Secure machine identities for IoT and OT

Your foundation for a connected future

- **Certificate lifecycle management**
- **Unlimited scalability**
- **Security by design**

Content

Secure communication in IoT and OT

The ECOS **TrustManagementAppliance®** offers a comprehensive platform for the secure management of cryptographic identities across IoT and OT environments.

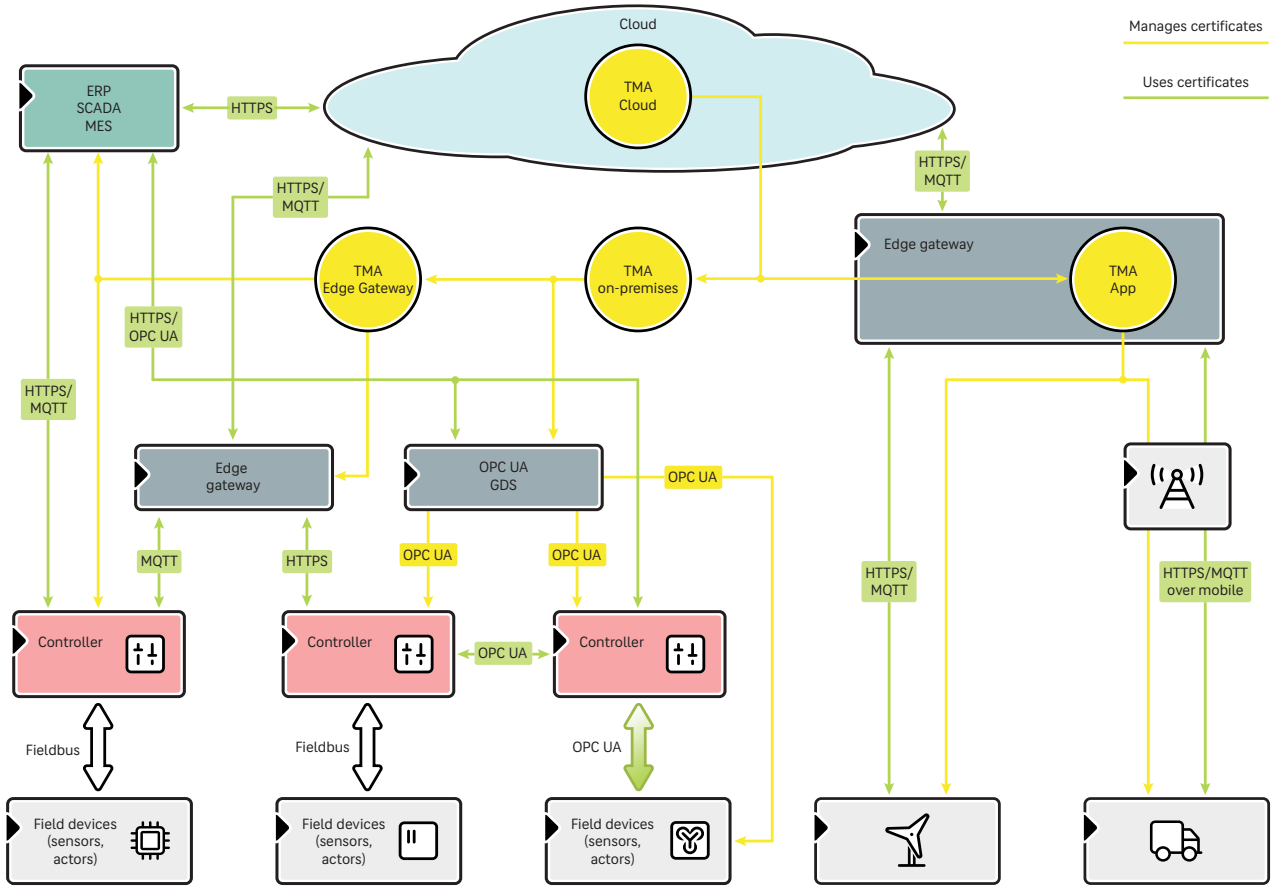
Its architecture is designed to ensure secure, scalable, and automated management of digital identities within connected infrastructures. It allows you to build your own Public Key Infrastructure (PKI) and automate all processes associated with the creation, management, distribution, and validation of certificates.

With extensive support for automated certificate distribution mechanisms, the Trust Management Appliance (TMA) streamlines the enforcement of security policies, while delivering comprehensive visibility into all certificates deployed within the organization. Its flexible design allows for seamless integration into existing IT or OT environments, accommodating specific requirements effectively.

The following sections of this document outline how the Trust Management Appliance assists organizations in developing a secure and efficient digital public key infrastructure within IT, OT, and IoT frameworks.

Functional scope of the ECOS TrustManagementAppliance®

Examples for the use of the ECOS TrustManagementAppliance® in an OT environment



While many fieldbuses provide only limited or no support at all for authentication and encryption, this is a standard feature of more recent protocols such as OPC UA. Further communication, e.g. via MQTT or HTTPS, can also be secured using TLS. The different components therefore require certificates. Certificates and digital keys may also be required for manufactured devices and must be securely applied during the manufacturing process.

