successstory

Zentrales Nervensystem für hochsichere Grenzkontrollen

Bundespolizei prüft elektronische Identitätsdokumente an deutschen Grenzen mit der secunet eID PKI Suite

secunet

herausforderung

Die zunehmende Verbreitung elektronischer Identitätsdokumente schafft an vielen Stellen Mehrwerte und deutlich effizientere Prozesse. In Verbindung mit modernen Technologien ermöglichen die im Chip elektronisch gespeicherten Daten des Passinhabers die Automatisierung von Prozessen. Gleichzeitig stellen ePass, nPA & Co. aber auch neue Anforderungen an den Identitätsschutz: Zu einer sicheren Identität gehört mit der Speicherung der elektronischen Daten mehr als nur ein fälschungssicheres Ausweisdokument.

Vielmehr ist die Bereitstellung hochsicherer, komplexer ID-Systeme im Hintergrund erforderlich, die einen sicheren Zugriff auf diese Identitätsdokumente ausschließlich durch dafür autorisierte Stellen regeln. Beim jedem Verifikationsprozess muss ein autorisiertes Inspektionssystem (IS), wie es an jedem Grenzkontrollpunkt eingesetzt wird, auf die in den elektronischen Dokumenten gespeicherten Daten zugreifen können. Hierzu bedienen sich Lesegerät und Identitätsdokument entsprechender Zertifikate (Public Key Infrastructure – PKI).

Einmal eingeführt, eröffnen diese ID-Systeme z. B. bei der Grenzkontrolle völlig neue Möglichkeiten.

In einem automatisierten Prozess können Reisepässe auf höchstem Sicherheitsniveau innerhalb von wenigen Sekunden zuverlässig kontrolliert werden. Grenzbeamte werden entlastet, das Potenzial moderner Identitätsdokumente vollumfassend ausgeschöpft.

auftraggeber

Sektor:
Behörden/Polizei

Organisation:
Die Bundespolizei ist mit ihren rund 40.000 Beschäftigten dem Bundesministerium des Innern in Berlin zugeordnet. Innerhalb der Sicherheitsarchitektur des Bundes nimmt die Bundespolizei vielfältige sonderpolizeiliche Aufgaben, insbesondere in den Bereichen Grenzschutz, Bahnpolizei und Luftsicherheit, wahr.

daten & fakten

secunet hat unter anderem die folgenden Dienstleistungen zur Verfügung gestellt:

- Bereitstellung der zentralen Server-infrastruktur für die Überprüfung von elektronischen Reisepässen und Personalausweisen
- Integration des neuen Systems in das vorhandene Server- und Authentifizie-rungsschema
- Softwareentwicklung und -wartung
- Benutzerschulung
- Bereitstellung der Schnittstelle zu allen EU-Mitgliedsstaaten

Verwendete Software und Technologie:

- Linux (SuSe, CentOS), Hochverfüg-barkeit (PaceMaker)
- Client-server authentication via TLS
- Webdienste
- Oracle, SQL
- Java, JCE, groovy Script
- XML, XSLT, XSL-FO
- JavaScript, Ajax, jQuery
- HTML, CSS, Servlet/JSP, Tomcat

anforderung

Zu den Kernaufgaben der deutschen Bundespolizei zählt der grenzpolizeiliche Schutz des Bundesgebietes. An vielen deutschen Flughäfen führt die Bundespolizei dazu grenzpolizeiliche Kontrollen der Flugreisenden durch. Das automatisierte Grenzkontrollsystem EasyPASS unterstützt dabei die eingesetzten Beamten an den passagierstärksten Flughäfen.

Mit dem Ziel, eine moderne wie sichere Prüfung der elektronischen Identitätsdokumente vornehmen zu können, war die Bundespolizei auf der Suche nach einem zuverlässigen, bezahlbaren und gleichsam effizienten ID-System. So lag es auf der Hand, die Ausstattung der 1.300 Inspektionssysteme mit erforderlichen Zertifikaten und Schlüsseln über einen zentralisierten Dienst zu versorgen.

Diesem Ansatz folgend, werden die IS-Schlüssel in einem zentralen Hardwaresicherheitsmodul (HSM) gespeichert.

Aufgrund der kurzen Gültigkeitsdauer der IS-Zertifikate, müssen die automatisierten Erneuerungsverfahren für die Zertifikate entsprechend der technischen Richtlinie TR-03129 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) eingehalten werden.

Darüber hinaus muss eine Master-Liste mit CS-Zertifikaten, sowie eine Defect-Liste mit speziellen, problematischen DS-Zertifikaten permanent aktualisiert werden, damit falsche Ausweisdokumente jederzeit zuverlässig erkannt werden können.

