safe and smart

ecos

ECOS TrustManagementAppliance

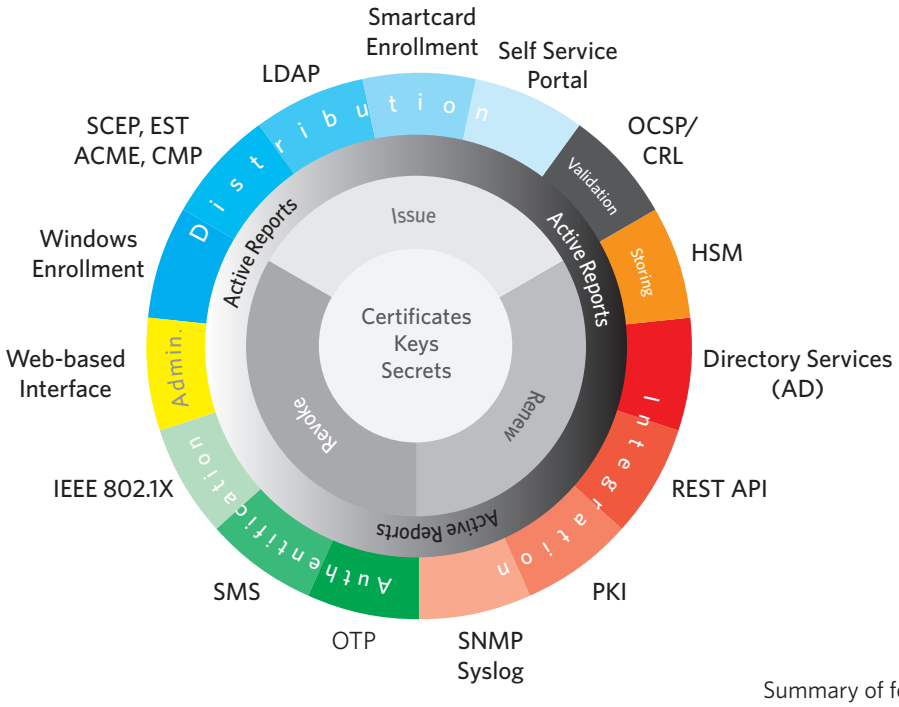
PKI and Key Management solution to secure
PCs, servers, processes, (I)IoT and mobile devices

- **All in one**
- **Active reports**
- **Open and future-proof**

IT-Security Solutions
Made in Germany

Security with key and certificate

The increasing digitalization blurs the lines between conventional IT, ICT and IoT. The ECOS TrustManagementAppliance (TMA) combines for all platforms the administration of certificates, symmetric keys and other secrets in one single PKI and key management solution and thus provides a core component for the security of IT, technology and infrastructure.



Summary of features »All in One«

Securing accesses or encrypting data and communication involves many areas inside a company. In the office area, the secure connection of mobile devices to WLAN, LAN desktops, Windows LogOn per smart card, encrypting and signing e-mails, a secure authentication at the VPN gateway, login to web applications or encryption of hard drives are certainly among the most frequent requirements. Securing server processes and web servers, signing apps, macros and other software are important topics for IT.

In manufacturing companies, engineering and product management are particularly concerned with the securing of accesses and communication encryption of non-IT devices. Resource-efficient procedures are particularly used in this area due to the properties of devices such as actuators, sensors, counters, controls or medical implants, just to name a few.

Certificates, secrets, keys

Certificates and the related asymmetric key pair are most often the basis for a secure authentication. the ECOS TrustManagementAppliance helps both to set up your own private-public key infrastructure (PKI), thus to generate, renew and revoke certificates, and to import, administrate and use certificates from a public CA. The certificates to be generated are fully parameterizable regarding content as well as criteria such as key length or signature algorithm. Through the TMA, all certificates can be made available in common formats like DER, PEM as well as container formats such as PKCS#7 and PKCS#12.

Secrets like passwords, credentials and other secrets require also a secure storage. The TMA allows to store and administrate them just as securely as certificates and keys. In areas where the administration of a certificate infrastructure would be too complex - for example with IoT and IIoT devices, which only present a low computing power and power supply - symmetric keys are frequently used. For the administration within the TMA, it is irrelevant whether the keys were generated within the TMA or factory-set and then imported into the TMA.

Life cycle management

The ECOS TrustManagementAppliance offers all possibilities to generated, import, store, validate or delete secrets. For a better overview and an easier administration, freely definable metadata can be assigned manually or automatically.

