TeleTrusT-EBCA "PKI-Workshop" 2025

Berlin, 18.09.2025

"Management of Secure Digital Identities in OT"

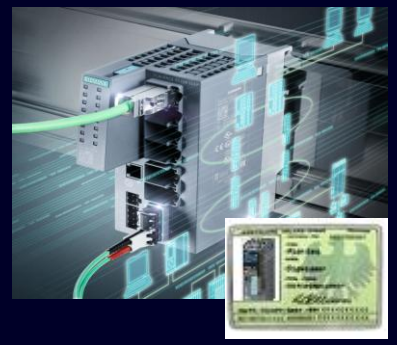
Anna Palmin, Siemens

Frank Laurig, Siemens

Secure Device Identities for OT products – Why?

Charter of Trust

For a secure digital world



Identity and access management: Connected devices must have secure identities and safeguarding measures that only allow authorized users and devices to use them.

https://www.charteroftrust.com/about/

Partners

Together we will shape Cybersecurity

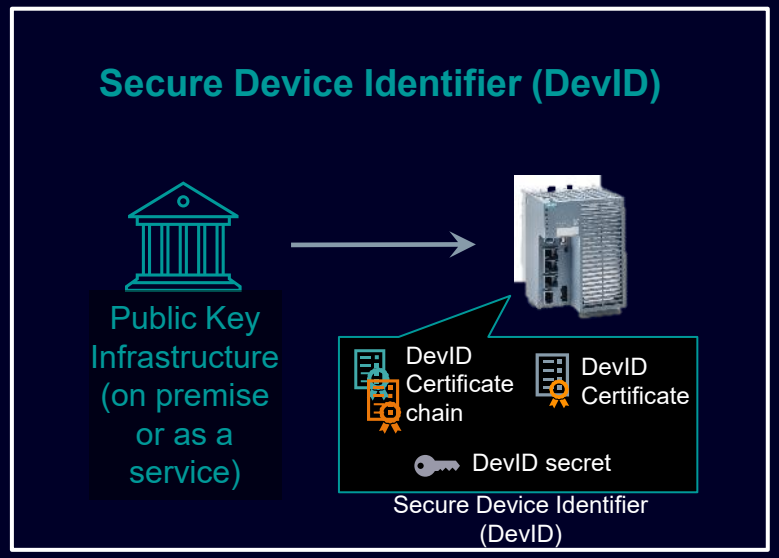
In order to keep pace with continuous advances in the market as well as threats from the criminal world, businesses and governments need to coordinate their actions in a targeted manner. We are therefore joining forces to protect our democratic and economic values against cyber and hybrid threats. In this charter, the signing partners outline the key principles we consider essential for establishing a new charter of trust between society, politics, business partners, and customers.

aes – Learn more
AIRBUS – Learn more
Allianz – Learn more
Atos – Learn more
BOSCH – To the Partner
DELL Technologies – Learn more
Deutsche Post DHL Group – To the Partner
IBM – Learn more
Infineon – Learn more
MITSUBISHI HEAVY INDUSTRIES – Learn more
msc – To the Partner
NTT – Learn more
NXP – Learn more
SGS – Learn more
SIEMENS – Learn more
TotalEnergies – To the Partner
TÜV SÜD

SIEMENS

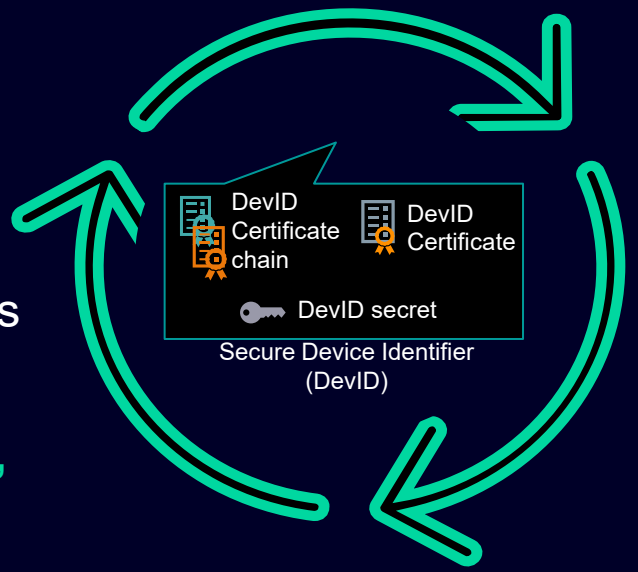
Secure Digital Identities in OT – as the Foundation of Trust in Connected systems

