Case Study

ECOS TrustManagementAppliance

Case Study | R. STAHL AG

PKI im Einsatz bei der R. STAHL AG

Die ECOS TrustManagementAppliance als zentrale Public-Key-Infrastruktur (PKI) bei der R. STAHL AG

- **Anwender:** R.STAHL AG
- **Branche:** Systeme & Dienstleistungen
- **Ziel:** Neue PKI für die Verwaltung sämtlicher Geräte im Unternehmen
- **Lösung:** Virtuell geclusterte PKI-Appliance | ECOS TrustManagementAppliance

Sicherheit genießt im IT-Netzwerk der **R. STAHL AG** höchste Priorität.

Über eindeutige Zertifikate gewährleistet der international tätige Explosionsschutz-Spezialist, dass ausschließlich bekannte, berechtigte Geräte Zugriff erhalten.

Thomas Merkel | Vice President Global IT | R. STAHL AG
»Mit der ECOS PKI realisieren wir im Vergleich zu früher mehr Sicherheit und mehr Funktionalität bei gleichzeitig weniger Aufwand.«

Sicherheit genießt auch im IT-Netzwerk der R. STAHL AG höchste Priorität. Über eindeutige Zertifikate gewährleistet der international tätige Explosionsschutz-Spezialist, dass ausschließlich bekannte, berechtigte Geräte Zugriff erhalten. Durch den Umstieg auf die ECOS TrustManagementAppliance wurde eine zentrale Plattform für die Bereiche PKI (Public-Key-Infrastruktur) und OTP (One-Time-Password) geschaffen, die gleichzeitig direkt an das Active Directory angebunden ist. Das Ergebnis: Mehr Sicherheit und höhere Funktionalität bei deutlich gesunkenem Aufwand für Wartung und Administration.

Über R. STAHL AG
Explosionsschutz auf höchstem Niveau: Die elektrischen und elektronischen Spezialprodukte von STAHL kommen weltweit überall dort zum Einsatz, wo im industriellen Bereich mit brennbaren Stoffen gearbeitet wird und bereits der kleinste Funke fatale Folgen haben könnte.

»Eine wichtige Anforderung an die neue PKI war für uns die Synchronisation mit dem Active Directory«

Thomas Merkel, Vice President Global IT | R. STAHL

Von Schaltern und Verteilern über Beleuchtung bis hin zu Bedien- und Signal-Systemen liefert das Unternehmen explosionsgeschützte Komponenten und Systemlösungen insbesondere für die Öl- und Gasindustrie, die Lebensmittelbranche, die Chemie- und Pharmaindustrie und den Schiffsbau.

Die börsennotierte Gesellschaft mit Sitz im baden-württembergischen Waldenburg nimmt dabei eine international führende Stellung ein. An den Produktionsstandorten in Deutschland, Norwegen, Indien sowie in den USA und in den Niederlanden beschäftigt R. STAHL rund 1.700 Mitarbeiter.

Sicherheit steht bei R.Stahl jedoch nicht nur bei den eigenen Produkten im Mittelpunkt. Auch an die internen Strukturen und Prozesse werden höchste Maßstäbe angelegt, um Mitarbeiter, Systeme, Daten, Know-how und Produktionsanlagen zu schützen. Dazu zählt auch die Vergabe von Zertifikaten für die im Firmennetzwerk agierenden Geräte. Hierbei setzte R. STAHL bislang auf eine Standard-PKI-Lösung für das Ausstellen, Prüfen und Verwalten dieser Zertifikate. Problematisch war dabei, dass damit zwar PCs und Notebooks erfasst werden, die stets wachsende Schar weiterer Netzwerk-Geräte, etwa auch solche jenseits der klassischen »Windows-Welt«, größtenteils aber außen vor blieb, beispielsweise Telefone oder mobile Endgeräte.