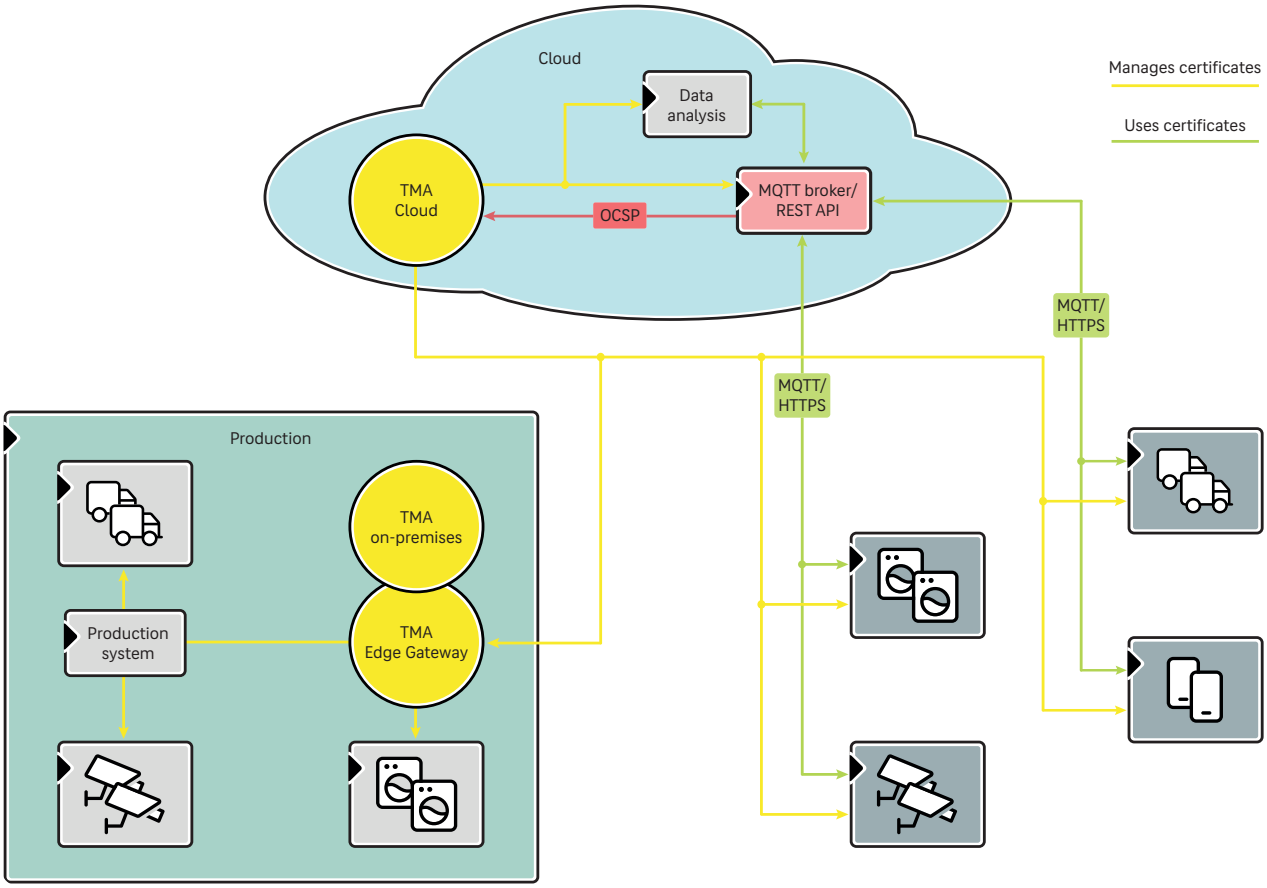
The Trust Management Appliance offers various options for organizing and automating the management and distribution of certificate. It can, for instance, provide certificates to an OPC UA Global Discovery Server, which then distributes them throughout the OPC UA network.

The TMA can also provide certificates for other systems through a variety of interfaces and flexible adaptability.

Depending on the requirements, the Trust Management Appliance can be operated as a virtual machine on-premises, as an app on an edge gateway from various manufacturers or in the cloud.

A new feature is the operation as ECOS TMA Edge Gateway, which is specially designed for manufacturing environments that require high availability and offline capability, but still need to be securely operated without special knowledge.

Examples for the use of the ECOS TrustManagementAppliance® in an IoT environment



Main features

Automatic distribution: Supports widespread standard protocols, OPC UA, Kubernetes and more.

Certificate management: Automates certificate issuance, renewal, and revocation processes. Supports OCSP and CRL.

Key storage: Secure storage on HSMs connected via USB, LAN or cloud.

Logging & Monitoring: Integrates with log aggregation systems and SNMP for event monitoring.

Interfaces & integration:

IoT- & OT compatibility: Supports cloud IoT and industrial production systems.

Protocols & APIs: REST API, SCEP, EST, ACME, CMP for seamless connection.

Directory service: Integrates with Active Directory (AD), Entra ID and other LDAP-based systems.

Self-Service & administration: Web-based interface and self-service portal for easy administration.

Certificates, Keys, Secrets

Certificates and certificate hierarchies

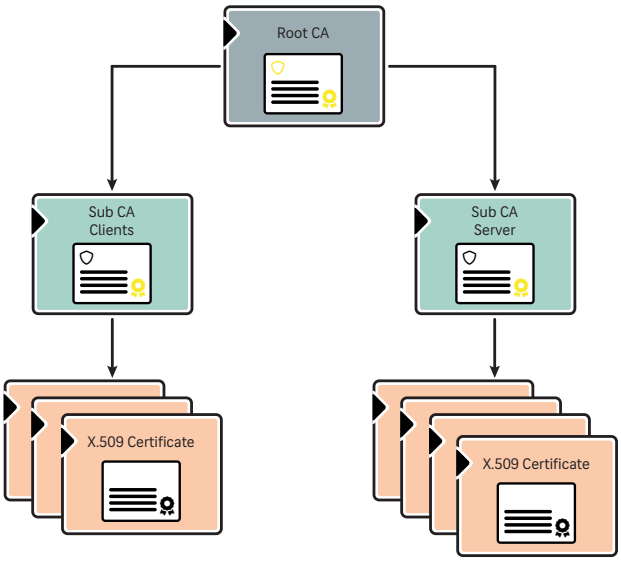
The Trust Management Appliance uses the X.509 standard to provide a uniform structure for certificate-based device, machine or user identities and guarantees a high level of interoperability due to its global distribution.

