

## Case Study | Flughafen Köln Bonn

# PKI und Key Management im Einsatz beim Flughafen Köln Bonn

Vom Handheld bis zur Anzeigentafel: Zertifikate für alle Geräte

- **Anwender:** Flughafen Köln Bonn GmbH
- **Branche:** Flughafenbetreiber
- **Ziel:** Umsetzung einer PKI-Lösung
- **Lösung:** Einführung der ECOS TrustManagementAppliance®



Köln Bonn Airport

# Absicherung durch PKI Schlanke, automatisierte Prozesse beim Flughafen **Köln Bonn Airport**

## Enorme Zeitersparnis beim Management von Zertifikaten mit der ECOS TrustManagementAppliance

**Alexander Händel**

*Datacenter & Shared Services  
Flughafen Köln Bonn GmbH*

»Es gelingt uns Zertifikate mit der ECOS PKI deutlich schneller und einfacher auszustellen. Die Zeitersparnis ist insgesamt enorm, wir benötigen pro Vorgang nur noch rund ein Viertel der Zeit«.

Keine Kompromisse bei der Sicherheit: Hardware-Zertifikate sorgen am Köln Bonn Airport dafür, dass ausschließlich berechnete Geräte innerhalb der Infrastruktur eingesetzt werden können. Mit der ECOS TrustManagementAppliance hat der Flughafen eine zentrale Lösung für die Erstellung der Zertifikate für sämtliche Gerätearten etabliert. Durch einen hohen Grad an Automatisierung und die integrierten Managementfunktionen konnte dabei gleichzeitig der Wartungsaufwand deutlich gesenkt werden.

### Über den Köln Bonn Airport

Über zehn Millionen Fluggäste pro Jahr machen den Köln Bonn Airport zu einem der wichtigsten Drehkreuze der Luftfahrt in Deutschland. Neben dem Passagierbetrieb spielt der rund um die Uhr geöffnete Flughafen auch im internationalen Frachtverkehr eine bedeutende Rolle. Mit rund 700.000 Tonnen Fracht pro Jahr liegt der Airport in diesem Segment beispielsweise deutlich vor München, Berlin-Tegel oder Düsseldorf.

Die hohen Anforderungen an die Sicherheit im sensiblen Flughafen-Umfeld bestimmen auch die Arbeit der zentralen IT-Abteilung. So muss etwa sichergestellt werden, dass innerhalb der Airport-eigenen Netzwerke ausschließlich entsprechend zugelassene und legitimierte Geräte eingesetzt werden können.

### Zertifikate für Geräte außerhalb der »Windows-Welt« waren aufwendig

Für das Erstellen und Verwalten von Hardware-Zertifikaten vertraute man am Köln Bonn Airport bisher auf eine Windowsbasierte PKI-Appliance. Diese wurde beispielsweise dafür genutzt, um Zertifikate für die rund 1.200 Windows-Clients am Flughafen sowie für Webservices und verschiedenste Handheld-Geräte zu beziehen und zu managen.

Die Lösung funktionierte zwar grundsätzlich, relativ kompliziert gestaltete sich jedoch der Umgang mit Geräten außerhalb der »Windows-Welt« sowie die Verwaltung der Zertifikate. So war es zum Beispiel sehr mühsam und zeitaufwendig, ein bestimmtes Zertifikat zu suchen, um dieses zu sperren. Auch das Hinterlegen von Regeln und Templates, um passende Zertifikate für speziellere Geräte zu erstellen, war mit dem Bestandssystem komplex.

»Wir hatten es zum einen mit immer mehr unterschiedlichen Handheld-Systemen zu tun, zum anderen kam auch das Thema der zertifikatsbasierten Netzwerkauthentifizierung auf die Agenda«, berichtet Kenan Salaka, Datacenter & Shared Services bei der Flughafen Köln Bonn GmbH. »Dies führte dazu, dass viele neue Geräte, die im Active Directory noch gar nicht vorhanden

