Sichere Maschinenidentitäten für IoT und OT

Ihre Basis für eine vernetzte Zukunft

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

Inhalt

Sichere Kommunikation in IoT und OT

Die ECOS **TrustManagementAppliance®** bietet eine umfassende Plattform zur sicheren Verwaltung kryptographischer Identitäten in IoT- und OT-Umgebungen. Ihre Architektur gewährleistet eine sichere, skalierbare und automatisierte Verwaltung digitaler Zertifikate und Maschinenidentitäten in vernetzten Infrastrukturen.

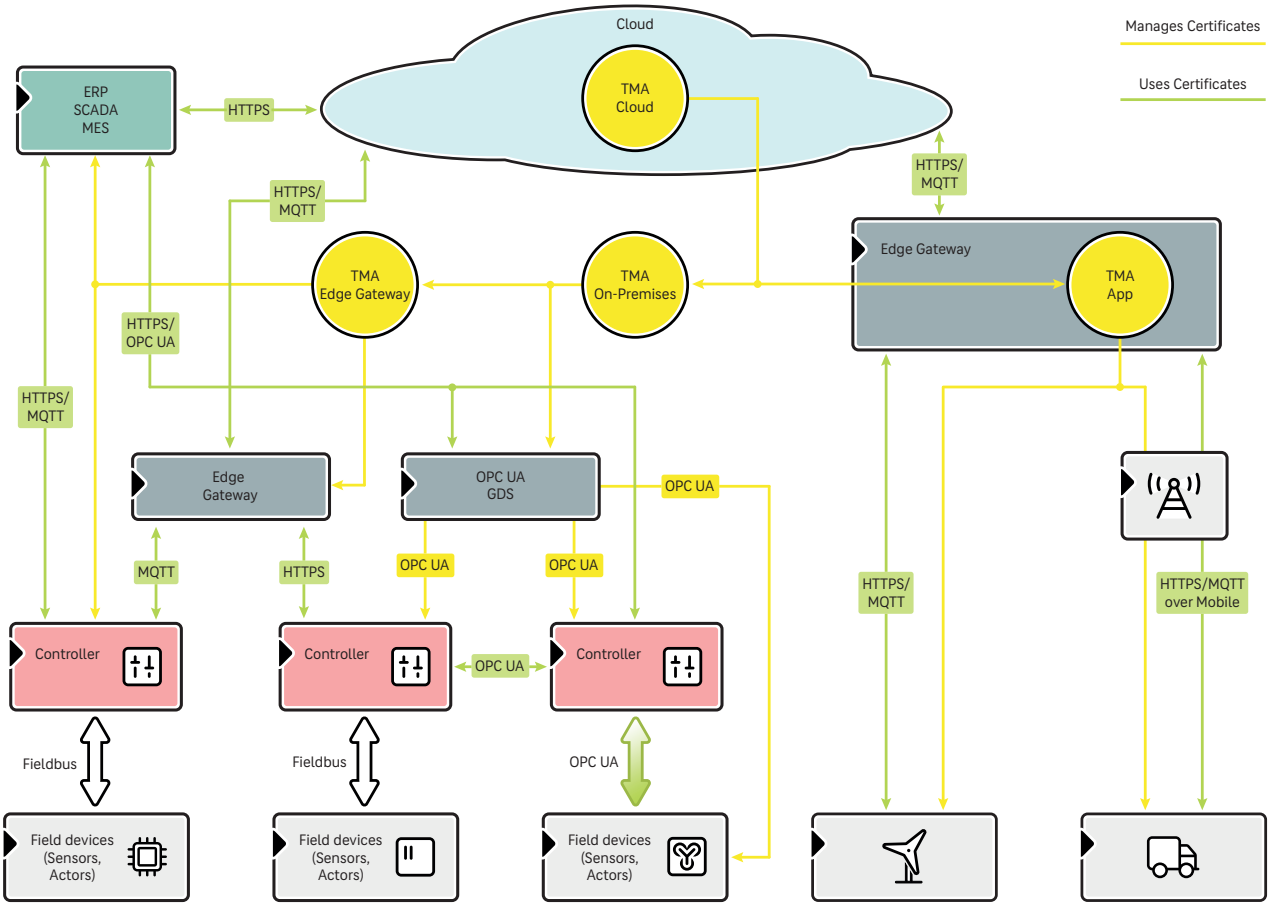
Sie ermöglicht den Aufbau einer eigenen PKI und die Automatisierung der dafür notwendigen Prozesse – von der Erstellung und Verwaltung bis hin zur Verteilung und Validierung von Zertifikaten.

Durch die breite Unterstützung automatisierbarer Zertifikatverteilungsmechanismen erleichtert sie die Durchsetzung von Sicherheitsrichtlinien, sorgt für eine vollständige Übersicht über alle unternehmensweit eingesetzten Zertifikate, passt sich flexibel an individuelle Anforderungen an und lässt sich so nahtlos in bestehende IT- und OT-Umgebungen integrieren.

Dieses Dokument beschreibt auf den folgenden Seiten, wie die TMA Unternehmen technisch dabei unterstützt, eine sichere und effiziente digitale Public-Key-Infrastruktur in IT-, OT- und IoT-Umgebungen aufzubauen.

Funktionsumfang der ECOS Trust ManagementAppliance®

Beispiele für den Einsatz der ECOS TrustManagementAppliance® in einer OT-Umgebung



