secunet

Central PKI: Confidence and Trust at the Border

Successstory: secunet eID PKI Suite enables the German Federal Police to check EAC1- and EAC2-protected ID documents at border control points


B

Indispensible: checking the electronic part of the passport

Due to the increasing demands on the control process, a reliable document verification with PKI as the core of this process is required.

Challenge

The demand for smart documents is growing. The high-tech eID documents such as ePassports or the German ID card (nPA) for example are leading the way in deploying robust technical measures that protect them against unauthorised access. An authorised inspection system (IS) is needed to gain access to the data stored in the eID documents. And because they use highly secure digital certificates, equally robust reading devices are required to access them.

This opens the door for border authorities to benefit from the full potential of electronic documents. For example, it enables them to reliably check each passenger's ePassport in seconds, while all stakeholders can be confident that border controls are truly secure.

Client

Sector:
Government / law enforcement

BUNDESPOLIZEI

Organisation:
The German Federal Police (Bundespolizei) and its approximately 45,000 employees are assigned to the Federal Ministry of the Interior in Berlin. They are acknowledged as a vital part of the country's national security system. Border protection, railway policing and aviation security belong to the Federal Police forces' core tasks.

Facts and Figures

secunet supplied a number of services including:

- the provision of central server infrastructure for ePassport and national ID card verification
- the integration of the new system with the existing server and authentication scheme
- software development and maintenance
- user training
- the provision of the interface to all European member states

Software and technology used:

- Linux (SuSe, CentOS), High availability (PaceMaker)
- Client-server authentication via TLS
- Web services
- Oracle, SQL
- Java, JCE, Groovy Script
- XML, XSLT, XSL-FO
- JavaScript, Ajax, jQuery
- HTML, CSS, Servlet/JSP, Tomcat

PKI ensures efficient and secure document verification when crossing the border

Requirements

The German Federal Police's main responsibilities include securing Germany's borders. Consequently, the Federal Police carries out border checks on passengers at a number of German airports. At the busiest airports, officers are assisted by the automated border control system EasyPASS. Aiming at a modern and – at the same time – highly secure eID check, the German Federal Police looked for a reliable and easy-to-use ID system that is excellent value.

Its approach meant that the IS keys also had to be stored in a hardware security module (HSM). However, because IS certificates are only valid for a short time, general renewal procedures have to comply with the German Federal Office for Information Security's (BSI) TR-03129 technical guideline. Furthermore, a master list containing country signing (CS) certificates and a defect list covering special document signing (DS) certificate issues has to be kept up to date to detect fake eID documents.

The German Federal Police therefore needed a solution that could:

- be integrated into an existing role-based authentication scheme
- meet the needs of the BSI's Country Verifying Certificate Authority (CVCA) policy
- comply with the EU's Extended Access Control (EAC) common certificate policy (BSI TR-03139)

How it works

An authorised inspection system (IS) needs to gain access to the data stored in the eID document. To prove that the IS is authorised it has to use the highly secured inspection system key that belongs to the Terminal Certificate to perform Terminal Authentication (TA). At the German border the corresponding security keys are stored in the hardware security module (HSM), which is an integral part of the Terminal Control Centre (TCC). The TCC performs all necessary key operations on behalf of the IS.

For example, when a German citizen returns from a trip to Japan and arrives at a border control point at Frankfurt Airport his ID document will be checked by a border guard using an IS. The eID document is placed on the IS and the TCC provides it with the necessary authentication data to perform TA.

Passive Authentication (PA) is also performed at every German border control point. This checks the data integrity and authenticity of the eID.

PA consists of two steps:

1. It confirms that the document signer (DS) certificate on the document has been issued by a trusted country signing authority (CSCA). It does this by validating the DS certificate signature against trusted CS certificates on the German master list.

2. The data signature is checked against the now validated DS certificate. To avoid having to provide the master list to each and every inspection system at the German border, the first step of PA is performed by the TCC.

