

TeleTrust-EBCA "PKI-Workshop" 2026

Berlin, 08.10.2026

Digital Trust in OT - Sichere Identitäten für die industrielle Transformation

Anna Palmin, Frank Laurig, Siemens

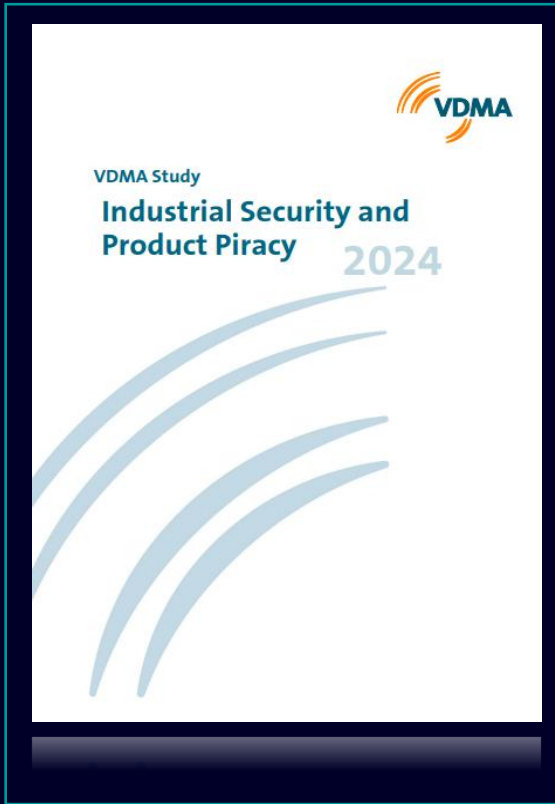


Secure Digital Identities in OT:

The foundation of trust in connected systems

Secure Digital Identities in OT

The importance and impact



46% of companies in the German mechanical and plant engineering sector report being affected by product or brand piracy. The estimated annual damage is **€4.1 billion**, equivalent to approximately **16,000** jobs lost.



Unfair imitation and brand piracy are the most common forms.



41% of companies report that counterfeits pose a direct risk to human safety. **More than half** say they threaten the safe operation of machinery.



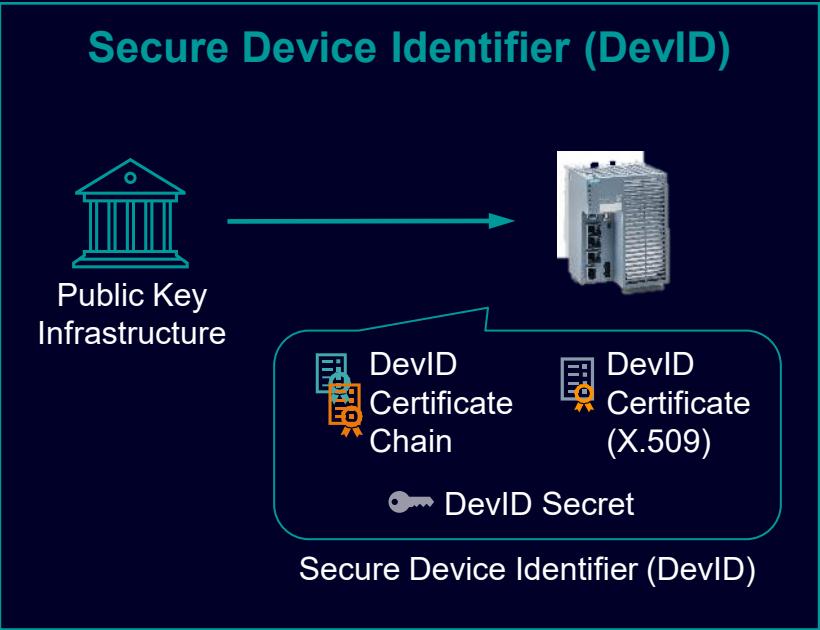
Around **24%** of companies experienced significant cyber incidents in the past two years.