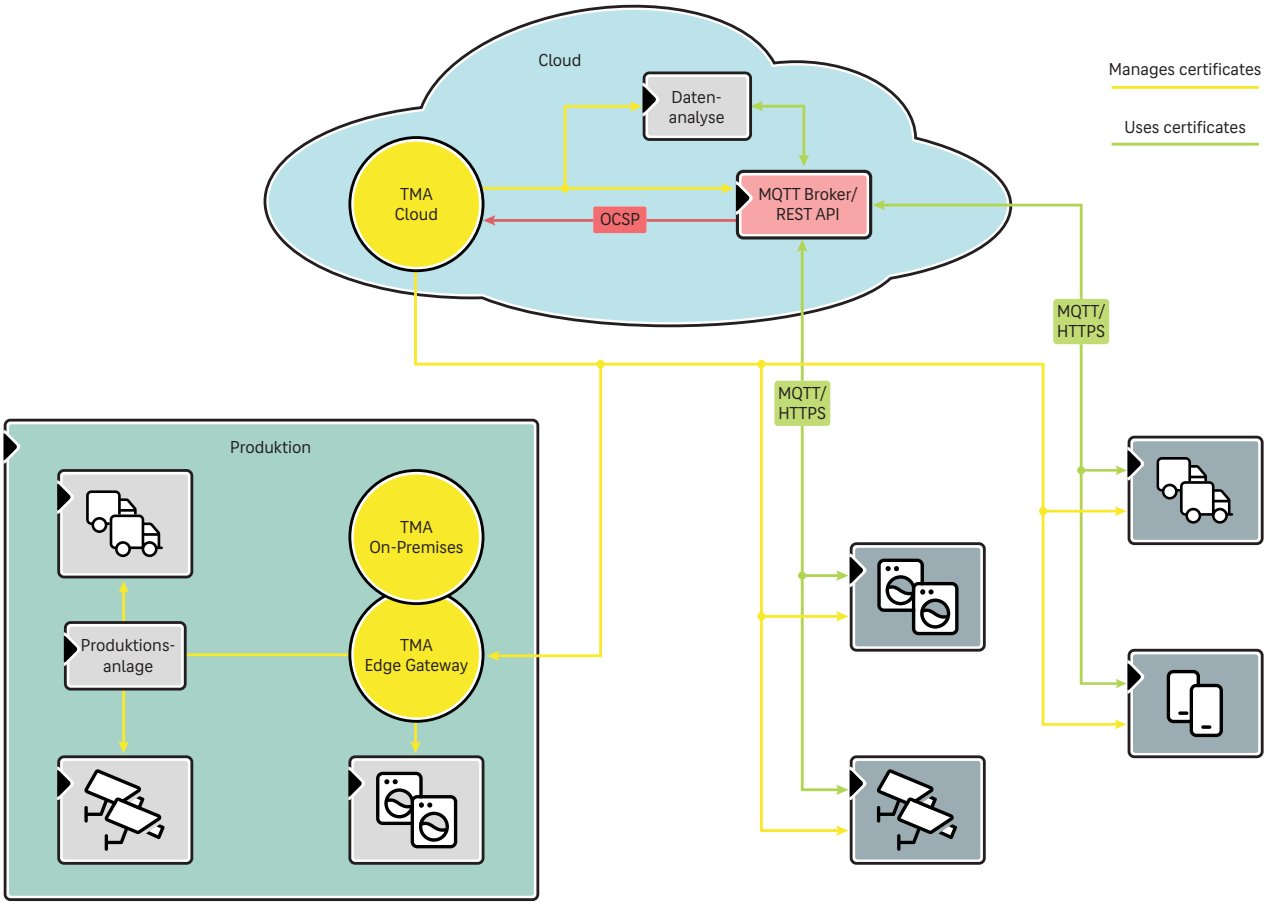
Während viele Feldbusse Authentisierung und Verschlüsselung gar nicht oder nur bedingt unterstützen, ist dies bei neueren Protokollen wie OPC UA bereits Teil des Standards. Auch die weitere Kommunikation, z.B. per MQTT oder HTTPS, kann durch TLS abgesichert werden. Dazu benötigen die einzelnen Komponenten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

Die Trust Managment Appliance 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 Trust Managment Appliance 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.

Beispiele für den Einsatz der ECOS TrustManagementAppliance® in einer IoT-Umgebung



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-Aggregation-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.

Zertifikate, Schlüssel, Geheimnisse

Zertifikate und Zertifikathierarchien

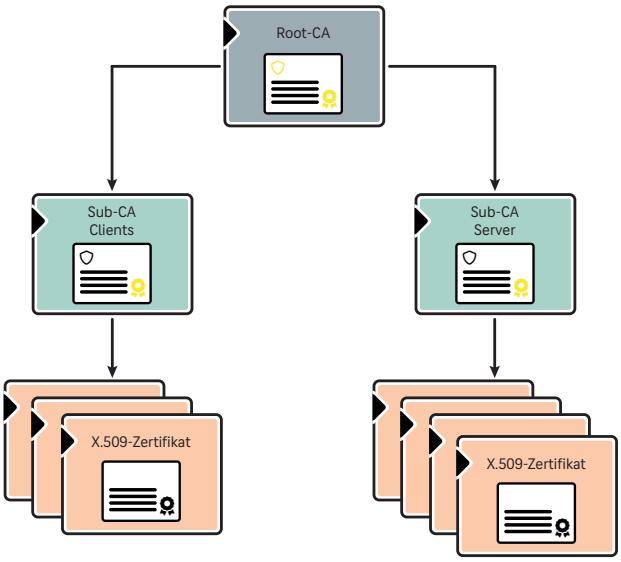
Der von der Trust Management Appliance verwendete X.509-Standard bietet eine einheitliche Struktur für alle zertifikatgebundenen Geräte-, Maschinen- oder Benutzeridentitäten und gewährleistet aufgrund seiner globalen Verbreitung eine hohe Interoperabilität.

Certificate Authority (CA)

Die Certificate Authority (CA) ist die Komponente einer Public-Key-Infrastruktur, die für den Aufbau hierarchischer Vertrauensketten zuständig ist.

Die Trust Management Appliance ermöglicht den Aufbau einer mehrstufigen Zertifikathierarchie mit beliebig vielen Root- und Sub-CAs, um auch komplexe Organisationsstrukturen in der Zertifikatverwaltung abzubilden.

Ein Stammzertifikat (Root-CA) signiert ihm untergeordnete CA-Zertifikate (Sub-CAs), welche wiederum ihnen untergeordnete Sub-CAs oder Endzertifikate signieren. So können ganze Zertifikatketten aufgebaut werden.



Zweistufige Zertifikathierarchie mit Root- und Sub-CAs

Das zentrale Management der TMA erlaubt eine beliebige Segmentierung zwischen verschiedenen Mandanten oder den verschiedenen Anwendungsfällen der PKI und somit den Einsatz granularer Sicherheitsmechanismen.

Was ist eine CA?

Die *Certificate Authority (CA)* oder auch Zertifizierungsstelle übernimmt innerhalb der Public-Key-Infrastruktur die Rolle der vertrauenswürdigen Drittinstanz.

Die CA bezeugt die Echtheit der von ihr ausgestellten Zertifikate, indem sie deren Metainformationen mit ihrem privaten Schlüssel signiert. Anhand des öffentlichen Schlüssels aus dem CA-Zertifikat kann eine Entität die Echtheit der von dieser CA ausgestellten und signierten Zertifikate überprüfen.

So kann eine Vertrauensstellung auch zwischen unbekannten Kommunikationspartnern aufgebaut werden.

Erstellen und Zurückziehen von Zertifikaten

Kernfunktion der Trust Management Appliance ist das Erstellen von Zertifikaten. Dabei können sowohl der zugehörige Schlüssel auf der TMA selbst erzeugt und gespeichert werden, als auch Zertifikate aus externen Certificate Signing Requests (CSR) erstellt werden.

Falls ein Zertifikat kompromittiert wurde, die zugehörige Identität nicht mehr gültig ist oder ein Schlüssel als unsicher eingestuft wurde, kann das Zertifikat über die TMA schnell und einfach zurückgezogen werden. Der Widerruf wird über eine → **Validation Authority (VA)** bekannt gegeben, sodass der Zertifikatstatus jederzeit überprüfbar ist.

Die TMA kann Zertifikate nach vordefinierten → **Policys** ausstellen. Diese enthalten z.B. Richtlinien für die Erzeugung von Zertifikaten, Schlüsselverwendung, kryptografische Verfahren, oder Schlüssellängen. Dadurch werden Vorgaben konsequent in der

gesamten Infrastruktur durchgesetzt. Diese können pro CA, aber auch für beliebige Teilmengen von Zertifikaten flexibel definiert werden.

Für die sichere Verwaltung kryptografischer Schlüssel kann ein → **Hardware Security Module (HSM)** an die TMA angebunden werden. Ein HSM ermöglicht die sichere Erzeugung, Speicherung und Nutzung privater Schlüssel durch eine speziell dafür gehärtete Hardware.

Was ist ein Zertifikat?

Ein Zertifikat ist ein standardisierter Datensatz, der einen öffentlichen Schlüssel mit allen erforderlichen Informationen zur Identität des Besitzers ergänzt. Dadurch, dass das gesamte Zertifikat von einer CA signiert wird, kann sichergestellt werden, dass die Information zum Besitzer und der Schlüssel zusammengehören.

