

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
- 2 2022-09-02 / Product & Solution Security at Phoenix Contact





Some Context...

Continuous growth together

Company headquarters and competence centers



Headquarters Blomberg | Germany

Corporate Presentations / Confidential (I)

Image: A state of the state of the

Continuous growth together

Company headquarters and competence centers





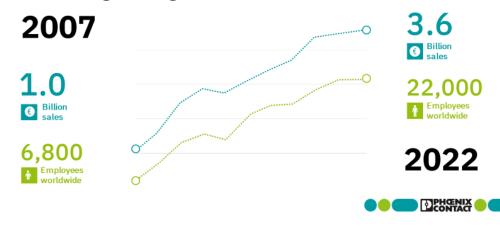


Group Center of Competence Harrisburg | USA Innovation Center Electronics Bad Pyrmont | Germany Group Center of Competence Nanjing | China



People and markets

Continuous growth together



Industrial Security with IEC 62443

Covering the complete topic of industrial security

General	Policies and procedures	System	Component	Profiles	Evaluation
1-1 Technology, concepts and models	2-1 Requirements for an IACS security management system	3-1 Security technologies for IACS (TR)	4-1 Secure product development lifecycle		6-1 Security evaluation methodology for IEC 62443 – Part 2-4 (TS)
1-2 Master Glossary of terms and abbreviations	2-2 Security Protection Rating	3-2 Security risk assessment and system	4-2 Technical security requirements for IACS		6-2 Security evaluation methodology for IEC
1-3 System security compliance metrics	2-3 Patch management in the IACS environment (TR)	design 3-3 System security	products		62443 – Part 4-2 (TS)
1-4 System security lifecycle and use case	2-4 Requirements for IACS solution suppliers	requirements and security levels			
1-5 Rules for IEC 62443 Profiles (TS)	2-5 Implementation Guidance for IACS Asset Owners				
Definitions Metrics	Security Requirements for plant owner and suppliers	Security Requirements for a secure system	Security Requirements for secure components	Profiles for IACS solution suppliers (and more?)	Evaluation methodologies for conformity assessment
		Process requirements		Functional requirements	

Industrial Security with IEC 62443

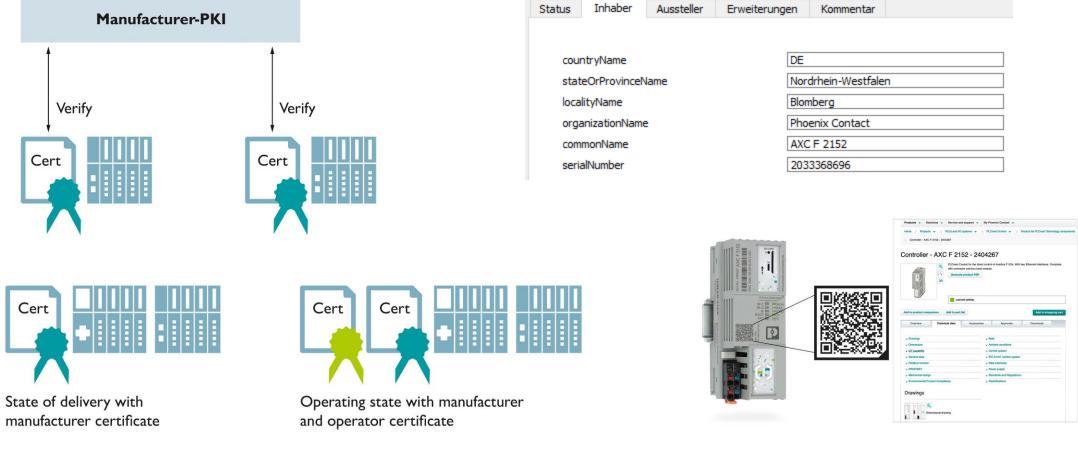
Requirements for Components

- -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 Keyfactor | #TechDays2023