Certificate Authority (CA)

The Certificate Authority (CA) is the component of a public key infrastructure that is responsible for establishing hierarchical chains of trust.

The Trust Management Appliance enables the creation of a multi-level certificate hierarchy with any number of root and sub-CAs in order to map even complex organizational structures in certificate management.

A root certificate (root CA) signs subordinate CA certificates (sub CAs), which in turn sign subordinate sub CAs or leaf certificates. In this way, entire certificate chains can be built up.



Two-tier certificate hierarchy with root and sub CAs

The central management of the TMA allows to segment between different the between different clients or the different use cases of the PKI and thus to implement granular security mechanisms.

What is a CA?

The *Certificate Authority (CA)* assumes the role of a trusted third party within the public key infrastructure.

The CA attests to the authenticity of the certificates it issues by signing their meta-information with its private key. Any entity can use the public key of the CA certificate to verify the authenticity of the certificates that have been issued and signed by that CA.

In this way, a chain of trust can be established even between communication partners who do not know each other.

Creating and revoking certificates

The core function of the Trust Management Appliance is the creation of certificates. Certificates can be generated from external Certificate Signing Requests (CSR), while the corresponding key can be created and stored on the TMA itself.

If a certificate has been compromised, the associated identity is no longer valid or a key has been classified as insecure, the certificate can be revoked quickly and easily via the TMA. The revocation is announced by a **→ Validation Authority (VA)** so the certificate status is always identifiable.

The TMA can create certificates based on predefined **→ Policies**. Policies can include rules for the generation of certificates, key usage, cryptographic procedures or key lengths. Security directives can thus be consistently enforced throughout the entire infrastructure. They can be flexibly defined per CA, but also for any subset of certificates.

For the secure management of cryptographic keys, a **→ Hardware security module (HSM)** can be connected to the TMA. An HSM enables the secure generation, storage and use of private keys using specially hardened hardware.

What is a certificate?

A certificate is a standardized data set that supplements a public key with all the necessary information on the identity of the owner. The entire certificate is signed by a CA. This ensures that the owner information and the key belong together.

Import of external certificates

In addition to creating certificates natively, the Trust Management Appliance is capable of importing external certificates as well as CA certificates from third-party certificate authorities. This process includes the provision of corresponding private keys and CA passwords. Imports can be performed on a per-certificate basis or in bulk via the designated import interface, facilitating the integration of both singular certificates and entire certificate hierarchies into the TMA's certificate management framework.

Support for certificate imports extends to DER and PEM formats, as well as PKCS#7 and PKCS#12. Additionally, CA password lists may be imported in CSV format.

Configurable metadata

The Trust Management Appliance provides functionality for attaching metadata in the form of key-value pairs to various objects, such as certificates. This feature is essential for managing supplementary information that falls outside of the core certificate data, facilitating usability for organizational purposes and evaluations, including but not limited to cost centers and serial numbers.

Keys

The Trust Management Appliance supports two asymmetric encryption algorithms:

- **Rivest-Shamir-Adleman (RSA)**
  With configurable key lengths up to 8192 bits.
- **Elliptic Curve Cryptography (ECC)**
  With configurable key lengths up to 571 bits and curves according to ANSI X9.62, SEC 2 or RFC 5639 standard.

To generate digital signatures, the TMA supports hash algorithms from the SHA-2 family up to SHA-512.

These core cryptographic functions are the foundation of Internet standards such as SSL/TLS, SSH, IPsec, and S/MIME.

The RSA method is the older and most proven of the two encryption methods. Due to its widespread use, it is compatible with almost all older protocols, operating systems or firmware.

Cryptography with elliptic curves is a more recent encryption method. It offers the same cryptographic strengths, but requires less computing power due to the significantly shorter key lengths, making it particularly suitable for small devices with limited computing capacity and for cases where many operations are required in a short time.

What does public key mean?

The core component of a PKI is the *public key cryptosystem*, which generates a key pair for each entity:

- a *public key* for encrypting and verifying signatures,
- a *private key* for decryption and signing.

Any cryptographic operation performed with one of the keys can only be decrypted with the other key .

The public key is shared, the private key remains strictly secret.

Symmetric keys

The Trust Management Appliance can securely generate and manage other secrets, e.g. symmetric keys or passwords.

Certificate lifecycle

Certificates require efficient generation, issuance, renewal, and revocation, particularly when dealing with large volumes. The Trust Management Appliance offers a comprehensive management system designed to securely handle certificates and key material across their entire lifecycle. In the context of the IoT environment, where a high quantity of certificates is prevalent, automated certificate management becomes essential.

With the TMA, the transfer of certificates to end devices and machines can be conducted automatically and securely during the production phase. Furthermore, certificates can be automatically revoked and removed when devices fail to meet quality standards, reach the end of their operational lifespan, or need to be decommissioned due to defects.

The limited validity period of certificates mandates regular updates to security-critical components, including key algorithms and key lengths, ensuring compliance with the latest security standards before they become outdated.

Validation

The verifiability of each certificate's status is essential. The Trust Management Appliance facilitates this through the use of Certificate Revocation Lists (CRLs) and the TMA's integrated Online Certificate Status Protocol (OCSP) service.

Certificate Revocation List (CRL)

A CRL is a regularly updated enumeration of the serial numbers pertaining to certificates that have been revoked by the issuing Certificate Authority (CA) and are no longer compliant with the established policy.

These blacklists are made available through the Trust Management Appliance via centrally configurable CRL distribution points.

Online Certificate Status Protocol (OCSP)

In addition, the integrated OCSP service permits real-time, online querying of the status of individual certificates through an OCSP responder.

The TMA provides OCSP responders for all CAs under its management, ensuring that certificate status information remains continuously current, as opposed to CRLs, which are updated at predetermined intervals.

