

Sichere Maschinenidentitäten für IoT und OT

Ihre Basis für eine vernetzte Zukunft

- ◆ Certificate Lifecycle Management
- ◆ Unlimited Scalability
- ◆ Security by Design

Cybersecurity 
Made in Germany

Sichere Maschinenidentitäten für IoT und OT

Ihre Basis für eine vernetzte Zukunft

Die digitale Transformation in der Industrie schafft Innovation, erhöht jedoch auch die Komplexität und die Anforderungen an die Cybersicherheit. Vernetzte Produktionsanlagen, IoT-Plattformen und smarte Geräte sind nicht nur der Motor moderner Industrien – sie sind auch ein attraktives Ziel für Cyberangriffe.

Mit der ECOS TrustManagementAppliance® (TMA) als Lieferant von digitalen Identitäten, Schlüsseln und Zertifikaten legen Sie den Grundstein für eine sichere und zukunftsfähige digitale Infrastruktur – das Fundament für Cybersicherheit.

Herausforderungen in IoT und OT: Sicherheit neu gedacht

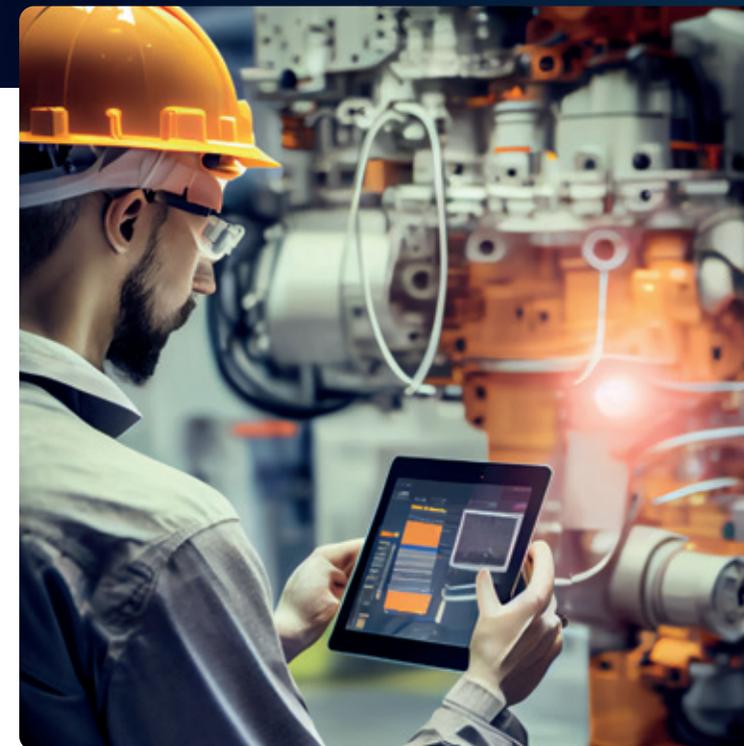
In IoT- und OT-Umgebungen gelten andere Regeln als in klassischen IT-Netzwerken.

◆ **Skalierbarkeit:** Millionen von Geräten, Sensoren und Aktoren tauschen in Echtzeit Daten aus. Jedes dieser Geräte benötigt eine eindeutige und vertrauenswürdige Identität.

◆ **Lebenszyklen:** IoT- und OT-Geräte sind oft Jahrzehnte im Einsatz. Langfristige Sicherheitsstrategien, die zukünftige Bedrohungen wie Quantencomputer berücksichtigen, sind entscheidend.

◆ **Ressourcenbegrenzung:** Viele IoT-Geräte verfügen nur über begrenzte Rechenleistung oder Speicherkapazitäten und benötigen speziell dafür optimierte Sicherheitslösungen.

◆ **Prozessintegration:** Digitale Zertifikate und Schlüssel müssen sich nahtlos in Produktionsprozesse und bestehende Systeme einfügen lassen.



Cybersecurity Made in Germany

Mit der Entwicklung, Consulting & Support in Deutschland können wir auf die Anforderungen unserer Kunden individuell und lösungsorientiert eingehen.