→ **The increasing convergence of product piracy and cyber threats highlights the need for stronger digital protection.**

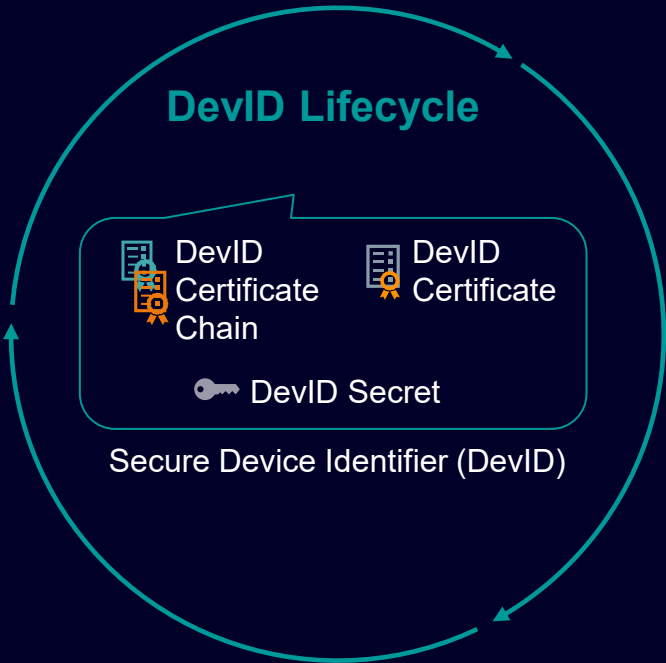
Secure Digital Identities **help ensure** that only **authentic, trusted devices and applications** are integrated into operational environments. [VDMA Studie Produktpiraterie](#)

Secure Digital Identities in OT

The foundation of trust in connected systems



- used to **authenticate** devices and applications
- essential for **protecting devices, machines, and systems** throughout various lifecycle scenarios
- must be **secure, verifiable, and scalable**



- IEEE 802.1AR
- IEC 62443
- PROFINET
- OPC UA
- Zero Trust
- Charter of Trust

Note: Each DevID is uniquely bound to the one specific device. Since the DevID secret is securely stored and operated on this specific device and the DevID certificate is issued by a securely operated PKI, a “fake” device cannot successfully authenticate itself using a stolen DevID certificate.



Standards, Technologies & Reference Architecture

Secure Digital Identities in OT

Reference architecture for automated management

atp article in 01-02/2026
“Zertifikatsmanagement für
heterogene OT-Umgebungen“

Certificate management for heterogeneous OT environments

Interoperable basis for protocol-
independent integration of OT
devices

Zertifikatsmanagement für heterogene OT-Umgebungen

Interoperable Grundlage für die protokollunabhängige Integration

#Public Key Infrastructure #Secure Digital Identities #OPC UA #CMP

*Sichere Kommunikationswege sind essenziell, um Produktionsumgebungen vor Cyber-
risiken zu schützen. Die Grundlage bilden
X.509-Zertifikate, ergänzt durch ein auto-
matisiertes Zertifikatsmanagement, das IT-
und OT-Systeme verbindet und Prozesse für
hohe Verfügbarkeit steuert. In Kooperation
zwischen BMW und Siemens wurde an-
hand eines Demonstrators eine skalierbare
Referenzarchitektur für heterogene OT-Um-
gebungen evaluiert. Basierend auf etablier-
ten Standards bietet diese Architektur eine
interoperable Grundlage für die protokollun-
abhängige Integration von OT-Geräten. Die
Lösung setzt auf etablierte Standards und
schafft eine interoperable Basis.*

