Keyfactor Tech Days 2023

Public Key and Signature Infrastructure for Industrial Security

Dr. Lutz Jänicke

Corporate Product & Solution Security Officer

Phoenix Contact GmbH & Co. KG

Dr. Lutz Jänicke – Corporate Product & Solution Security Officer

- 2002-2015 Innominate Security Technologies AG (now: Phoenix Contact Cyber Security GmbH)
  - CTO; IT Security Manager
- 2016- Corporate Product & Solution Security Officer
  - Phoenix Contact Group/Digital Processes & Solutions

- Plattform Industrie 4.0
  - WG Security of networked systems; SWG Secure Communication for Industrie 4.0
- DKE
  - UK 931.1 IT-Sicherheit in der Automatisierungstechnik (→ IEC 62443)
  - TBKON Cybersecurity; TBINK AK „Safety & Security“
  - Advisory Board CERT@VDE
- ZVEI
  - WG Cybersecurity; WG Industrial Security
- VDMA
  - WG Cybersecurity, WG Secure Remote Maintenance

PHOENIX CONTACT
INSPIRING INNOVATIONS

Some Context…

Continuous growth together

Company headquarters and competence centers

Headquarters
Blomberg | Germany

Continuous growth together

Company headquarters and competence centers

Group Center of Competence
Harrisburg | USA

Innovation Center Electronics
Bad Pyrmont | Germany

Group Center of Competence
Nanjing | China

Over
100,000
innovative
products

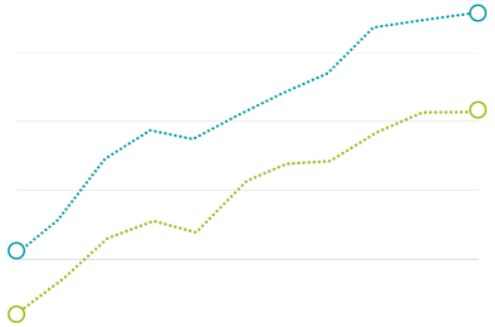
People and markets

Continuous growth together

2007

1.0
Billion sales

6,800
