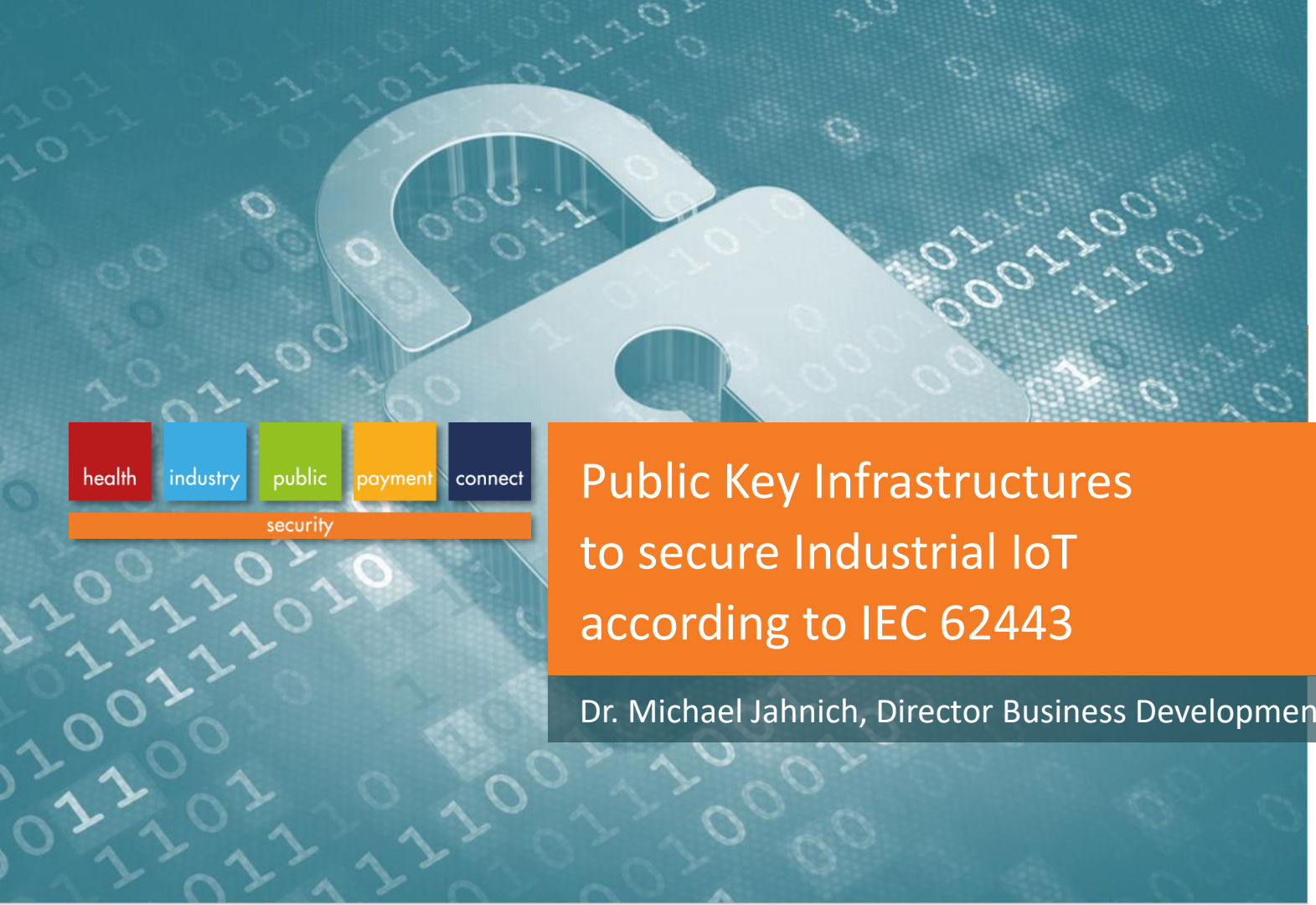


achelos

health industry public payment connect

security

Public Key Infrastructures to secure Industrial IoT according to IEC 62443

Dr. Michael Jahnich, Director Business Development

Integriertes Managementsystem ISO 9001 ISO/IEC 27001

Allianz für Cyber-Sicherheit Partner

SecurITy made in Germany

NIS 2.0 and CRA

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

IEC 62443

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

Industrial trends

- Connected manufacturing
- Cloud services/ IoT hubs
- Digital type plate
- Admin Asset Shell
- Zero Trust Architectures