Import externer Zertifikate

Neben dem Erstellen von Zertifikaten auf der Trust Management Appliance selbst können über eine Importschnittstelle externe Zertifikate sowie CA-Zertifikate externer Zertifizierungsstellen mit den dazugehörigen privaten Schlüsseln und CA-Kennwörtern einzeln oder massenimportiert werden. So lassen sich nicht nur einzelne Zertifikate, sondern ganze Zertifikathierarchien in das Zertifikatmanagement der TMA integrieren.

Zertifikate können in DER- und PEM-Formaten, als PKCS#7- oder PKCS#12 importiert werden. CA-Kennwörterlisten können als CSV-Datei importiert werden.

Frei definierbare Metadaten

Die Trust Management Appliance bietet die Möglichkeit, an diverse Objekte, z.B. Zertifikate, Metadaten in Form von Schlüssel-Wertepaaren anzuhängen. Diese dienen dazu, Zusatzinformationen, die kein Bestandteil des Zertifikats selbst sind, zu verwalten und für die Organisation und für Auswertungen nutzbar zu machen (z.B. Kostenstellen, Seriennummern etc.).

Schlüssel

Die Trust Management Appliance unterstützt zwei asymmetrische Verschlüsselungsalgorithmen:

- **Rivest-Shamir-Adleman (RSA)**
  Mit konfigurierbaren Schlüssellängen bis 8192 Bit.
- **Elliptic Curve Cryptography (ECC)**
  Mit konfigurierbaren Schlüssellängen bis 571 Bit und Kurven nach ANSI X9.62, SEC 2 oder RFC 5639-Standard.

Für die Erzeugung digitaler Signaturen unterstützt die TMA Hash-Algorithmen der SHA-2-Familie bis SHA-512.

Diese kryptografischen Grundfunktionen bilden die Basis von Internet-Standards wie SSL/TLS, SSH, IPsec und S/MIME.

Das RSA-Verfahren ist das ältere und bewährteste der beiden Verschlüsselungsverfahren. Aufgrund seines Verbreitungsgrads ist es mit nahezu allen älteren Protokollen, Betriebssystemen oder Firmware kompatibel.

Kryptografie mit Elliptischen Kurven ist ein jüngeres Verschlüsselungsverfahren. Es bietet die gleichen kryptografischen Stärken, benötigt jedoch weniger Rechenleistung aufgrund der deutlich kürzeren Schlüssellängen, wodurch es sich besonders für kleine Geräte mit begrenzterer Rechenkapazität eignet sowie für Fälle, in denen viele Operationen in kurzer Zeit notwendig sind.

Was bedeutet Public Key?

Das Herzstück einer PKI ist das *Public-Key-Kryptosystem,* das für jede Entität ein Schlüsselpaar erzeugt:

- einen *öffentlichen Schlüssel* zum Verschlüsseln und Prüfen von Signaturen,
- einen *privaten Schlüssel* zum Entschlüsseln und Signieren.

Jede kryptographische Operation mit dem einen Schlüssel kann nur mit dem anderen entschlüsselt werden.

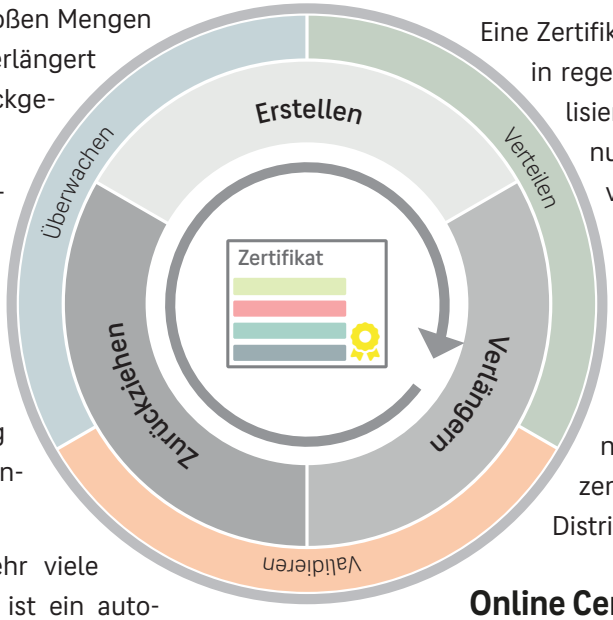
Der öffentliche Schlüssel wird geteilt, der private bleibt strikt geheim.

Symmetrische Schlüssel

Die Trust Management Appliance kann sonstige Geheimnisse, z.B. symmetrische Schlüssel oder Kennwörter, sicher erzeugen und verwalten.

Zertifikatlebenszyklus

Zertifikate müssen oft in großen Mengen erzeugt, ausgegeben, verlängert und ggf. auch wieder zurückgezogen werden können.



Die Trust Management Appliance stellt ein umfassendes Managementsystem zur Verfügung, mit dem Zertifikate und Schlüsselmaterial über ihren gesamten Lebenszyklus hinweg sicher verwaltet werden können.

Im IoT-Umfeld, in dem sehr viele Zertifikate im Einsatz sind, ist ein automatisiert verwaltbarer Zertifikatlebenszyklus umso wichtiger.

Mit der TMA können Zertifikate bereits im Produktionsprozess automatisch und sicher auf Endgeräte und Maschinen gebracht werden. Gleichermaßen können Zertifikate automatisiert widerrufen und entfernt werden, wenn z.B. Geräte eine Qualitätsprüfung nicht bestehen, ihr Betriebsende erreicht haben oder aufgrund von Defekten vorzeitig außer Betrieb genommen werden müssen.

Die begrenzte Gültigkeit der Zertifikate stellt sicher, dass sicherheitskritische Komponenten wie Schlüsselalgorithmen oder Schlüssellängen nicht veralten, sondern dem aktuellen Sicherheitsstandard in regelmäßigen Abständen angepasst werden müssen.

Validierung

Der Status jedes Zertifikats muss immer überprüfbar sein. Die Trust Management Appliance unterstützt die Zertifikatvalidierung mithilfe von Certificate Revocation Lists (CRLs) und des in der TMA integrierten OCSP-Dienstes.

Certificate Revocation List (CRL)

Eine Zertifikatsperrliste oder CRL ist ein in regelmäßigen Abständen aktualisiertes Verzeichnis der Seriennummern aller Zertifikate, die von der jeweils ausstellenden CA widerrufen wurden und nicht mehr den Richtlinien entsprechen.

Diese "schwarzen Listen" werden von der Trust Management Appliance über zentral konfigurierbare CRL Distribution Points bereitgestellt.

Online Certificate Status Protocol (OCSP)

Alternativ erlaubt die Verwendung des integrierten OCSP-Dienstes, den Status einzelner Zertifikate bei einem OCSP-Responder online und in Echtzeit abzufragen.

Die TMA kann OCSP-Responder für alle von ihr verwalteten CAs zur Verfügung stellen und so gewährleisten, dass Zertifikatstatusinformationen immer aktuell sind – im Gegensatz zu CRLs die zyklisch aktualisiert werden.

Je nach Größe der CRL und Häufigkeit der Anfragen an den OCSP-Dienst kann dies zu einer Reduktion der notwendigen Netzwerkbandbreite beitragen.

