safe and smart

ecos

ECOS TrustManagementAppliance

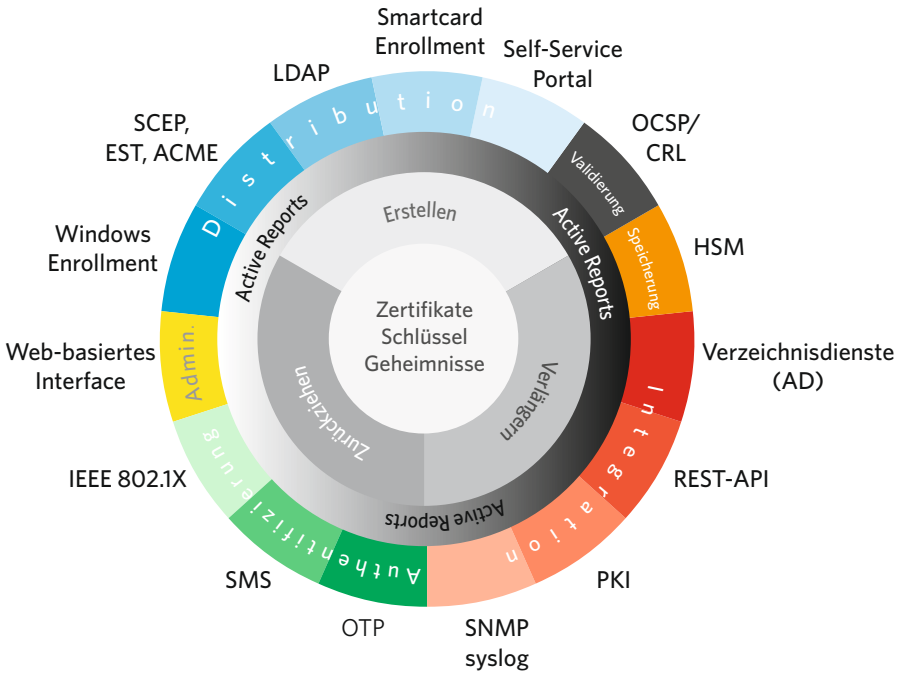
PKI und Key Management Lösung zur Absicherung
von PCs, Servern, Prozessen, (I)IoT und mobilen Geräten

- **All-in-one**
- **Aktive Reports**
- **Offen und zukunftssicher**

IT-Security Solutions
Made in Germany

Sicherheit mit Schlüssel und Zertifikat

Mit zunehmender Digitalisierung verschwimmen die Grenzen zwischen der klassischen IT, ITK und IoT. Die ECOS TrustManagementAppliance (TMA) bündelt die Verwaltung von Zertifikaten, symmetrischen Schlüsseln und sonstigen Geheimnissen - für alle Plattformen - in einer PKI und Key Management Lösung und stellt damit einen zentralen Baustein bei der Sicherung der IT, Technik und Infrastruktur.



Übersicht der Funktionen - »All-in-one«

Die Absicherung von Zugängen sowie Verschlüsselung von Daten und Kommunikation umfasst viele Bereiche im Unternehmen. Im Office-Bereich gehören die sichere Anbindung mobiler Devices im WLAN, Desktops im LAN, Windows LogOn per Smartcard, die Verschlüsselung und Signierung von E-Mails, eine sichere Authentifizierung am VPN-Gateway, Anmeldung für Webanwendungen oder Verschlüsselung von Festplatten sicher zu den häufigsten Anforderungen. Für die IT sind die Sicherung von Server-Prozessen und Webservern oder das Signieren von Apps, Makros und sonstiger Software wichtige Themen.

In Produktionsunternehmen befassen sich Technik und Produktmanagement im Besonderen mit der Absicherung von Zugängen und der Verschlüsselung der Kommunikation IT-fremder Geräte. Aufgrund der Beschaffenheit von Geräten wie Aktoren, Sensoren, Zählern, Steuerungen und medizinischer Implantate, um nur einige zu nennen, kommen hier besonders ressourcensparende Verfahren zur Anwendung.

