Case Study

ECOS TrustManagementAppliance®

ecos

Case Study | Cologne Bonn Airport

PKI and Key Management at Cologne Bonn Airport

From handheld to scoreboard: certificates for all devices

- ◆ **Operator:** Airport Köln Bonn GmbH
- ◆ **Sector:** Airport Operator
- ◆ **Objective:** Implementing a PKI solution
- ◆ **Solution:** ECOS TrustManagementAppliance®

Köln Bonn Airport

Achieving security through PKI
Lean and automated processes at
Cologne Bonn Airport

Significant time savings in certificate management with the ECOS TrustManagementAppliance

Alexander Händel
Datacenter & Shared Services Flughafen Köln Bonn GmbH

»It is clearly faster and easier to issue certificates with the ECOS PKI. The overall time saving is tremendous, it only takes the quarter of the previous time per operation.«.

No compromise on security: hardware certificates ensure that only authorized devices can be used inside the infrastructure of the Cologne Bonn Airport. The ECOS TrustManagementAppliance is the airport's central solution for issuing certificates to all types of devices. At the same time, the high automation level and the integrated management functions reduced maintenance efforts considerably.

About Cologne Bonn Airport
With over ten million passengers per year, Cologne Bonn Airport is one of the major airport hubs in Germany. Aside from passenger traffic, the non-stop operating airport also plays a significant role in airfreight traffic.

With about 700,000 metric tons of freight per year, the airport is clearly ahead of Munich, Berlin Tegel and Düsseldorf in this field. The high demands placed on security in the sensitive environment of an airport also determine the work of the central IT department. For example, only approved and authorized devices are to be used on the airport's own networks.

### Issuing certificates to non-Windows devices was cumbersome
For the creation and administration of hardware certificates, Cologne Bonn Airport previously

relied on a Windows-based PKI appliance to provision and manage certificates for approximately 1,200 airport Windows clients, Web services, and various handheld devices. While the solution was basically sound, handling of non-Windows devices and certificate management was highly complicated. Finding a specific certificate to revoke, for example, was very tedious and time-consuming. The existing system also made it difficult to define rules and templates to create appropriate certificates for specific devices.

»On the one hand, we had an increasing number and variety of handheld systems that we needed to manage. On the other hand, certificate-based network authentication came up on the agenda«, relates Kenan Salaka, Datacenter & Shared Services at the Flughafen Köln Bonn GmbH.»As a result, the many new devices that do not yet exist in Active Directory should be provisioned with certificates from the start.«

Raising the security level
One argument for extending certificate issuance to as many device types as possible was to further increase the level of security. For example, the network ports on the scoreboards in the public areas were secured only by MAC address, which had long been a thorn in the side of the IT department. This was complex to set up because
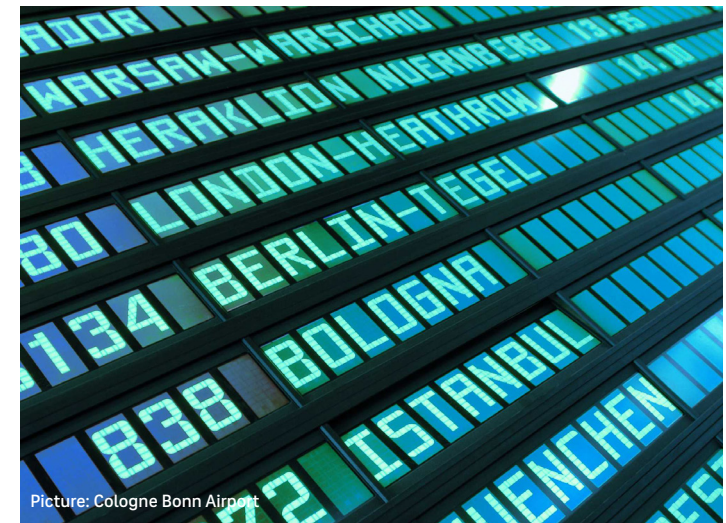
Picture: Cologne Bonn Airport

Scoreboard at Cologne Bonn Airport
The ECOS Trust Management Appliance not only secures the handheld devices, but also the display boards.

