achelos

security health industry public connect

Key Management Solutions for Connected Factories

Dr.-Ing. Michael Jahnich, Director Business Development

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Secur|Ty made in EU

Trust Seal www.teletrust.de/itsmie

NIS 2.0

- New essential and important sectors
- Manufacturing industry
- Mandated product security for critical components

IEC 62443

- CSMS for operators
- Development process certification
- security-by-design
- Product certification

Industrial trends

- Connected manufacturing
- Cloud services
- Digital twins
- Remote device management

Cyber security trends

- Zero Trust
- Protection against professional hackers
- Post-quantum cryptography

Supplier – Systems Integrator – Operator

Security Consulting by achelos

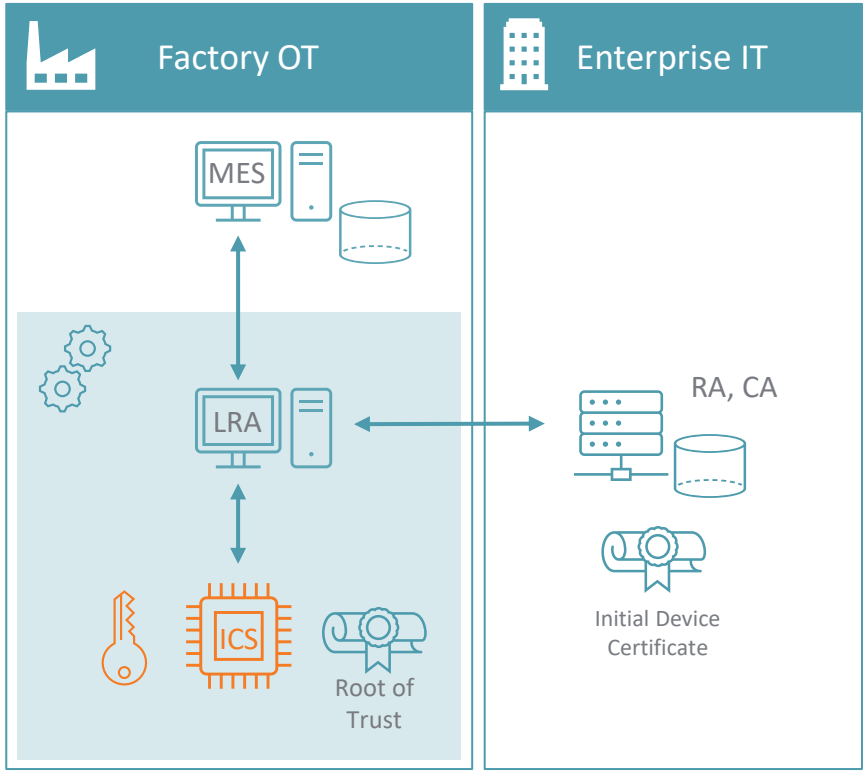
Cybersecurity for connected solutions in industry and traffic

- Public key infrastructures are essential for the cybersecurity of intelligently connected devices, machines and systems:
  - for the digitalization of industrial processes
  - in the development of future connected transport and traffic solutions

High-quality electronic certificates to prove the authenticity of hardware and software in the manufacturing industry