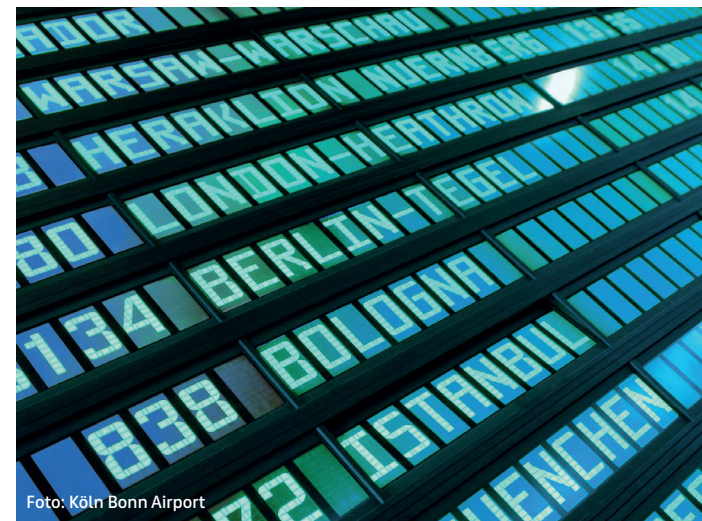


Foto: Köln Bonn Airport

### Anzeigentafel Köln Bonn Airport

Neben Handhelds werden u.a. auch die Anzeigentafeln mit der Trust Management Appliance von ECOS abgesichert.



### ECOS Partner Devoteam

Devoteam ist ein führendes Beratungsunternehmen mit Schwerpunkt auf digitaler Strategie, Plattform-Technologien, Cybersecurity und Business Transformation. Die Umsetzung der ECOS PKI beim Flughafen Köln Bonn wurde von Devoteam begleitet und umgesetzt.

## All-in-One-PKI-Lösung für die Absicherung sämtlicher Geräte bei der Flughafen Köln Bonn GmbH



Foto: Köln Bonn Airport

sind, möglichst von Anfang an mit Zertifikaten versorgt werden sollten.«

### Das Sicherheitsniveau erhöhen

Die Ausweitung der Ausgabe von Zertifikaten auf möglichst viele Gerätetypen hatte auch den Hintergrund, das Sicherheitsniveau weiter zu erhöhen. So waren etwa bei Anzeigetafeln in den öffentlichen Bereichen des Flughafens die Netzwerkports lediglich per MAC-Adresse abgesichert, was der IT-Abteilung schon länger ein Dorn im Auge war. Die Einrichtung war aufwendig, da zum Teil zwei oder noch mehr MAC-Adressen pro Gerät eingetragen werden mussten, während gleichzeitig die Sicherheit nicht mehr den Vorstellungen entsprach.

Die Gerätevielfalt am Airport ist darüber hinaus generell groß und reicht weit über die klassische Client-Welt hinaus: Von den Handhelds, mit denen die Mitarbeiter auf dem Vorfeld Informationen rund um ihre Aufgaben und abzufertigende Flugzeuge abrufen, über spezielle mobile Geräte der Sicherheitsmitarbeiter bis hin zu Tablets, die in den »Follow-me-Fahrzeugen« verbaut sind. Grund genug für die IT-Verantwortlichen des Flughafens, sich nach einer besser und universeller geeigneten PKI-Lösung für die Erstellung und Verwaltung von Zertifikaten umzusehen. Neben der Unterstützung von Windows und Linux sowie

der Active-Directory-Authentifizierung stand dabei vor allem auch die Automatisierung im Mittelpunkt, um den Wartungsaufwand zu senken. Es sollte ein so weit wie möglich automatisierter Prozess für alle Arten von Clients geschaffen werden, um Zertifikate auf die Geräte herunterzuladen und bei Bedarf selbsttätig zu erneuern.

### ECOS TrustManagementAppliance überzeugte bei Proof of Concept

Nachdem man auf die PKI-Lösung Trust Management Appliance von ECOS Technology aufmerksam wurde, startete ein Proof of Concept am Köln Bonn Airport. Dabei wurden verschiedenste Client- und Gerätetypen testweise mit Zertifikaten versorgt: Von Windows-Clients über Drucker, Telefone und Linux-Server bis hin zu (beispielsweise bei Anzeigeräten genutzten) Raspberries sowie speziellen Handhelds unter Android und weiteren mobilen Betriebssystemen.