This capability can significantly optimize network bandwidth utilization, particularly in scenarios involving large CRLs and frequent OCSP service requests.

Policies and reporting

Policies

The Template/Policy feature of the Trust Management Appliance provides an easy way to assign fixed values to certificates and keys, and pre-configure them with appropriate validation rules.

Certificate policies serve as directives that delineate conditions for the issuance and use of certificates. By specifying default values for key attributes (such as key usage, validity period, and the CA involved) these policies streamline the certificate issuance process. Additionally, they can outline criteria for identity verification, acceptable cryptographic algorithms, key management practices, and other essential security measures.

Validation rules are implemented to ensure that certificates can only be created or modified based on the established conditions. Administrators can configure specific criteria for the application of defaults and validation rules, enabling organizations to enforce granular security levels and deploy certificates tailored for particular use cases.

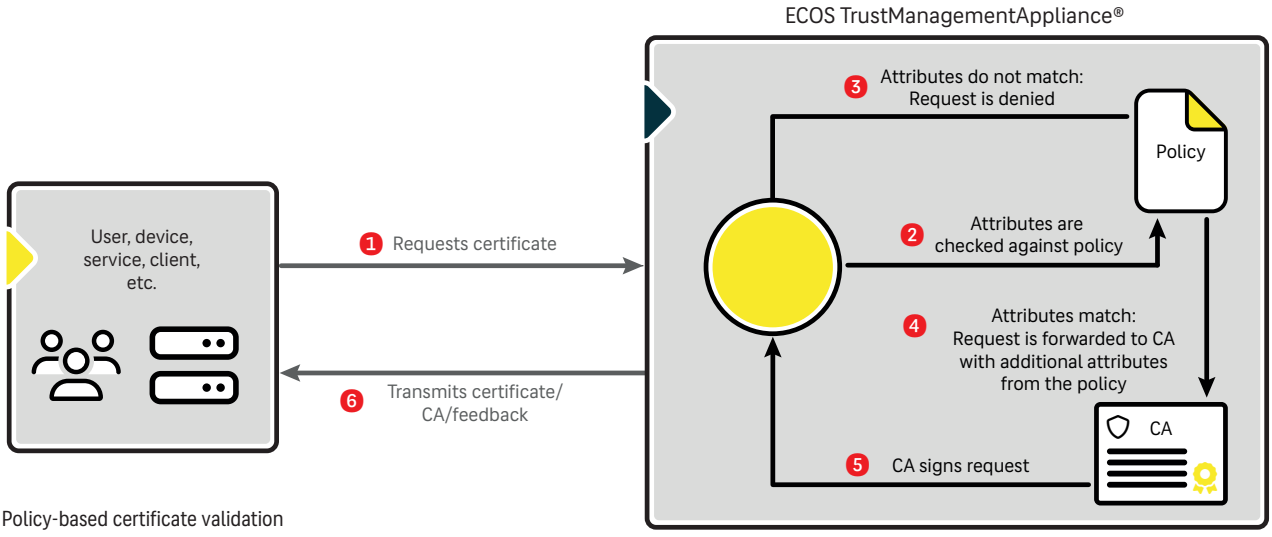
Policies can be defined with flexibility to accommodate any CA and/or any select group of certificates.

Reporting

Employees may depart from the organization, machines may fail, and devices may be misplaced. To mitigate the risk of orphaned certificates serving as potential access points for cyberthreats or causing operational disruptions due to unnoticed certificate expirations, it is essential that all certificates and keys within a public key infrastructure remain visible at all times.

The Trust Management Appliance features an automated reporting and notification system that maintains a comprehensive overview of the certificate lifecycle, ensuring timely renewal, suspension, or revocation of each certificate. Customizable queries for attribute values enable administrators to identify which devices, machines, or users possess specific certificates at any given moment. The graphical representation of pertinent attribute values supports statistical analysis effectively.

Furthermore, administrators can establish criteria that prompt automated actions, such as email notifications or escalation procedures, when a certificate approaches expiration.



Policy-based certificate validation

Storage

The Trust Management Appliance securely stores root certificates, private keys, and CA passwords within an encrypted file system.

In addition, the TMA facilitates the secure management of other critical secrets, such as symmetric keys and passwords, which applications require to connect to databases or similar systems.

Hardware Security Module (HSM)

An HSM is a specialized device equipped with secure cryptoprocessing chips. It ensures the secure storage of digital cryptographic materials in hardware while performing essential cryptographic operations.

For environments demanding enhanced security measures, the Trust Management Appliance includes an interface for connecting to an HSM, adding an extra layer of protection.

Certificates can be generated directly on the HSM, much like a smartcard. All operations that utilize the private key are executed within the HSM, guaranteeing that sensitive keys, including the CA's private keys, remain completely inaccessible.

Authentication

IEEE 802.1X

IEEE 802.1X defines a standard for port-based network access control, enabling an authentication framework for devices attempting to connect to a local area network (LAN) switch or wireless local area network (WLAN) access point.

The Trust Management Appliance features an integrated RADIUS server designed for access control in compliance with this IEEE standard. Network devices communicate their client certificates through the RADIUS protocol to the TMA, which subsequently verifies their authenticity.

Distribution

To effectively distribute certificates on a large scale across diverse environments, a PKI solution must not only automate the distribution processes but also offer a variety of distribution mechanisms.

The Trust Management Appliance addresses this need by supporting standard enrollment protocols while also providing adaptable interfaces for systems and environments that do not conform to established standards. This flexibility ensures the automatic distribution of certificates to devices or machines and facilitates seamless interaction between the TMA and various applications.

Standard enrollment protocols

Standard protocols such as ACME, SCEP, EST and CMP automate the issuance and distribution of certificates, to enhance the management of digital identities in large IT environments. Furthermore, these protocols bolster security by implementing standardized authentication and encryption frameworks.