Security Consulting by achelos

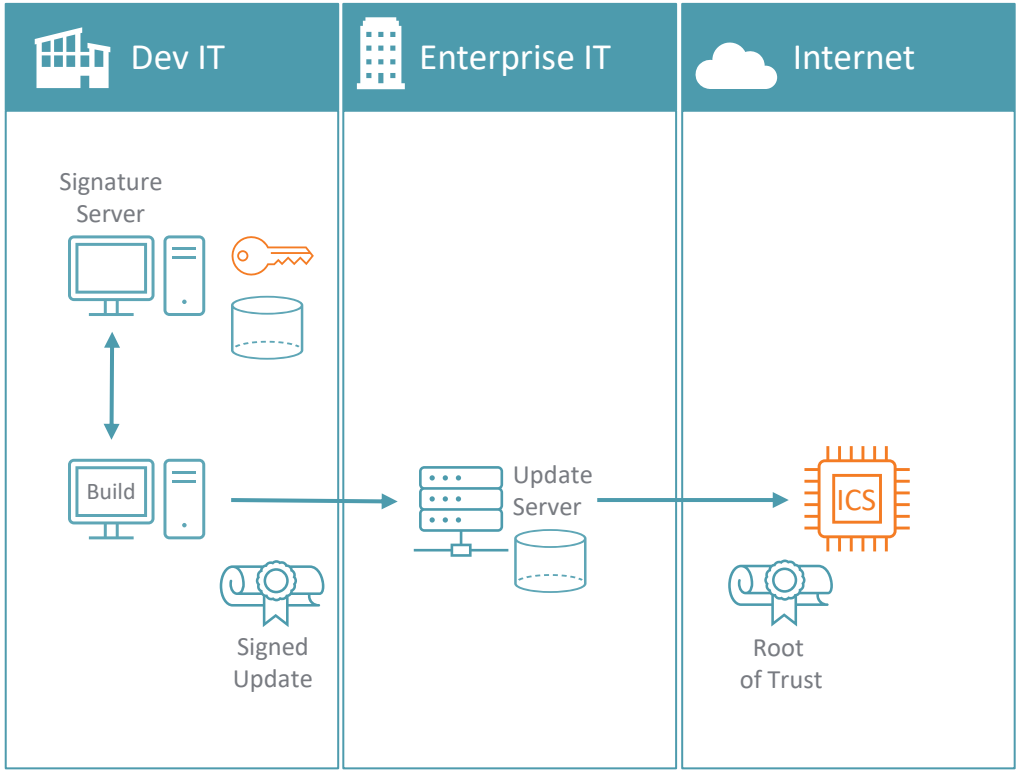
Secure Device ID



- **Initial device ID generated** in the production process for a certificate-based authentication
- **Automated processes**
  - Registration
  - Secure key generation
  - Certificate generation
- Compliant with IEEE 802.1AR
- Standardized protocols EST, CMP, ACME, SCEP