Hochwertige Sicherheitsstandards – Ein Muss in der Industrie

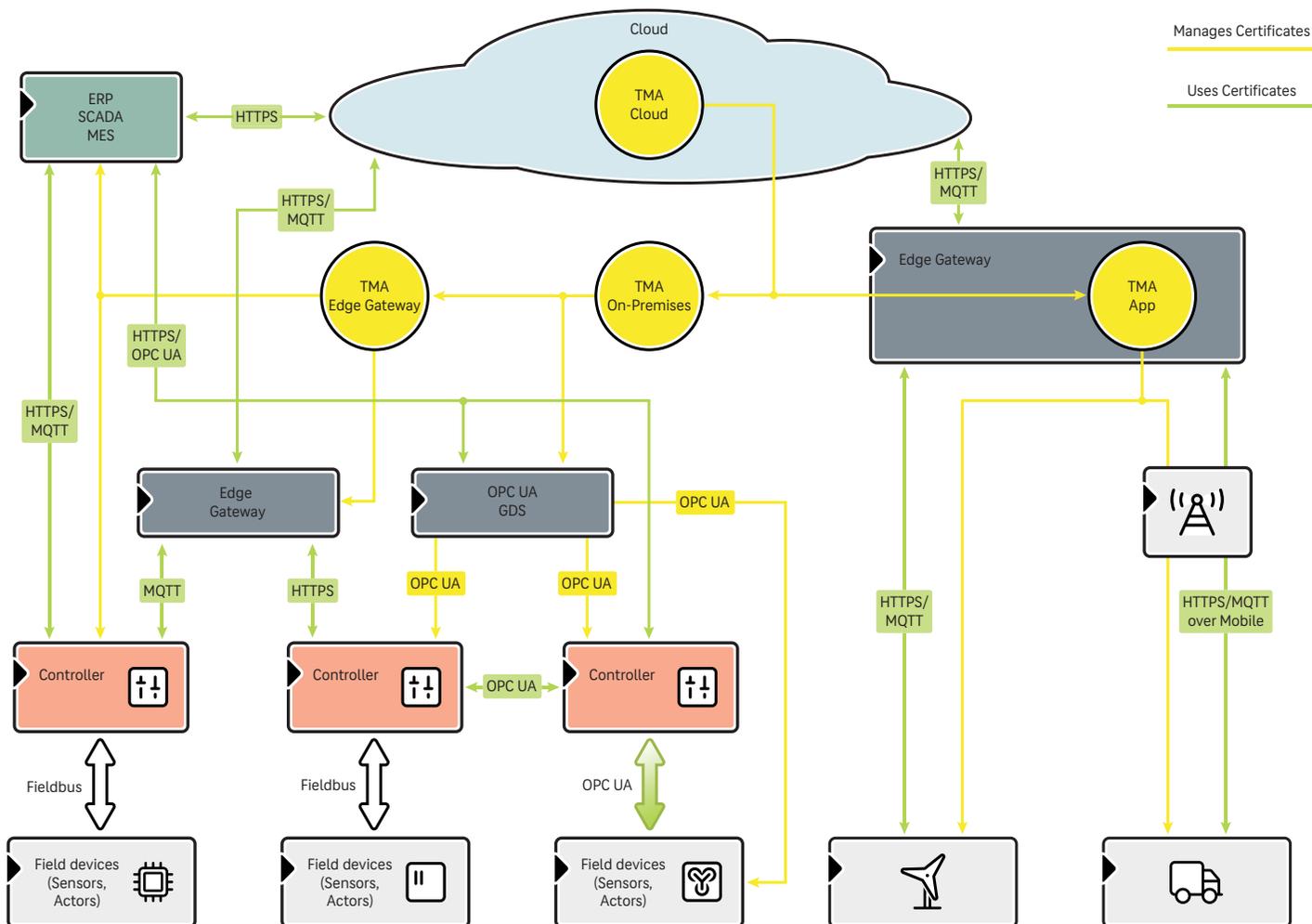
Mit zunehmender Regulierung durch Vorgaben wie NIS-2 und dem Cyber Resilience Act wird Security by Design unverzichtbar.

ECOS unterstützt Unternehmen mit der ECOS TrustManagementAppliance® und durch umfassende Beratung bei Planung, Implementierung und Nutzung, um nicht nur Compliance zu erreichen, sondern auch Ihre Prozesse nachhaltig zu verbessern.

Sichere Kommunikation in IoT- und OT-Infrastrukturen

Mit der ECOS TrustManagementAppliance®

Beispiele für den Einsatz der ECOS TMA in einer OT-Umgebung



Das Schaubild zeigt eine beispielhafte OT-Umgebung, in der die einzelnen Komponenten miteinander kommunizieren.

