IoT / OT Security Conference

TEMET
end-to-end IT security

www.infosec-iot.ch

TEMET
end-to-end IT security

Vernetzte Identitäten

Warum Zero Trust in IoT/OT mit "sicheren" Identitäten beginnt

André Clerc, TEMET AG

19.05.2026, Cham ZG

Über den Referenten

André Clerc
Dipl. Inf.-Ing. FH, CISSP,
CAS Project Management

Managing IT Security Consultant
Tätig in der Information Security seit 2000

Kern Kompetenzen

- Security Consulting und Engineering
  Entwicklung von Systemen/Lösungen, welche gegenüber von Böswilligkeit, Fehlern oder Missgeschicken resistent sind
- PKI/M, angewandte Kryptographie
- Kontinuierliche Systemhärtung
- Business Process Modelling (BPMN 2.0)

Engagements

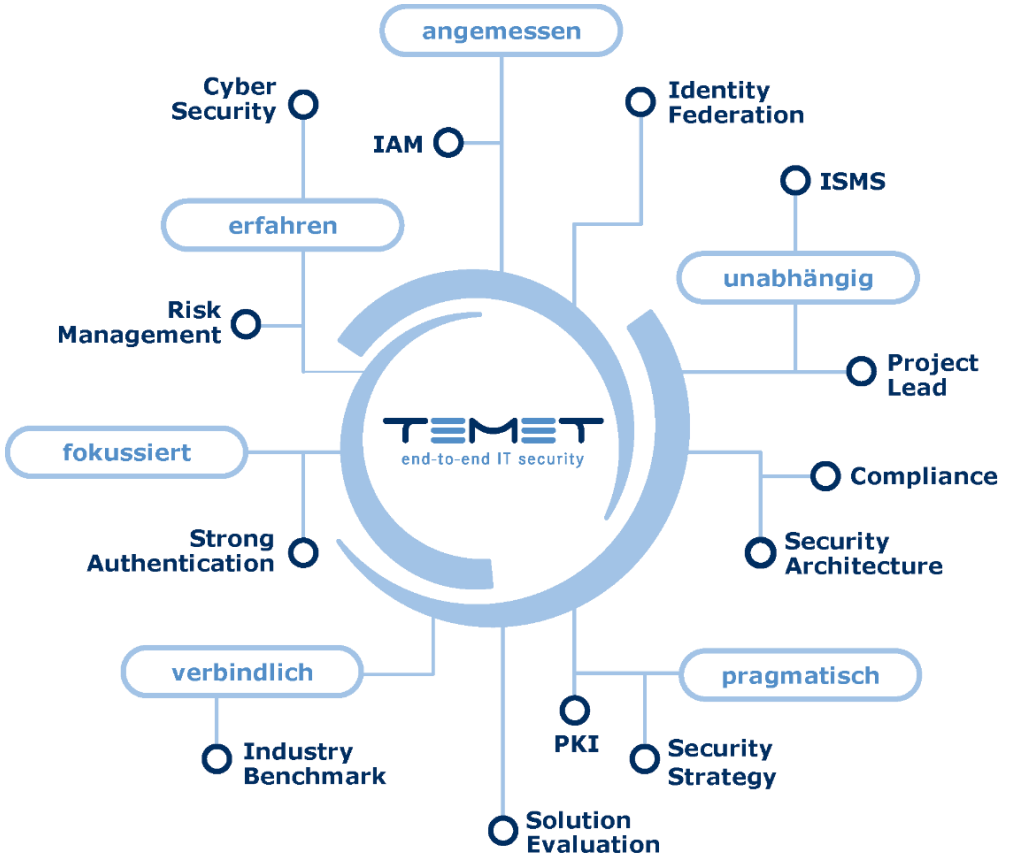
- Founder of About & Beyond Trust Conference
- Author of PKI Education @ SwissSign

TEMET
end-to-end IT security

TEMET AG

- 14 erfahrene Security Consultants
- Über **250 Jahre** Erfahrung
- **100% unabhängig** – produktneutral und nur unseren Kunden verpflichtet
- Über **160 Kunden** aus unterschiedlichen Branchen
- In der ganzen Schweiz tätig - Sitz im Herzen von Zürich

Wir planen, konzipieren und realisieren Sicherheitsvorhaben und unterstützten unsere Kunden bei der nachhaltigen Gewährleistung ihrer Security.