Security Consulting by achelos

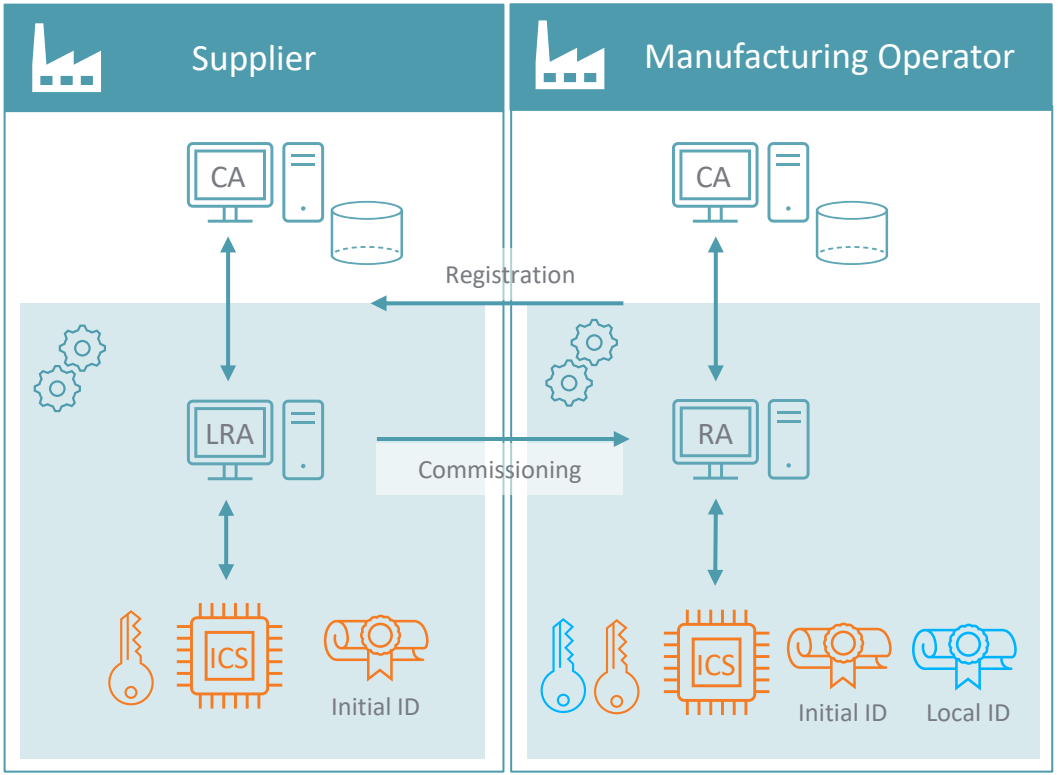
Secure Firmware Update Management



- **Signed** firmware updates by the manufacturer
- Verification of the authenticity of a firmware update
- Protection against malware and software modifications
- Centralized key management
- Java, MS Authenticode, CMS, Android Apps …

Security Consulting by achelos

Secure Device Commissioning



- Generation of a locally significant device ID after authentication
- Goal: commissioning of the device in the operator's security zone / Bootstrapping
- No common „root of trust“

Industry-grade PKI

Standards requirements for PKI

IEC 62443-4-2

- „Capability to operate a PKI according to commonly accepted best practices or obtain certificates from existing PKI“
- Certificate Policy based on risk assessment based on RFC 3647
- Security Level 2 to 4

IEEE 802.1AR

- Defines DevID Trust Model
- Manufacturer shall publish CP / CPS and trust anchor for each IDevID
- No requirements on PKI operations

Lightweight CMP profile

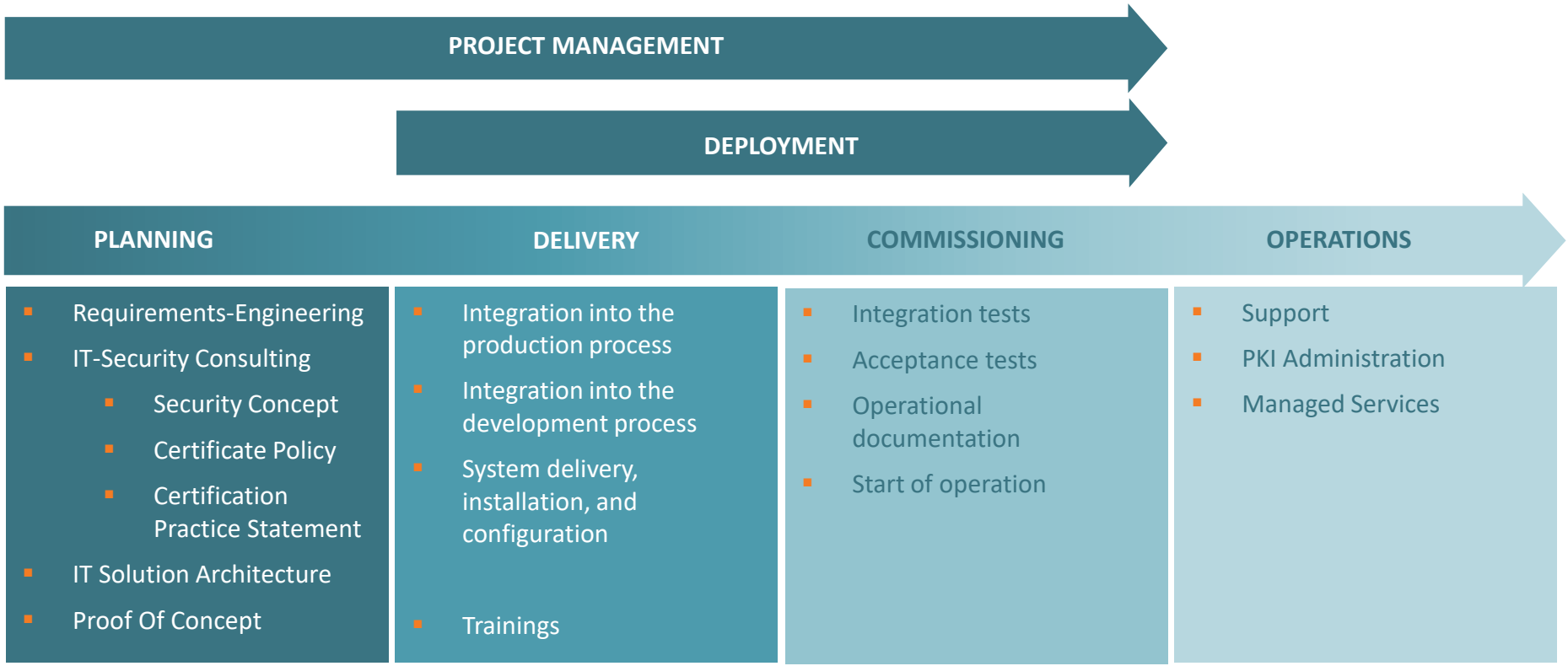
- Proper processes for issuance, management, verification, revocation, and audit for authorized devices, users and processes.
- PKI operation according to commonly accepted best practices