Supplier – Systems Integrator – Operator

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

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

Security Consulting by achelos

Zoo of Cybersecurity Standards

Standard	Factory OT	General IT	IT/OT - BSI
ISMS / CSMS	IEC 62443-2-*	ISO 27001	IT-Grundschutz
System security	IEC 62443-3-* PKI on system level	ISO 27033 and 33	IND: Industrielle IT
Secure Dev Life-cycle	IEC 62443-4-1		
Product security	IEC 62443-4-2 PKI for components		
PKI operations	„best practices“	ISO 27099 ISMS for PKI	TR 3145 Secure CA operation

Industry-grade PKI: Standards requirements

IEC 62443-3-1

- 7.3 – Public key encryption and key distribution
- Basic introduction
- Authentication to establish a secure channel
  - SSH
  - IPSec/IKE
  - TLS
  - Kerberos

IEC 62443-3-3 (system)

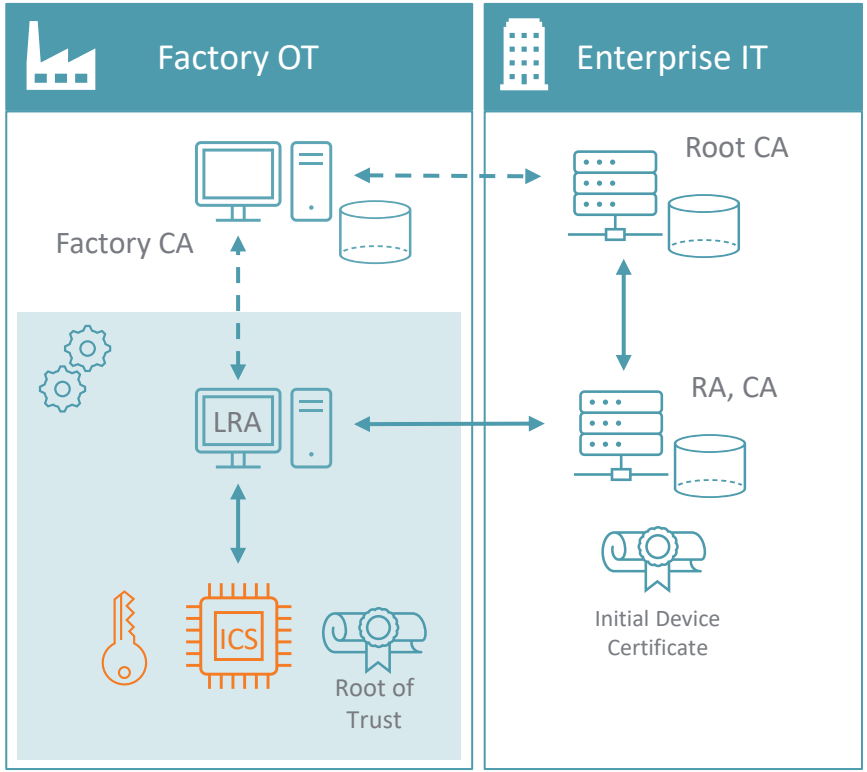
- SR1.8 – PKI
- Enrollment using a secure process
- PKI should consider the organization's certificate policy acc RFC 3647
- Validation of certificates (e.g. OCSP)
- Revocation of certificates
- Trusted Hardware > SL2

IEC 62443-4-2 (component)