TEMET
end-to-end IT security

TEMET
end-to-end IT security

Einleitung

Wenn Firewalls hinfällig werden

- Durch die OT/IoT und IT Konvergenz werden klassische Sicherheitsmodelle (Perimeter Security) hinfällig
  - **Erosion des Perimeters**
    Durch Vernetzung lösen sich die klassischen Netzwerkgrenzen auf
  - **Implizites Vertrauen**
    Ein Standort (Herkunft -IP/Port) ist kein Beleg für Integrität
  - **Laterale Ausbreitung**
    (Lateral Movement)
    Uneingeschränkten Zugriff auf das gesamte interne Netz

- **Makro- → Mikrosegmentierung**
  Perimeter-Schutz → granularer Schutz von Ressource (Netz intern)

- **Paradigmenwechsel ist notwendig**
  Sicherheit muss direkt ans Asset (das Objekt) gebunden werden

  Implicit Trust → Explicit Trust (Zero Trust)

Neues Architektur-Paradigma: Zero Trust

- **Herausforderung**
  - Identitäts- und Asset-Management
  - Etablieren des Vertrauens (Trust)
  - Sicherstellung der Funktionalität (Latenz Echtzeit-Anforderungen)
  - Nachrüsten
  - Perfomance & Ressourcen
  - Verfügbarkeitsanforderungen (CIA- vs. AIC-Pyramide)
- **Regulatorische Anforderungen** (Security/Safety)
  - **Cybersicherheit** notwendig
  - **Kryptographie** wird Pflicht (vgl. CRA, NIS2)

TEMET
end-to-end IT security

Zero Trust in OT/IoT

Was ist Zero Trust (für OT)

- **Explizites Vertrauen**
  - Jedes Datenpaket muss seine Herkunft (Identität) und seine Daseinsberechtigung (Kontext) belegen
- **Ziel**
  Binden des Schutzes an das Asset (Netzwerk: ungesicherter Transport)

- **Vertrauenskette in der Produktion (Werkshalle)**
  - **Identität**: Wer sendet Daten? (Steuerung oder ein Angreifer?)
  - **Integrität**: Sind die Daten integer? (Wurden Steuerbefehle manipuliert?)
  - **Kontext**: Dürfen Daten in diesem Kontext vorkommen? (Ist ein Firmware-Update-Befehl um 03:00 legitim?)