ECOS Partner Devoteam
Devoteam is a leading consulting firm specializing in digital strategy, platform technologies, cybersecurity, and business transformation. The implementation of the ECOS PKI at Cologne Bonn Airport was supported and realized by Devoteam.

we connect **IT** | we protect **IT**

ecos

All-in-one PKI solution secures devices at Cologne Bonn Airport

Picture: Cologne Bonn Airport

two or more MAC addresses needed to be registered for each device, and the security level no longer met the requirements.

Airports typically offer a wide variety of devices that extend far beyond the traditional client world: from the handhelds used by the apron traffic staff to get information on their tasks and the aircrafts to be handled, to specific mobile devices of the security employees, through to tablets that are installed in the 'follow-me' vehicles«. This was reason enough for the airport's IT department to look for a better, more global PKI solution for the creation and management of certificates. Besides the support for Windows, Linux and Active Directory authentication, the main focus also lied on automation to reduce maintenance efforts. The goal was to create as automated a process as possible for all types of clients to deliver certificates to devices and automatically renew them as needed.

ECOS TrustManagementAppliance with persuasive proof of concept

After the airport's IT department learned about ECOS Technology's PKI solution, the Trust Management Appliance, a proof of concept was launched at the Cologne Bonn Airport in the beginning of 2018. Wide-ranging clients and device types were provided with certificates as a test,

from Windows clients to printers, phones and Linux servers, through to Raspberries (used in display units), as well as special handhelds with Android and other mobile operating systems.

»The tests performed during the proof of concept were very successful, everything was very easily configurable«, says Salaka. »This led us to discuss whether we should focus on one PKI system, understand it in detail, and use it as an all-in-one solution to secure all devices.«

Today, the airport operates the ECOS Trust Management Appliance (TMA) as VMware-based virtual appliance. Clustering ensures redundancy and reliability. As the airport operates around the clock, seven days a week, the high availability of the solution is crucial. A load balancer sits in front of the Trust Management Appliance to distribute requests. The client, which fetches the certificates from the appliance, was rolled out to the endpoint devices during the weekly software deployment, with no user intervention required. Now, when a device logs in by VPN, the hardware certificate verifies if it's a trustworthy device with an airport certificate. An Online Certificate Status Protocol (OCSP) additionally counter-checks whether the certificate is really currently valid.

Significant time savings in certificate handling

After a time of live operation, the airports PKI experts have recognized the clear benefits of the ECOS TMA, which has led to a significant reduction of maintenance efforts. This concerns both the certificate issuance and the management, as Alexander Händel, Kenan Salaka's colleague at

Datacenter & Shared Services of the Flughafen Köln Bonn GmbH, relates:
»Since the implementation of the ECOS PKI, it is clearly faster and easier to issue certificates. This is particularly evident in special cases with devices that are not in Active Directory. In addition, searching for certificates is much more convenient, for example to check what exactly has been issued or to revoke a certificate. The overall time saving is tremendous, it only takes the quarter of the previous time per operation.« Monthly e-mail reports detail which certificates have recently been added, which have expired, and which have been revoked (withdrawn or temporarily revoked) for a more complete picture. To automatize future processes, the airport plans in the medium-term to set up a self-service portal for IT employees in the application area. Should they need, for example, a certificate for a web server, the portal will provide it automatically for the respective, clearly defined area, which will further relieve the central IT.

Case study profile

Operator
Cologne Bonn Airport

Sector
Airport operator

Challenge
Certificates for devices beyond the Windows world

Solution
Implement the ECOS TrustManagementAppliance for all devices

About Flughafen Köln Bonn GmbH
With more than ten million passengers per year, Cologne Bonn Airport is one of the major airport hubs in Germany. Aside from passenger traffic, the non-stop operating airport also plays a significant role in airfreight traffic.

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

+49 6133 939 200
info@ecos.de

www.ecos.de