Während viele Feldbusse Authentisierung und Verschlüsselung gar nicht oder nur bedingt unterstützen, ist dies bei neueren Protokollen wie **OPC UA** bereits Teil des Standards. Auch die weitere Kommunikation, z.B. per **MQTT** oder **HTTPS**, kann durch **TLS** abgesichert werden. Dazu benötigen die einzelnen Komponenten Zertifikate. Zertifikate und digitale Schlüssel werden aber u.U. auch für die produzierten Geräte benötigt und müssen im Produktionsprozess sicher aufgebracht werden.

Die ECOS **TrustManagementAppliance** bietet diverse Möglichkeiten die Zertifikatverwaltung und -verteilung zu organisieren und automatisieren. Dabei kann sie z.B. einem OPC UA Global Discovery Server Zertifikate zur Verfügung stellen, der diese dann im OPC UA-Netzwerk verteilt. Aber auch andere Systeme versorgt die TMA über eine Vielzahl von Schnittstellen und einer flexiblen Anpassbarkeit mit Zertifikaten.

Die ECOS **TrustManagementAppliance** kann dabei je nach Anforderung als virtuelle Maschine on-Premises, als App auf einem Edge Gateway diverser Hersteller oder in der Cloud betrieben werden. Eine Neuheit ist der Betrieb als ECOS **TMA Edge Gateway**, das speziell für Produktionsumgebungen ausgelegt ist, die eine hohe Verfügbarkeit und Offline-Fähigkeit erfordern und trotzdem ohne Spezialwissen sicher betrieben werden müssen.

ECOS TrustManagementAppliance®

Cybersecurity Made in Germany

Die ECOS TMA wurde speziell für die Anforderungen von IoT- und OT-Umgebungen entwickelt.

Mit der ECOS **TrustManagementAppliance** schaffen Sie die Grundlage für eine langfristig sichere digitale Infrastruktur. Unsere Lösung vereinfacht die Erstellung, Verwaltung und Verteilung von digitalen Schlüsseln und X.509-Zertifikaten – essenziell für **Vertraulichkeit, Integrität** und **Authentizität** in IoT- und OT-Infrastrukturen.

Unsere Zertifikate sind die Voraussetzung für den Schutz durch:

- ◆ **Verschlüsselung:** Schützt sensible Daten und Kommunikation vor unbefugtem Zugriff – ob zwischen Geräten, Systemen oder Standorten.
- ◆ **Signierung:** Gewährleistet, dass Daten und Software nicht manipuliert wurden, und sorgt für die Integrität von Programmen und Maschinensteuerungen.
- ◆ **Authentifizierung:** Ermöglicht vertrauenswürdige Maschinenidentitäten, die essenziell für Zero Trust-Konzepte und sichere Netzwerke sind.

Egal ob Steuergeräte, SCADA, SPS, IoT-Plattformen oder ERP-Systeme: Unsere Lösungen liefern den Schlüssel zu einer sicheren Kommunikation – unabhängig von Protokollen wie **MQTT, OPC UA** oder **HTTPS**.

Verschlüsselung, Signierung, Authentifizierung

Mit der ECOS TMA verwalten Sie digitale Schlüssel und Zertifikate mühelos – für verschlüsselte, signierte und authentifizierte Kommunikation in IoT- und OT-Systemen.

Ihre Vorteile im Überblick

Zertifikate und Schlüssel leicht gemacht

- ◆ Automatisierte **Erstellung, Verwaltung und Verteilung** von Zertifikaten und Schlüsseln.
- ◆ **Certificate Lifecycle Management:** Behalten Sie den Überblick über Lebenszyklen, verlängern Sie Zertifikate automatisch und sperren Sie kompromittierte Schlüssel zuverlässig.
- ◆ Unterstützung aller relevanten Standards: **X.509-Zertifikate, symmetrische und asymmetrische Schlüssel, Protokolle wie SCEP, ACME, EST und CMP** und vieles mehr.

Nahtlose Integration in Ihre Umgebung

- ◆ **Flexibel einsetzbar:** Integration in bestehende PKIs, Betrieb als Root- oder Sub-CA und Anbindung an öffentliche CAs.
- ◆ **Offene Schnittstellen:** REST-API, AD-Synchronisation, SCIM, Radius, SNMP und Log-Aggregation
- ◆ **Produktionstauglich:** Zertifikataufbringung im laufenden Produktionsprozess durch maßgeschneiderte Anpassungen.
- ◆ **Überall verfügbar:** Egal ob on-Premises, in der Cloud, als Edge Gateway in externen Anlagen oder bei Dienstleistern – Online oder Offline.