Zertifikate, Geheimnisse, Schlüssel

Zertifikate und das zugehörige asymmetrische Schlüsselpaar stellen vielfach die Basis einer sicheren Authentisierung. Mit der ECOS TrustManagementAppliance lassen sich sowohl eine eigene private Public Key Infrastructure (PKI) aufbauen und damit Zertifikate erstellen, verlängern und zurückziehen, als auch Zertifikate einer öffentlichen CA importieren, verwalten und nutzen. Die zu erstellenden Zertifikate sind frei parametrisierbar, sowohl deren Inhalt, als auch Parameter wie z.B. Schlüssellänge oder Signaturalgorithmus. Die Zertifikate lassen sich über die TMA in allen gängigen Formaten zur Verfügung stellen, wie DER, PEM oder Containerformate wie PKCS#7 und PKCS#12.

Geheimnisse wie Passwörter, Zugangsdaten oder sonstige schützenswerte Informationen verlangen ebenso eine sichere Aufbewahrung. Mit der TMA lassen sich diese, genauso wie Zertifikate und Schlüssel, sicher verwalten und speichern. An Stellen, an denen die Verwaltung einer Zertifikatsinfrastruktur zu aufwendig ist, z.B. bei Geräten im Bereich IoT und IIoT, welche

oft nur über eine geringe Rechenleistung und Stromversorgung verfügen, kommen häufig symmetrische Schlüssel zum Einsatz. Für die Verwaltung innerhalb der TMA macht es dabei keinen Unterschied, ob die Schlüssel innerhalb der TMA generiert wurden oder auf den Geräten werkseitig aufgebracht und erst dann in die TMA importiert wurden.

Life Cycle Management

Die ECOS TrustManagementAppliance bietet alle Möglichkeiten Geheimnisse anzulegen, zu importieren, zu archivieren, abzufragen und zu löschen. Zum besseren Überblick und zur einfacheren Verwaltung lassen sich frei definierbare Metadaten manuell oder automatisiert zuordnen.

Bei symmetrischen Schlüsseln kommt neben der Import-Funktionalität die Möglichkeit hinzu, n-Bit Schlüssel über hochwertigen Zufall direkt aus der TMA heraus zu generieren. Schlüssel lassen sich wie Geheimnisse mit Metadaten anreichern, exportieren und im Bedarfsfall löschen. Bei Zertifikaten müssen diese von einer CA signiert werden und weitere Informationen wie z.B. Gültigkeit enthalten. Neben der Funktionalität Zertifikate und damit verbundene asymmetrische Schlüssel zu erzeugen und von einer CA signieren zu lassen, kommen Prozesse zur manuellen oder automatisierten Verlängerung hinzu.

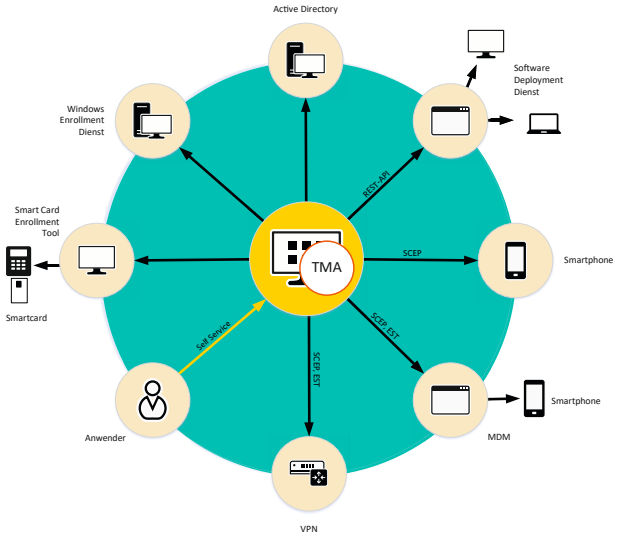
Die Verlängerung der Zertifikate kann automatisch, nach voreingestellten Kriterien oder auf Knopfdruck erfolgen. Dabei hat der Administrator oder die Administratorin jederzeit eine detaillierte Übersicht über die Laufzeit und die anstehenden Verlängerungen. Scheiden Mitarbeiter aus dem Unternehmen aus oder sollen aus anderen Gründen Zertifikate zurückgezogen werden, kann dies manuell oder auch automatisch erfolgen, beispielsweise durch Löschen des Benutzer-Accounts im Active Directory (AD) oder sonstigen Verzeichnisdiensten. Die Informationen zu gesperrten Zertifikaten werden zur Abfrage durch andere Systeme als Certificate Revocation List (CRL) zur Verfügung gestellt. Alternativ kann der Status jedes Zertifikats direkt per Online Certificate Status Protocol (OCSP) über den von der TMA bereitgestellten Dienst geprüft werden. Die TMA erlaubt es, Zertifikate in unterschiedliche Zertifikatskategorien wie z.B. User, Webserver oder Netzwerk-Authentisierung zu strukturieren und zu klassifizieren.