»Die Tests im Rahmen des Proof of Concept verliefen sehr erfolgreich, alles ließ sich sehr einfach einrichten« sagt Salaka. »Das löste bei uns auch die Diskussion aus, sich generell auf ein PKI-System zu konzentrieren, dieses wirklich im Detail zu verstehen und dann gewissermaßen eine Rundum-Lösung für die Absicherung sämtlicher Geräte nutzen zu können.«

Heute kommt die ECOS TrustManagement-Appliance (TMA) als virtuelle Appliance auf VMware-Basis am Flughafen zum Einsatz. Durch Clustering wird für Redundanz und Ausfallsicherheit gesorgt – da der Airport rund um die Uhr an sieben Tagen pro Woche in Betrieb ist,



ist die Hochverfügbarkeit der Lösung essentiell. Vor der Trust Management Appliance ist zudem ein Loadbalancer zur Verteilung der Anfragen geschaltet. Der Client zur Abholung der Zertifikate von der Appliance wurde im Rahmen der normalen wöchentlichen Softwareverteilung auf die Endgeräte ausgerollt, ohne dass die Anwender selbst eingreifen mussten. Bei der Anmeldung eines Gerätes per VPN wird nun über das Hardware-Zertifikat geprüft, ob es sich um ein vertrauenswürdiges Gerät mit Zertifikat vom Flughafen handelt. Dabei erfolgt mittels Online Certificate Status Protocol (OCSP) zusätzlich eine Gegenprüfung, ob das Zertifikat zum aktuellen Zeitpunkt wirklich gültig ist.

#### **Deutliche Zeitersparnis beim Umgang mit Zertifikaten**

Nach einiger Zeit im Live-Betrieb haben sich für die PKI-Verantwortlichen am Airport klare Vorteile der ECOS TrustManagementAppliance herauskristallisiert, die zu einer deutlichen Reduzierung des Wartungsaufwands geführt haben. Dies

betrifft sowohl die Ausstellung der Zertifikate als auch das Management, wie Alexander Händel berichtet, Kollege von Kenan Salaka im Bereich Datacenter & Shared Services bei der Flughafen Köln Bonn GmbH:

»Es gelingt uns seit der Implementierung der PKI-Lösung von ECOS zunächst einmal deutlich schneller und einfacher, die Zertifikate überhaupt auszustellen. Das zeigt sich gerade bei den Sonderfällen, also zum Beispiel bei Geräten, die nicht im Active Directory sind. Wesentlich komfortabler ist außerdem die Suche nach Zertifikaten, um etwa zu prüfen, was genau ausgestellt wurde oder um ein Zertifikat zurückzuziehen. Die Zeitersparnis ist hier insgesamt enorm, wir benötigen pro Vorgang nur noch rund ein Viertel der Zeit«

Für Übersicht sorgt auch ein monatliches Reporting per E-Mail, das darüber informiert, welche Zertifikate neu hinzugekommen sind, welche abgelaufen sind oder welche gesperrt wurden (zurückgezogen oder temporär gesperrt).

Um die Abläufe künftig noch weiter zu automatisieren, ist am Flughafen mittelfristig zudem die Einrichtung eines Self-Service-Portals für IT-Mitarbeiter und Mitarbeiterinnen aus dem Application-Bereich geplant. Benötigen diese beispielsweise ein Zertifikat für einen Webserver, so soll dies künftig dann für den jeweiligen, klar abgegrenzten Bereich selbsttätig möglich sein, was die zentrale IT weiter entlasten wird.

#### **Case Study - Szenario**

##### **Anwender**

Flughafen Köln Bonn GmbH

##### **Branche**

Flughafenbetreiber

##### **Herausforderung**

Zertifikate für Geräte außerhalb der »Windows-Welt«

##### **Lösung**

Einführung der ECOS TrustManagementAppliance für sämtliche Geräte

##### **Über die Flughafen Köln Bonn GmbH**

Über zehn Millionen Fluggäste pro Jahr machen den Köln Bonn Airport zu einem der wichtigsten Drehkreuze der Luftfahrt in Deutschland. Neben dem Passagierbetrieb spielt der rund um die Uhr geöffnete Flughafen auch im internationalen Frachtverkehr eine bedeutende Rolle.

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

+49 6133 939 200  
info@ecos.de

www.ecos.de