- CR 1.8 – PKI certificates
- „Capability to operate a PKI according to commonly accepted best practices …"
- Certificate Policy based on risk assessment based on RFC 3647
- Security Level 2 to 4
- Trusted Hardware > SL2

Security Consulting by achelos

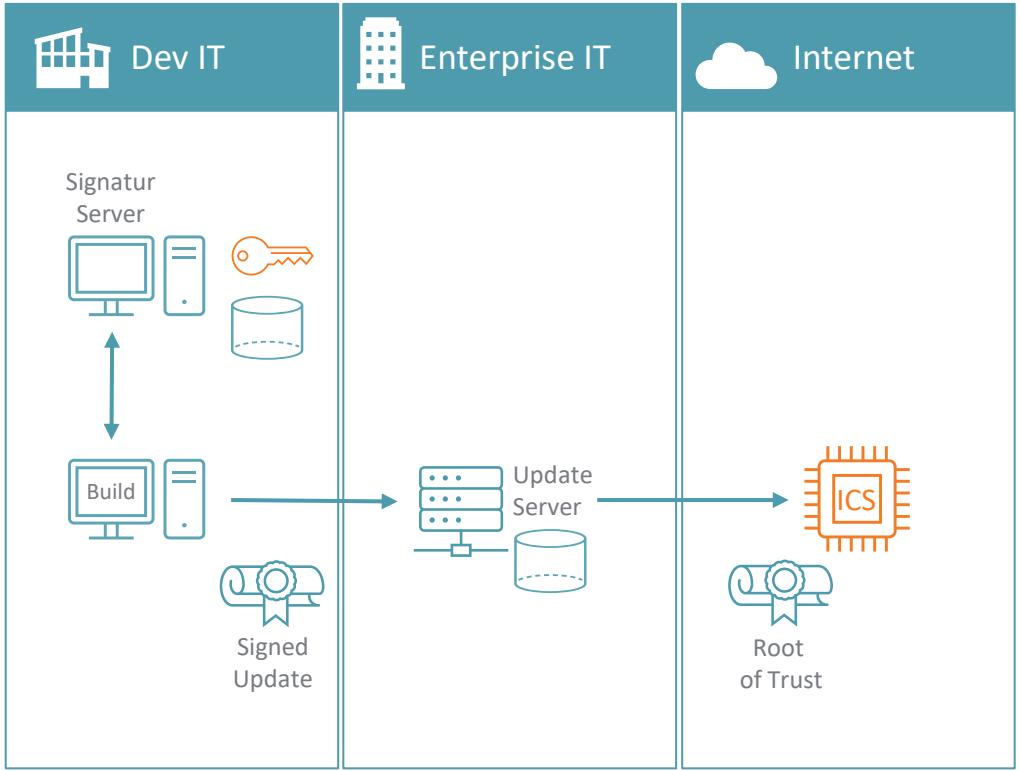
Secure Device ID



- **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
- Online versus limited connectivity