Die optimale Lösung für die Bundespolizei musste Folgendes gewährleisten:

- Integration in ein vorhandenes rollenbasiertes Authentifizierungsschema
- Einhaltung der Anforderungen der CVCA-Richtlinie (Country Verifying Certificate Authority) des BSI
- Einhaltung der EAC-Zertifikatsrichtlinie der EU-Mitgliedsstaaten (BSI TR-03139)

PKI – Multitasker im Grenzkontrollprozess

Bei der automatisierten Grenzkontrolle muss an jedem Grenzkontrollpunkt ein autorisiertes Inspektionssystem auf die im elektronischen Ausweisdokument gespeicherten Daten zugreifen können. Um zu belegen, dass das System über die entsprechende Autorisierung für diesen Zugriff verfügt, muss es eine Terminal-Authentifizierung über den sicher gespeicherten, sogenannten IS-Schlüssel und dem zugehörigen Terminal-Zertifikat durchlaufen. Für die deutsche Grenze werden die entsprechenden Sicherheitsschlüssel in einem Hardwaresicherheitsmodul gespeichert, das eine wesentliche Komponente des Terminal Control Center ist. Das Terminal Control Center führt wiederum alle erforderlichen Schlüsselvorgänge für das Inspektionssystem durch.

Ein Beispiel: Ein deutscher Staatsbürger kehrt von seiner Reise nach Japan zurück und landet am Frankfurter Flughafen, wo sein nPA am Grenzkontrollpunkt durch einen Grenzbeamten geprüft wird. Dieser benutzt dazu das Inspektionssystem, auf das er den elektronischen Reisepass legt. Das Terminal Control Center stellt – im Hintergrund – die erforderlichen Authentifizierungsdaten für die Terminal-Authentifizierung bereit.

Zudem erfolgt an jedem deutschen Grenzkontrollpunkt eine „passive Authentifizierung“, mit der die Datenintegrität und die Authentizität des elektronischen Ausweisdokuments sichergestellt werden. Diese passive Authentifizierung umfasst zwei Schritte:

1. Zunächst wird bestätigt, dass das Document Signer (DS)-Zertifikat im Ausweisdokument von einer vertrauenswürdigen Country Signing Authority (CSCA) ausgestellt wurde. Dafür wird die DS-Zertifikatsignatur mit vertrauenswürdigen CS-Zertifikaten auf der deutschen Master-Liste verglichen.

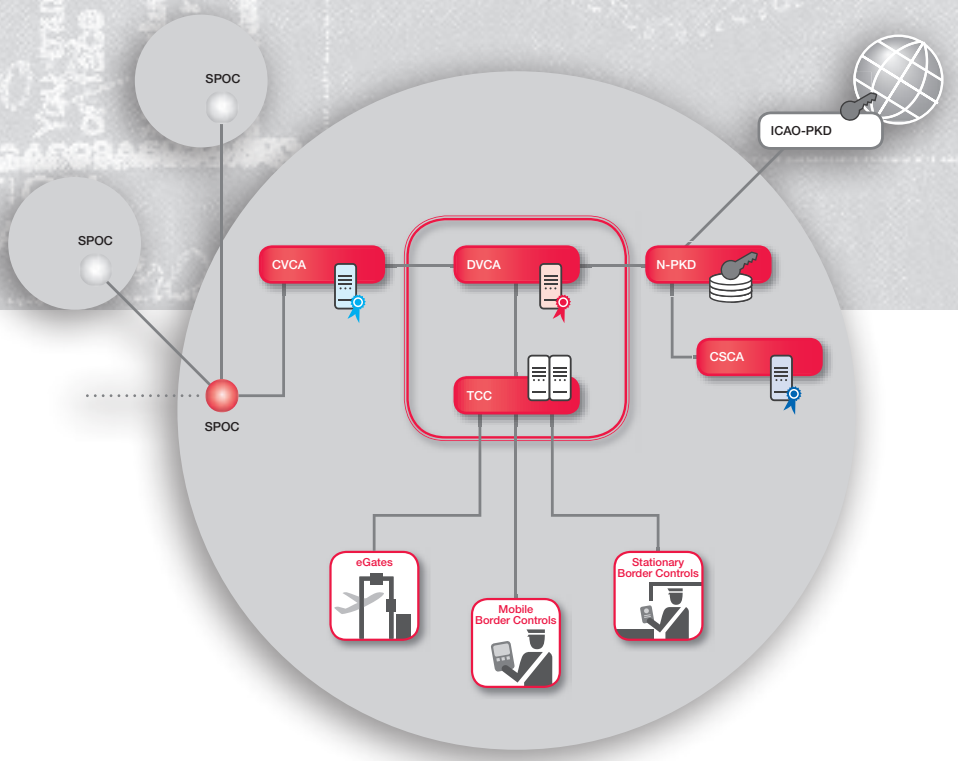
2. Die Datensignatur wird mit dem (jetzt validierten) DS-Zertifikat verglichen. Um zu verhindern, dass jedem einzelnen Inspektionssystem an der deutschen Grenze die Master-Liste bereitgestellt werden muss, wird der erste Schritt der passiven Authentifizierung am Terminal Control Center durchgeführt.