Concepts involving Digital Certificates

Zero Touch Provisioning to Digital Nameplate



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

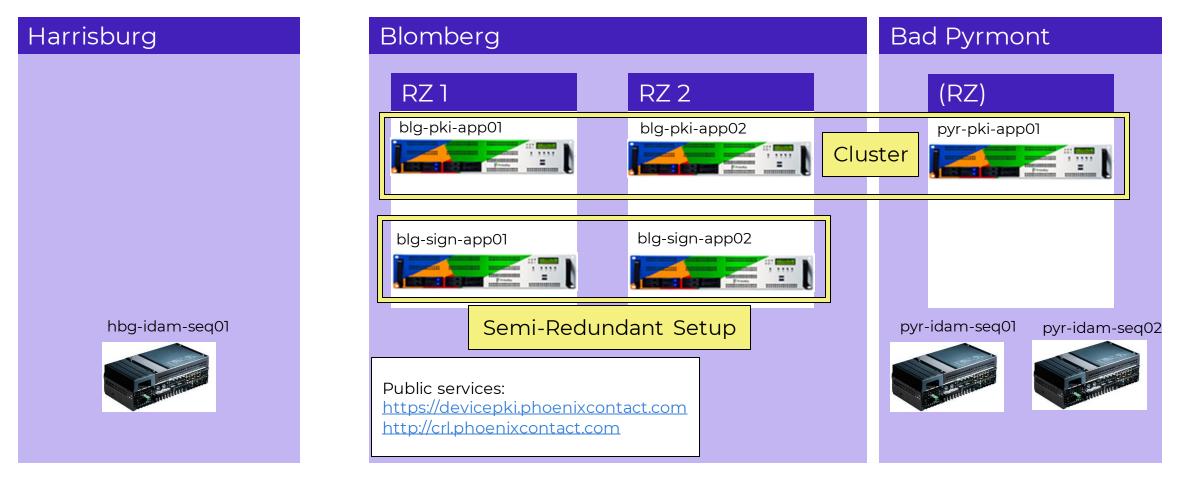
Boundary Conditions

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

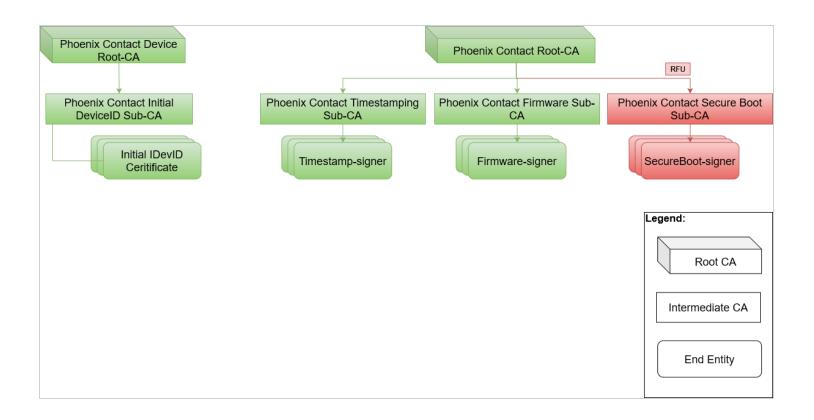
Setup at Phoenix Contact

Using PrimeKey Appliances



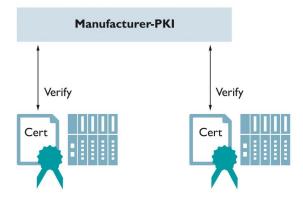
Certificate Hierarchy

Phoenix Contact Device PKI



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





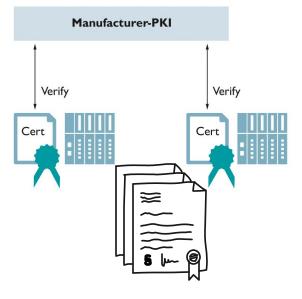
State of delivery with manufacturer certificate