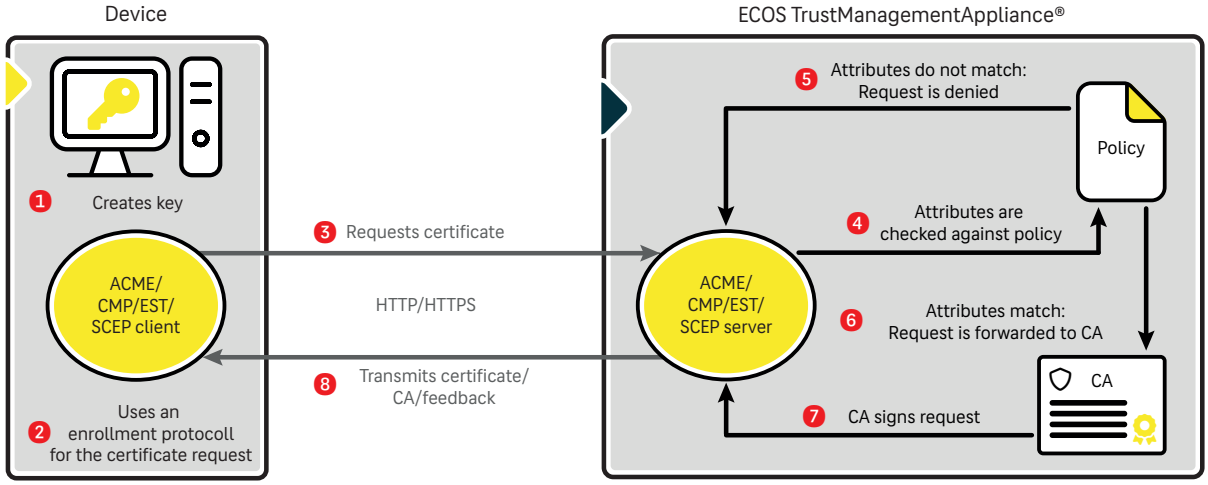
Automatic Certificate Management Environment (ACME)

ACME is an HTTPS-based protocol designed to ease the automation of interactions between CAs and the servers of their users. Initially created to make the enrollment process for web server certificates from Let's Encrypt more efficient, the ACME protocol is today supported by various CAs, PKI providers, and web browsers.

The Trust Management Appliance includes an integrated ACME service that enables web services to directly acquire certificates from the TMA.

One of the key advantages of ACME is its capability to

Automated certificate distribution with ACME, SCEP, EST and CMP



A key is generated on the device. The device sends a certificate request to the TMA server (❶, ❷ and ❸).

The request attributes are compared against the predefined policies(❹). If the attributes match, the request is forwarded to the Certificate Authority (CA) and, once successfully signed, sent back to the device. (❻, ❼ and ❽).
If the attributes do not match, the request is rejected (❺).

The Trust Management Appliance thus ensures secure and compliant certificate provisioning in IoT and OT infrastructures through a structured process.

allow client devices to demonstrate proof of identity without requiring human intervention or validation by a CA. To achieve this, ACME offers a series of challenges that a CA can present to the client, allowing for the verification of domain or hostname ownership specified as the identity for the certificate to be issued.

Simple Certificate Enrollment Protocol (SCEP)

The HTTP-based SCEP allows network devices to efficiently request digital certificates through a URL and a challenge mechanism.

SCEP has become a widely accepted protocol and is now considered an industry standard for the processes of requesting, deploying, and renewing digital certificates, with support from the majority of devices and systems.

The Trust Management Appliance features a SCEP server designed to automate the issuance and renewal of certificates on third-party devices.

Enrollment over Secure Transport (EST)

EST is a protocol that simplifies the automated issuance of certificates to web servers, devices, and applications via a secure HTTPS connection.

A distinguishing characteristic of EST is its utilization of Transport Layer Security (TLS) to ensure data encryption. This separation of security performance from the enrollment process enables EST to support elliptic curve cryptography. Much like SCEP, EST also accommodates the rollout and renewal of certificates.

The Trust Management Appliance includes a built-in EST service to streamline these tasks.

Certificate Management Protocol (CMP)

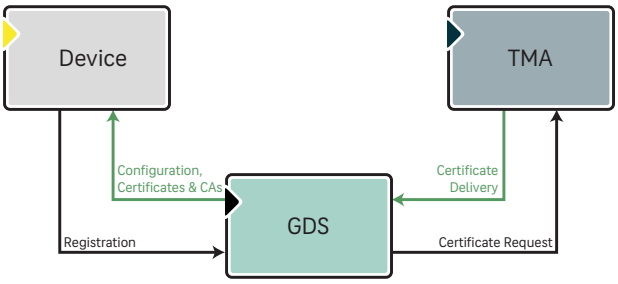
CMP is a comprehensive protocol that supports the registration, renewal, and revocation of certificates between client devices and CAs. CMP messages are self-contained, allowing for independence from the transport mechanism.

The Trust Management Appliance incorporates an integrated CMP service to facilitate these operations.

OPC Unified Architecture (OPC UA)

OPC UA is a standard facilitating data exchange and control information across machines, independent of the manufacturer or platform. It utilizes a certificate-based system, ensuring that all connections are secured with TLS encryption.

The Trust Management Appliance provides an interface to connect with a Global Discovery Server (GDS), streamlining the processes of issuing, rolling out, renewing, and revoking certificates for OPC UA networked controllers.