Employees worldwide



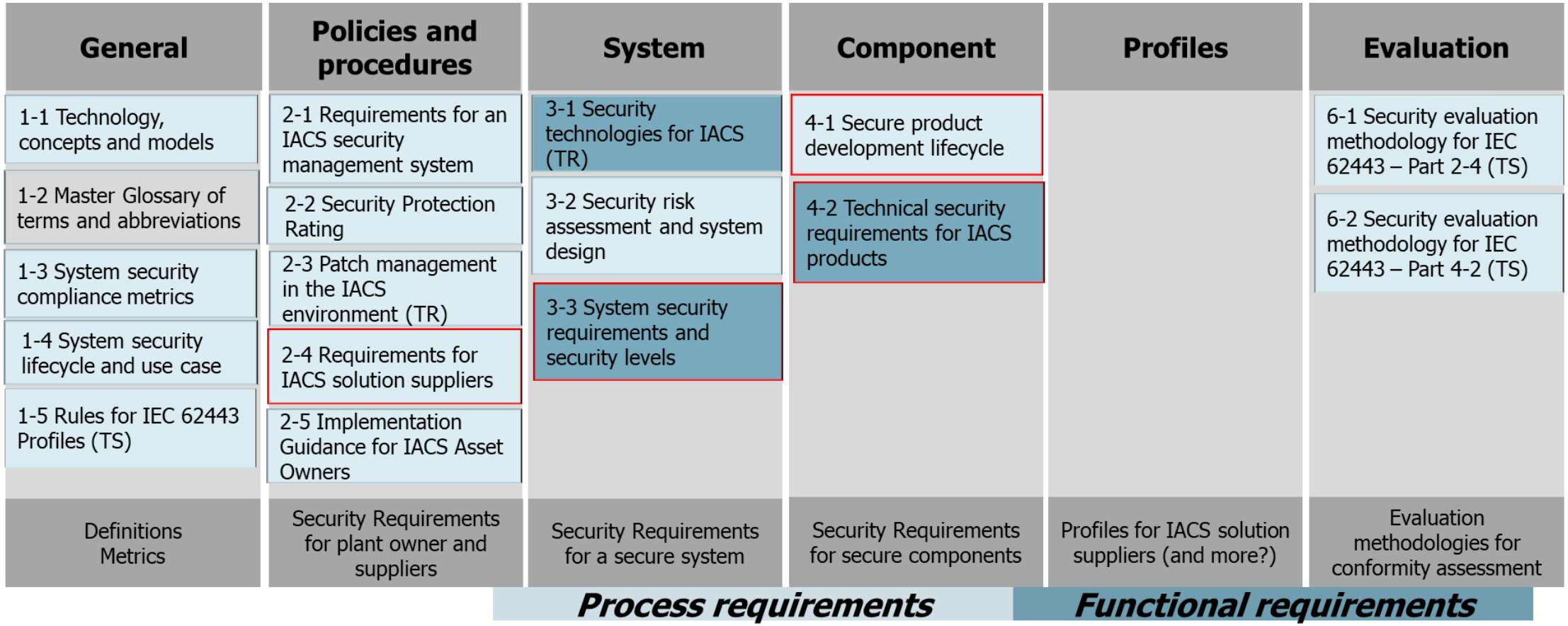
3.6
Billion sales

22,000
Employees worldwide

2022

Industrial Security with IEC 62443

Covering the complete topic of industrial security



Industrial Security with IEC 62443

Requirements for Components

-4-1: SM-7: Development environment security

-4-1: SM-8: Controls for private keys

-4-1: SUM-4: Security update delivery

-4-2: CR 1.8 – Public key infrastructure certificates

-4-2: CR 1.9 – Strength of public key-based authentication

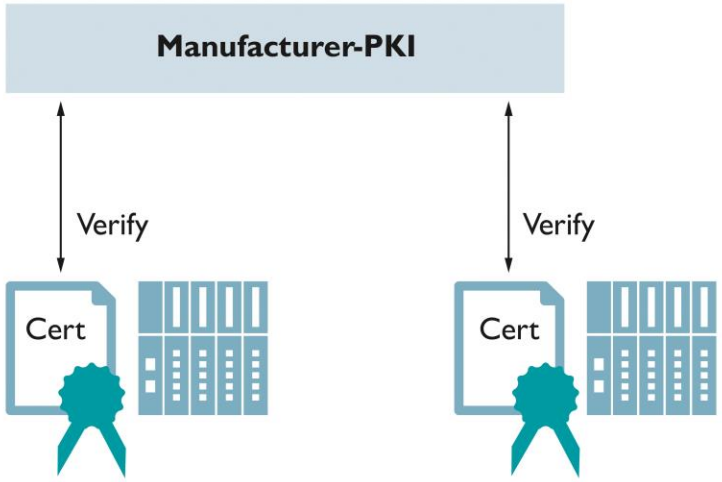
-4-2: CR 3.12 – Provisioning product supplier roots of trust

-4-2: CR 3.13 – Provisioning asset owner roots of trust

-4-2: CR 3.14 – Integrity of the boot process

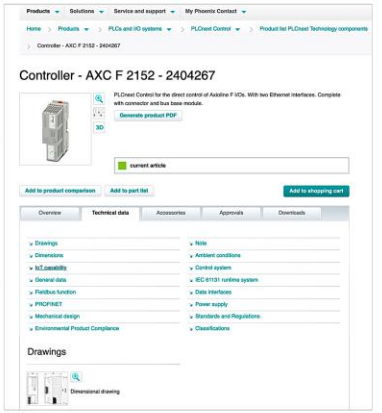
Concepts involving Digital Certificates

Zero Touch Provisioning to Digital Nameplate



State of delivery with manufacturer certificate

Operating state with manufacturer and operator certificate



Required: PKI and Digital Signatures

Overview

- PKI:
  - Providing Secure Digital Identities for Devices
    - Based on/creating Phoenix Contact Root of Trust
  - Providing Root of Trust for (Firmware) Signatures
- Digital Signatures:
  - Signing of (Windows) Software and Drivers based on public CA
  - Signing of Firmware updates based on own Root of Trust
  - Signing of Firmware images for secure boot (plain or CA hierarchy based)