Policys und Reporting

Policys

Mithilfe der Vorlagen-/Policy-Funktion der Trust Management Appliance können Zertifikaten und Schlüsseln feste Werte vorgegeben und mit entsprechenden Validierungsregeln vorbelegt werden.

Certificate Policys sind Zertifikatrichtlinien, die Bedingungen für die Ausstellung und Verwendung von Zertifikaten festlegen. Sie vereinfachen die Zertifikatausstellung, indem sie Standardwerte für Einstellungen wie den Verwendungszweck eines Zertifikats, seine Gültigkeitsdauer oder die zu verwendende Zertifizierungsstelle (CA) vorgeben. Zudem können sie Anforderungen an die Identitätsprüfung, zulässige kryptografische Algorithmen, Schlüsselverwaltung und weitere Sicherheitsmaßnahmen definieren.

Validierungsregeln stellen sicher, dass Zertifikate nur gemäß den vorgegebenen Bedingungen erstellt oder geändert werden können. Dabei können auch spezifische Bedingungen festgelegt werden, unter denen Standardwerte und Validierungsregeln angewendet werden. Dies ermöglicht Unternehmen, differenzierte Sicherheitsstufen zu implementieren und Zertifikate gezielt für bestimmte Anwendungsfälle einzusetzen.

Policys können pro CA und/oder für beliebige Teilmengen von Zertifikaten flexibel definiert werden.

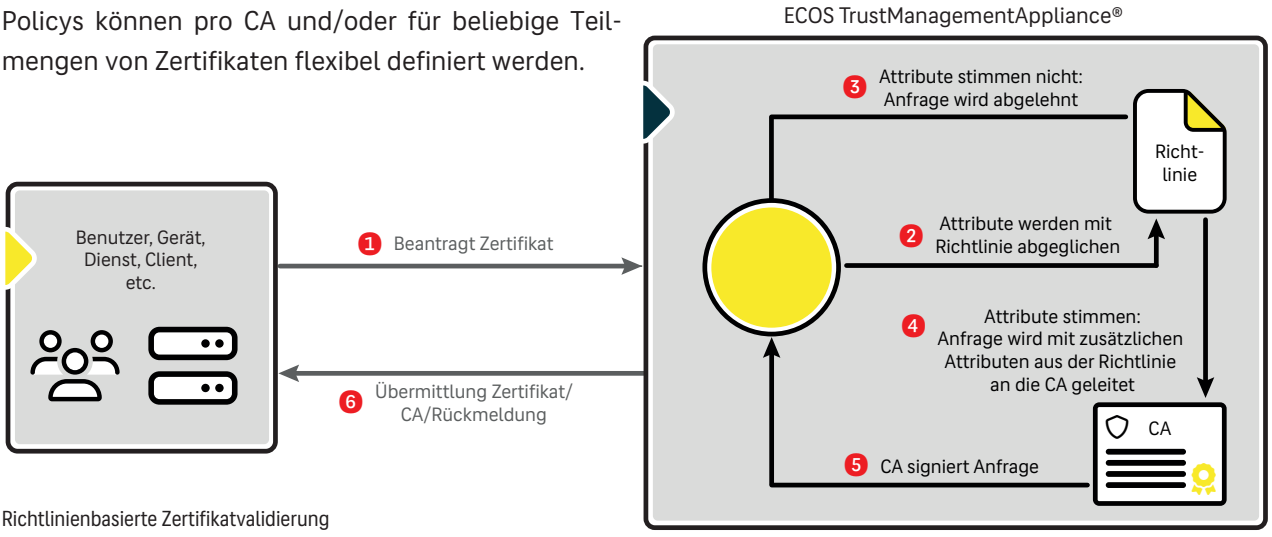
Reporting

Mitarbeiter scheiden aus einem Unternehmen aus, Maschinen können einen Defekt haben, Geräte verloren gehen. Damit verwaiste Zertifikate nicht zum Einfallstor für Cyberangriffe werden oder der Betrieb stehen bleibt, weil ein Zertifikat unbemerkt abgelaufen ist, müssen alle Zertifikate jederzeit sichtbar sein.

Das automatische Reporting- und Benachrichtigungssystem der Trust Management Appliance sorgt dafür, dass stets der Überblick über den Zertifikatlebenszyklus gewahrt bleibt und jedes Zertifikat zum rechten Zeitpunkt verlängert, gesperrt oder widerrufen werden kann.

Durch frei konfigurierbare Abfragen von Attributwerten kann jederzeit dargestellt werden, welche Geräte, Maschinen oder Benutzer welche Zertifikate besitzen. Die grafische Darstellung relevanter Attributwerte erleichtert die statistische Auswertung.

Zusätzlich können Kriterien definiert werden, die Aktionen wie den Versand einer E-Mail auslösen oder Eskalationsprozeduren bei Zertifikatablauf definieren.



Richtlinienbasierte Zertifikatvalidierung

Speicherung

Die Trust Management Appliance speichert Root-Zertifikate, private Schlüssel und CA-Kennwörter standardmäßig in einem verschlüsselten Filesystem sicher ab.

Die TMA gewährleistet außerdem die sichere Verwaltung sonstiger Geheimnisse, z.B. symmetrischer Schlüssel und Kennwörter, die bei Applikationen für den Zugriff auf Datenbanken o.ä. notwendig sind.

Hardware Security Module (HSM)

Ein HSM ist ein Gerät, das über einen oder mehrere sichere Kryptoprozessorchips verfügt. Es speichert das digitale Kryptomaterial sicher in Hardware und führt die kryptografischen Operationen dort aus.

Für Umgebungen mit erhöhten Sicherheitsanforderungen bietet die Trust Management Appliance eine Schnittstelle zur Anbindung an ein HSM für ein zusätzliches Plus an Sicherheit.

Ähnlich wie bei einer Smartcard können Schlüssel direkt auf dem HSM erzeugt werden und verlassen dieses auch nie. Alle Operationen, die mit dem privaten Schlüssel ausgeführt werden, werden innerhalb des HSM ausgeführt. Das stellt sicher, dass niemals ein Zugriff auf sensible Schlüssel wie z.B. die privaten Schlüssel der CA möglich ist.

Authentisierung

IEEE 802.1X

IEEE 802.1X ist ein Standard für die portbasierte Netzzugangskontrolle und bietet einen Authentifizierungsmechanismus für Geräte, die sich mit einem LAN-Switch oder WLAN-Access-Point verbinden wollen.

Für die Zugangskontrolle nach diesem IEEE-Standard verfügt die Trust Management Appliance über einen RADIUS-Server. Switche oder WLAN-Access-Points senden dabei die Client-Zertifikate der Netzwerkgeräte via RADIUS-Protokoll zur TMA, die diese dann prüfen kann.

Distribution

Um Zertifikate in großen Mengen in die unterschiedlichsten Umgebungen zu verteilen, muss eine PKI-Lösung nicht nur die Verteilungsprozesse automatisieren können, sie sollte auch über breitgefächerte Verteilungsmechanismen verfügen.

Die Trust Management Appliance unterstützt daher nicht nur Standard-Enrollment-Protokolle, sondern bietet auch flexible Schnittstellen zu Systemen und Umgebungen, die diese Standards nicht nutzen, um die automatische Verteilung von Zertifikaten an Geräte oder Maschinen und die reibungslose Interaktion zwischen TMA und Anwendungen zu gewährleisten.