Security Consulting by achelos

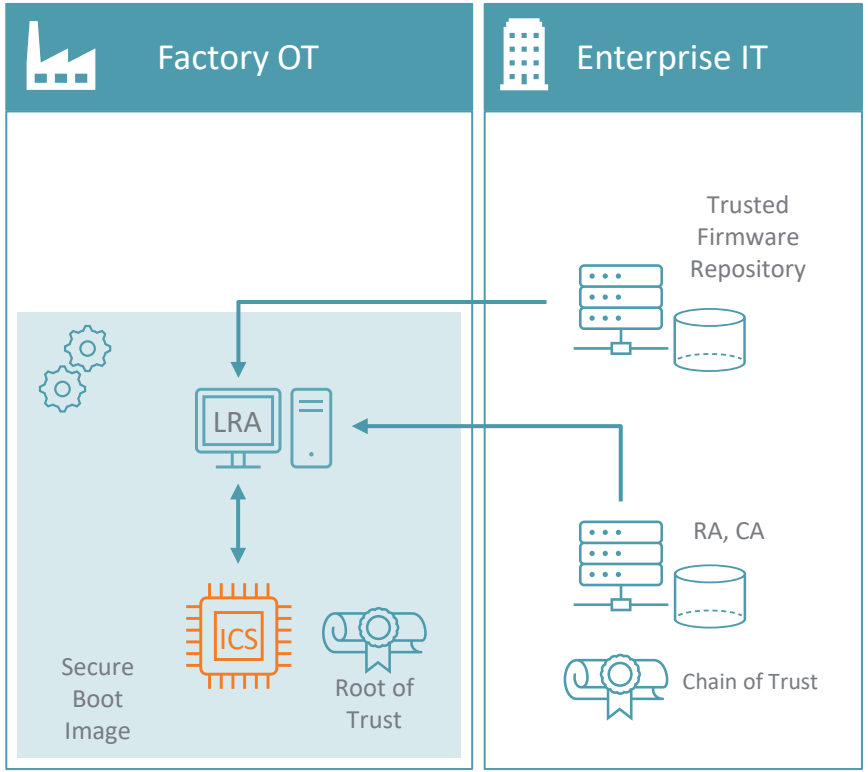
Secure Firmware Update



- **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

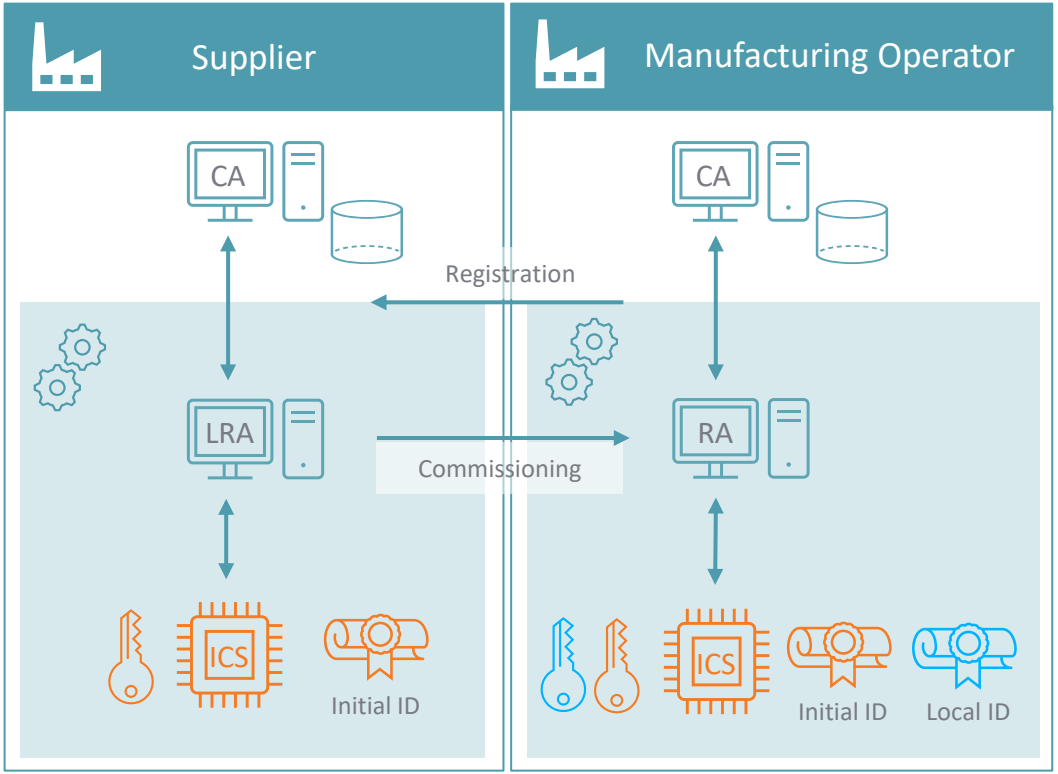
Secure Device Boot



- Secure Boot Image Generation
- Checking the integrity of firmware at system boot
- Goal: Achieve a secure device state at power-up.
- PKI providing Chain of Trust
- Secure certificate management