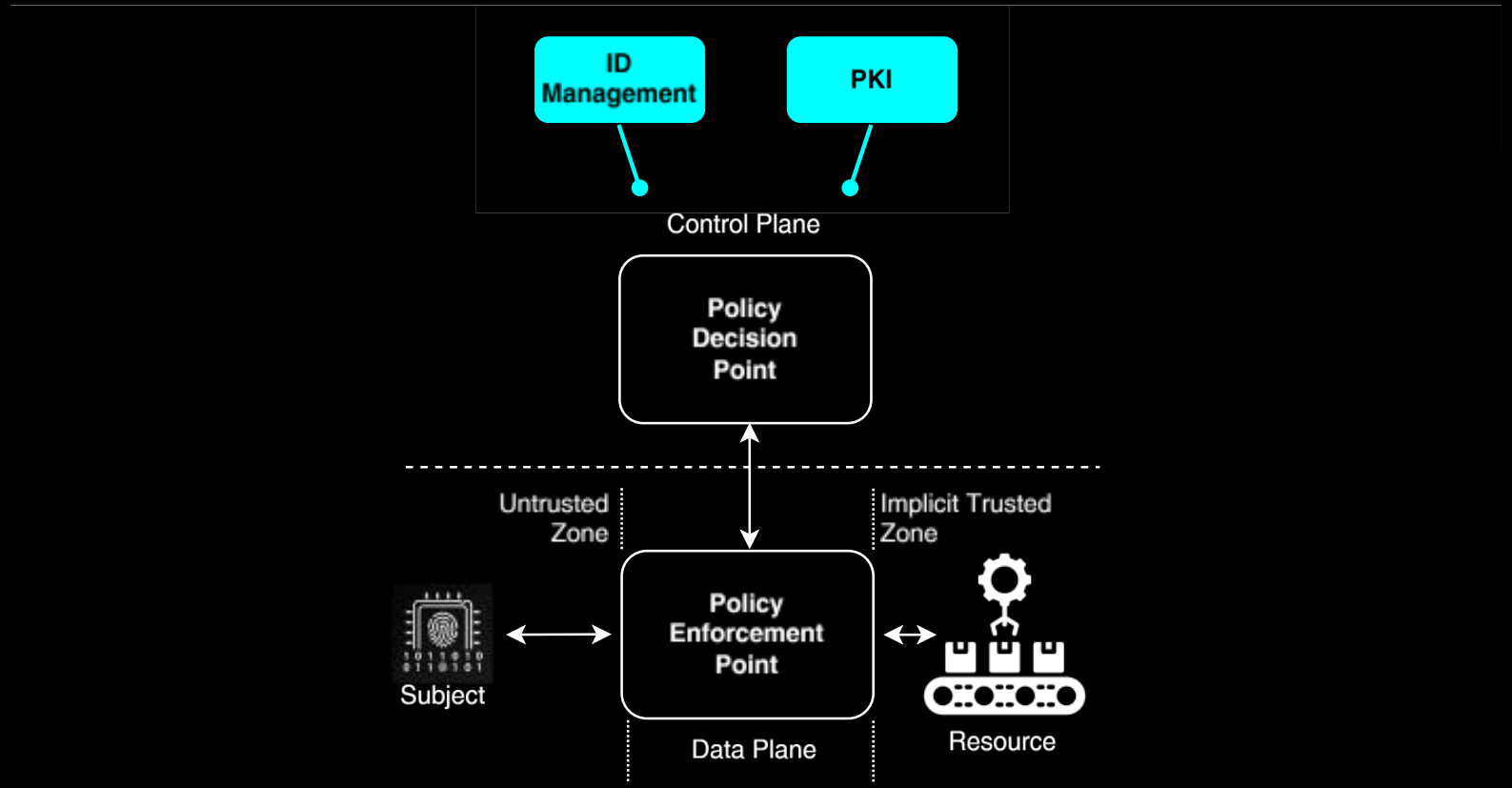
Zero Trust Grundhaltung & Prinzipien

- **Zero Trust ≠ fertiges Produkt**

- **Strategische Grundhaltung**
  - **Never Trust, Always Verify**
    Standardzustand für Subjekt & Datenverbindung:
    nicht vertrauenswürdig
  - **Assume Breach** (Annahme einer Sicherheitsverletzung)
    Annahme: Angreifer ist *bereits im System* oder Einbruch ist unvermeidbar

- **Strategische Leitprinzipien**
  - **Verify Explicitly**
    (Vertrauen ist kein Standard)
  - **Least Privilege** *&*
    Just-in-Time / Just-Enough Access
  - **Minimize Blast Radius**

Zero Trust Kernkomponenten



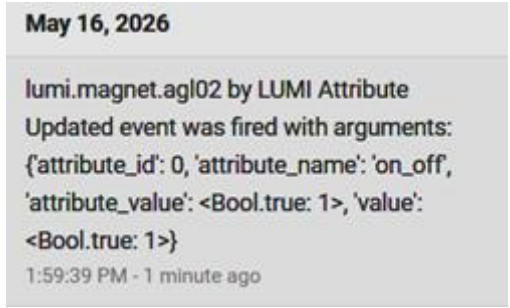
NIST SP 800-207

Strukturelle ZTA Aufbau

- **Identitätsmanagement (IdM)** (Subject)
  - Identitäten-Inventar
    → IdM/IAM
  - Geräte-Inventar
    → Unified Endpoint Management (UEM)
- **IdM & PKI**
  - Ermöglicht das verifizieren des Subjects
    (wer, Rolle, Berechtigung)
  - Establish **temporary Subject Trust** (Authentication)
- **Weitere Komponenten**
  - Ermöglicht das verifizieren des Kontexts
  - Establish **temporary Context Trust** (Authorization)

Trust Base

- **Eindeutige Identität**
  - Nachweisbare & fälschungssicher
  - Unverzichtbare Fundament von Zero-Trust-Architektur



- **X.509-Zertifikate**
  - Etablierter Standard
  - Kann für Unternehmen im IoT/OT-Umfeld zur Herausforderung werden