Standard-Enrollment-Protokolle

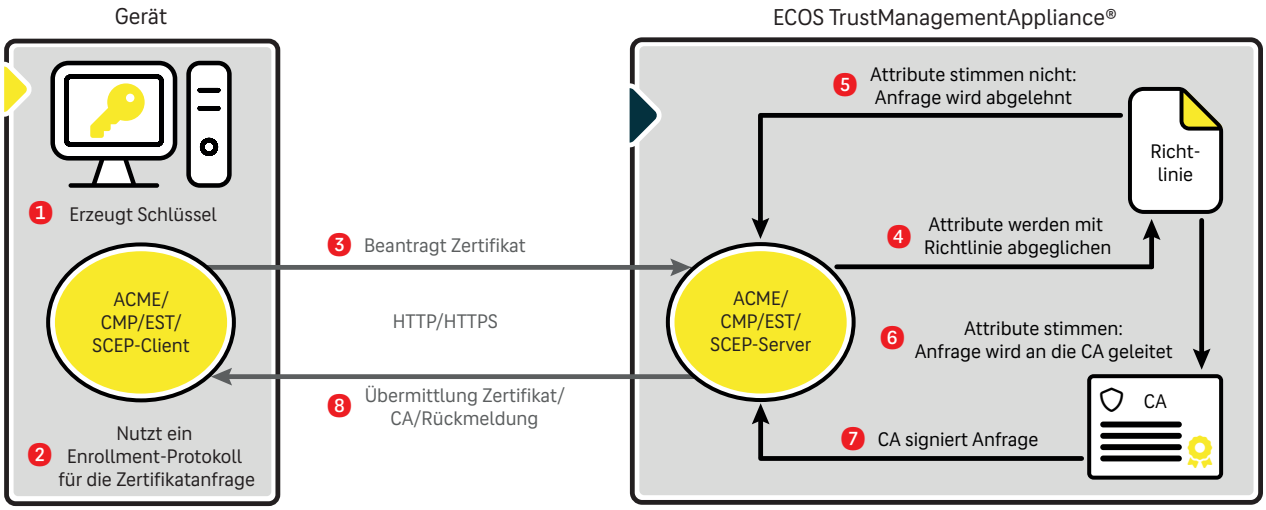
Standardprotokolle wie ACME, SCEP, EST und CMP automatisieren die Ausstellung und Verteilung von Zertifikaten, was eine effiziente Verwaltung von digitalen Identitäten in großen IT-Umgebungen ermöglicht. Sie verbessern außerdem die Sicherheit durch standardisierte Authentifizierungs- und Verschlüsselungsmechanismen.

Automatic Certificate Management Environment (ACME)

ACME ist ein HTTPS-basiertes Protokoll zur Automatisierung der Interaktion zwischen CAs und den Servern ihrer Nutzer. Ursprünglich wurde ACME für die einfache Automatisierung des Enrollments von Webserverzertifikaten von Let's Encrypt entwickelt. Heute unterstützen verschiedene andere CAs, PKI-Anbieter und Browser das Protokoll.

Die Trust Management Appliance stellt einen eigenen ACME-Dienst bereit, über den Webdienste Zertifikate direkt von der TMA beziehen können.

Automatisiertes Zertifikatenrollment mit ACME, SCEP, EST und CMP



Auf dem Gerät wird ein Schlüssel erzeugt. Anschließend sendet das Gerät eine Zertifikatanfrage an den TMA-Server (❶, ❷ und ❸).

Dort werden die Anfrageattribute mit den definierten Richtlinien abgeglichen (❹).
Stimmen die Attribute überein, wird die Anfrage an die Zertifizierungsstelle (CA) weitergeleitet und nach erfolgreicher Signierung an das Gerät zurückgesendet (❻, ❼ und ❽).
Stimmen die Attribute nicht überein, wird die Anfrage abgelehnt (❺).

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

Der Vorteil von ACME ist, dass Clientgeräte den Identitätsnachweis erbringen können, ohne dass eine menschliche Interaktion oder Überprüfung durch eine CA erforderlich ist. Hierzu stellt ACME eine Reihe von Challenges bereit, mit denen eine CA dem Client anbieten kann, das Eigentum an einer Domain/einem Hostnamen nachzuweisen, die als Identität dieses Zertifikats angegeben werden soll.

Simple Certificate Enrollment Protocol (SCEP)

Mit dem HTTP-basierten SCEP können Netzwerkgeräte über eine URL und eine Challenge schnell und einfach ein digitales Zertifikat anfordern.

SCEP ist ein altbewährtes Protokoll und heute praktisch ein Industriestandard für das Anfordern, Ausrollen und Verlängern von Zertifikaten, der von den meisten Geräten und Systemen unterstützt wird.

Die Trust Management Appliance stellt einen integrierten SCEP-Dienst zur Verfügung, um Zertifikate auf Fremdgeräten automatisch auszurollen und zu verlängern.

Enrollment over Secure Transport (EST)

EST ist ein Protokoll zur automatischen Bereitstellung von Zertifikaten für Webserver, Geräte und Anwendungen über eine HTTPS-Verbindung.

Das Hauptmerkmal von EST ist die Verwendung von TLS als Transportsicherheitsschicht, um Daten verschlüsselt zu übertragen. Dies trennt im Vergleich zu SCEP die Sicherheitsleistung vom eigentlichen Enrollment. Dadurch kann EST auch mit Elliptic-Curve-Cryptography umgehen. Wie SCEP unterstützt EST das Ausrollen und Verlängern von Zertifikaten.

Auch hier stellt die Trust Management Appliance einen integrierten EST-Dienst zur.

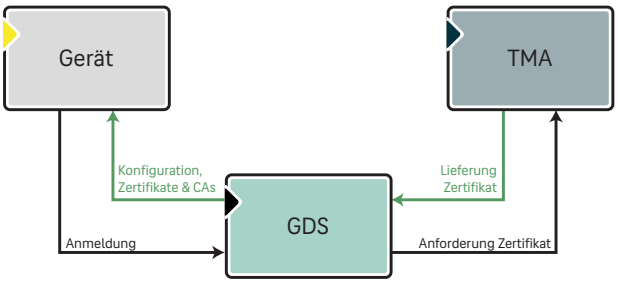
Certificate Management Protocol (CMP)

CMP ist ein sehr umfassendes Protokoll, das die Registrierung, Erneuerung und Sperrung von Zertifikaten zwischen Clientgeräten und CAs ermöglicht. CMP-Nachrichten sind in sich geschlossen, was das Protokoll unabhängig vom Transportmechanismus macht. Die Trust Management Appliance verfügt hierzu über einen integrierten CMP-Dienst.

OPC Unified Architecture (OPC UA)

OPC UA ist ein Standard, mit dem Maschinen hersteller- und plattformunabhängig Daten und Steuerinformationen untereinander austauschen. OPC UA arbeitet zertifikatbasiert, d.h., dass alle Verbindungen TLS-verschlüsselt sind.

Die Trust Management Appliance stellt eine Schnittstelle für die Anbindung an einen Global Discovery Server (GDS) zur Verfügung, um das automatische Ausstellen, Ausrollen, Verlängern und Zurückziehen von Zertifikaten für OPC UA-vernetzte Steuerungsgeräte zu ermöglichen.