Über Vorlagen lassen sich bestimmte Werte für Objekte wie Zertifikate und Schlüssel vorgeben und/oder erzwingen, sowie durch konfigurierbare Validierungen sicherstellen, das nur Objekte im Rahmen der Vorgaben angelegt und geändert werden können. Darüber hinaus lassen sich über entsprechende Policies Berechtigungen für das Erstellen, Verlängern und Entziehen von Zertifikaten festlegen, abhängig von der jeweiligen Sicherheitsklasse.

Was für Zertifikate gilt, gilt gleichermaßen auch für die CA. Auch diese können innerhalb der TMA erstellt, verlängert und zurückgezogen werden. Dabei gibt es keine Begrenzung für die Anzahl der gleichzeitig genutzten CAs. Diese können parallel als mehrere Root-CAs oder als deren Sub-CAs oder einer Mischung aus beiden organisiert werden.

Distribution

Für die Distribution der Zertifikate an die unterschiedlichsten Geräte und Systeme mit ihren jeweiligen Betriebssystemen stehen unterschiedliche Mechanismen zur Verfügung. Für die Provisionierung von Windows Geräten hat ECOS einen Windows-Dienst entwickelt, welcher im Rahmen des Software-Deployments auf die Geräte aufgebracht wird. Hierfür stellt ECOS das entsprechende MSI-File zur Verfügung. Meldet sich der Dienst bei der ECOS TrustManagementAppliance, so wird nach erfolgreicher Authentisierung ein Zertifikat gemäß der vorgegebenen Parameter erzeugt und auf das Windows-Gerät übertragen. Dabei überwacht der Windows Dienst auch die Gültigkeit des Zertifikats und fordert bei entsprechender Einstellung rechtzeitig ein



Distribution

neues an, so dass sich diese bis zu einem Zurückziehen oder Sperren durch den Administrator stets automatisch verlängert.

Für die Provisionierung von Linux-, Mac OS X-, iOS- und Android-Geräten, sowie VPN-Gateways, Routern, VoIP-Telefonen, sonstigen ITK-Geräten und Webservern unterstützt die TMA diverse Protokolle, wie SCEP, EST und ACME. Ähnlich wie für Windows beschrieben, holt sich z.B. der SCEP-Client über den TMA-seitig integrierten SCEP-Server sein Zertifikat und legt es in dem jeweils vorgesehenen Zertifikatsspeicher ab.

Alternativ zu Software-Deployments-Tools, lassen sich Zertifikate per Website-Download, MDM oder den Versand von Profilen per E-Mail distribuieren. Kommt ein Software-Deployment auf Basis von anpassbaren Scripts zum Einsatz, lässt sich das Verteilen und Verlängern von Zertifikaten auch durch die von dem TMA zur Verfügung gestellten REST-API automatisieren.

Für den Abgleich oder die Synchronisation mit AD oder anderen Verzeichnisdiensten stellt die TMA eine Verzeichnissynchronisation zur Verfügung. So lassen sich Nutzerdaten in die ECOS TrustManagementAppliance übernehmen, in welcher die Zertifikate ausgestellt und zur weiteren Verteilung wieder in das AD zurückgeschrieben oder auf anderem Wege distribuiert werden. Dies ermöglicht bei Bedarf z.B. die komplette Fernsteuerung der TMA über das AD.