Operating state with manufacturer and operator certificate

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





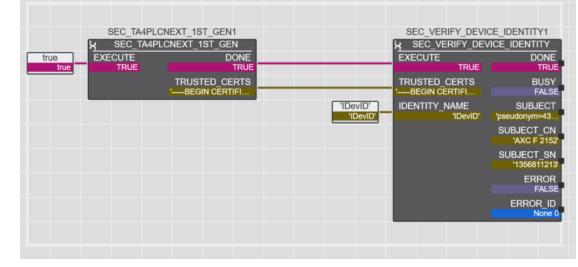


State of delivery with manufacturer certificate

Operating state with manufacturer and operator certificate

Engineering Tool and PLC Program

PLANT	Class X	COMPONENTS			
Valuet	District Internation & Venetice & Discours 0				
> (] PLCnort (2)	10000 +	🛩 🚞 Programming (292)			
V Distanteinationary (1)	Sense of the sense				
Constraints Constrain	COT_HALT Energies (Step for the which plant Exercise (Step for the which plant Energies (Step for the which plant TOT_HALT Energies (Step for the which plant BUBICS Energies (Step for the which plant BUBICS Exercise (Step for the which plant BUBICS Exercise (Step for the which plant Exercise (Step for the which plant Exercise (Step for the which plant BUBICS Exercise (Step for the which plant BUBICS Exercise (Step for the which plant	Colo System Color System C			
	Safety_Door_SG1 Guard Loding for the safety door 101	PLCIest Components & Program PLCiest Components & Program PLCiest Statestrk (221) Eccut			
	Line Line <thline< th=""> Line Line <thl< td=""><td>3 ■ Annorehi Sta → Branner P Index (7), → Branner P Index (7), 3 ■ Reinsport (1) 3 ■ Continue (vine (2)) 3 ■ Manuel (1) 3 ■ Manuel (2), 3 ■ Manuel (2), 4 ■ Manuel (2), 5 ■ Manuel (2),</td></thl<></thline<>	3 ■ Annorehi Sta → Branner P Index (7), → Branner P Index (7), 3 ■ Reinsport (1) 3 ■ Continue (vine (2)) 3 ■ Manuel (1) 3 ■ Manuel (2), 3 ■ Manuel (2), 4 ■ Manuel (2), 5 ■ Manuel (2),			
	Local Line Contract				
		> K Librarias (2)			