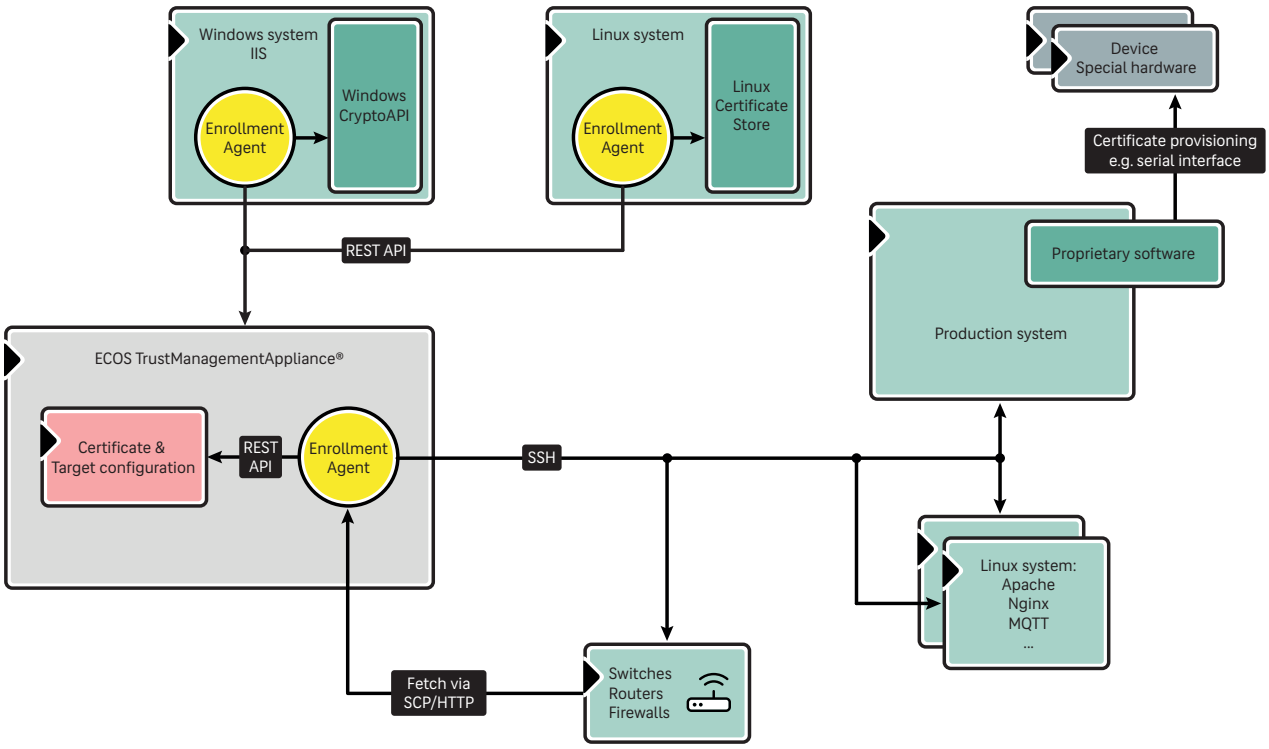
The GDS is tasked with distributing these certificates to all devices within the OPC UA network, managing their renewal, and distributing certificate revocation lists (CRLs).

Windows Enrollment

Numerous Windows systems operating control software remain prevalent in contemporary OT and IoT environments. Consequently, machine certificates required by Windows-based services must be deployed automatically.

The Trust Management Appliance offers an efficient enrollment service that can be installed on Windows systems, automating the distribution and renewal of certificates as necessary.

Enrollment Agent



The Trust ManagementAppliance features an enrollment agent designed for the automatic provisioning of certificates on devices such as routers, switches, firewalls, and Linux systems that do not support standard protocols, OPC UA or other protocols.

The Enrollment Agent can interface with a target system via command line or can be installed directly to execute various operations, such as rolling out or renewing certificates and distributing CA certificates.

This approach allows for flexible and versatile integration of disparate systems, regardless of their inherent capabilities.

Cert Manager

Cert-Manager is a certificate controller for Kubernetes and OpenShift. It obtains certificates from various issuers, including public and private entities, and ensures they remain valid and current, initiating renewal processes before their expiration as configured.

The Trust Management Appliance includes a corresponding plugin that integrates seamlessly with Cert Manager, facilitating the rollout and renewal of certificates within Kubernetes ecosystems.

Smartcard Enrollment

Trust ManagementAB Appliance is also equipped to automate the rollout of certificates to smartcards. The smartcards can be accessed through compatible smartcard middleware, and any middleware supporting the PKCS#11 interface can be integrated with the Trust Management Appliance to manage a wide array of smartcards.

For environments requiring large-scale distribution, the TMA offers batch enrollment functionality for smartcard printers.

Integration

The effectiveness of a PKI hinges on its seamless integration with the prevailing IT ecosystem.

Data synchronization

Data synchronization guarantees data consistency across the various systems within an organization.

By coupling the Trust Management Appliance with Active Directory (AD) or other directory services, organizations can synchronize information regarding registered users and computers, while automating associated processes.

Beyond AD, the Trust Management Appliance also supports Entra ID, Microsoft Azure's cloud identity and access management solution, as well as offering synchronization with multiple cloud services.

RESTful API

What is REST?

Representational State Transfer (REST) is used in software development to create stateless, reliable web-based applications. REST does not encode any method information in the URI, only the location and name of the resource.

The advantage of REST is that a large part of the infrastructure required for REST (e.g. web and application servers, HTTP-capable clients, HTML parsers, etc.) is already available on the World Wide Web and many web services are therefore REST-compliant by default.

The ECOS REST API is a RESTful application programming interface designed to facilitate efficient integration across multiple systems utilizing standard HTTP methods.

All functionalities of the Trust Management Appliance can be controlled remotely via the ECOS REST API, allowing operations such as requesting, distributing, or renewing certificates for web servers. The primary emphasis is on enabling machine-to-machine communication.

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

POST Request via **ECOS REST API**

PKI integration

The Trust Management Appliance can be incorporated into an existing PKI framework, operating as either a root or subordinate Certificate Authority (CA).