BSI-Empfehlungen mit Bestandslösung nicht erfüllbar
Neben dieser Einschränkung ließ die Bestandslösung auch in anderen Bereichen Wünsche offen. So waren etwa die Möglichkeiten beim Reporting unzureichend. Immer wieder kam es dadurch vor, dass das Auslaufen von Zertifikaten sehr spät bemerkt wurde. Mit dem System, das vom Hersteller auch abgekündigt wurde, war zudem aus technischer Sicht kein Umstieg auf den Hash-Algorithmus SHA-2 möglich.

Da das Bundesamt für Sicherheit in der Informationstechnik (BSI), an dessen Vorgaben sich R. STAHL bei IT-Sicherheitsmaßnahmen orientiert, genau diesen Umstieg jedoch dringend empfieht, stand der Entschluss fest: Es galt, eine neue, geeignete PKI zu finden und zu implementieren. Diese sollte nicht nur »State of the Art« hinsichtlich Sicherheit, sondern auch in der Lage

safe and smart

ecos

Mit PKI und Key Management die zukunft sichern – ECOS **TrustManagementAppliance**

Aufgrund der sehr konkreten Anforderungen zeigte sich bei einer ersten Marktanalyse, dass nur wenige Anbieter in der Lage sind, alle Kriterien der R. STAHL AGzu erfüllen.

sein, Zertifikate für sämtliche Geräte im Unternehmen verwalten zu können.

»Eine wichtige Anforderung an die neue PKI war für uns die Synchronisation mit dem Active Directory«, erklärt Thomas Merkel, Vice President Global IT bei R. STAHL.

Entscheidung für die ECOS TrustManagement-Appliance

Aufgrund der sehr konkreten Anforderungen zeigte sich bei einer ersten Marktanalyse, dass nur wenige Anbieter in der Lage sind, alle diese Kriterien zu erfüllen.

Die Trust Management Appliance (TMA) von ECOS Technology überzeugte die Verantwortlichen bei R. STAHL durch die Möglichkeit, sämtliche Zertifikate sowie bei Bedarf auch symmetrische Schlüssel und OTP-Token über eine Appliance zu erstellen, zu speichern, zu validieren und zu verwalten. Da sich die ECOS TMA direkt mit dem Active Directory (oder, falls gewünscht, anderen Verzeichnisdiensten) koppeln lässt, können alle Einzelheiten zu Benutzern und Clients synchronisiert werden, was den Weg für eine sehr weitreichende Automatisierung freimacht.
Nach einer erfolgreichen Teststellung kommt die PKI-Lösung von ECOS heute als virtuell geclusterte Appliance bei R. STAHL weltweit zum Einsatz, wodurch gleichzeitig Redundanz gegeben ist. Die Haupteinsatzgebiete sind die Authentifizierung von Geräten im Netzwerk, der Windows-Anmeldevorgang der Benutzer, die Zwei-Faktor-Authentifizierung bei Remotezugängen sowie die Verschlüsselung von Daten auf Datenträgern.

Hohe fünfstellige Zahl an Validierungen pro Stunde

Hierzu erhält jeder Client im Unternehmen ein Zertifikat: Telefone, Access Points, Server, mobile Endgeräte sowie teilweise auch (neuere) Anlagen und Maschinen in der Produktion. Insgesamt verwaltet R. Stahl inzwischen rund 8.000 Zertifikate über die ECOS TMA. Allein auf das klassische Rechner-Segment mit PCs, Notebooks und Thin Clients entfallen rund 2.000 Zertifikate, die in kurzen und regelmäßigen Abständen für eine Re-Authentifizierung validiert werden – die PKI-Appliance leistet hierdurch eine hohe fünfstellige Anzahl an Validierungen pro Stunde.
Um größtmögliche Sicherheit zu gewährleisten, nutzt R. STAHL für die Prüfung der Gültigkeit täglich aktualisierte Zertifikatssperrlisten (CRL/ Certificate Revocation List) mit den zurückgezogenen Zertifikaten. Zusätzlich greift man applikationsabhängig auf einen OCSPDienst (Online Certificate Status Protocol) zurück, der über eine Abfrage an die ECOS TMA in Echtzeit klärt, ob das jeweilige Zertifikat tatsächlich noch gültig ist.