IEEE 802.1AR



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

DevID Lifecycle

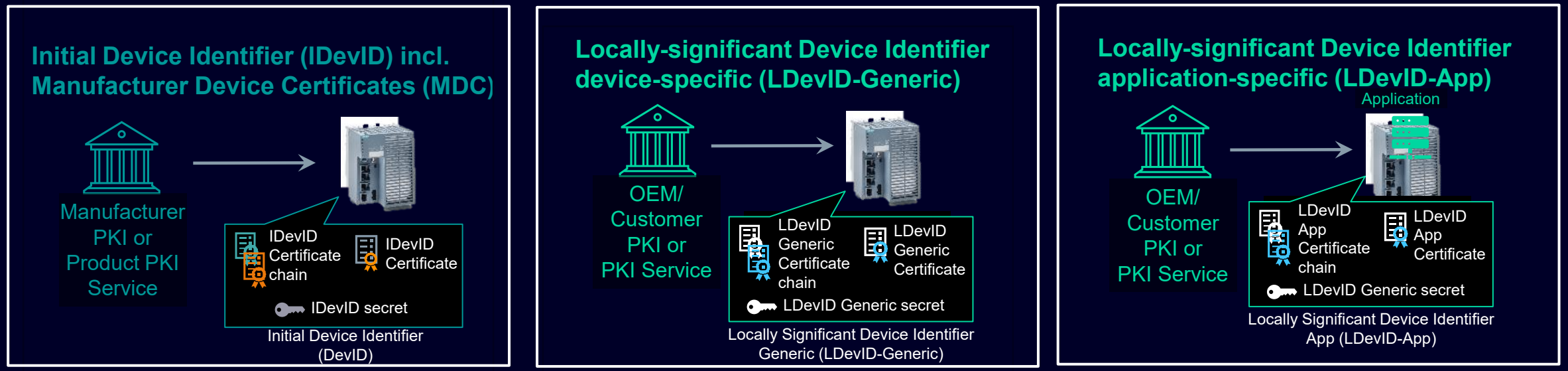


EU Cyber Resilience Act | IEC 62443 | PROFINET | OPC UA | never trust always verify | Charter of Trust

SIEMENS

Secure Digital Identities in OT – Different Types for Binding to Specific Operational Contexts