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“
- Zero Trust environments
- Zero touch (BRSKI)

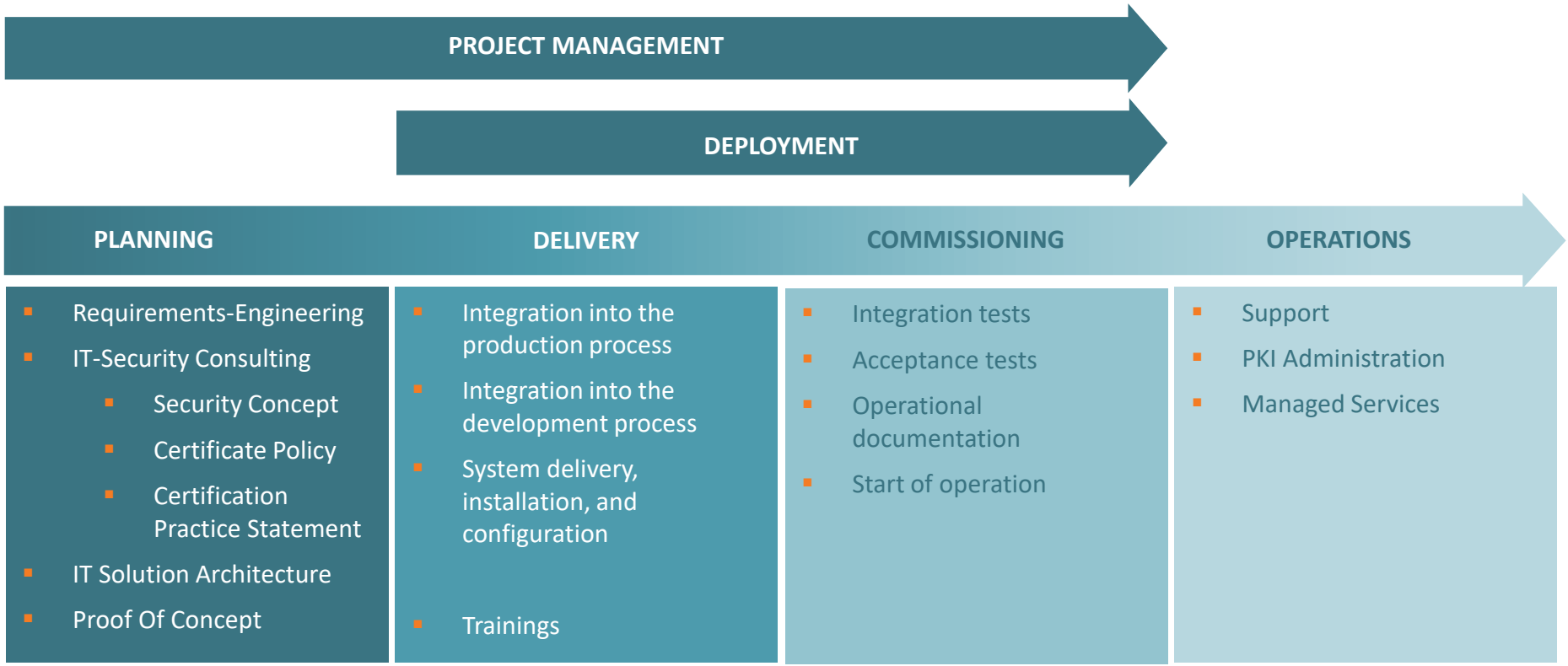
achelos

What are PKI best practices in the Industrial Sector?

Customer Expectations

- Compliance with standards based on **best practices**: RFC 3647, ISO27099, TR-03145
- Certificate Policies and Operations Documentation implemented in the OT/IT
- Automated certificate life-cycle processes
- Use of HSMs
- Seamless production integration

System Consulting – Project Phases



Vielen Dank! | Thank you!

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