Zur Betankung von Smartcards stellt ECOS das Smartcard Enrollment Tool bereit. Dieses wird als Windows App aus der Administrationsoberfläche oder dem Self-Service-Portal völlig installations- und konfigurationsfrei gestartet. Für die Nutzung unterschiedlichster Smartcards reicht es aus eine Middelware mit PKCS#11-Unterstützung auf der TMA zu hinterlegen. Eine lokale Installation ist damit nicht mehr erforderlich. Das Smartcard Enrollment Tool unterstützt zwei unterschiedliche Verfahren für die Ausstellung von Zertifikaten auf Smartcards. Dienen die Zertifikate z.B. zur Absicherung von Zugängen, wird der Private Schlüssel direkt auf der Smartcard erzeugt. Da der Schlüssel die Smartcard nicht verlassen kann, ist sichergestellt, dass dieser niemals in fremde Hände gelangt.

Werden die Zertifikate z.B. für die Verschlüsselung von Dokumenten eingesetzt, empfiehlt es sich den Privaten Schlüssel auf der TMA zu erzeugen und auf der Smartcard abzulegen. So kann bei Verlust eine neue Smartcard mit identischen Schlüsseln ausgestellt werden, um mit dieser wieder Zugriff auf die verschlüsselten Dokumente zu erhalten.

Mit dem ECOS Self-Service-Portal stehen den Anwendern Assistenten zur Verfügung, mit denen sie, je nach Berechtigung Zertifikate und Smartcards beantragen oder auch selbst erstellen, verlängern und sperren können. Über die Rollen- und Berechtigungsvergabe können die Genehmigungs- und Enrollment-Prozesse eines Unternehmens in der TMA abgebildet werden.

So können die Anwender in ihrem Self-Service-Portal Zertifikate beantragen und nach erfolgter Freigabe einsetzen, während

im Self-Service-Portal des Freigabeberechtigten alle Anträge aufgelistet, genehmigt und signiert werden. Mittels E-Mail-Benachrichtigung werden Antragsteller und Freigabeberechtigte über Anträge und deren Status informiert. Das Self-Service-Portal wird als webbasierter Dienst über die TMA bereitgestellt und kann vom Administrator frei an die Bedürfnisse des Unternehmens angepasst werden.

Validierung

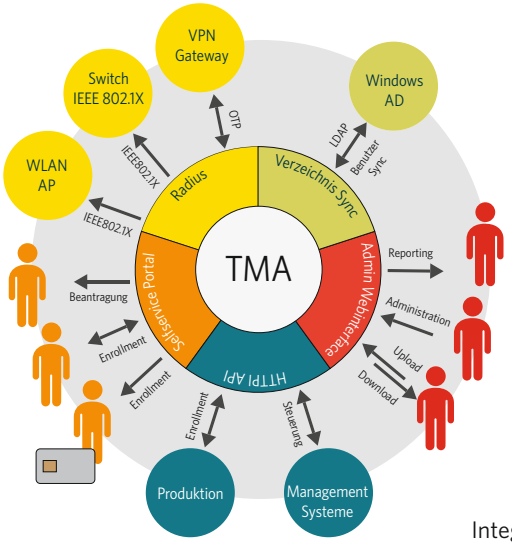
Für die Validierung eines Zertifikats stehen zwei Verfahren zur Verfügung. Soll die Abfrage ohne permanente Online-Verbindung erfolgen, so geschieht dies gegenüber einer CRL (Certificate Revocation List). Diese listet alle Seriennummern der Zertifikate auf, die von der CA für ungültig erklärt wurden und ist daher in angemessenen Intervallen zu aktualisieren. Hierfür stellt die ECOS TrustManagementAppliance eine Download-Möglichkeit für CRLs per http oder https zur Verfügung. Ist eine Online-Verfügbarkeit gegeben, so empfiehlt sich eine real-time Abfrage über einen OCSP-Server (Online Certificate Status Protocol). Dieser Dienst ist Teil der TMA und kann im Master-/Slave-Betrieb redundant und über verteilte Standorte betrieben werden.

Zertifikatsspeicher

Im einfachsten Fall lassen sich Root-Zertifikate, CA-Schlüssel und Private Schlüssel auf einer abgesicherten Festplatte abspeichern. Unter Sicherheitsaspekten empfiehlt sich aber der Einsatz eines Hardware Security Moduls (HSM), wobei die ECOS TrustManagementApplianceeine netzwerkmäßige Anbindung der Hardware Security Module von utimaco unterstützt. Die Anbindung anderer Hersteller ist auf Anfrage möglich. Wie bei einer Smartcard können die Zertifikate direkt auf dem HSM erzeugt werden. E-Mails oder sonstige Dokumente und Dateien lassen sich direkt innerhalb des HSM signieren.