Concerning symmetric keys and apart from the import feature, the TMA also offers the possibility to generate n-bit keys through high-quality randomness directly from within. Keys, just like secrets, can be enriched with metadata, exported and deleted if necessary. Regarding certificates, these keys must be signed by a CA and include further information such as validity. Besides the certificate feature, the related generation of asymmetric keys and the signature by a CA, there are also processes allowing the manual or automatic renewal.

Certificates can be renewed automatically, according to pre-set criteria, or at the touch of a button. Also, the administrator has a detailed overview of duration and pending renewals at any time. When staff leave the company or when certificates must be revoked for other reasons, they can be revoked manually or automatically, for example by deleting the user account in the Active Directory (AD) or other directory services. Information about revoked certificates is made available as Certificate Revocation List (CRL), so it can be requested by other systems. Alternatively, the status of any certificate can be checked directly per Online Certificate Status Protocol (OCSP) through the service provided by the TMA. The TMA allows to organize and arrange certificates in different certificate categories such as user, web servers or network authentication.

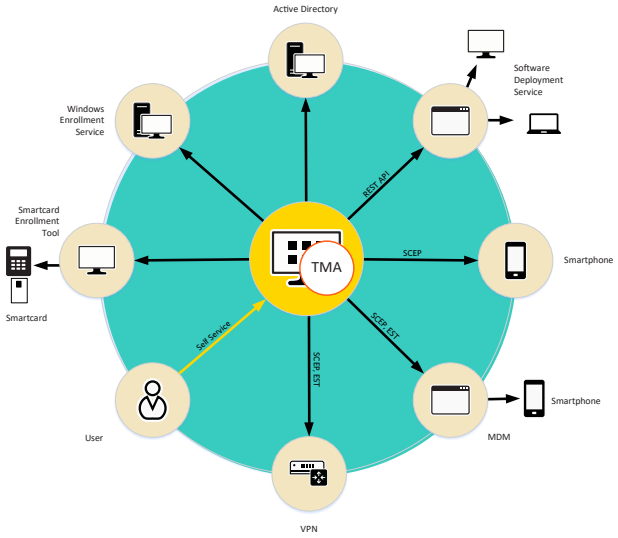
Templates offer the possibility to specify and/or enforce particular values on objects like certificates or keys and ensure through configurable validations that objects can only be created and modified within these parameters. Additionally, appropriate policies allow to determine permissions in order to generate, renew and revoke certificates according their respective security class. The same applies for the CA. CA too can be generated, renewed or revoked through the TMA. The number of simultaneously used CA is not limited. They can be arranged in parallel as different root CA, as their sub-CA or a mixture of both.

Distribution

There are various methods to distribute the certificates to the different devices and systems and their respective operating systems. For the provisioning of Windows devices, ECOS has developed a Windows service which will be installed on the devices during the software deployment - ECOS provides the respective MSI file. When the service gets in touch with the ECOS TrustManagementAppliance after the successful authentication, a certificate will be generated according to the pre-set parameters and transmitted to the Windows device. The Windows service will also monitor the validity of the certificate and, if pre-set, request a new one in time to ensure that the certificate will always be renewed automatically unless it is revoked or suspended by the administrator.

For the provisioning of Linux, Mac OS X, iOS and Android devices as well as VPN gateways, routers, VoIP telephones and other ICT devices the TMA supports miscellaneous protocols such as SCEP, CMC, EST and CMP. As described for Windows, the SCEP client will get its certificate from the TMA-side integrated SCEP server and store it in the respective certificate store. As an alternative to software deployment tools, certificates can also be distributed by website download, MDM or by dispatching profiles via e-mail. If a software deployment based on customizable scripts is used, the distribution und renewal of certificates can also be automatized by the http API provided by the TMA.

For the reconciliation or synchronization with AD and other directory services, the TMA provides a directory synchronization. User data can thus be loaded into Trust Management Appliance



Distribution

which will issue the certificates and then write them back to the AD for further distribution. This allows, if required, to wholly and remotely control the TMA through the AD.

ECOS provides the Smartcard Enrollment Tool for smart cards. It can be started as Windows app in the administration interface or in the Self Service Portal and requires no installation or configuration. For the usage of a range of smart cards, it's sufficient to depose a middleware with PKCS#11 support on the TMA. A local installation is thus no longer necessary. The Smartcard Enrollment Tool supports two different procedures to generate certificates on smart cards. If certificates are intended to secure accesses, the private key will be generated directly on the smart card. As the key can't leave the smart card, it is thus ensured that it can never fall into the wrong hands.