What are PKI best practices in the Industrial Sector?

Customer Expectations

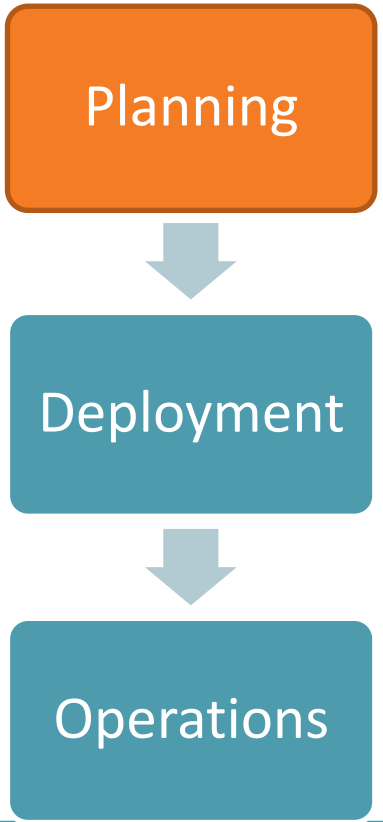
- Compliance/orientation with standards based on **best practices**: ISO27001, IEC 62443, TR-03145
- Policies and rules to be implemented in the OT/IT
- Definition of effective security measures
- Automated certificate processes
- Use of HSMs
- Seamless production integration

System Consulting – Project Phases



Industrial PKI best practices – planning 1

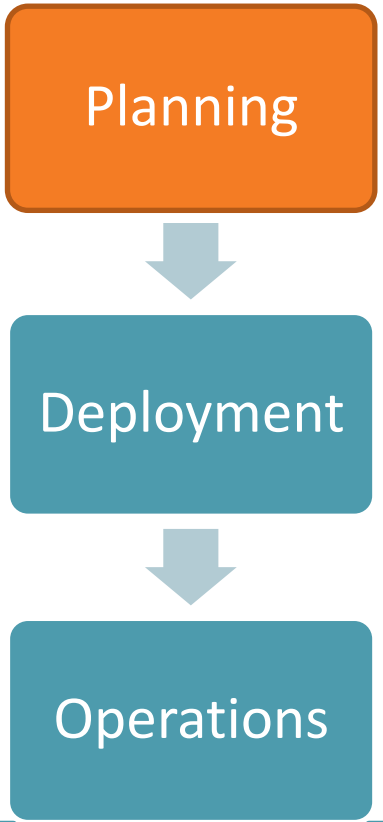
- Objective: lay foundation of secure industrial PKI operations
- PKI solution architecture
  - Use cases – current and future
  - IT infrastructure
  - System interfaces
  - Operational, adminstrative, physical measures and processes
  - Implementation and operational costs