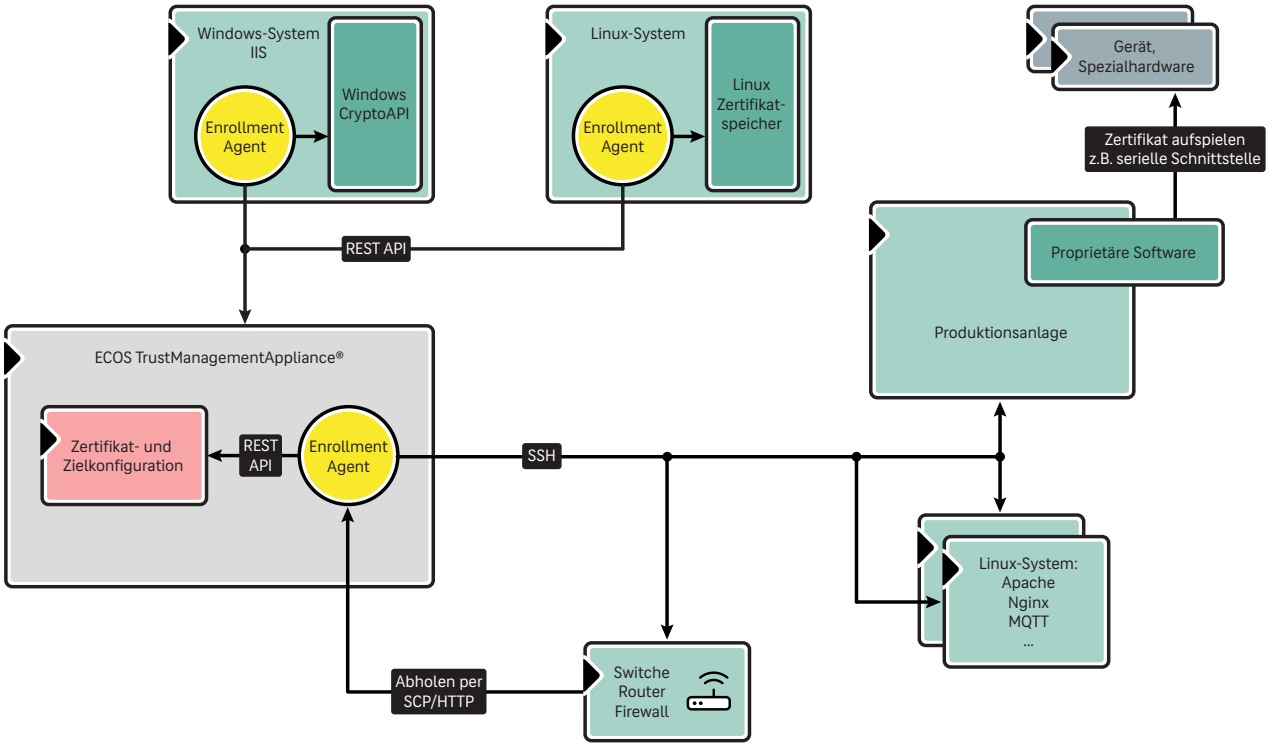


Der GDS wiederum verteilt Zertifikate an alle Geräte, die Teil des OPC UA-Netzwerkes sind. Ebenso ist er dafür zuständig diese Zertifikate zu erneuern und Sperrlisten (CRLs) zu verteilen.

Windows Enrollment

Im OT- und IoT-Umfeld sind heute noch viele Windows-Systeme im Einsatz, auf denen Steuerungssoftware läuft. Auch hier müssen automatisierbar Maschinenzertifikate verteilt werden, die von Windows-basierten Diensten benötigt werden. Die Trust Management Appliance bietet dafür einen kompakten Enrollment-Dienst, der unter Windows installiert werden kann, um Zertifikate automatisch dorthin auszurollen, wo sie benötigt werden oder zu verlängern.

Enrollment Agent



Für die automatische Zertifikatbereitstellung auf Geräten (z.B. Router, Switche, Firewalls und Linux-Systeme), die weder Standardprotokolle noch OPC UA oder andere Protokolle unterstützen, stellt die Trust Management Appliance einen Enrollment Agent zur Verfügung.

Der Enrollment Agent kann sich über Kommandozeile auf einem Zielsystem anmelden oder direkt auf diesem installiert werden, um dort verschiedene Befehle auszuführen, z.B. Zertifikate auszurollen, zu verlängern oder CA-Zertifikate zu verteilen.

Dies ermöglicht eine sehr flexible und universelle Einbindung von unterschiedlichsten Systemen, unabhängig von ihren integrierten Möglichkeiten.

Cert-Manager

Cert-Manager ist ein Zertifikatcontroller für Kubernetes- und OpenShift. Er kann Zertifikate von verschiedenen Ausstellern beziehen, darunter bekannte öffentliche und private Aussteller, stellt deren Gültikeit und Aktualität sicher und erneuert sie vor Ablauf zu einem konfigurierten Zeitpunkt.

Die Trust Management Appliance verfügt über ein entsprechendes Plugin, das sich in den Cert-Manager integriert, um das Ausrollen und Verlängern von Zertifikaten in Kubernetes-Umgebungen zu ermöglichen.

Smartcard Enrollment

Auch das Ausrollen von Zertifikaten auf Smartcards kann mit der Trust Management Appliance automatisiert werden. Der Zugriff auf Smartcards erfolgt mithilfe der zur Smartcard passenden Middleware. Zur Verwaltung einer breiten Palette von Smartcards kann jede Middleware in die TMA eingebunden werden, welche die PKCS#11-Schnittstelle unterstützt.

Für hohe Stückzahlen verfügt die TMA über eine Batch-Enrollment-Funktion für Smartcard-Drucker.

Integration

Der Erfolg einer PKI wird maßgeblich von den Möglichkeiten zur Integration in vorhandene IT- oder OT-Infrastrukturen bestimmt.

Datensynchronisation

Datensynchronisation gewährleistet die Einheitlichkeit von Daten innerhalb der verschiedenen Systeme einer Organisation.

Über die Kopplung der Trust Management Appliance mit AD oder anderen Verzeichnisdiensten können Informationen über registrierte Benutzer und Rechner synchronisiert und die damit verbundenen Prozesse automatisiert werden.

Neben AD unterstützt die TMA auch das für Microsoft Azure entwickelte cloudbasierte Identitäts- und Zugriffsmanagement Entra ID sowie die Synchronisation mit diversen Cloud-Diensten.

RESTful API

Was ist REST?

Representational State Transfer (REST) wird in der Softwareentwicklung eingesetzt, um zustandslose, zuverlässige webbasierte Anwendungen zu erstellen. REST kodiert dabei keine Methodeninformation in den URI, sondern nur Ort und Name der Ressource.

Der Vorteil von REST ist, dass ein Großteil der für REST notwendigen Infrastruktur (z.B. Web- und Applikationsserver, HTTP-fähige Clients, HTML-Parser etc.) bereits im World Wide Web vorhanden ist und viele Webdienste daher von Haus aus REST-konform sind.

Die ECOS REST API ist eine Anwendungsprogrammierschnittstelle, die durch die Nutzung von HTTP-Methoden die effiziente Integration einer PKI in verschiedene Systeme erlaubt.

