchor can be loaded as a plugin
- Allows hardware manufacturers to implement hardware access (driver / hardware plugin)
- No changes in applications required for different hardware



SIEMENS
Ingenuity for life

6. IEC 62443 SL-3 Challenge

Securely boot x86 devices

6. Challenge
Securely boot x86 systems

SIEMENS
Ingenuity for life

IEC 62443 requirement for SL-3

- The products manufacturers root of trust shall be used to verify the boot process.

Root of trust

- For x86 UEFI devices the manufacturer root of trust has to be installed in the UEFI

Dual boot

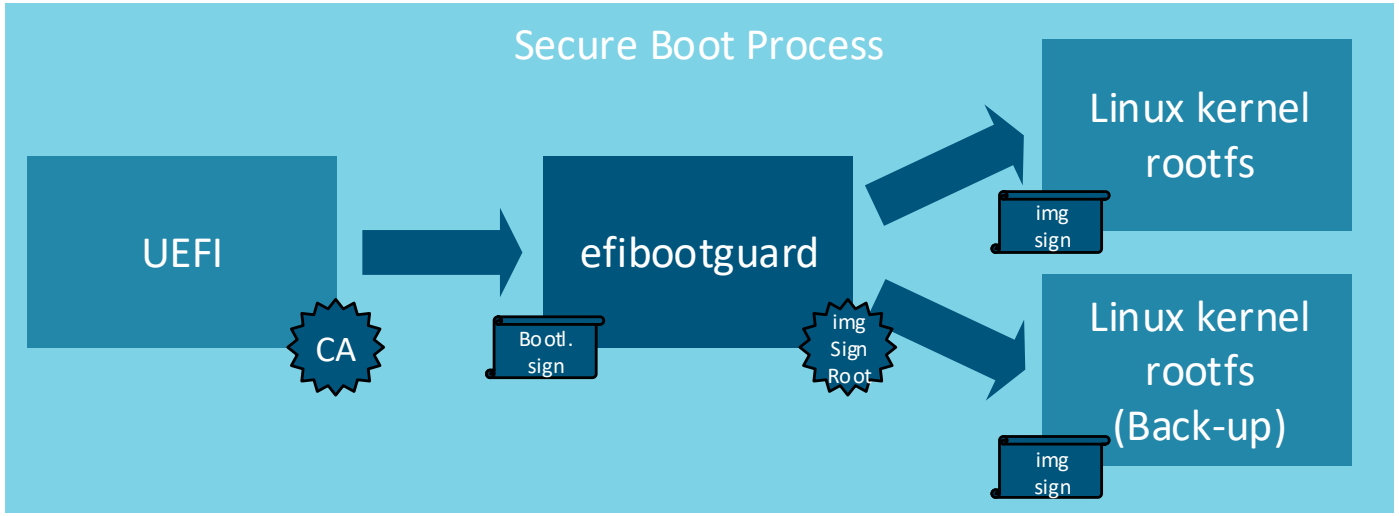
- A/B partition scheme required for reliable remote software update

6. Solution
Use efibootguard

SIEMENS
Ingenuity for life

Open Source UEFI Bootloader

- https://github.com/siemens/efibootguard
- GPL-2
- Already supports swupdate for A/B partition update
- UEFI Secure Boot support planned for Q3/2020



Possible scheme for Secure Boot implementation, final solution t.b.d.

Outlook: Siemens Mobility OSS Projects

SIEMENS
Ingenuity for life

New projects

Trust Anchor API

Target: Q2/20

Sponsorship

CMPforOpenSSL/openSSL 3.0

Target: Q1/20

efibootguard – Secure Boot

Target: Q3/20

ISAR

Continuous

A lot of space for upcoming contributions!

SIEMENS
Ingenuity for life

Stay safe and secure

Contact
Benjamin Schilling
schilling.benjamin@siemens.com

Contact
Yasin Demirci
yasin.demirci@siemens.com