IEEE 802.1AR



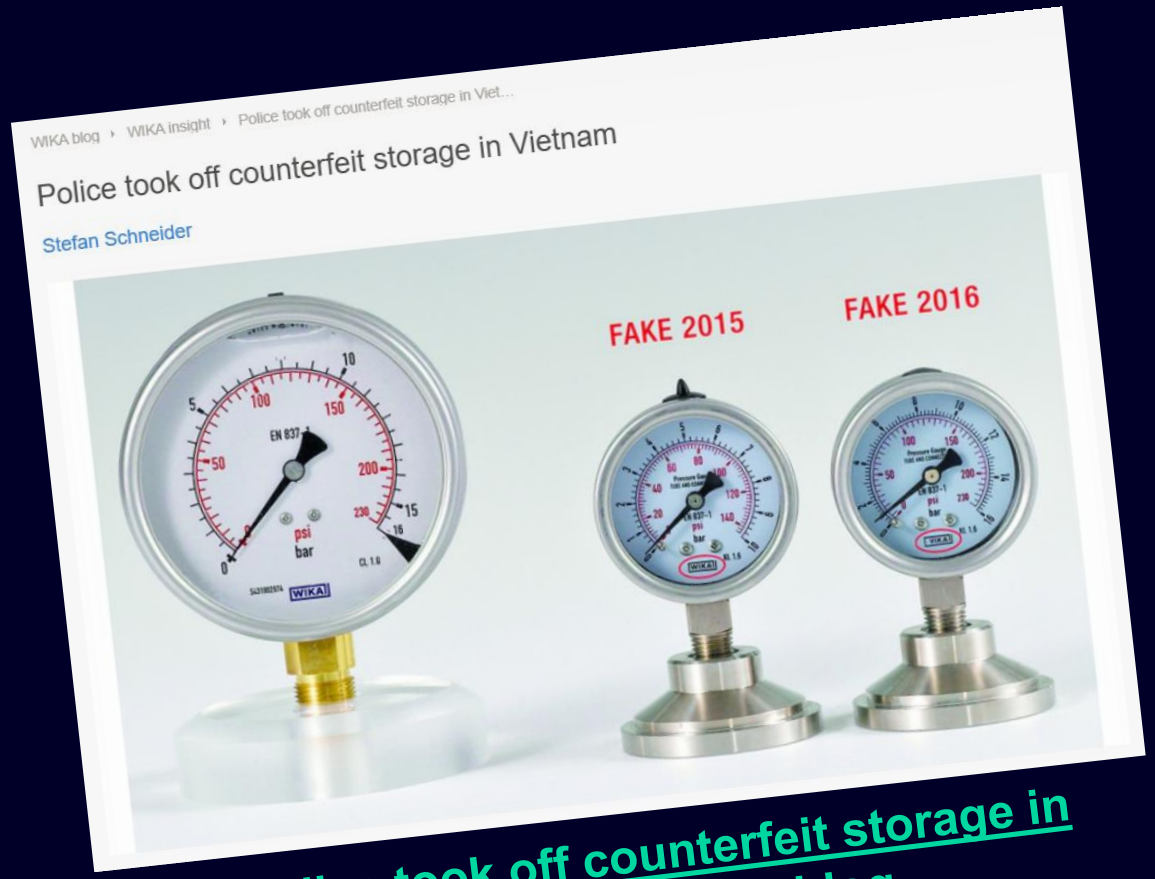
EU Cyber Resilience Act

IEC 62443

never trust always verify

SIEMENS

Secure Digital Identities in OT – Why they matter



Police took off counterfeit storage in Vietnam - WIKA blog

Gotcha! Counterfeit devices in Malaysia - WIKA blog

SIEMENS

Secure Digital Identities in OT – Why they matter

VDMA[1] Report on Counterfeit and Pirated Products in Mechanical Engineering

VDMA Studie Produktpiraterie

72% of companies in the German mechanical and plant engineering sector report being affected by product or brand piracy.
The estimated annual damage is **€6.4 billion**, equivalent to approximately **29,000** jobs lost.

Unfair imitation (53%) and brand piracy **(47%)** are the most common forms.

Most frequent: components and external design **(each ~60%).**
Also affected: entire machines, spare parts, catalogs, and increasingly websites and online shops **(21%).**

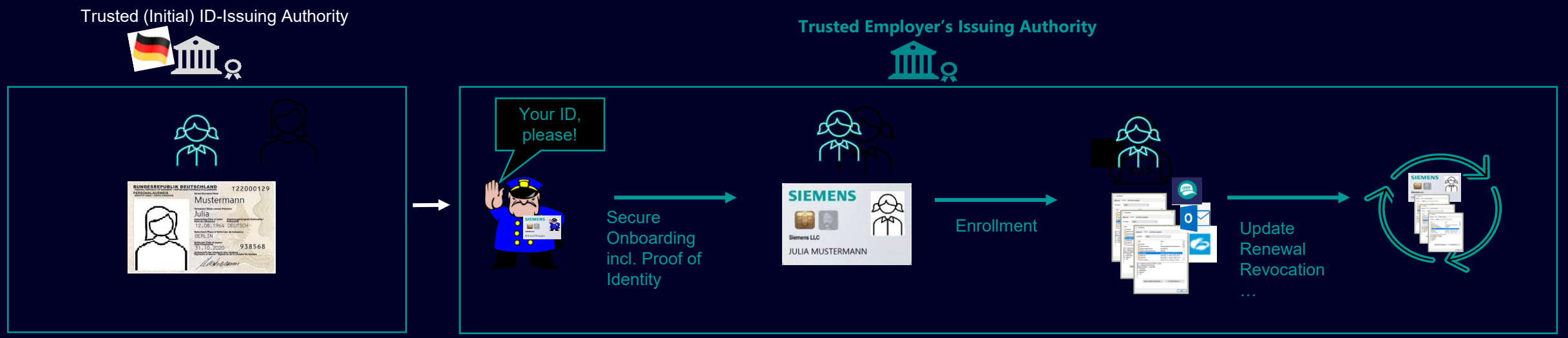
41% of companies report that counterfeits pose a direct risk to human safety.
52% say they threaten the safe operation of machinery.

Secure Digital Identities **help ensure** that only **authentic, trusted devices** are integrated into operational environments.