Alle Funktionen der Trust Management Appliance können über die ECOS REST API ferngesteuert werden, z.B. um Zertifikate für Webserver anzufordern, zu verteilen oder zu verlängern.

Der Schwerpunkt liegt dabei auf der Machine-to-Machine-Kommunikation.

Im IoT-Umfeld können Produktionsanlagen die ECOS REST API nutzen, um Zertifikate und Schlüssel für die zu fertigenden Geräte zu generieren und abzurufen.

```
POST https://tma.domain.de/api/v2.0/cert_server
{
   "data" : {
      "type" : "cert_server",
      "attributes" : {
          "cn": "Certificate",
          "cert_days": 3650
      }
   }
}
```

POST Request über die **ECOS REST API**

PKI-Integration

Ebenso ist die Integration der Trust Management Appliance in eine bereits bestehende PKI mit einem Betrieb als Root- oder als Sub-CA möglich.

Einbinden externer CAs

Die Trust Management Appliance kann nicht nur Zertifikate mithilfe ihrer verschiedenen Dienste ausstellen, sie kann auch als Client anderer CAs fungieren. Externe/öffentliche CAs können so nahtlos integriert werden. Einmal konfiguriert, werden Zertifikate genauso erstellt und verwaltet, als wären sie von der Trust Management Appliance selbst erzeugt worden.

Die TMA stellt Clients für **→ ACME, SCEP, EST und CMP** zur Verfügung. Alle externen/öffentlichen CAs, die einen dieser Standards unterstützen, können nahtlos in die TMA eingebunden werden.

Monitoring & Log-Aggregation

Monitoring und Log-Aggregation dienen dazu, Systemmetriken und Log-Daten aus der gesamten IT-Umgebung einer Organisation zu Überwachungs- und Analysezwecken abzufragen, zu sammeln und zu konsolidieren.

Simple Network Management Protocol (SNMP)

SNMP ist ein Standardprotokoll, das Informationen über verwaltete Netzwerkgeräte zentral sammelt und organisiert.

Für die Integration in ein bestehendes Monitoring-System können über die SNMP-Schnittstelle der Trust Management Appliance Parameter wie Speicherauslastung, CPU-Auslastung oder laufende Prozesse abgefragt werden und automatische Benachrichtigungen versendet werden, wenn die überwachten Systemressourcen festgelegte Grenzwerte über- oder unterschreiten.

Syslog

Syslog ist ein Protokollstandard, mit dem Log-Meldungen von Netzwerkgeräten an einen Logging-Server übertragen werden und wird von den meisten Betriebssystemen unterstützt.

Über die Syslog-Schnittstelle kann die TMA ihre Log-Meldungen externen Aggregationstools bereitstellen.

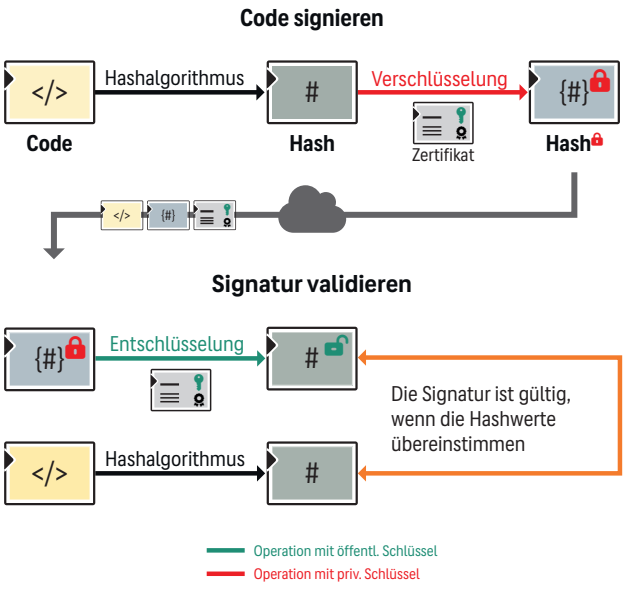
Kryptografie

CryptoAPI

Die CryptoAPI der Trust Management Appliance dient der Durchführung von Kryptooperationen für externe Systeme (z.B. Produktionsanlagen), wenn das Schlüsselmaterial die TMA nicht verlassen darf.

Code Signing

Die Trust Management Appliance stellt für externe Signierungsoftware Zertifikate zur Verfügung, um Programmcode digital zu signieren.



Code-Signing stellt Authentizität und Integrität von Code sicher

Administration

Webbasiertes Interface

Die Trust Management Appliance bietet eine webbasierte Administrationsoberfläche mit einer Standard- und einer Expertenansicht. Jede Ansicht verfügt über eine integrierte Online-Hilfe, um Administratoren bei der Nutzung zu unterstützen.

Für erhöhte Sicherheit kann der Zugriff auf die Administrationsoberfläche zusätzlich per Smartcard abgesichert werden.

Standardansicht

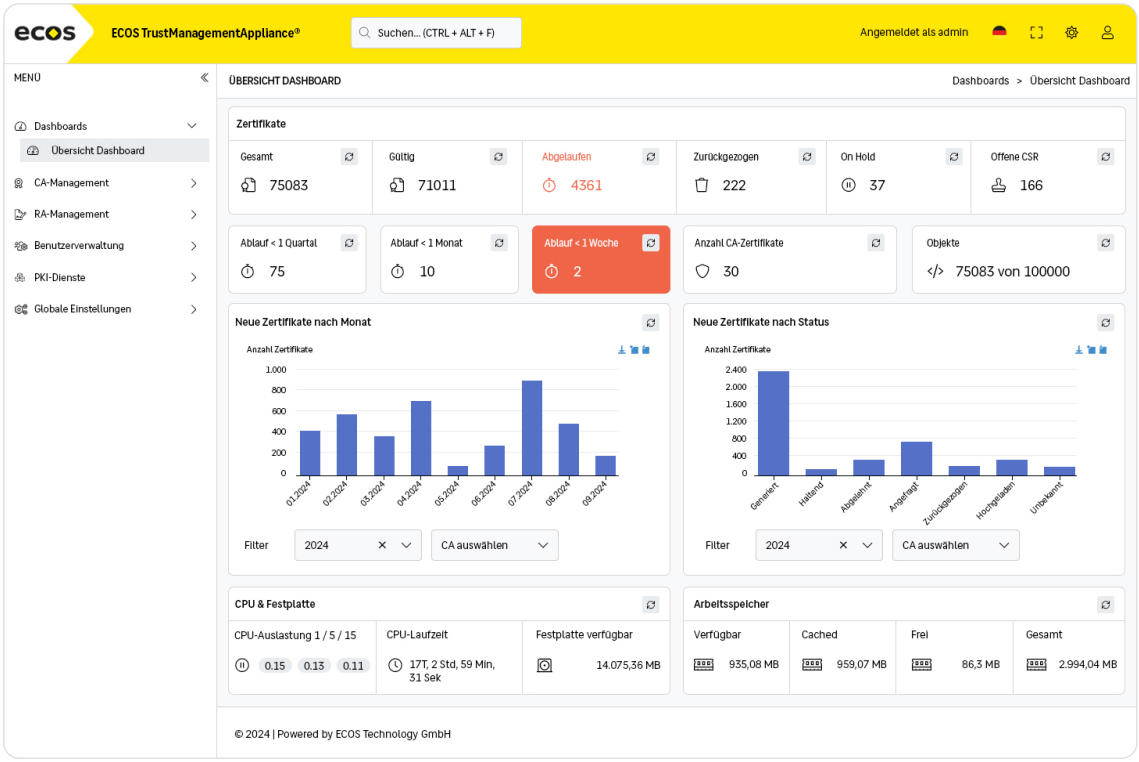
Die Standardansicht enthält ein Dashboard zur Übersicht der im Umlauf befindlichen Zertifikate sowie Systemmetriken. Sie ermöglicht eine schnelle und intuitive Bedienung und macht die Verwaltung von Zertifikaten besonders benutzerfreundlich.