Device Identities with IEEE 802.1 AR

X.509 for Device Identity

- Device has multiple identities
  - Initial Device ID
    - Provided by manufacturer
    - Protection by secure element recommended
      - Quality of X.509 certificate described in Certificate Policy and Certification Practices Statement
    - Validity infinite (31-12-9999)
  - Local Device ID
    - Provided by operating entity
    - Following local policies

Boundary Conditions

Interface to the real life

- OT equipment is hardly allowed Internet connectivity
  - OCSP is no option, CRL already is a stretch
- OT equipment and setup has lifetimes of decades
  - Concepts need to take into account certificate expiry
  - Public CAs may change their business model or go out of business
- PKI is considered vodoo by (OT) users
- PKI and Digital Signatures are hardly understood in depth even in IT and software development

Setup at Phoenix Contact

Using PrimeKey Appliances

Harrisburg

hbg-idam-seq01

Blomberg

RZ 1

RZ 2

blg-pki-app01

blg-pki-app02

Cluster

blg-sign-app01

blg-sign-app02

Semi-Redundant Setup

Public services:
https://devicepki.phoenixcontact.com
http://crl.phoenixcontact.com

Bad Pyrmont

(RZ)

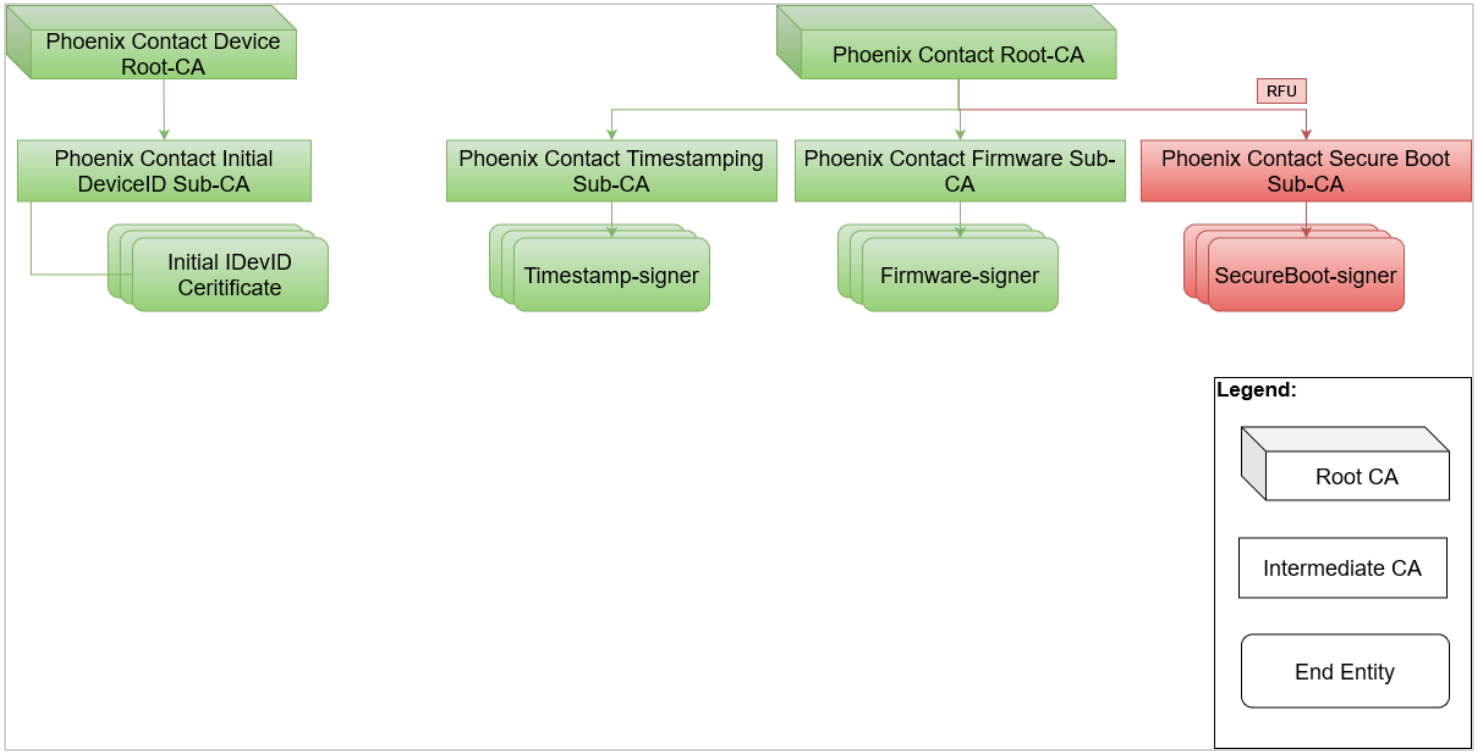
pyr-pki-app01

pyr-idam-seq01

pyr-idam-seq02

Certificate Hierarchy

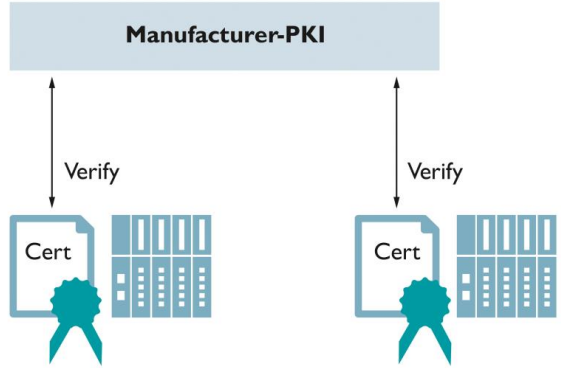
Phoenix Contact Device PKI



Use Case Device Identity

Manufacturer PKI

- Initial Device Identities need to identify the device by manufacturer and serial number (and …)
- No commercial CA is issuing such certificates
- No manufacturer would like to pay significant fees for each device certified
- Therefore: manufacturers create their own Device-PKIs



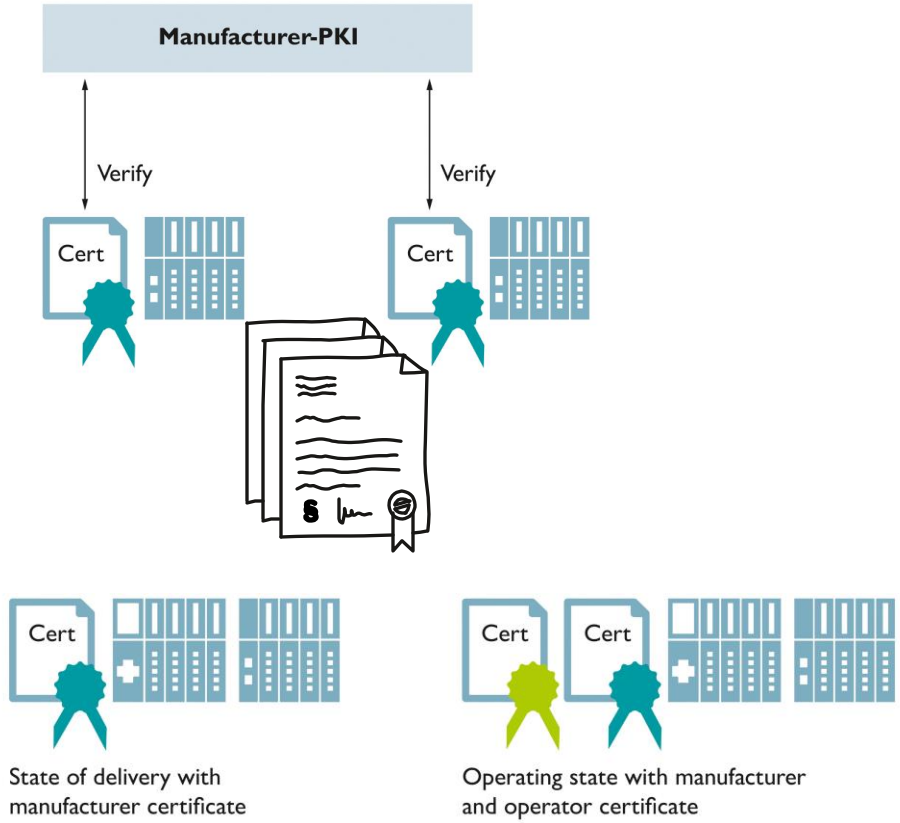
State of delivery with manufacturer certificate