If the certificates are required for purposes such as encrypting documents, it is recommended to generate the private key on the TMA and then store it on the smart card. Thus, if the smart card gets lost, it is possible to issue a new one with identical keys to regain access to the encrypted documents.

Validation

There are two methods to validate a certificate. If the request is to be made without a permanent online connection, it will use a CRL (Certificate Revocation List). The CRL lists all serial numbers that have been declared invalid by the CA and should consequently be updated regularly. For this purpose, the ECOS TrustManagementAppliance provides a download option for CRLs through http or https. If there's an online availability, a real-time request through an OCSP server (Online Certificate Status Protocol) is recommended. This service is part of the TMA and can be operated in master/slave mode redundantly and cross-site.

Certificate store

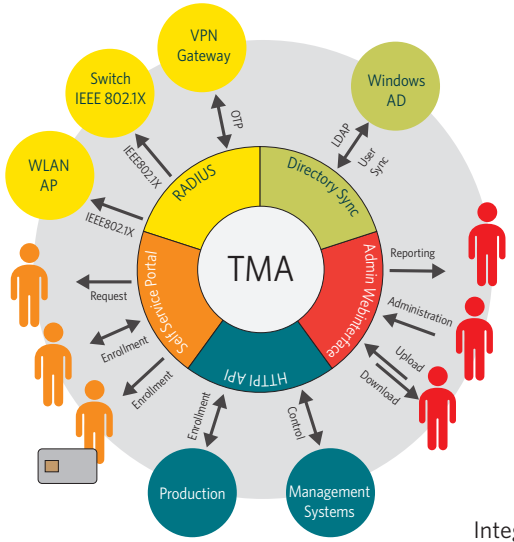
In the simplest case, root certificates, CA key and private key can be stored on a secured hard drive. However, under security aspects, a hardware security module (HSM) is recommendable. the ECOS TrustManagementAppliance supports the network-side connection of utimaco's hardware security modules. The implementation of other manufacturers is possible on demand. Similar to the smart card, the certificates can be generated directly on the HSM. E-mails and other documents or files can be signed directly within the HSM.

Integration with infrastructure

The successful introduction of a new PKI depends significantly on the implementation possibilities offered by the existing IT infrastructure. By coupling the ECOS TrustManagementAppliance with AD or other directory services, information about existing users and computers can be synchronized and related processes automatized. Thus, when creating a new user in AD, the required certificates for Windows logon, hard drive and e-mail encryption can be generated and then written back into the AD.

A mapping table allows to define procedures for single users,

groups or roles very granularly and neatly. Users of ECOS' Self Service Portal can use their Windows credentials through AD synchronization to log into the portal. The HTTP API allows to control all TMA functions remotely. For example, Linux deployment tools use the API to request, distribute and renew certificates for web servers. In the IoT area, manufacturing plants use the API to generate and request keys for the devices to be produced. The counterpart for the subsequent communication decryption is automatically stored in the TMA.



Integration

The ECOS TrustManagementAppliance allows to build up a multilevel and hierarchical structure of root and sub CA which helps to map even complex structures of the company or organization in the certificate administration. This also includes the operation and central administration of any number of root CA, thus ensuring a client-based separation of the different areas. For the operation of an autarkic site, the PKI issues a certificate request for a sub CA which will sign the root CA and thus allow the stand-alone issuing of certificates. When integrated into an existing PKI and key management environment, the TMA can be operated as both root and sub CA. An import interface for the administration of public certificates is available for purposes such as signing e-mails, client authentication, server authentication or code signing. The interface also allows to take over information, certificates and keys from a previous PKI into the TMA. For the integration into an existing monitoring system, an SNMP interface is provided. This interface allows to request parameters such as CPU load, memory usage, disk space or running processes and integrate them into existing monitoring processes.

The ECOS TrustManagementAppliancelogs all systemically relevant information to evaluate them in the integrated Active Reports or make them available through the aggregation tools of the integrated syslog interface. The TMA is delivered as a virtual appliance for operation under VMware, Microsoft Hyper-V and other virtualization solutions. The operation on dedicated hardware or datacenter is also possible. An ISO image containing the specially hardened ECOS Secure Linux operating system and the TMA components required for an easy installation of the TMA is available.

Authentication

Besides certificates, OTP-based (One Time Password) procedures are often used alternatively or additionally for a secure authentication. The ECOS TrustManagementAppliance supports a wide range of marketable solutions with the integrated Radius server.