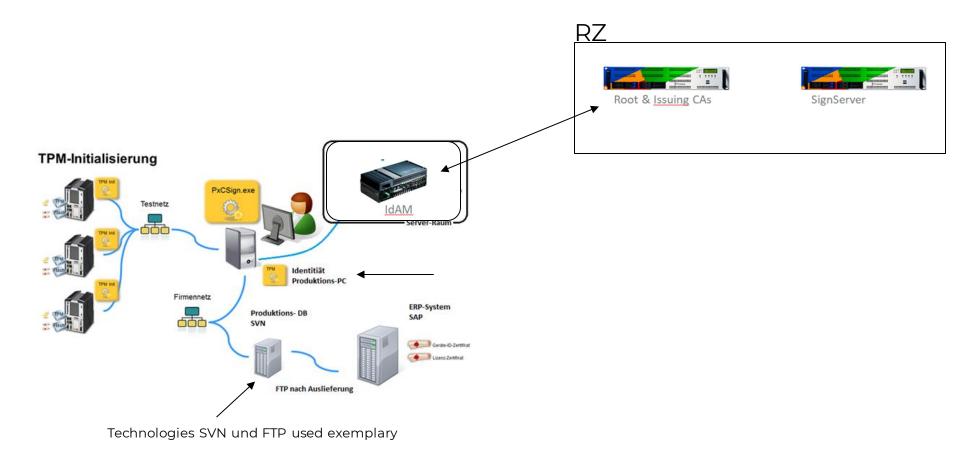
-

TLS connection with authentication



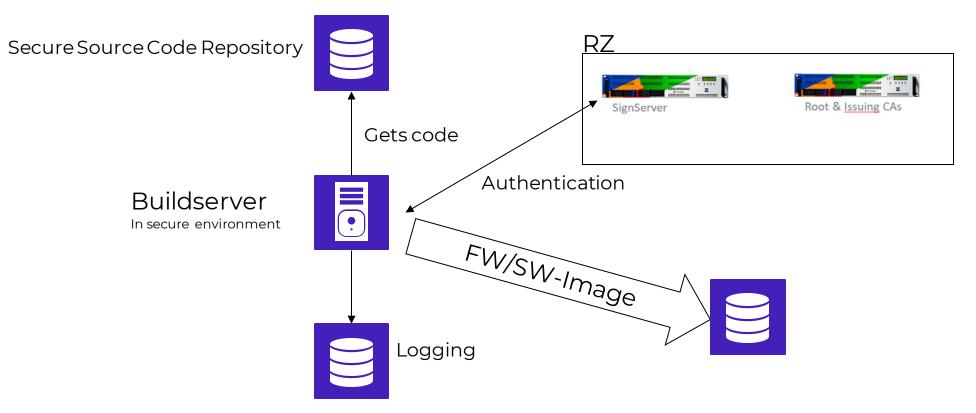
→ 🔥 axc-f-2152-1 : AXC F 2152 🔰			
 ✓ (?) PLCnext (2) ✓ <u>11</u>, ESM1 (1) ✓ (C) Cyclic100 (1) 	IP-Adresse: Stationsname: Verbunden:	192.168.1.10 axc+2152-1 Ja	
MainInstance : I	Debuggen:	Ja	
1H ESM2	Geräte-Seriennummer. Gerätestatus:	1356811213 Betrieb	
HMI Webserver OPC UA Wrofinet (0)	Angemeldet: Benutzername: Rollen:	Ja admin Admin	
Axioline F (0) PLCnext-Komponenten (0)	Seriennummer: Zertifikatsnr.: >Seriennummer: >Zertifikatsnr.: >Zertifikatsnr.:	N/A PhoenixSign License Root CA G1 N/A PhoenixSign License PLCnext Sub CA G1 8949017230002848467 PL Cnext Paring Signer CA	
	>Zertifikatsnr.: >Seriennummer: >Zertifikatsnr.:	PLCnext Device Signing CA 1356811213 AXC F 2152	

Implementing the certificate enrollment/programming



Use Case Software/Firmware Signing

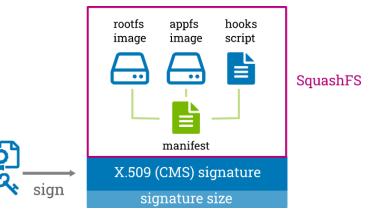
Integration into build infrastructure



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)

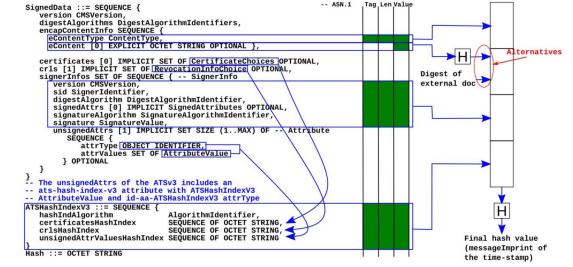


Source: https://rauc.readthedocs.io/en/latest/advanced.html

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 319122-1 VI.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)

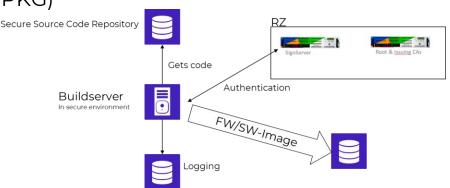
- Challenge: No redundancy due to certificates issued for different Signservers
- Solution: Use cloned Signservers using the same HSM key material and setup
 - As not fully supported concept, configuration must be held synchronous manually

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







"

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