Auch im Rahmen der Festplatten- und Fileverschlüsselung werden Zertifikate im Unternehmen eingesetzt, denn die Anmeldung an der standardbasierten Verschlüsselung aller Rechner

mit einem lokalen Speicher läuft ebenfalls über die PKI. Bei der Fileverschlüsselung einzelner Dateien oder Ordner wird über die ECOS TMA zudem für eine eindeutige digitale Signatur der Files gesorgt, um absolute Manipulationssicherheit zu gewährleisten. Ebenfalls über die PKI-Appliance erfolgt die Synchronisierung der öffentlichen Schlüssel im Active Directory für die standardbasierte E-Mail-Verschlüsselung (Outlook und S/MIME).

Für die Zugangssicherheit und die Anmeldung der Mitarbeiter im Netzwerk setzt R. STAHL auf Multicards. Die früheren Zugangskontrollkarten wurden hierzu auf Smartcards umgestellt, um sie ebenfalls über die PKI verwalten zu können. Die Multicards fungieren zusätzlich auch als Mitarbeiterausweis und für die Zeiterfassung. Um individuelle Vorlieben der Anwender abdecken zu können, lässt der Explosionsschutz-Spezialist seinen Mitarbeitern dabei die Wahl zwischen Lösungen mit Karte und mit USB-Token.

Mehr Sicherheit und Funktionalität, weniger Aufwand

Ein integriertes Reporting sorgt dafür, dass bei ablaufenden Zertifikaten rechtzeitig eine Erinnerung per E-Mail erfolgt. Um die Prozesse beim Auslaufen und Erneuern der Zertifikate, die jeweils für ein Jahr laufen, so schlank wie möglich zu halten, führt R. STAHL künftig zusätzlich ein Self-Service-Portal ein. Über dieses Webportal sollen Mitarbeiter zum Beispiel auch in der Lage sein, abgelaufene Smartcards neu zu bespielen oder Token zu synchronisieren – ein wichtiger Aspekt, um Mitarbeitern unnötige Wege zu ersparen.

»Mit der ECOS PKI realisieren wir im Vergleich zu früher mehr Sicherheit und mehr Funktionalität bei gleichzeitig weniger Aufwand. Das System deckt unsere Anforderungen vollständig ab und läuft sehr zuverlässig und störungsfrei. Gleichzeitig setzen wir damit unseren Wunsch nach einer zentralen Plattform für PKI und OTP inklusive Anbindung an das Active Directory um. Wir sind mit der Lösung von ECOS sehr zufrieden«, fasst Merkel zusammen.

Case Study - Szenario

Anwender
R.Stahl AG

Branche
Systeme und Dienstleistungen für den Explosionsschutz

Herausforderung
Neue PKI für die Verwaltung sämtlicher Geräte im Unternehmen

Lösung
Virtuell geclusterte PKI Appliance für die Authentifizierung von Geräten im Netzwerk, der Windows-Anmeldevorgang der Benutzer, die Zwei-Faktor-Authentifizierung bei Remotezugängen sowie die Verschlüsselung von Daten auf Datenträgern.

Über R. STAHL AG
Explosionsschutz auf höchstem Niveau: Von Schaltern und Verteilern über Beleuchtung bis hin zu Bedien- und Signal-Systemen liefert das Unternehmen explosionsgeschützte Komponenten und Systemlösungen insbesondere für die Öl- und Gasindustrie, die Lebensmittelbranche, die Chemie- und Pharmaindustrie und den Schiffsbau.

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

+49 6133 939 200
info@ecos.de

ecos.de

143.CS_STAHL.2023/02.DE.01.6