Operating state with manufacturer and operator certificate

Use Case Device Identity

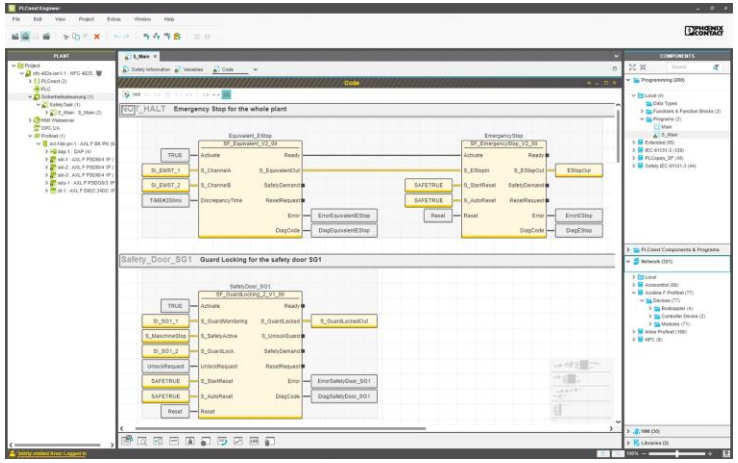
Models for Distributing Trust

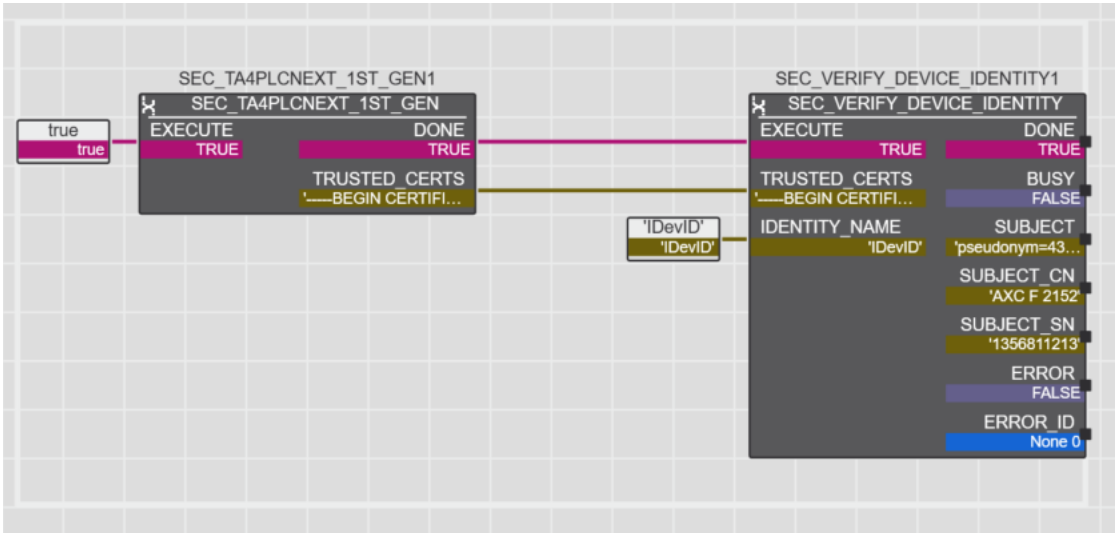
- Customers load manufacturer root of trust for the initial commissioning
  - Challenging with large numbers of manufacturers
  - Difficult to automate for Zero Touch Provisioning
- Additional trust information can be used
  - OPC UA Part 21 „Device Onboarding“ uses additional „Ticket“ with device information, signed with certificate from commercial CA
  - RFC 8995 „Bootstrapping Remote Secure Key Infrastructure (BRSKI)” uses online verification concepts