Integration in die Infrastruktur

Der Erfolg bei der Einführung einer neuen PKI wird maßgeblich von den Möglichkeiten der Integration in die vorhandene IT-Infrastruktur mitbestimmt. Über die Kopplung der ECOS TrustManagementAppliance mit AD oder sonstigen Verzeichnisdiensten lassen sich Informationen über hinterlegte Benutzer und Rechner synchronisieren und die damit verbundenen Prozesse weitgehend automatisieren. So können beim Anlegen eines neuen Benutzers im AD die notwendigen Zertifikate für die Windows-Anmeldung, Festplatten- und E-Mail-Verschlüsselung erzeugt und wieder ins AD zurückgeschrieben werden.



Integration

Über eine Mapping-Tabelle lassen sich die Vorgänge für einzelne Nutzer, Gruppen oder Rollen sehr granular und übersichtlich festlegen. Nutzer des ECOS Self-Service-Portals können über die AD-Synchronisation ihre Windows-Credentials für die Anmeldung am Portal nutzen. Über die REST-API lassen sich sämtliche Funktionen der TMA fernsteuern. So nutzen beispielsweise Linux Software-Deployment-Tools die API, um Zertifikate für Webserver anzufordern, zu verteilen und zu verlängern. Im IoT-Umfeld nutzen Produktionsanlagen die API um Schlüssel für die zu fertigenden Geräte zu generieren und abzurufen. Das Gegenstück für die spätere Entschlüsselung der Kommunikation wird dabei automatisch auf der TMA hinterlegt.

Die ECOS TrustManagementAppliance erlaubt den Aufbau mehrstufig hierarchisch gegliederter Root- und Sub-CA, worüber sich auch komplexe Konzern- und Organisationsstrukturen in der Zertifikatsverwaltung abbilden lassen. Dies umfasst auch den Betrieb und die zentrale Verwaltung beliebig vieler Root-CA und ermöglicht damit mandantenbasierte Trennung der einzelnen Bereiche. Für den Betrieb eines autark operierenden Standorts stellt die PKI ein Zertifikats-Request für eine Sub-CA aus, welches die Root-CA signiert und damit ein selbstständiges Ausstellen von Zertifikaten ermöglicht. Bei der Integration in eine bestehende PKI- und Key Management-Umgebung, kann die TMA sowohl als Sub- als auch als Root-CA betrieben werden. Für die Verwaltung öffentlicher Zertifikate für Zwecke wie E-Mail-Signierung, Client-Authentisierung, Server-Authentisierung oder Code-Signierung steht eine Import-Schnittstelle zur Verfügung. Über diese lassen sich auch Informationen, Zertifikate und Schlüssel einer abzulösenden PKI in die TMA übernehmen. Für die Integration in ein bestehendes Monitoring System wird eine SNMP-Schnittstelle bereitgestellt. Hierüber lassen sich Parameter wie CPU-Auslastung, Speicherauslastung, Plattenplatz oder laufende Prozesse abfragen und in bestehende Überwachungsprozesse einbinden.

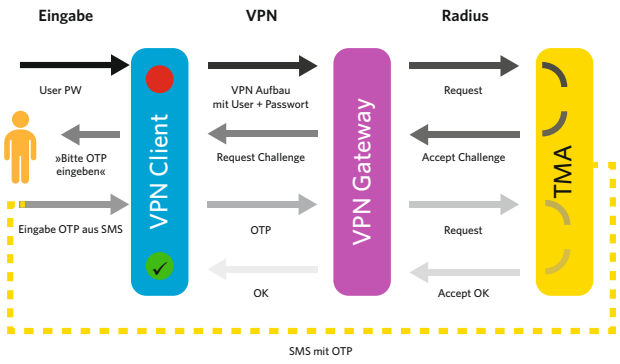
Die ECOS TrustManagementAppliance loggt sämtliche systemrelevante Informationen, um diese über die integrierten ActiveReports auszuwerten, oder aber über die integrierte syslog-Schnittstelle bestehenden Aggregations-Tools bereitzustellen. Die TMA wird als virtuelle Appliance geliefert, zum Betrieb unter VMware, Microsoft Hyper-V oder anderen Virtualisierungslösungen. Ein Betrieb auf dedizierter Hardware oder im Rechenzentrum ist ebenso möglich. Für die Installation steht ein ISO-Image zur Verfügung, bestehend aus dem speziell gehärteten ECOS Secure Linux-Betriebssystem und den TMA-Komponenten, mittels dieser sich die TMA einfach installieren lässt.