Industrial PKI best practices – planning 2

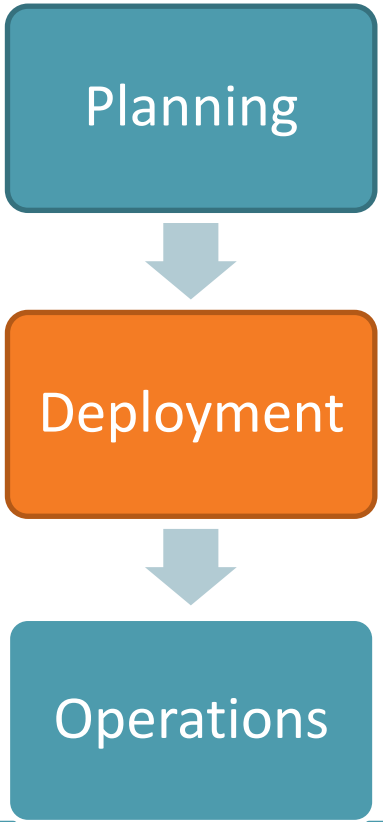
- Risk Assessment for each use case
- Certificate Policy
- Certification Practice Statement

- Implementation options
  - Public or private PKI
  - On-premise or cloud services
  - Managed services



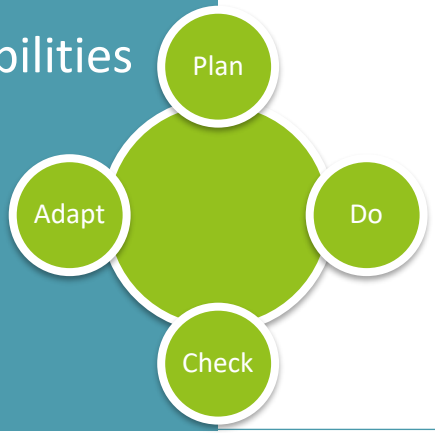
Industrial PKI best practices – deployment

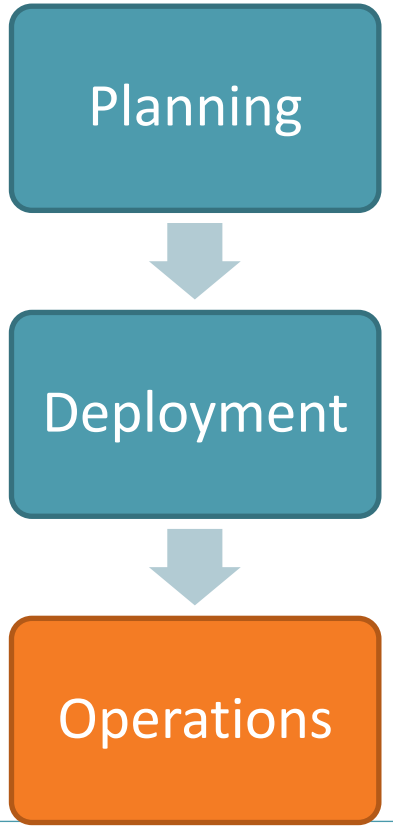
- Integration into existing IT
  - Build process
  - Manufacturing process
- Integration and acceptance testing
- Integration into ISMS / CSMS
- Internal/external audit/evaluation
- Enable people to operate PKI
- Document operational processes



Industrial PKI best practices – operations

- Objective: maintain security
- Regular audits
- Maintain and improve the quality of your documentation
- Maintain roles and responsibilities and abilities to operate PKI
- Train staff





achelos

Vielen Dank! | Thank you!

achelos GmbH
Vattmannstraße 1 | 33100 Paderborn | GERMANY
T +49 5251 14212-0 | info@achelos.de
achelos.de | IoT.achelos.com