Solution

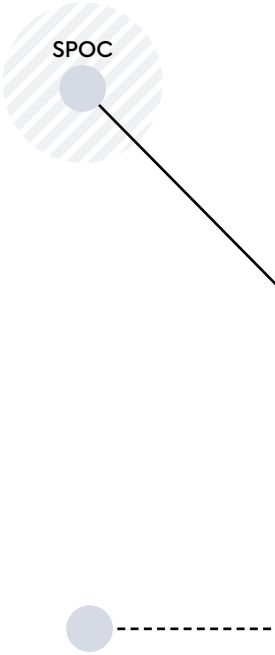
Because secunet had recently implemented the TCC for the BSI, it was well positioned to develop a border control application to read and verify electronic identity documents at the German border. The secunet experts have worked closely with the German Federal Police to develop a precisely fitting solution that provides these functionalities:

- At the heart of secunet's offering is the provision of the Document Verifier Certificate Authorities (DVCA) to generate the digital certificates, which are transmitted to the Terminal Control Centre (TCC). The TCC performs the cryptographic functions and key management for the border control posts and the automated border control system EasyPASS.
- Online communication between the DVCA and CVCA and the DVCA and TCC complies with BSI TR-03129. To guarantee secure communication, a TLS-CA is included.
- The secret key material is stored in an HSM, so in order to enable the HSM to operate with the eID PKI Suite, secunet also had to implement a Java Cryptography Extension (JCE) provider for the Utimaco/R&S CryptoServer Deutschland-HSM/3 CS10/CS50 LAN used in this solution.

Confidence and trust in documents through PKI support the border guards in their daily work

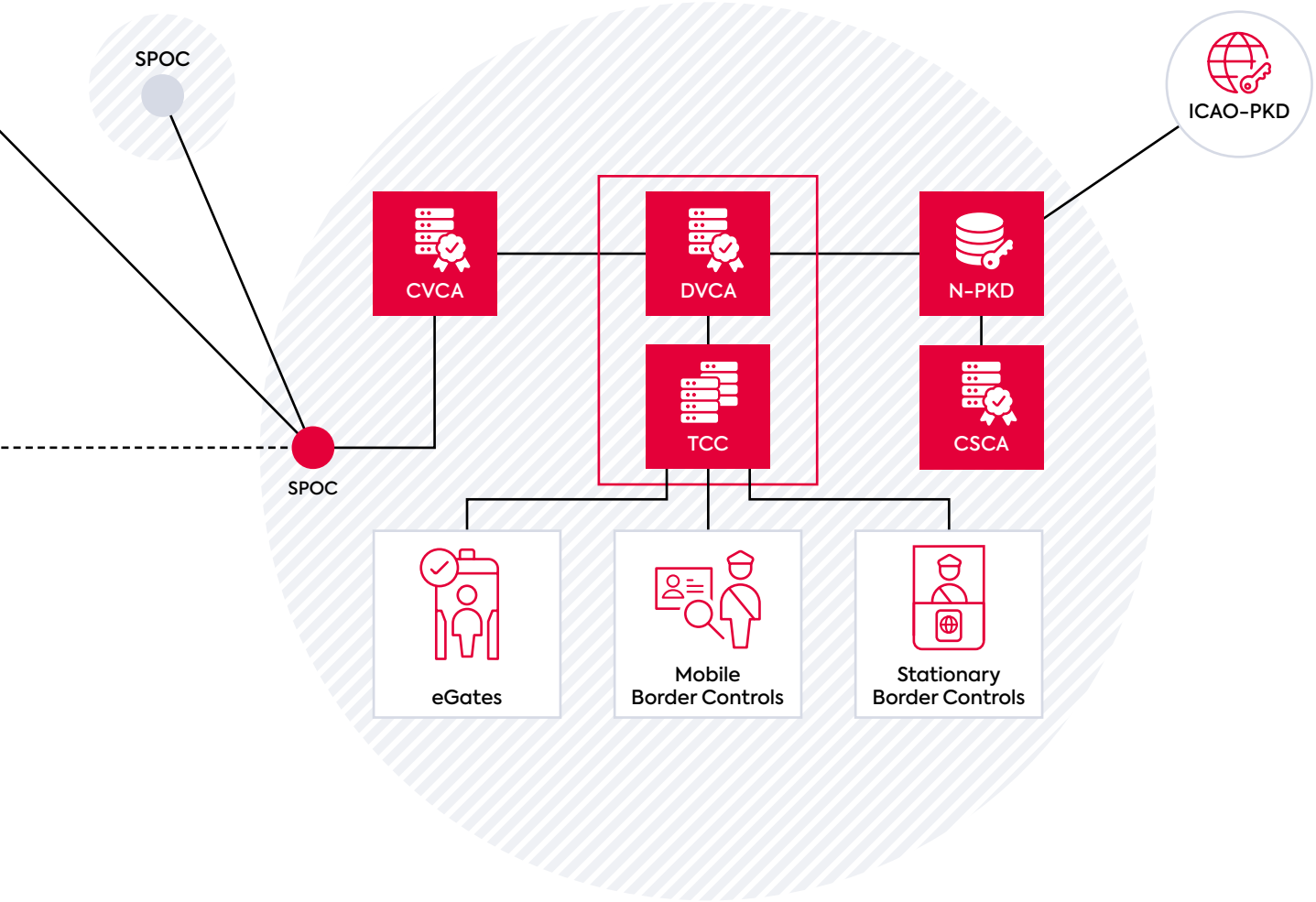
“We have been success-fully operating our central PKI system since 2011. Following a smooth, simple implementation, the entire system has proved itself to be incredibly efficient and reliable on a daily basis.”