Authentifizierung

Für die sichere Authentifizierung eines Benutzers kommen neben Zertifikaten häufig OTP-basierte Verfahren (One Time Password) alternativ oder ergänzend zum Einsatz. Über den integrierten Radius-Server unterstützt die ECOS TRUST MANAGEMENT APPLIANCE eine breite Auswahl marktgängiger Lösungen.

Dabei werden sowohl das Zeit-basierte Verfahren TOTP als auch das Event-basierte HOTP unterstützt. Für die User-Authentisierung per Software Token unterstützt die TMA die gängigen OTP-Apps für iOS, Android und Windows Phone, welche auf HOTP oder TOTP basieren. Die Verknüpfung und Synchronisation zwischen dem Radius-Server und der App erfolgt über einen QR-Code, welcher der Benutzer mit seinem Smartphone über das ECOS Self-Service-Portal einscannt. Darüber hinaus können auch klassische OTP-Token zur Authentisierung genutzt werden.

Als weitere Möglichkeit bietet die ECOS TrustManagementAppliance den Versand von Einmalpasswörtern (OTP) per SMS an die hinterlegte Mobilfunknummer des Benutzers an, welche beispielsweise aus der AD-Synchronisation übernommen wurde. Für die Authentisierung sind erst Benutzername und Passwort und anschließend das Einmalpasswort einzugeben. Der Versand der SMS erfolgt über ein On Premise betriebenes SMS-Gateway



Authentifizierung

oder einen entsprechenden Online-Dienst.
Die Authentisierung mobiler Geräte und PCs am WLAN oder am Ethernet Switch erfolgt gemäß dem IEEE 802.1.X Standard. Dabei leitet der Access-Point oder Switch das Zertifikat per Radius-Protokoll an die TMA weiter, welches dieser zuvor von dem zu verbindenden Gerät empfangen hat. Nach erfolgreicher Validierung durch den Radius-Server wird dann der Netzzugang freigeschaltet.

Administration

Die Bedienung der ECOS TrustManagementAppliance erfolgt über ein Web-basiertes Admin-Interface. Über eine granulare Rechtevergabe lassen sich die einzelnen Rollen und Rechte, vom Mitarbeiter im Helpdesk bis zum IT-Verantwortlichen, genau abbilden. So hat jeder Benutzer eine übersichtliche Darstellung genau der Funktionen, welche für den jeweiligen Aufgabenbereich erforderlich sind.

Active Reports

Die ECOS TrustManagementAppliance bringt standardmäßig bereits eine breite Auswahl an Reports mit. Diese geben dem Admin einen bestmöglichen Überblick über beantragte und ausgestellte Zertifikate, abgelaufene Zertifikate und solche, die zur Verlängerung anstehen. Der integrierte Report-Editor erlaubt den flexiblen Zugriff auf alle relevanten Informationen hinsichtlich Benutzer, Zertifikaten, Schlüsseln und Log-Daten. Umfassende Abfragen, Filter, Gruppierungen und Kennzeichnungen erlauben es dem Administrator komplexen Anforderungen von IT und Controlling gerecht zu werden. Einmal generierte Reports lassen sich abspeichern und anderen Berechtigten zur Verfügung stellen. Active Reports ermöglichen es Admin und Anwender proaktiv über bestimmte Informationen und Vorgänge zu informieren oder vordefinierte Aktionen auszulösen. So können die Active Reports beispielsweise den Administrator wöchentlich per E-Mail über anstehenden Zertifikatsverlängerungen oder Zertifikatsanforderungen durch den Anwender informieren.