Expertenansicht

Die Expertenansicht bietet Zugang zu allen Funktionen der TMA und richtet sich an Experten, die detaillierte Einstellungen und komplexe Konfigurationen vornehmen möchten.

Self-Service-Portal

Im OT/IoT-Bereich, wo nicht Endbenutzer, sondern Maschinen provisioniert werden, dient das Self-Service-Portal als Registration Authority, bei der z.B. Fachkräfte der Produktion in ihrem jeweiligen Verantwortungsbereich Zertifikate beantragen können.



Standardansicht der Trust Management Appliance mit Dashboard

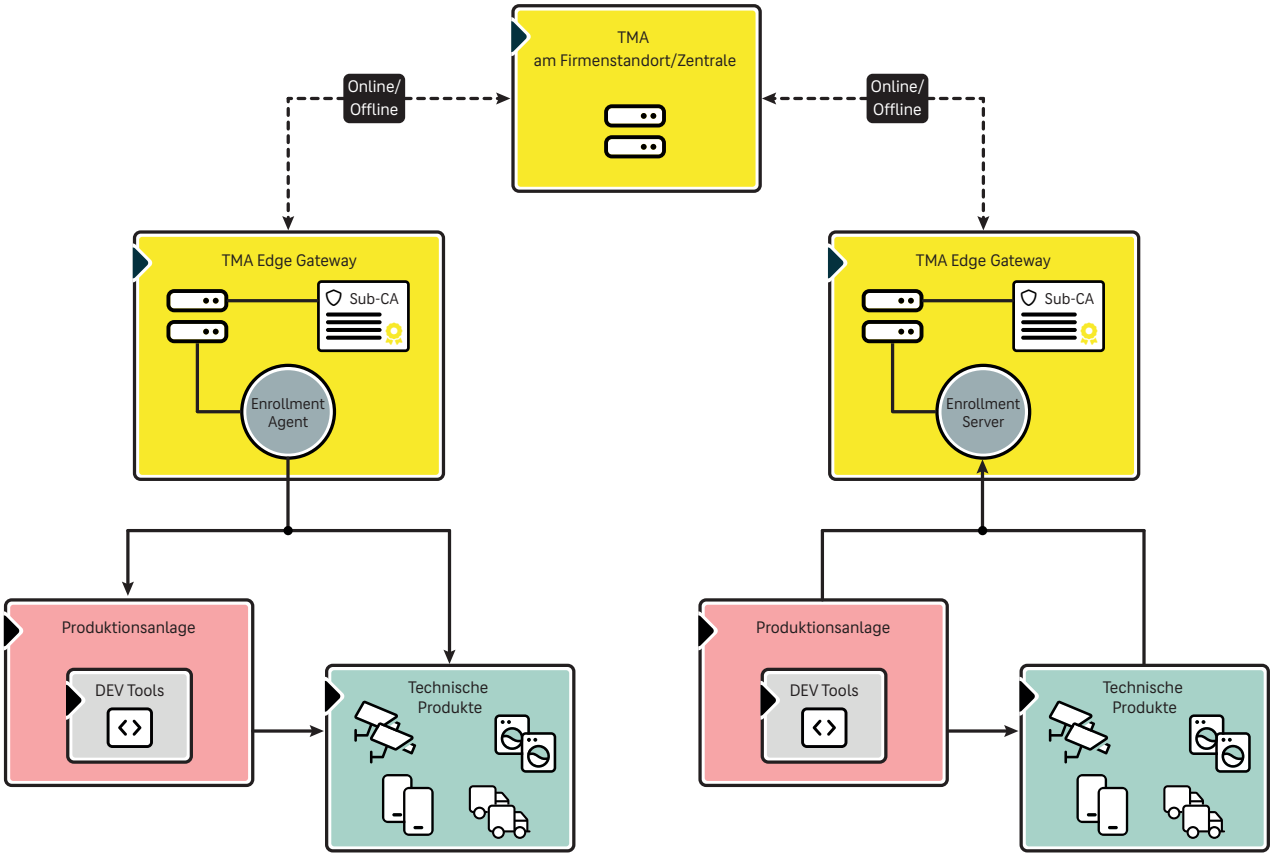
TMA Edge Gateway

Das Edge Gateway der Trust Management Appliance ist eine kompakte und robuste Lösung für die Zertifikatdistribution in Produktionsanlagen im In- und Ausland, egal ob in der eigenen Umgebung oder bei Dienstleistern.

Das TMA Edge Gateway kann Zertifikate erzeugen, ausrollen und Maschinenidentitäten direkt im Produktionsprozess sicher auf die produzierten Geräte aufbringen.

In Produktionsbereichen mit besonderen Sicherheitsbedingungen kann das TMA Edge Gateway offline genutzt werden, um z.B. Zertifikate zwischenzuspeichern. Bei der nächsten Online-Verbindung synchronisiert sich das Gateway wieder mit der TMA des Hauptstandorts.

Diese Fähigkeit macht es auch unabhängig von der Netzwerkanbindung bzw. deren Stabilität oder sonstigen Umwelteinflüssen.



Das TMA Edge Gateway ist für Produktionsumgebungen ausgelegt, die hohe Verfügbarkeit sowie Offline-Fähigkeit erfordern und trotzdem ohne Spezialwissen sicher betrieben werden müssen.

Über ECOS Technology

ECOS Technology GmbH ist ein deutscher Softwarehersteller und seit 1999 auf IT-Sicherheitsprodukte spezialisiert.

Wir entwickeln Lösungen zur Verwaltung von Schlüsseln und Zertifikaten – die Grundlage für IT-, OT- und IoT-Sicherheit. Außerdem bieten wir Produkte für sicheres Remote Working, Remote Access und sichere Videokonferenzen. Dazu gehören auch Lösungen, die vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Geheimhaltungsstufe VS-NfD, EU- und NATO Restricted zugelassen sind.

Mit der ECOS **TrustManagementAppliance®**, unserer Lösung für Schlüssel- und Zertifikatmanagement, fokussieren wir uns im Bereich IoT/OT auf die Branchen Automatisierungstechnik, Mess-, Regel- und Sensortechnik sowie Mikro- und Medizintechnik.

Vom Aufbringen der Maschinenidentität noch in der Produktion über sichere Update-Prozesse im laufenden Betrieb bis hin zur sicheren Außerbetriebnahme decken wir mit unserem breitgefächerten Know-how den gesamten Lebenszyklus der Produkte unserer Kunden mit Blick auf Einsatzgebiet, Leistungsfähigkeit oder Energieverbrauch ab.

Kontaktieren Sie uns

Vereinbaren Sie einen Gesprächstermin und lassen Sie sich von uns beraten!

Sie erreichen uns unter:

Internet: https://www.ecos.de

Tel: +49 6133 939-222

E-Mail sales@ecos.de