Zukunftssichere Lösungen

- ◆ **Post-quantum resilience:** Vorbereitung auf eine Ära mit Quantencomputern durch Kryptoagilität und Hybridzertifikate.
- ◆ **Skalierbarkeit:** Ob 100 oder 100 Millionen Zertifikate – die ECOS TMA wächst mit Ihren Anforderungen.
- ◆ **Investitionssicherheit:** Eine Lösung, die auch langfristig kommende Sicherheitsansprüche erfüllt.

Langfristige Partnerschaft

- ◆ **Fokussierung:** Spezialisiertes Know-how für Lösungen für OT und IoT.
- ◆ **Effizienz:** Schnelle Implementierung in Ihre bestehende Infrastruktur.
- ◆ **Beratung und Support:** Begleitung bei der Planung, Implementierung und Nutzung sicherer Maschinenidentitäten – bereits ab der Entwicklungsphase.

PKI und Lifecycle-Management von Zertifikaten und Schlüsseln für IoT/OT

Sicherheit beginnt mit vertrauenswürdigen Identitäten

TMA Universe

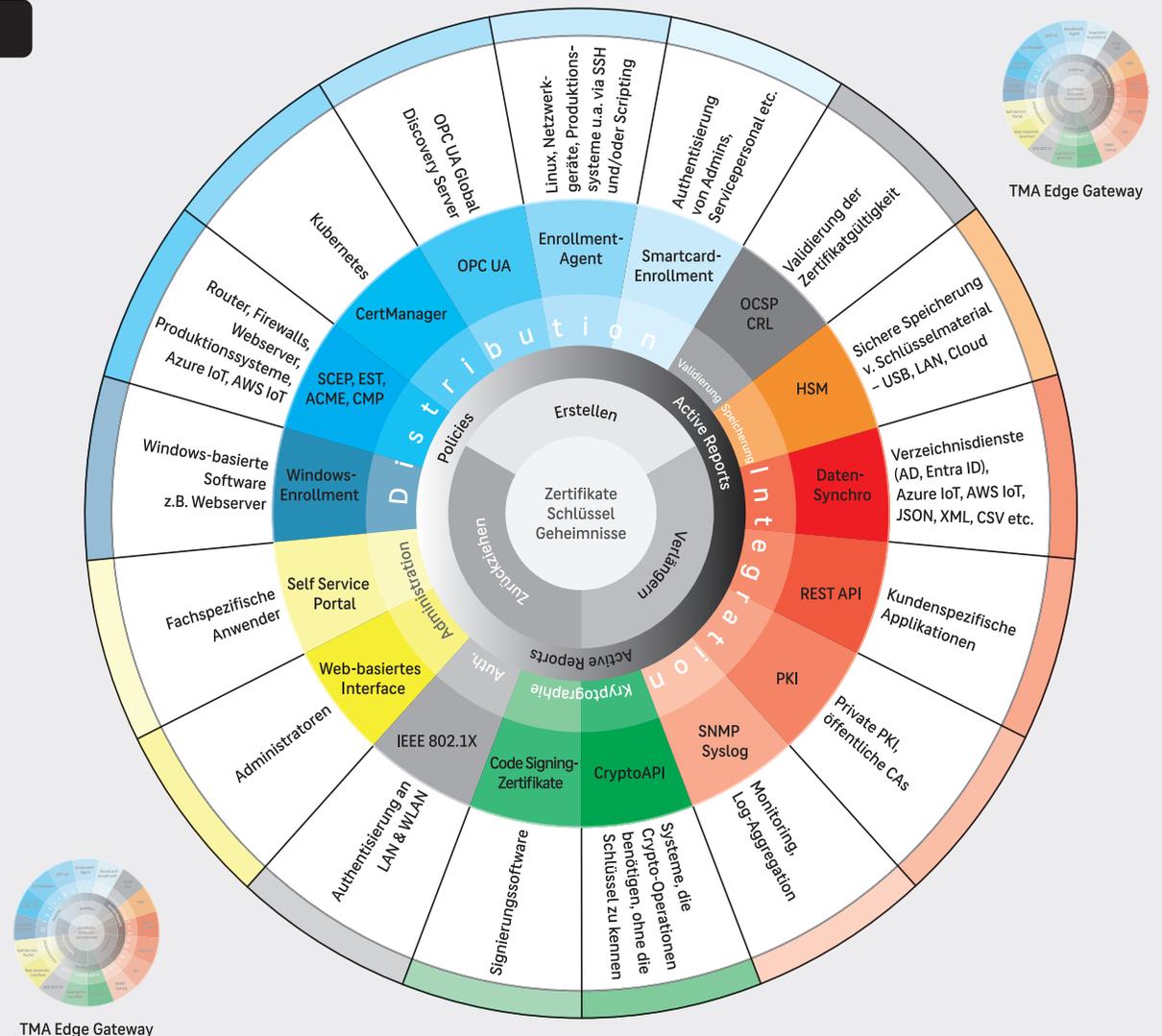
Für das Management digitaler Schlüssel und Zertifikate bietet die ECOS TrustManagementAppliance® eine umfassende Plattform zur sicheren Verwaltung kryptographischer Identitäten in IoT- und OT-Umgebungen. Ihre Architektur mit den zentralen Funktionen **Erstellung, Speicherung, Verteilung, Validierung** und **Administration** gewährleistet eine sichere, skalierbare und automatisierte Verwaltung digitaler Identitäten in vernetzten Infrastrukturen.