Vorteile auf einen Blick

+ PKI und Key-Management »Out of the Box«
+ Zertifikate, symmetrische Schlüssel und sonstige Geheimnisse
+ Unterstützt alle Plattformen, Systeme und Devices:
  Win, Linux, Mac OS X, iOS, Android, Windows Phone, IoT
+ Authentifizierung mobiler Geräte am WLAN über IEEE 802.1.x
+ OTP-User-Authentifizierung per Software-Token, Token und SMS
+ Automatisches Benachrichtigungssystem über Active Reports
+ Nahtlose Integration in die bestehende Infrastruktur
+ Frei skalierbar und optional hochverfügbar

Benachrichtigungen an die Benutzer selbst lassen sich ebenfalls automatisieren, beispielsweise die Mitteilung ihre Smartcard über das Self-Service-Portal zu verlängern. Ebenfalls automatisieren lassen sich Eskalationsstufen, wenn die Verlängerung nicht innerhalb des vorgegebenen Zeitraums erfolgt. Für die Active Reports lässt sich auch auf bestimmte Informationen aus den Zertifikaten selbst zurückgreifen. So kann beispielsweise das Gültigkeitsdatum sowohl in der E-Mail selbst, als auch als Trigger für deren Versand genutzt werden.

Hochverfügbarkeit

Die ECOS TrustManagementAppliance erlaubt es optional Radius- oder OCSP-Servern im Master-/Slave-Betrieb einzusetzen und damit die Benutzer-Authentifizierung beim möglichen Ausfall eines Systems weiterhin sicherzustellen.

Über das optional erhältliche ECOS HA-Modul lässt sich die TMA zu einem Hochverfügbarkeitscluster ausbauen, auch über mehrere Standorte hinweg. Gleichzeitig ermöglicht das HA-Modul über die LoadBalancing-Funktionalität eine beliebige Skalierung und Aufbau einer Hoch-Performance-PKI.

ecos

safe and smart

Leistungsmerkmale
◆ Erstellen, verlängern, zurückziehen von Zertifikaten
◆ Zertifikate, Geheimnisse und symmetrische Schlüssel
◆ Schlüssellänge und Signaturalgorithmus frei konfigurierbar
◆ Frei definierbare und zuordenbare Metadaten
◆ Automatische Verlängerung von Zertifikaten
◆ Automatisierbare Zertifikatsregistrierung (certificate enrollment | Basis va SCEP)
◆ Automatisierbare Zertifikatserneuerung (certificate renewal | Basis via SCEP)
◆ Distribution der Zertifikate per LDAP, SCEP, ACME oder Windows Dienst
◆ Unterstützung von Windows-/Linux-Server sowie Clients, weitere Endgeräte (insb. Android und iOS via Mobile Device Management)
◆ Betanken oder Erzeugung von Zertifikaten auf der Smartcard
◆ Self-Service-Portal für Anwender, Helpdesk und Admin
◆ Frei konfigurierbare Workflows z.B. für ◆ die Beantragung von Zertifikaten ◆ die Genehmigung von Zertifikatsanforderungen ◆ den Download und die Installation von Zertifikaten ◆ das Enrollment auf Smartcards ◆ regelmäßige Helpdesk-/Admin-Arbeiten
◆ Validierung der Zertifikate per CRL oder OCSP
◆ Sichere Speicherung im Hardware Security Modul möglich
◆ Kopplung mit AD oder sonstigem Metadirectory
◆ Steuerung und Konfigurierbarkeit sämtlicher Funktionen per REST-API
◆ Integration in bestehende PKI, als Sub- oder Root-CA
◆ Cluster-Betrieb, auch standortübergreifend
◆ Mehrstufig gegliederte Root- und Sub-CAs
◆ Import-Schnittstelle für Öffentliche und Private Zertifikate
◆ SNMP-Schnittstelle für die Anbindung eines Monitoringsystems
◆ syslog-Schnittstelle für die Anbindung eines Aggregations-Tools
◆ Virtuelle Appliance zum Betrieb unter VMware, Microsoft Hyper-V oder anderen Virtualisierungslösungen
◆ Vorkonfiguriertes ISO-Image mit ECOS Secure Linux und TMA
◆ Unterstütztes Benachrichtigungssystem über Active Reports
◆ Zentrale Web-Oberfläche
◆ Granulare Rechtevergabe für das Admin-Interface

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