[1] VDMA: Mechanical Engineering Industry Association of Germany

SIEMENS

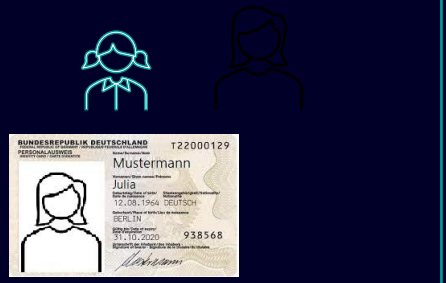
Secure Digital Identities in OT – How they work?

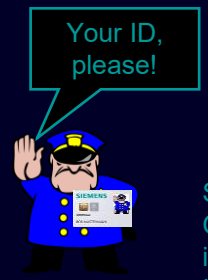


SIEMENS

Secure Digital Identities in OT – How they work?

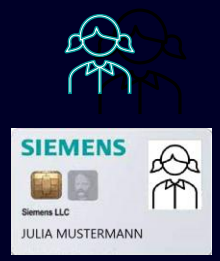
Trusted (Initial) ID-Issuing Authority



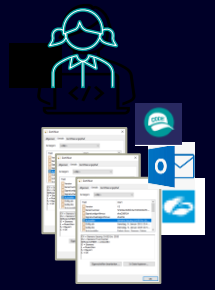


Secure Onboarding incl. Proof of Identity

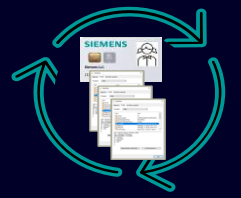
Trusted Employer's Issuing Authority



Enrollment



Update
Renewal
Revocation
…



Trusted Manufacturer's Issuing Certificate Authority

IDevID Certificate chain

IDevID Certificate

IDevID secret

Initial Device Identifier (IDevID)

Trusted Distributor's / OEM's / Customer's Issuing Certificate Authority

Secure Device Onboarding, Registration & Certificate Mgt.

Secure Device Onboarding incl. Proof of Identity

LDevID Generic Certificate chain

LDevID Generic Certificate

LDevID Generic secret

Locally Significant Device Identifier Generic (LDevID-Generic)

Enrollment

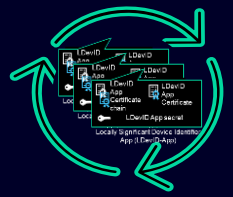
LDevID App Certificate chain

LDevID App Certificate

LDevID App secret

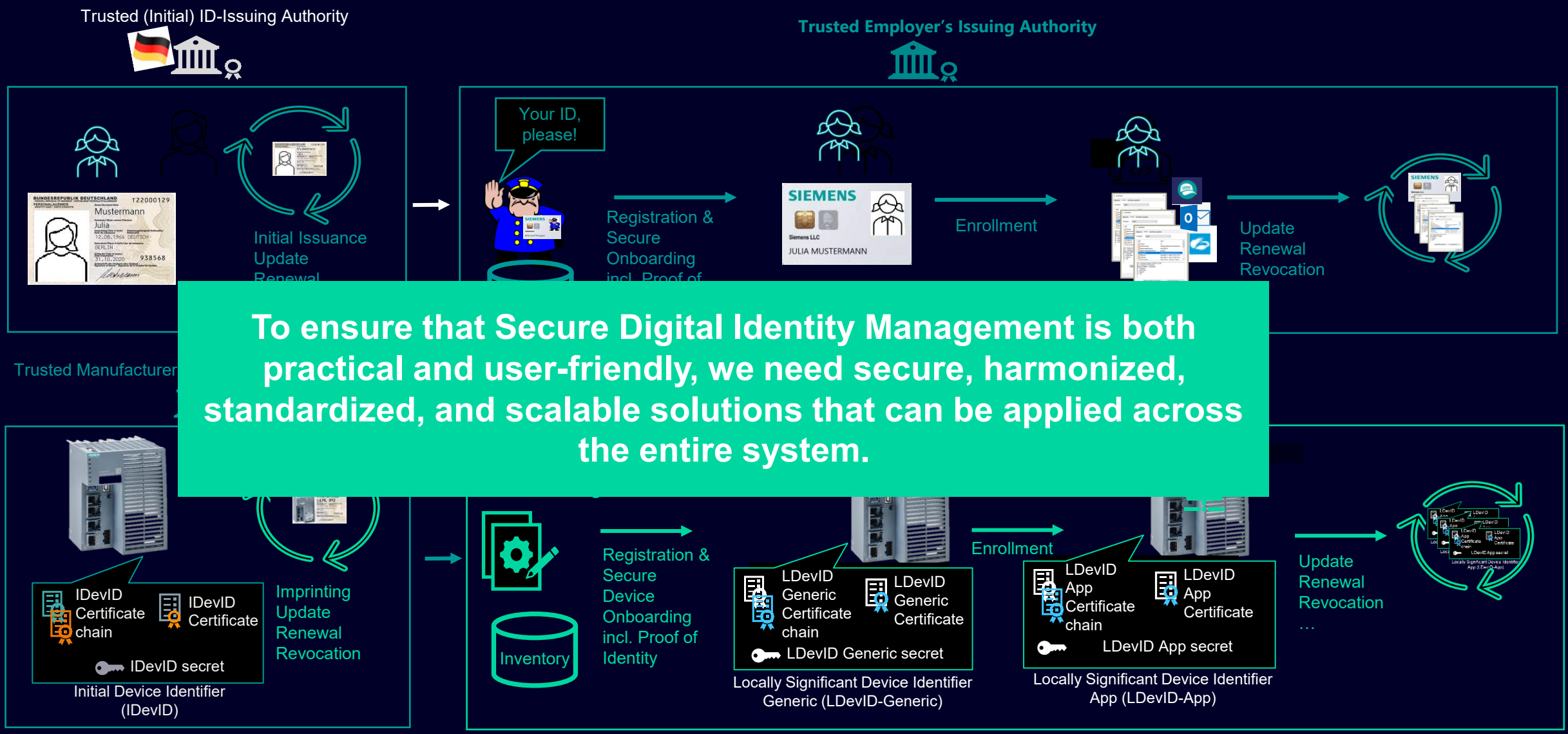
Locally Significant Device Identifier App (LDevID-App)