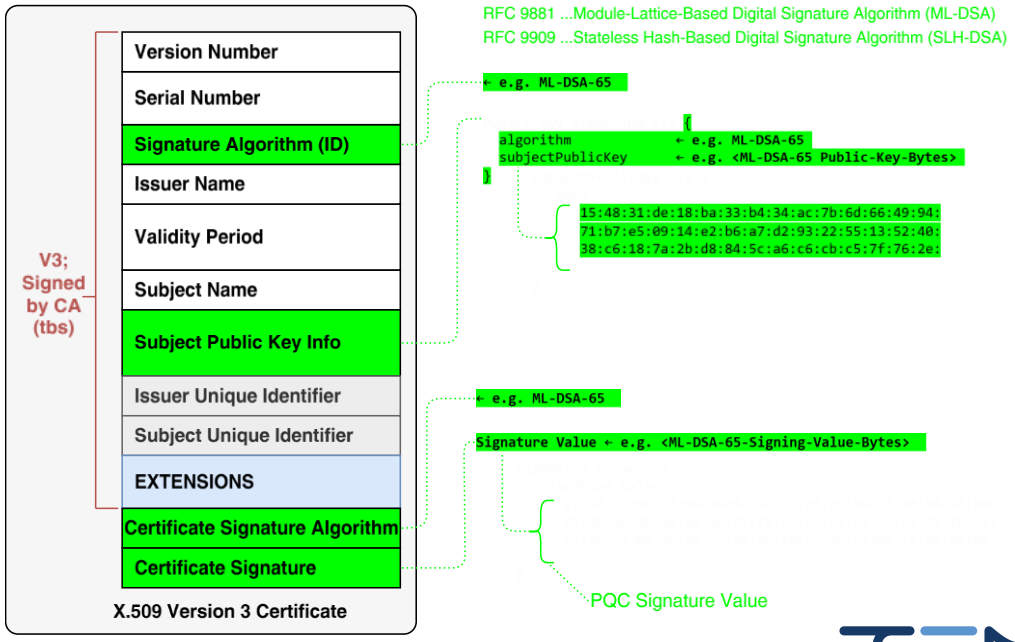
TEMET
end-to-end IT security

TEMET
end-to-end IT security

Digitale Device-DNA

Zero Trust in der Produktion

- **Netzwerk-Port → Geräte-ID**
  - Es nicht entscheidend, wie ein Gerät angeschlossen ist, sondern wer oder was es ist
- **Digitale Identität als Sicherheitsanker**
  - Eindeutige und sichere Identität wird zur einzigen Konstante



TEMET end-to-end IT security

X.509 - Digitale Device-DNA

- **Kryptografische Eindeutigkeit (Binding)**
  - **Identität** wird untrennbar an einen öffentlichen Schlüssel gebunden
- **Integrität der Metadaten**
  - Manipulationsgeschützte Informationen (Hersteller, Modell, SN, etc.)
- **Dezentrale Validierung (Offline-Fähigkeit)**
  - **Chain of Trust** ermöglicht eine unabhängige Identitätsprüfung (Essenziell Echtzeit-Anforderungen)
- **Herstellerübergreifende Interoperabilität**
  - Ermöglichten sichere Kommunikation in heterogenen Umgebungen (Multi-Vendor-Strategie)

TEMET
end-to-end IT security

Diskrepanz zwischen Zero-Trust-Anspruch & Realität

Operative Sicherheitslücke im industriellen Deployment

- **Fehlende Identität**
- **«Insecure-by-Design»**
- **Fehlende Plattform-Integrität**
  - **Hardening**
    Minimierung der Angriffsfläche
  - **Secure Boot**
    Sicherstellung Codeintegrität

Hardware-Limitierung
Systemressourcen für Krypto vs. 30 Jahre alte Chips (Legacy Debt)

Fehlende Hardware-Anker

Bestandsgeräte haben keinen sicheren Speicherort (z.B. TPM) für geheime Schlüssel
(Release Datum < 2016)

Fehlende Offenheit
(Closed Systems)

Import von Fremdzertifikaten nicht möglich
(Proprietäre Steuerungen)

Operative Sicherheitslücke im industriellen Deployment

- **Das Brownfield-Problem**
  Maschinen mit einer Lebensdauer von 30+ Jahren verstehen kein modernes Zertifikatsmanagement
- **Lifecycle-Management**
  Skalierung in Industriellen Massstab (automatisiertes Enrollment/Renewal)
- **Konnektivität**
  Widerrufsprüfung (CRL) in isolierten "Air-Gapped" Netzen
- **Infrastruktur-Hürden**
  Zeit-Synchronisation (NTP) als kritischer Artefakt
- **Folge**
  Zero Trust scheitert oft an der **fehlenden, sicheren Identität** & **unflexibler Hardware**