Anna Palmin,
Frank Laurig,
Sebastian Fruth,
Siemens;
Johann Schnagl,
BMW

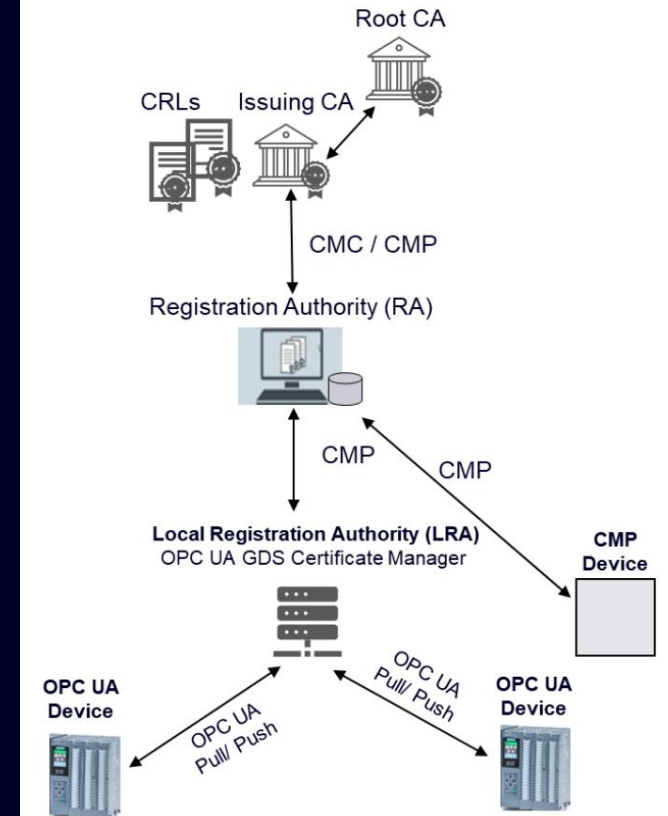


Abbildung 1: Struktur und Funktionalitäten.

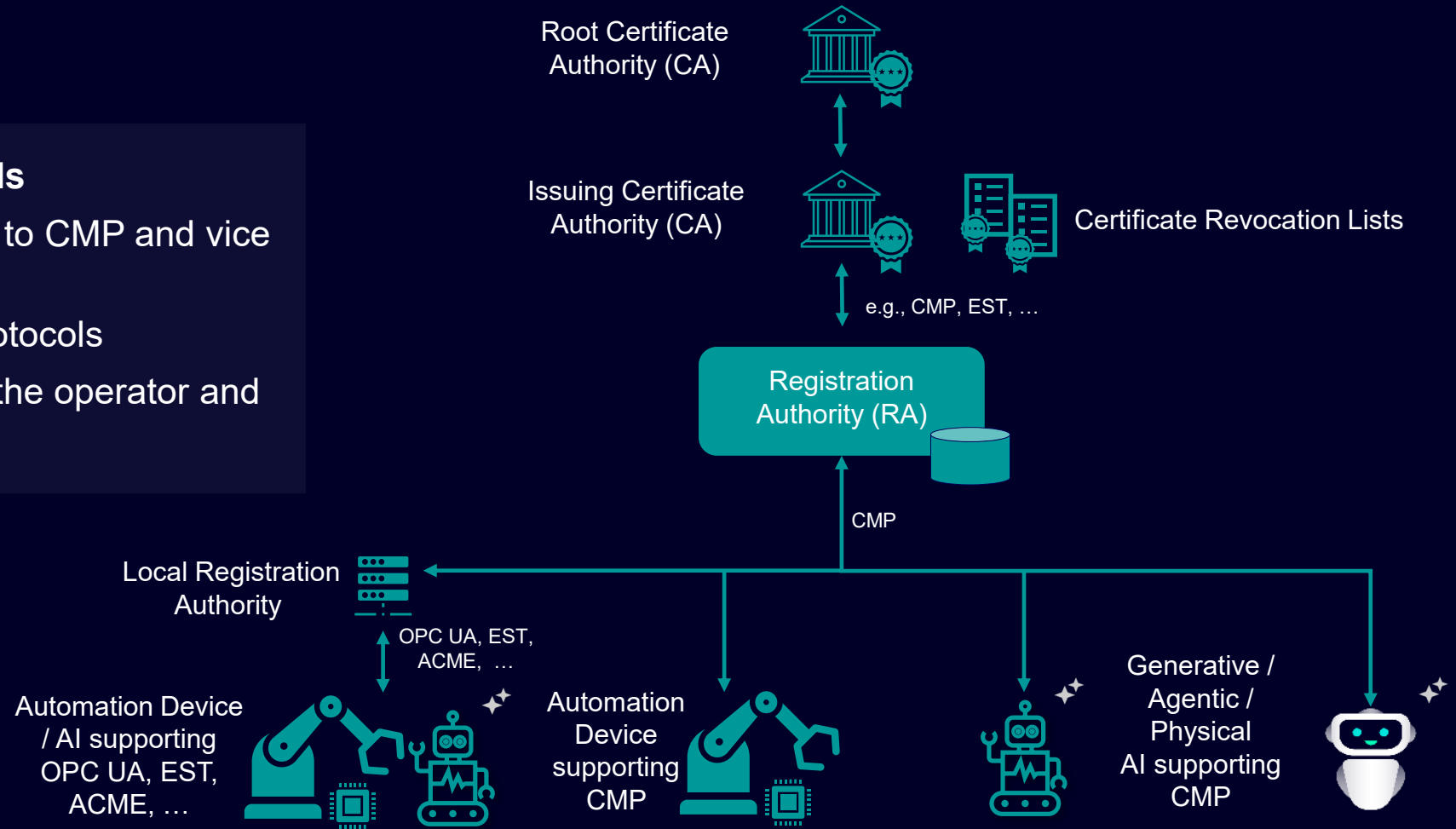
Abbildung 1: Struktur und Funktionalitäten.