Mathias Grell,
EasyPASS Project Manager,
Department 54,
German Federal Police



Implementation

A mission-critical system such as German border control needs to be ultra-reliable and highly secure, so secunet is running it on a clustered Linux platform and integrated the entire system into the client’s existing IT infrastructure. This ensured minimal downtime and maximum security.



Since the implementation of the full central PKI in 2011, secunet has been supporting the Federal Police with software maintenance, helpdesk facilities and user and operator training.

Success

secunet's team of PKI experts ensured that the existing eID document checking system was migrated to the new server infrastructure on time and within budget.

The firm's successful implementation of a PKI solution for the German Federal Police means that border control posts across the country are now connected, ensuring that the EAC-protected data in national eID documents can be captured and checked. Thanks to the centralised solution, all of the 1,300 stations are now provided with fresh certificates.

The solution also complies with complex national and international interfaces to meet the BSI TR-03129 and CSN 369791:2009 standards, assuring stakeholders that this system truly offers the appropriate level of security.

The German authorities can now be confident that only legitimate eID documents are used to cross their borders. The secunet system is already proving its worth by identifying fake and manipulated documents. It also authorises the IS and enables it to access EAC1- and EAC2-protected personal data, while also guaranteeing that only authorised inspection systems can do so.

For both stationary and mobile border control, the PKI works in the background. It builds the backbone for a reliable and secure control of eID documents

System Benefits

- Enables more than one million border crossings quickly, conveniently and securely each year
- Complies with the strictest data protection regulations
- Reliably detects forged and false ID documents
- Requires minimal user interaction
- Supports all types of border control (mobile, stationary, automated)

secunet – protecting digital infrastructures

secunet is Germany's leading cybersecurity company. In an increasingly connected world, the company's combination of products and consulting assures resilient digital infrastructures and the utmost protection for data, applications and digital identities. secunet specialises in areas with unique security requirements – such as cloud, IIoT, eGovernment and eHealth. With security solutions from secunet, companies can maintain the highest security standards in digitisation projects and advance their digital transformation.

Over 1,000 experts strengthen the digital sovereignty of governments, businesses and society. secunet's customers include federal ministries, more than 20 DAX-listed corporations as well as other national and international organisations. The company was established in 1997, is listed in the SDAX and generated revenues of around 337 million euros in 2021.

secunet is an IT security partner to the Federal Republic of Germany and a partner of the German Alliance for Cyber Security.

secunet Security Networks AG
Kurfürstenstraße 58 · 45138 Essen · Germany
T +49 201 5454-0 · F +49 201 5454-1000
info@secunet.com · secunet.com