Wesentliche Funktionen:

- ◆ **Automatische Distribution:** Unterstützung aller gängigen Standardprotokolle sowie OPC UA, Kubernetes und weitere.
- ◆ **Zertifikatverwaltung:** Automatisierte Prozesse zur Ausstellung, Verlängerung und Sperrung. Unterstützung von OCSP und CRL.
- ◆ **Schlüsselspeicherung:** Sichere Ablage auf HSMs, USB, LAN oder Cloud.
- ◆ **Protokollierung & Monitoring:** Integration in Log-Aggregations-Systeme und SNMP zur Ereignisüberwachung

Schnittstellen & Integration:

- ◆ **IoT & OT-Kompatibilität:** Unterstützung für Cloud-IoT und industrielle Produktionssysteme.
- ◆ **Protokolle & APIs:** REST API, SCEP, EST, ACME, CMP für nahtlose Anbindung.
- ◆ **Verzeichnisdienste:** Integration mit Active Directory (AD), Entra ID und anderen LDAP-basierten Systemen.
- ◆ **Self-Service & Administration:** Web-basiertes Interface und Self-Service-Portal für einfache Verwaltung.



Automatisiertes Zertifikatmanagement Mit der ECOS TrustManagementAppliance®



Warum Maschinenidentitäten unverzichtbar sind

Von Sensoren und Aktoren bis hin zu komplexen Produktionsmaschinen – die Identität eines jeden Geräts muss zweifelsfrei nachweisbar sein, um die Grundlagen der Industrial Cybersecurity zu schaffen.

Verhindern von Industriespionage und Informationsbeschaffung für potenzielle Cyberangriffe durch die Verschlüsselung aller Datenströme.

Sicherstellen von Authentizität und Vertrauenswürdigkeit bei der Maschinenkommunikation.

Absichern industrieller Infrastrukturen gegen Manipulationen oder Angriffe, die ganze Produktionsketten gefährden können.

Schnell. Sicher. Automatisiert.

Automatisierte Zertifikatverwaltung:

Sicher und effizient mit der ECOS TMA

Unterstützung gängiger Standards:

Für eine nahtlose Integration

Regelkonformer Zertifikatprozess:

Abgleich mit vordefinierten Richtlinien

Sichere Zertifikatbereitstellung:

Nur genehmigte Anfragen werden weitergeleitet

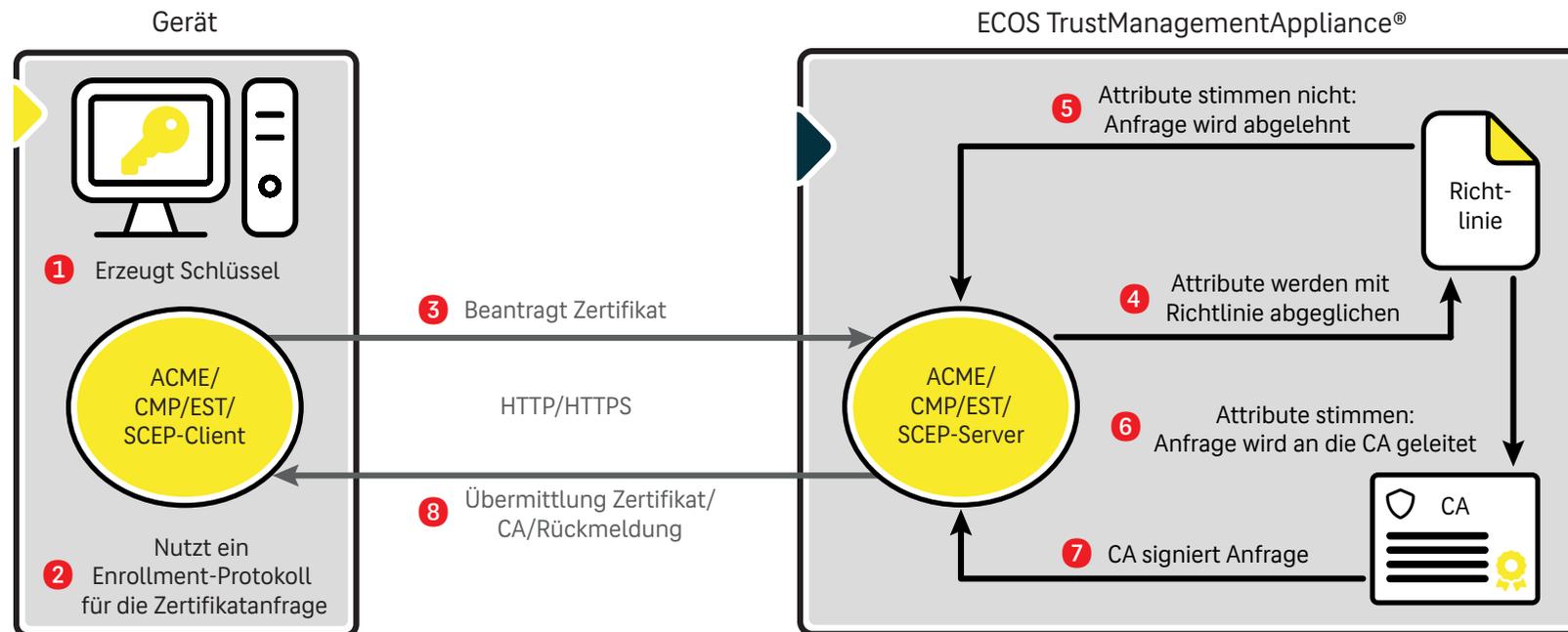
Vollständig automatisierter Ablauf

Die ECOS TrustManagementAppliance®

Sicherheit beginnt mit vertrauenswürdigen Identitäten

ECOS TrustManagementAppliance®

Prozess der Zertifikatausstellung und -verlängerung bei Nutzung eines Enrollment-Protokolls



Ablauf des automatischen Zertifikatenrollments

Auf dem Gerät wird ein Schlüssel erzeugt. Anschließend sendet es eine Zertifikatanfrage an den ECOS TrustManagementAppliance®-Server (1, 2 und 3).

Dort werden die Anfrageattribute mit den definierten Richtlinien abgeglichen (4). Stimmen die Attribute überein, wird die Anfrage an die Zertifizierungsstelle (CA) weitergeleitet und nach erfolgreicher Signierung

an das Gerät zurückgesendet (6, 7 und 8).

Stimmen die Attribute nicht überein, wird die Anfrage abgelehnt (5).

Durch diesen strukturierten Prozess gewährleistet die ECOS TrustManagementAppliance® eine sichere und regelkonforme Zertifikatbereitstellung in IoT- und OT-Infrastrukturen.



ECOS TrustManagementAppliance®

Ihr Partner für Industrial Cybersecurity Made in Germany

Vertrauen Sie auf eine Lösung, die speziell für die Anforderungen von IoT- und OT-Umgebungen entwickelt wurde. Mit unserer Erfahrung und Expertise schaffen wir sichere Grundlagen für eine vernetzte Zukunft – **effizient, skalierbar und investitionssicher**.

Wir verbinden höchste Sicherheitsstandards mit den Anforderungen Ihrer individuellen Umgebung.

Setzen Sie auf die ECOS TrustManagementAppliance® und gestalten Sie gemeinsam mit uns Ihre sichere digitale Zukunft.

ECOS Technology GmbH
Sant' Ambrogio-Ring 13 a-b
55276 Oppenheim Germany

+49 6133 939 200
sales@ecos.de

www.ecos.de

Vereinbaren Sie einen Gesprächstermin
und lassen Sie sich beraten!



Für detaillierte Informationen zur
ECOS TrustManagementAppliance®
steht das Technical Whitepaper zum
Download bereit.