Secure Digital Identities in OT

Reference architecture for automated management - components explanation

Protocols on the different levels

- Any protocol can be converted to CMP and vice versa
- Clients will support different protocols
- CA configuration is defined by the operator and the CA products

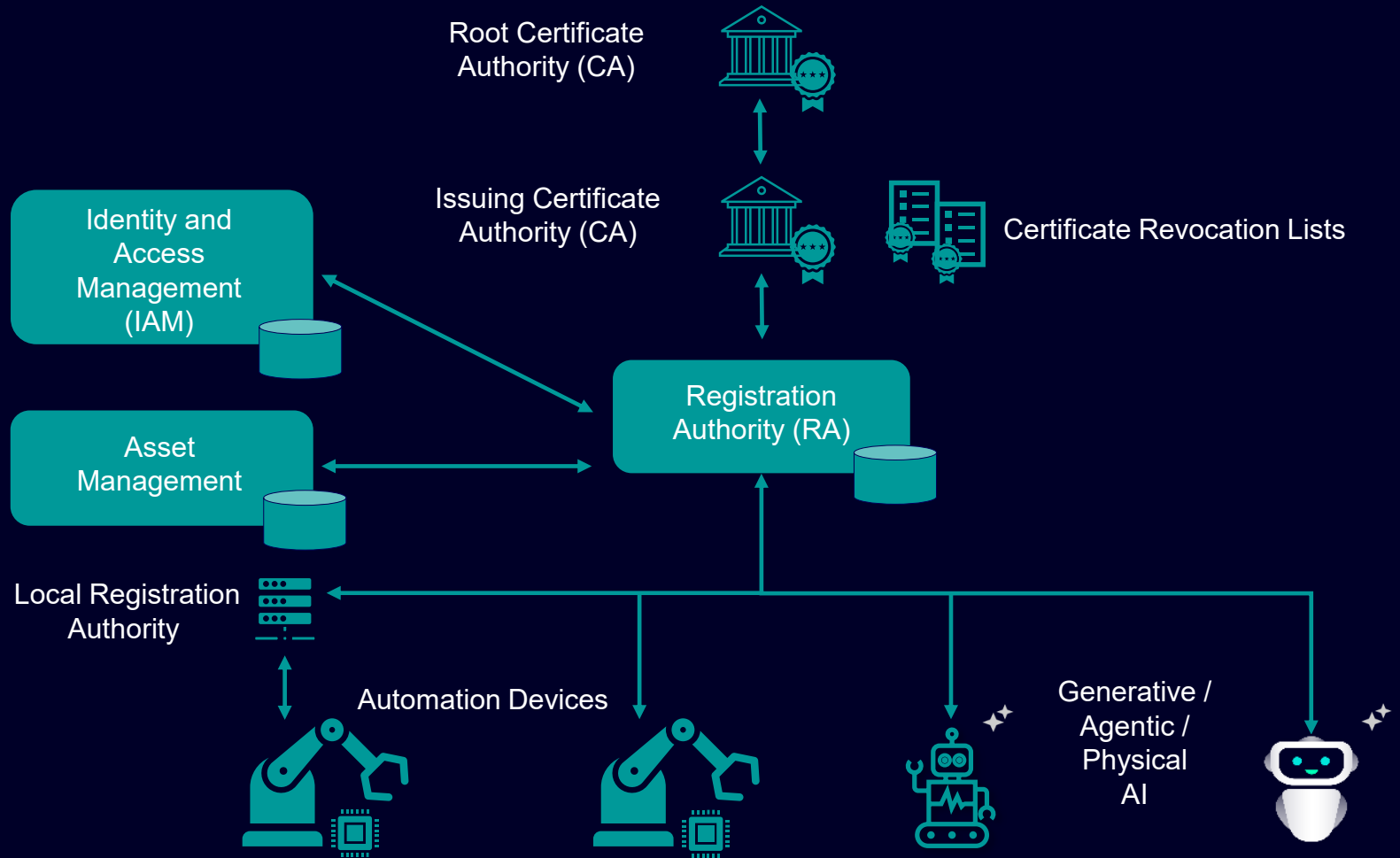


Secure Digital Identities in OT

Reference architecture for automated management - components explanation

Connectors of the Registration Authority will support operators

- to the asset management to get a better overview of the actual certificate clients or to keep the allow list centrally
- to the IAM to establish a Zero Trust architecture by exchanging Information between the PKI and the Policy decision point about the existing but also new entities and their corresponding identities

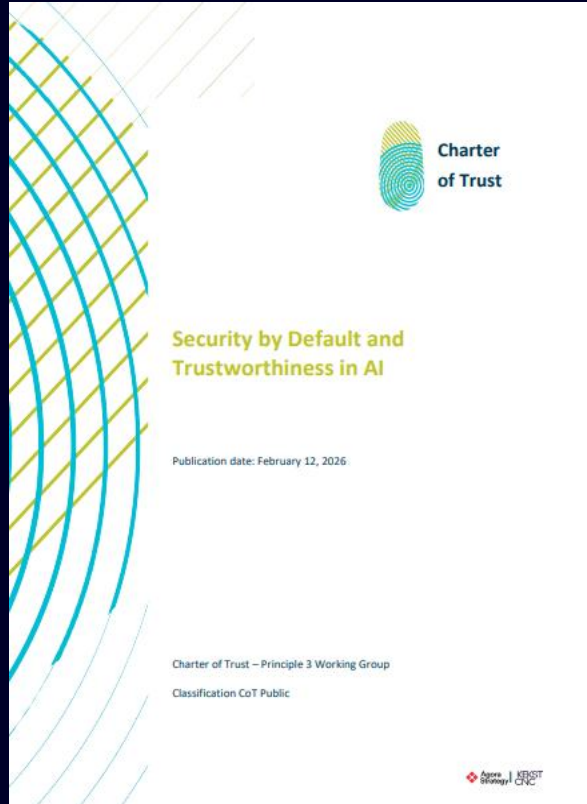




Challenges and Trends

Secure Digital Identities in OT

Trustworthy AI



Last but not least: Secure digital identities are essential for trustworthy AI, enabling traceability, integrity and control across the lifecycle.

Quantum attacks and computers pose a fundamental threat to IT/OT cybersecurity

No cybersecurity is possible if quantum attacks break cryptography

Main threats:

- > **“Stored now – decrypted later”**
No confidentiality, e.g., encrypted mails, encrypted patient data, etc.
- > **“Signed now – forged later”**
No integrity and authentication: e.g., manipulated firmware updates, manipulated audit trails, etc.
- > **“Deployed now – attacked later”**
No availability, e.g., bypass of security measures, leading to disruption of critical infrastructures, etc.

- BSI 2024 “assessment shows that it is likely that a CRQC¹ will be feasible in a maximum of 16 years (i.e. by 2040 or earlier)”
- “However, this period could be significantly reduced to 10 years if current heuristics [...] are fully verified”

[EU PQC Roadmap 23.06.2025, page 4](#)





Let's dive deeper in our workshop!