Update
Renewal
Revocation
…



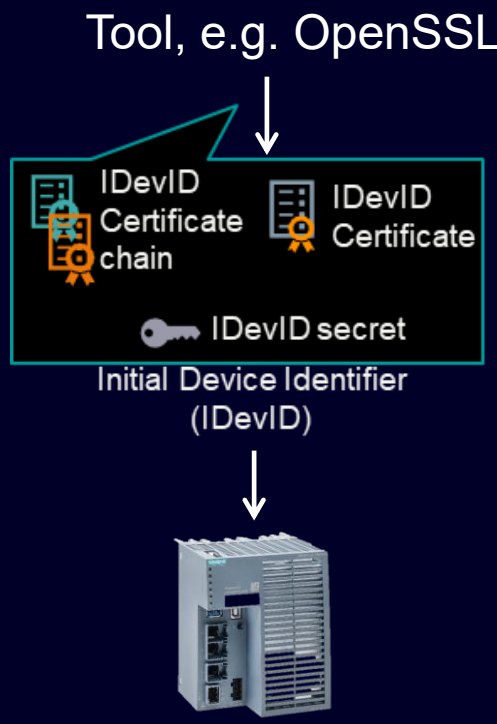
SIEMENS

Secure Digital Identities in OT – How they work?



SIEMENS

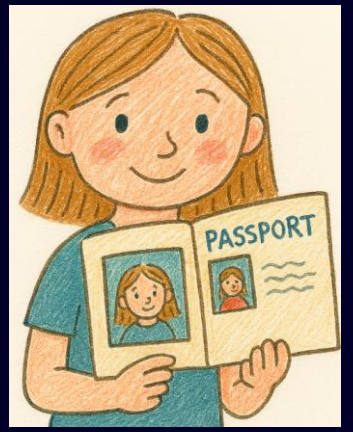
Secure Digital Identities in OT – Initial concept – Boundary conditions (1)



Don't use self-signed certificates

With **OpenSSL** or similar tools, **anyone can generate and sign certificates** themselves.
But self-signed certificates are:

- ❌ **Not verifiable** by external systems
- ❌ **Easily spoofed** by attackers
- ❌ **Not scalable** for secure supply chains or multi-party environments



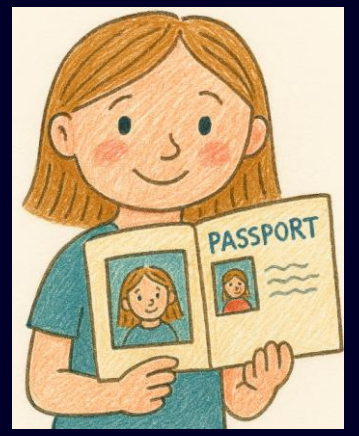
SIEMENS

Secure Digital Identities in OT – Initial concept – Boundary conditions (1)