Integration of external CAs

In addition to issuing certificates through its built-in services, the Trust Management Appliance can function as a client for external Certificate Authorities. Public or external CAs can be integrated seamlessly, with certificates being generated and managed in the same manner as if they originated from the AB Appliance.

The Trust Management Appliance supports client functionalities for → **ACME, SCEP, EST, and CMP** protocols, thereby enabling effortless integration of any external/public CA that adheres to one of these standards.

Monitoring & Log aggregation

Monitoring and Log Aggregation serves to query, collect, and consolidate system metrics and log data from across an organization's IT environment for monitoring and analysis purposes.

Simple Network Management Protocol (SNMP)

SNMP is a standard protocol that gathers and organizes information from managed network devices.

The Trust Management Appliance is equipped with an SNMP interface that allows integration with existing monitoring systems. This interface can be utilized to query metrics such as memory and CPU usage, as well as active processes. Additionally, it can send automated alerts when monitored system resources surpass or drop below established thresholds.

Syslog

Syslog is a protocol standard for for the transmission of log messages from network devices to a centralized logging server, which is compatible with most operating systems. The Trust Management Appliance is capable of sending log messages to external aggregation tools through its syslog interface.

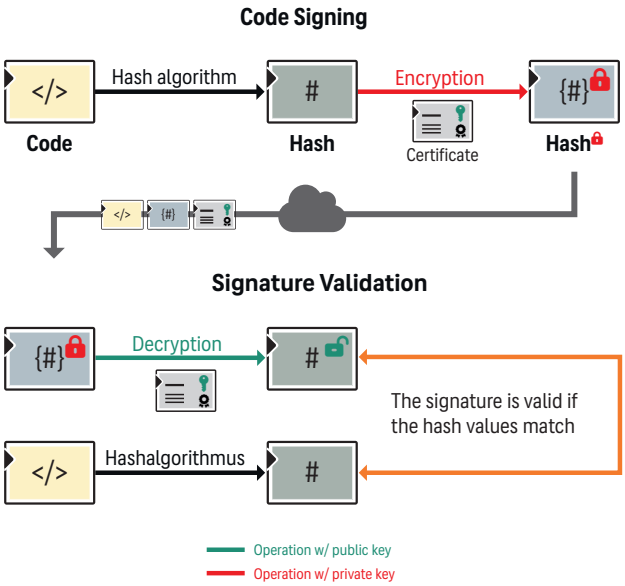
Cryptography

CryptoAPI

The Trust Management Appliance's CryptoAPI is designed to execute cryptographic operations for external systems (e.g., manufacturing systems) in scenarios where the key material must remain within the TMA.

Code signing

The Trust Management Appliance offers certificates for external software that requires signing, enabling the digital signing of program code.



Code signing ensures authenticity and integrity of code

Administration

Web-based interface

The Trust Management Appliance offers a web-based administration interface with a standard and an expert view. Each view has built-in online help to assist administrators.

For enhanced security, aaccess to the administration interface can be secured through the use of a smartcard.

Standard view

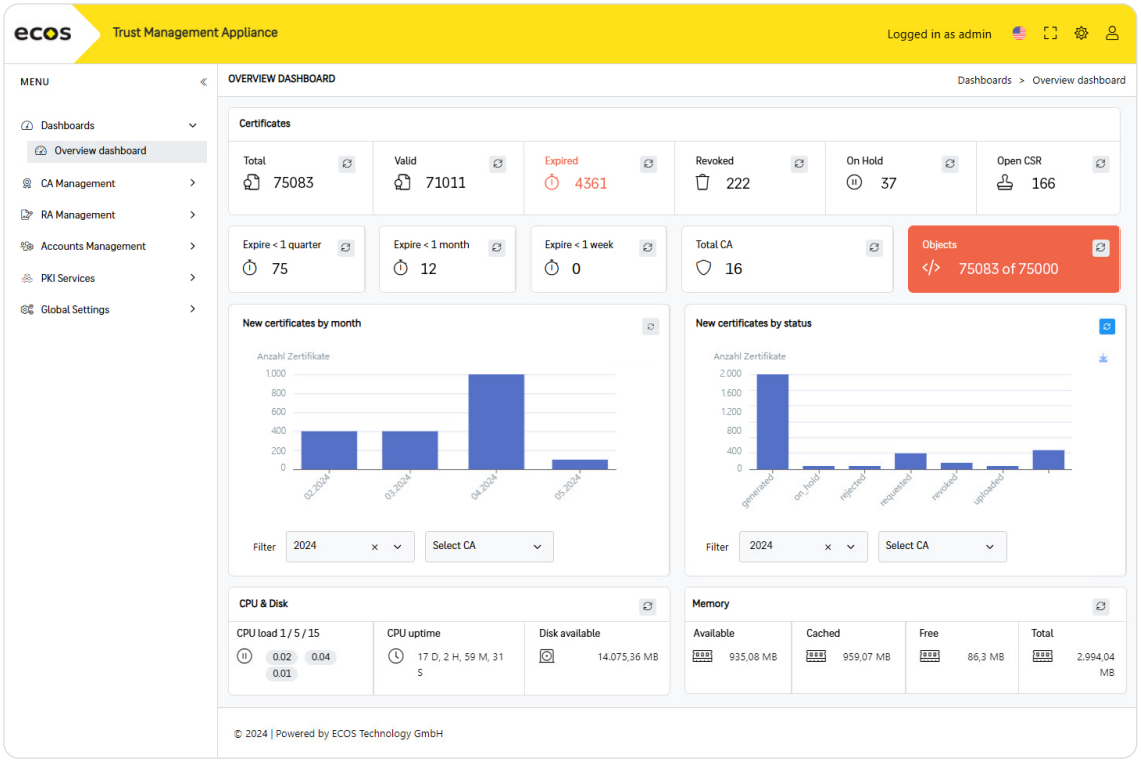
The standard view provides a dashboard that displays an overview of the certificates in circulation, along with relevant system metrics. This interface is designed for quick and intuitive navigation, ensuring that certificate management remains user-friendly.