TEMET
end-to-end IT security

Lösungsansätze – Identität „injizieren“

Nachrüsten (Retrofitting) digitaler IDs (OT-ID)

- **Natives Nachrüsten**
  (wo immer möglich)
  - **Geräte ab ~2016**
    - Unterstützen oft bereits TLS/DTLS 1.2 und können ggf. mit einem FW Update TLS/DTLS 1.3 unterstützen
  - **Moderne SPS**
    - z. B. unterstützt die SIMATIC S7 TLS 1.3 ab Juni 2021 (ab FW 2.9 / TIA V17)
- **Zero Trust Ready**
  - Native Authentisierung und Verschlüsselung ermöglicht direkte Kommunikation mit dem Policy Decision Point

Nachrüsten (Retrofitting) der digitalen ID (OT-ID)

- **Externes Nachrüsten** (Sicherheits-Gateway)
  Implementierung als Hardware-basierter Policy Enforcement Point

- **Edge Gateway**
  - Protokoll-sensitive Applikations-Gateways, L4-L7
  - Übernimmt die OT-ID stellvertretend, bricht Datenverkehr auf, übersetzt Protokolle

- **Transparent Proxy**
  - Inline Sicherheitsbrücken, L2/L3
  - Schaltet sich unsichtbar in den Datenstrom für Kapselung/Verschlüsselung
  - Zwingend erforderlich **Out-of-Band-Schnittstelle** zum Policy Decision Point

Technologische Enabler für Sicherheits-Gateway/Proxies

- **Trust Anchors & TPMs** (Hardware-Sicherheit)
  - Nutzung von Hardware-Sicherheitsmodul (z. B. TPM 2.0)
- **Krypto-Agility**
  - PQC Ready
- **Zero Touch Provisioning** (ZTP) (Skalierbarkeit)
  - Beim ersten Einschalte; vollautomatisch konfigurieren → sicherer Bezug ihrer OT-ID
- **Virtual Layering** (Netzwerk-Erzwingung)
  - Technologische Basis für den Transparent Proxy
  - Mittels SDN oder Overlay-Netzwerken (wie MACsec/IPsec) wird die Identität & Verschlüsselung auf Netzwerkebene erzwungen (völlig isoliert und unsichtbar vom eigentlichen Endgerät)

TEMET
end-to-end IT security

Quintessenz

Key Takeaways - Identität als Fundament

- **Identität vor Architektur**
  - Zero Trust ist ohne eineindeutige Identität unmöglich
- **Identität wird zur Währung**
  - Mit der Vernetzung ist bewiesene Identität das wertvollste Gut
- **X.509 - kryptografischer Anker**
  - Etablierter (kryptographischer) Standard & Echtzeit-Abfragen unabhängig
  - «Einzige» Lösung für komplexe IoT/OT-Umgebungen
- **Pragmatismus schlägt Perfektionismus**
  - Wenn Deployment scheitert → Brückentechnologien nutzen
  - Sichere Identitäten sind vor oder neben dem Gerät zu etablieren
- **Strategie schlägt Tooling**
  - IdM, IAM & PKI sind wichtiger als neue Firewalls
- **Trust**
  - Muss jedes Mal neu verdienen werden

¿ Fragen ?

Backup Slides

Start ZTA-Transition

TEMET
end-to-end IT security

ZTA-Transition

- **Analyse und Inventarisierung**
  → Sofort beginnen
  - OT/IoT/Krypto-Inventar erstellen
    - **Externe Kommunikation**
    - **Interne Kommunikation**
    - **Gespeicherte Daten (Data-at-rest)**
    - **Software-Entwicklung**
  - Risikobewertung
  - Krypto-Agilität anstreben

- **Strategie, Planung & Pilotprojekte**
  … Kurz- bis mittelfristig
  - Roadmap entwickeln
  - Hersteller-Kommunikation
  - Testen-Szenarien erstellen

- **Schrittweise Umsetzung**
  … Mittelfristig
  - Externe Systeme zuerst
  - Neue Projekte ZTA-Ready machen
  - Interne Systeme und Daten Absichern

ZTA-Transition

Standards & sind verfügbar

Technologien sind verfügbar

Anbieter unterstützen X.509 Zertifikate und TLS Protokolle

Neue Produkte, SW, etc. sollten TLS 1.3 unterstützen

ZTA-Transition sofort **starten**

Beginne mit Analyse & Inventarisierung