Both the time-based TOTP application and the event-based HOTP are supported. For user authentication by software token, the TMA supports the common OTP apps for iOS, Android and Windows Phone which are based on HOTP or TOTP. The linkage and synchronization between the Radius server and the app is made with a QR code that the user scans with his smartphone in ECOS's Self Service Portal. Additionally, classical OTP token can also be used for authentication. As another option, the ECOS TrustManagementAppliance offers to send one-time passwords (OTP) by SMS to the user's specified mobile phone number that

has, for example, been taken from the AD synchronization. For authentication, first mention the user name and password, then the one-time password. SMS dispatch is made by an on-premise SMS gateway or a suitable online service.

The authentication of mobile devices and PC in WLAN or at the Ethernet switch is done according to IEEE 802.1.X standard. The access point or switch forwards the certificate that it has previously received from the device to be connected to the TMA by Radius protocol. After the successful validation by the Radius server the access will be activated.

Administration

The ECOS TrustManagementAppliance is operated through a web-based admin interface. The different roles and rights, from helpdesk staff to IT management, can be set accurately with a granular permission assignment. Thus, every user has a clear display of the features that are required for the respective range of tasks

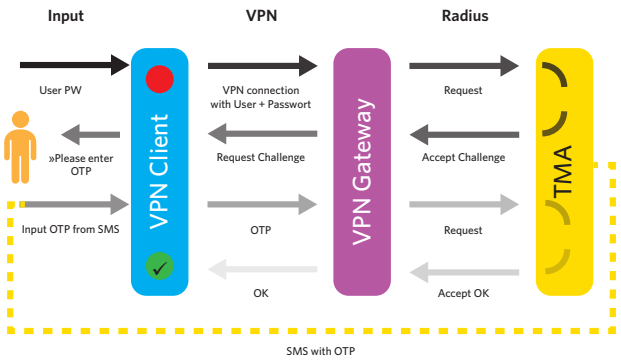
Active Reports

ECOS TrustManagementAppliance provides by default a large range of reports, which offer administrators the best possible overview of requested and issued certificates or certificates that have to be renewed. The integrated report editor allows a flexible access to all relevant information about users, certificates, keys and log files. Extensive queries, filters, groupings and tagging help the administrator to meet the complex requirements of IT and controlling.

Once generated, reports can be stored and made available to any authorized staff. Active Reports allow admins and users to advise proactively about particular information and processes or to initiate predefined actions. For example, Active Reports can inform the administrator weekly about certificate renewals or certificate requests by users. User notification can also be automatized, for example to invite them to renew their smart card in the Self Service Portal. Also automatable are escalation levels when the renewal hasn't been made in time. Active Reports allow furthermore to have recourse to specific data of the certificates themselves. It is thus possible to use the validity date both in the e-mail itself and as a trigger for the e-mail dispatch.

High availability

The ECOS TrustManagementAppliance allows to optionally operate Radius or OCSP servers in master/slave mode to ensure the user authentication in case of system failure. With the optionally available ECOS HA module, the TMA can be turned into a high availability cluster, even cross-site. In the same time, the HA module allows a random scalability and the development of a high performance PKI through the load/balancing functionality.



Authentication

ecos

safe and smart

Leistungsmerkmale

- Certificate creation, renewal and revocation
- Certificates, secrets and symmetric keys
- Key length and signature algorithm fully configurable
- Fully definable and allocable metadata
- Automatic certificate renewal
- Classification and structuring of certificates
- Certificate distribution by LDAP, SCEP, CMC, EST, CMP or Windows service
- Filling up or creation of certificates on the smart card
- Self Service Portal for users, helpdesk and admin
- Safe storage in hardware security module
- Coupling with AD and other metadirectories
- Process automatization with scripts and mapping tables
- Control of all functions by HTTP API
- Multilevel root and sub CA
- Central administration of client-specific root CA
- Integration into existing PKI as root or sub CA
- Import interface for public and private certificates
- SNMP interface for monitoring systems
- Syslog interface for aggregation tools
- Operation under VMware, Microsoft Hyper-V and other virtualization platforms or dedicated hardware
- Preconfigured ISO image with ECOS Secure Linux and TMA
- Certificate validation per CRL or OCSP
- Radius server for authentication by IEEE 802.1X
- Support of OTP token, software token and SMS
- Granular permission assignment for admin interface
- Predefined reports and own report editor
- Automatic notification system through Active Reports
- Cluster operation, also cross-site

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

+49 6133 939 200
info@ecos.de

www.ecos.de

124.PB.2023/02.DE.02.8