Use Case Device Identity

Engineering Tool and PLC Program

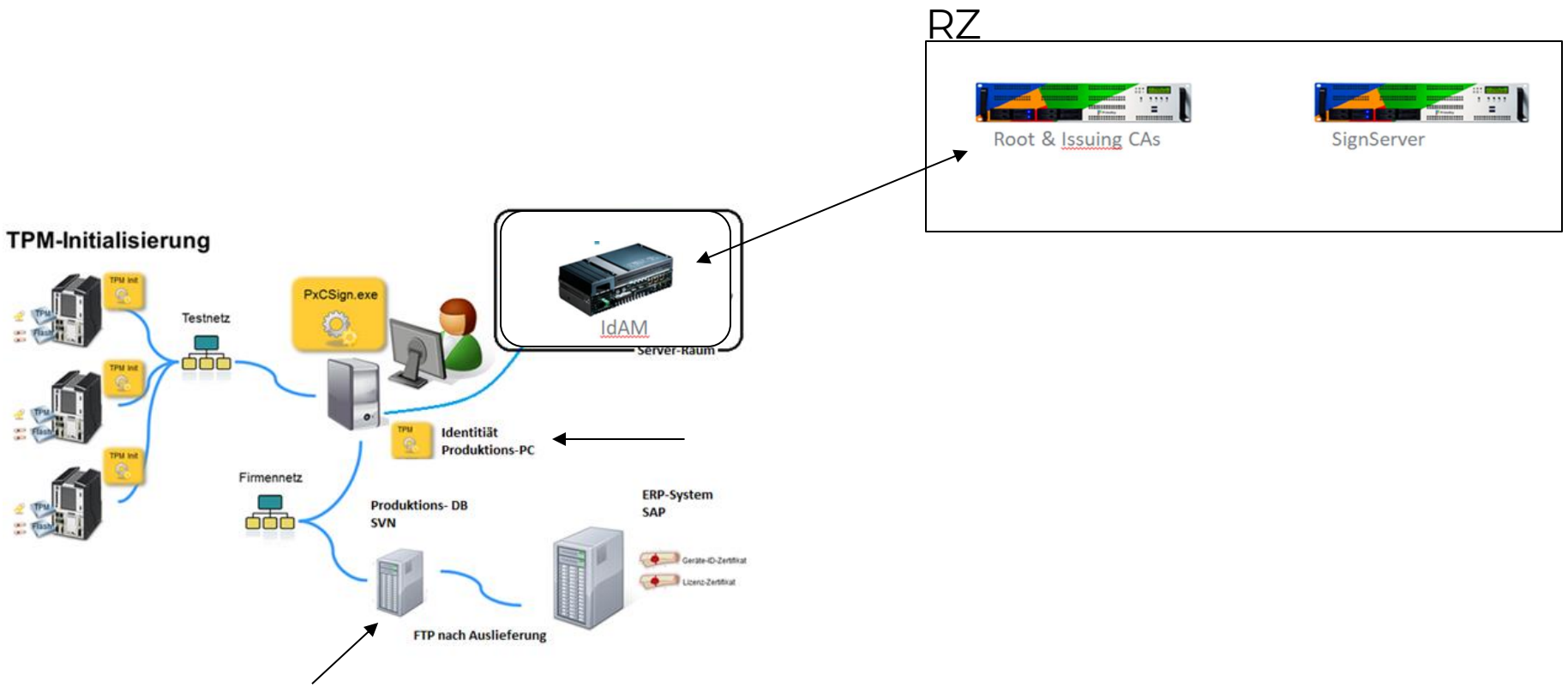




TLS connection with authentication

Use Case Device Identity

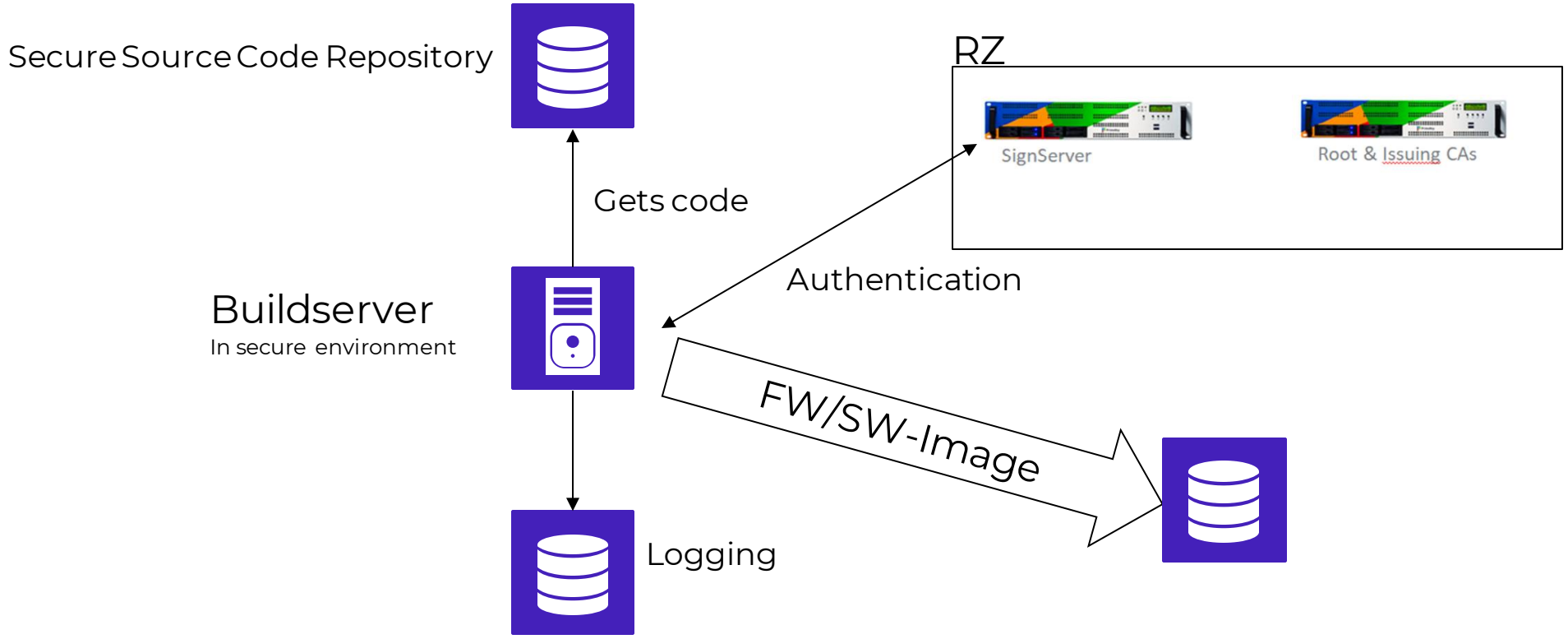
Implementing the certificate enrollment/programming



Technologies SVN und FTP used exemplary

Use Case Software/Firmware Signing

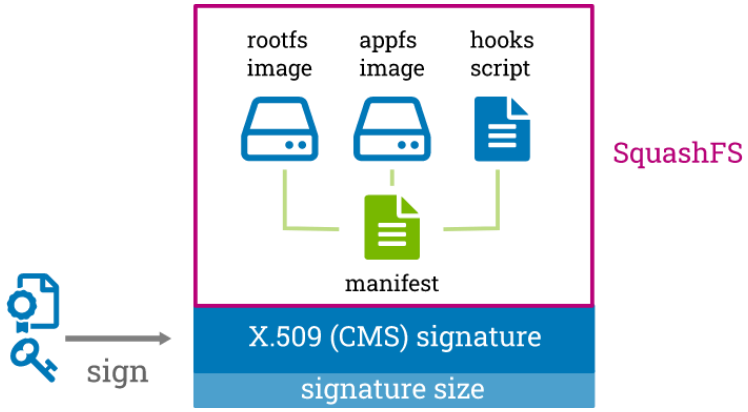
Integration into build infrastructure



Use Case Firmware Signing

Digital Signature of Firmware Updates

- Signatures depend on the technology used
- One important technology is RAUC
- RAUC is using Cryptographic Message Syntax (CMS)