Don't use self-signed certificates

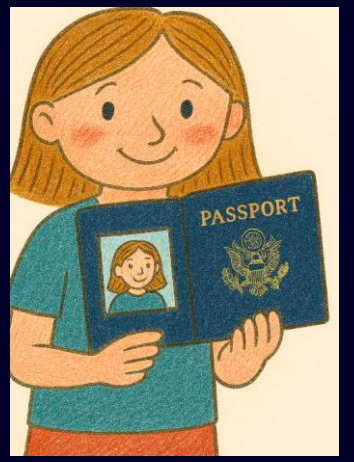
With **OpenSSL** or similar tools, **anyone can generate and sign certificates** themselves.
But self-signed certificates are:

- ❌ **Not verifiable** by external systems
- ❌ **Easily spoofed** by attackers
- ❌ **Not scalable** for secure supply chains or multi-party environments



Better Alternative:

Only certificates issued by a **trusted (state-of-the art) Certificate Authority (CA)** enable **secure**, **interoperable**, and **auditable** device identities.



SIEMENS

Secure Digital Identities in OT – Initial concept – Boundary conditions (2)

Don’t build your own Certificate Authority (CA)

- **No external trust:**
- Self-developed CAs are not recognized by external systems or partners.
- **High complexity:** Secure key management, certificate revocation, auditing, and compliance require deep expertise.
- **Scalability issues:** Managing identities across large, distributed environments is challenging.
- **Security risks:** Misconfigurations or weak protection can lead to impersonation and unauthorized access.

SIEMENS

Secure Digital Identities in OT – Initial concept – Boundary Conditions (2)

a state-of-the-art CA

Don’t build your own Certificate Authority (CA)

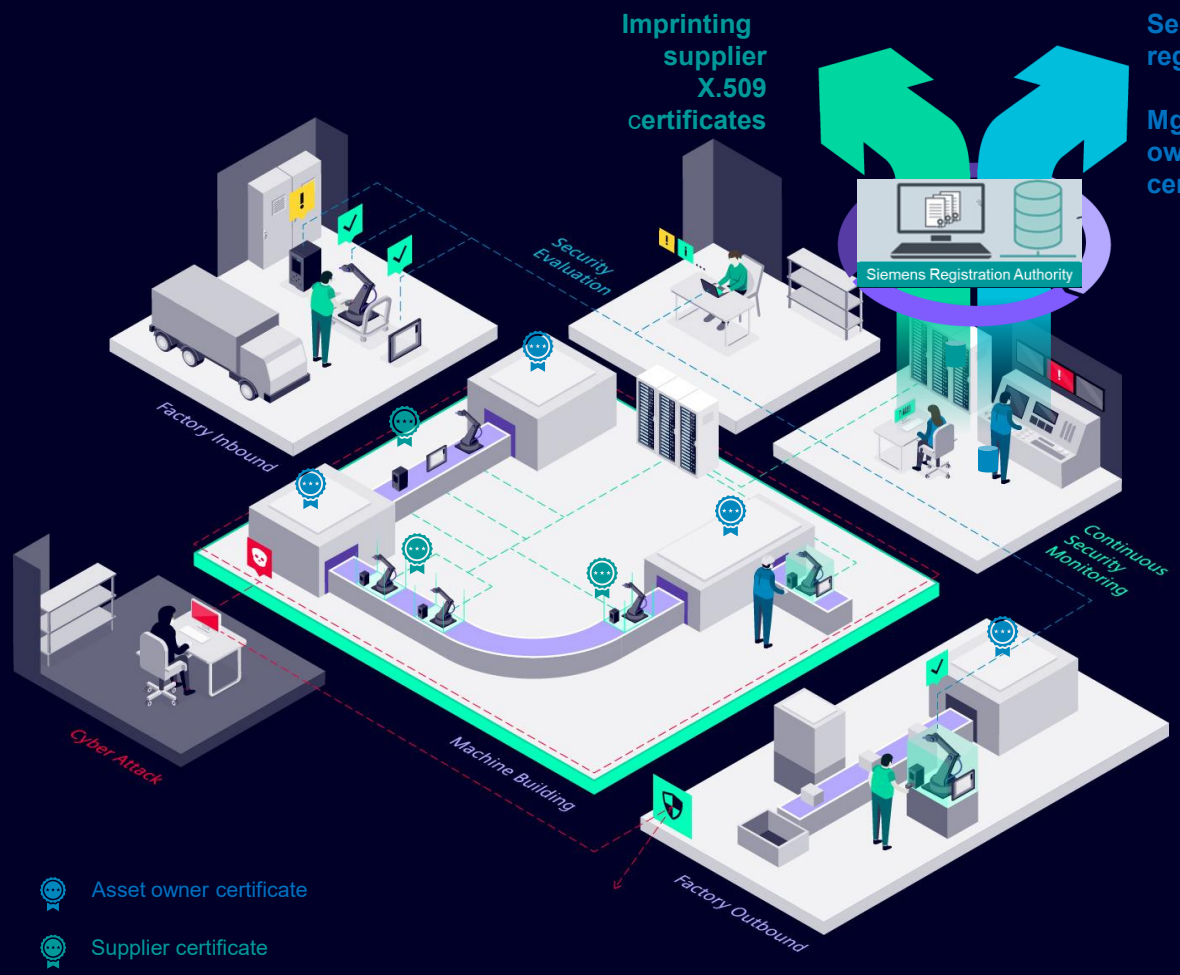
- **No external trust**:
- Self-developed CAs are not recognized by external systems or partners.
- **High complexity**: Secure key management, certificate revocation, auditing, and compliance require deep expertise.
- **Scalability issues**: Managing identities across large, distributed environments is challenging.
- **Security risks**: Misconfigurations or weak protection can lead to impersonation and unauthorized access.