Expert view

The expert view grants access to all TMA functionalities, catering to experts seeking to configure detailed settings and execute complex configurations.

Self-Service Portal

In the OT/IoT domain, where provisioning is primarily conducted for machines rather than end users, the self-service portal acts as a registration authority. Here, production specialists can apply for certificates relevant to their operational responsibilities.



Standard view of the Trust Management Appliance with dashboard

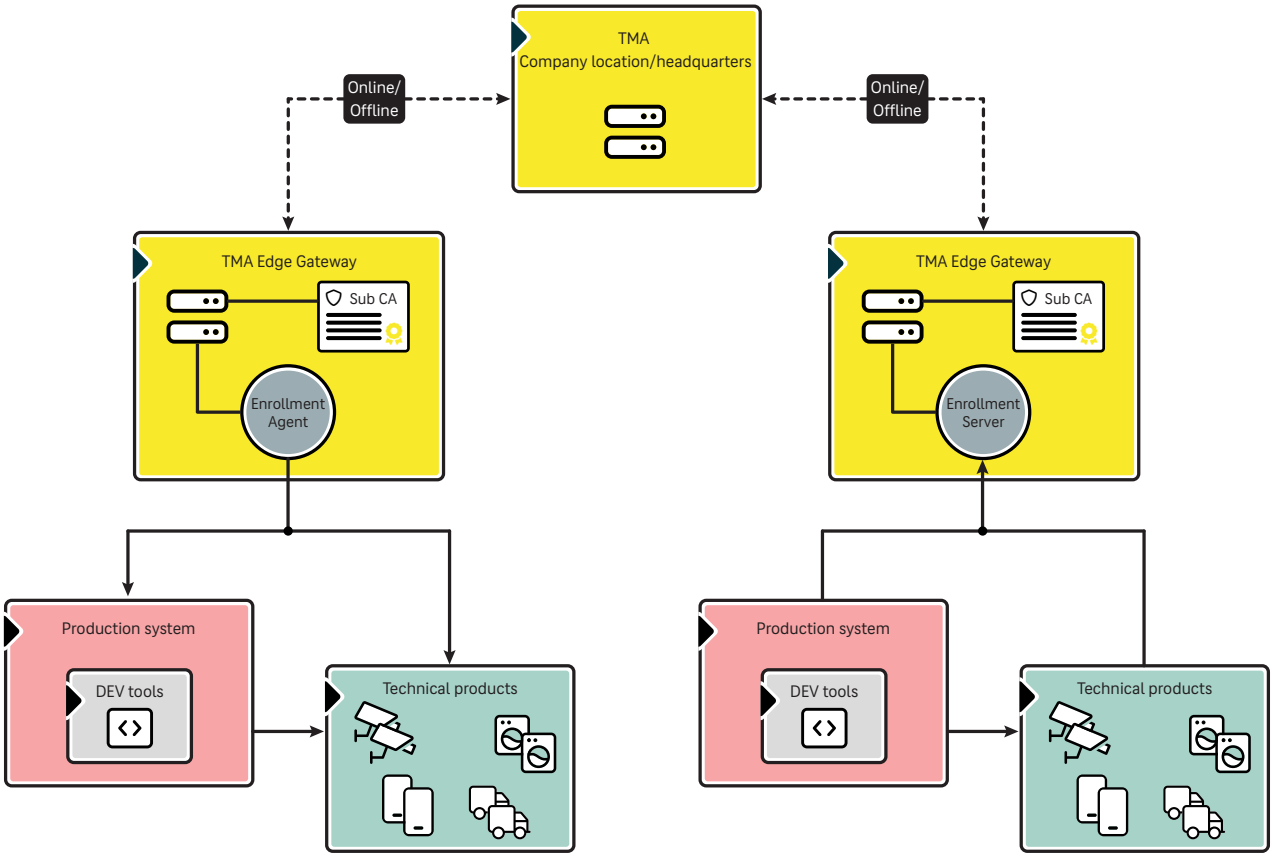
TMA Edge Gateway

The Edge Gateway of the Trust Management Appliance is a compact and robust solution for the distribution of certificates to production sites, both domestically and internationally. This applies whether within an organization's environment or through third-party service providers.

The TMA Edge Gateway is capable of generating and deploying certificates, as well as securely applying machine identities to devices directly during the production process.

In production environments with heightened security requirements, the TMA Edge Gateway can operate offline, allowing certificates to be temporarily stored. Upon re-establishing an online connection, the gateway synchronizes with the main location's TMA.

This functionality provides autonomy from network connectivity issues and external environmental factors.



The TMA Edge Gateway is designed for production environments that require high availability and offline capability and still need to be operated securely without specialist knowledge.

About ECOS Technology

ECOS Technology GmbH is a German software manufacturer specialized in IT security products since 1999.

We develop certificate and key management solutions to help secure IT, OT and IoT. We also offer products for secure remote working, remote access and secure video conferencing. Our product palette includes solutions approved by the German Federal Office for Information Security (BSI) for classification level VS-NfD, EU- and NATO Restricted.

The ECOS **TrustManagementAppliance®**, our solution for key and certificate management, focuses on the IoT/OT sectors of automation technology, measurement, control and sensor technology as well as micro and medical technology.

We offer our customers comprehensive expertise across the whole product life cycle, from the initial machine identity assignment during production to secure update processes in operation and secure decommissioning. Our services are tailored to the specific requirements of each application, taking into account performance and energy consumption.

Contact us

Get in touch for a consultation!

You can reach us as follows:

Internet: https://www.ecos.de

Phone: +49 (6133) 939-222

E-Mail sales@ecos.de