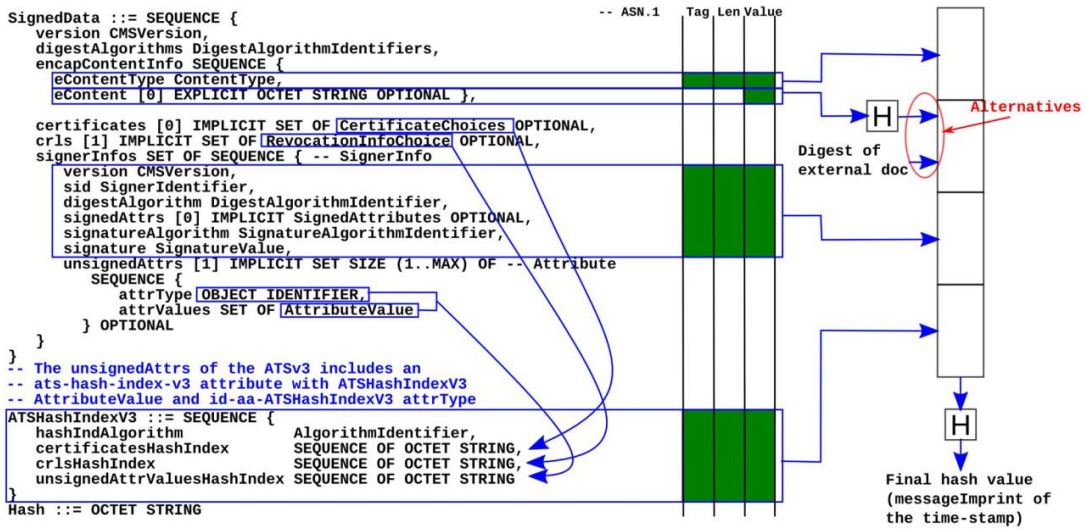


Source: https://rauc.readthedocs.io/en/latest/advanced.html

Use Case Firmware Signing

Digital Signature of Firmware Updates

- Challenge: „standard“ CMS signature verification fails with expiry of the certificate (chain)
- Solution: add time stamp using the CAdES (CMS Advanced digital Electronic Signature) concept
  - Using own signing tool based on EU Digital Signature Service (DSS) Open Source offering
    - Using PlainSigner Worker
  - Extend OpenSSL to support CAdES Baseline-T and higher formats (Work in Progress)



Source: Draft ETSI EN 319 122-1 V1.1.5 (2021-07)

Use Case Secure Boot

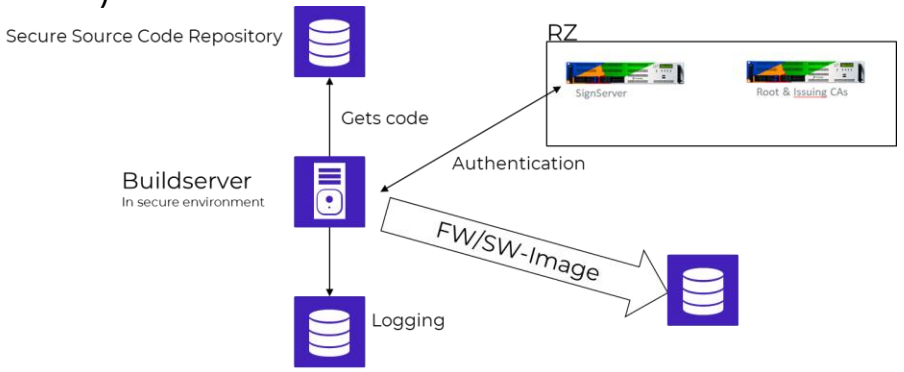
Dependent on the Capabilities of the Processor

- Everything is possible (raw signature … X.509 certificate hierarchy supported)
- Our first live experience:
  - Processor using raw RSA-PSS signatures agains single RSA public key
  - Created own application using a Plainsigner Worker (Processor manufacturer added an interface into their signature toolchain)
- Challenge: No redundancy due to certificates issued for different Signservers
- Solution: Use cloned Signservers using the same HSM key material and setup
  - As not fully supported concept, configuration must be held synchronous manually

Use Case Windows Signing

Simple… on the first glance

- During project setup interviews were conducted and tests performed
  - Signatures needed for EXE, DLL, MSI, JAR
  - Tested and used with PrimeKey signclient application
- Once going productive new formats popped up
  - Visual Studio Extensions (VSIX), NuGet Packages (NUPKG)
- Finally signing of (old!?) drivers
  - CAT, CAB
- Just recently
  - .NET MAUI: MSIX



“

Trustworthiness of identities and signatures comes from policy and procedures. Technology is important but only in a supporting manner.

Dr. Lutz Jänicke

Corporate Product & Solution Security Officer

Phoenix Contact GmbH & Co. KG