Better Alternative:

- Use a **trusted, standards-compliant (commercial) CA** to ensure **secure**, **scalable**, and **interoperable** digital identities
- Most companies already operate a **Certificate Authority (CA)** within their **Enterprise PKI infrastructure**.
- OT devices and applications **do not need their own CA** – they simply require a **secure gateway** to connect to the existing enterprise CA.

SIEMENS

Certificate Management in OT
Solutions to the challenges due to standards and regulations



- **Provisioning product supplier roots of trust**
  Imprinting of supplier X.509 certificates and roots of trust
- **Secure OT communication**
  Management of asset owner X.509 certificates (e.g. OPC UA certificates) in an automatic way for any OT protocols, devices and applications
- **Secure registration of devices and applications incl. proving their identity/ originality**
  Secure onboarding incl. providing a proof of identity originality

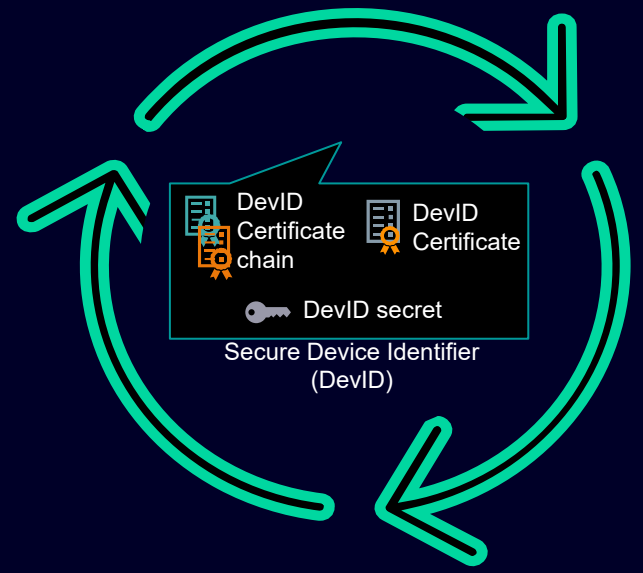
SIEMENS

Secure Digital Identities in OT – Final Thoughts

Secure Digital Identities are the foundation for cybersecurity in OT.

They enable Zero Trust, support lifecycle authentication, simplify integration between IT and OT systems and strongly contribute to the asset transparency and trackability across the lifecycle.

By automating identity processes and promoting standardized solutions we boost cybersecurity and operational efficiency across our ecosystem.



SIEMENS

Contact

Anna Palmin
Distinguished Key Expert Cyber Security
Digital Industries – Process Automation – Siemens
anna.palmin@siemens.com

Frank Laurig
Product Owner FDS Registration Authority
System Engineer Professional
Foundational Technology – Siemens
frank.laurig@siemens.com

SIEMENS