> *Wir haben das zentrale PKI-System seit 2011 erfolgreich im Einsatz. Nach der reibungslosen Implementierung hat sich die eID PKI Suite im laufenden Betrieb als äußerst zuverlässig und stabil erwiesen. Systemausfälle könnten wir uns bei der hoheitlichen Aufgabe der Grenzkontrolle auch gar nicht leisten.*
>
> Mathias Grell, Projektleiter EasyPASS, Referat 54, Bundespolizei

lösung

Durch die Implementierung des Terminal Control Center für das BSI waren die secunet Experten bestens mit den besonderen Anforderungen vertraut und für die Entwicklung der Grenzkontrollanwendung optimal gerüstet. In enger Zusammenarbeit mit der Bundespolizei entwickelten sie die passgenaue PKI-Lösung, die sämtliche spezifische Anforderungen berücksichtigt und folgende Funktionalitäten bereitstellt:

- Document Verifier Certificate Authorities (DVCA) für die Generierung der digitalen Zertifikate, die zum Terminal Control Center (TCC) übertragen werden – das TCC führt die kryptografischen Funktionen sowie die Schlüsselverwaltung für die Grenzkontrollposten und das automatisierte Grenzkontrollverfahren EasyPASS durch.
- Eine zur BSI TR-03129 konforme Onlinekommunikation zwischen der DVCA und der CVCA sowie zwischen der DVCA und dem TCC – die enthaltene TLS-CA gewährleistet die sichere Kommunikation.
- Privates Schlüsselmaterial, hochsicher gespeichert in einem HSM – für die Verwendung mit der eID PKI Suite wurde ein Java Cryptography Extension (JCE)-Modul für das in dieser Lösung eingesetzte Utimaco/R&S CryptoServer Deutschland-HSM/3 CS10/CS50-LAN implementiert.



implementierung

Ein einsatzkritisches hoheitliches System, und dazu zählt die deutsche Grenzkontrolle, muss jederzeit äußerst zuverlässig und hochsicher funktionieren. Dem entsprechend haben die secunet Experten eine Linux-Clusterplattform als Basis für die zentrale PKI-Lösung ausgewählt und diese in die vorhandene IT-Infrastruktur des Kunden integriert.

Hierdurch konnten Ausfallzeiten minimiert und die maximale Sicherheit gewährleistet werden.

Seit der Implementierung der zentralen PKI-Komponenten in 2011, unterstützt secunet die Bundespolizei fortwährend mit Softwarewartungen, Helpdesk-Funktionen sowie Benutzer- und Bedienerschulungen.

erfolg

Die secunet PKI-Experten haben das vorhandene Prüfsystem für elektronische Ausweisdokumente termingerecht und innerhalb des vorgesehenen Budgets zur neuen Serverinfrastruktur migriert. Die hohen Sicherheitsanforderungen der Bundespolizei werden durch die Konformität zu komplexen nationalen und internationalen Schnittstellen in vollem Umfang erfüllt.

Die zentrale PKI-Lösung sorgt dafür, dass die Grenzkontrollpunkte der Bundespolizei jetzt bundesweit miteinander verbunden sind. So ist sichergestellt, dass EAC-geschützte Daten in den nationalen elektronischen Identitätsdokumenten erfasst und in den Dokumenten der Schengen-Nationen geprüft werden können.

Dank der zentralisierten Lösung sind alle 1.300 Grenzkontroll-Clients stets mit aktuellen Zertifikaten ausgestattet und können somit auf die EAC- und SAC-geschützten Daten zugreifen. Gleichzeitig ist sichergestellt, dass nur autorisierte Inspektionssysteme diesen Zugriff auf die persönlichen Identitätsdaten erhalten.

vorteile

- Mehr als eine Millionen schnelle, komfortable und gleichzeitig hochsichere Grenzkontrollen pro Jahr
- Berücksichtigung strengster Datenschutzbestimmungen
- Gefälschte oder manipulierte Identitätsdokumente werden zuverlässig erkannt
- Minimale Benutzerinteraktion erforderlich
- Unterstützt manuelle wie auch automatisierte Grenzkontrollpunkte (eGates)

secunet Security Networks AG

secunet, seit 2004 Sicherheitspartner der Bundesrepublik Deutschland, ist einer der führenden Anbieter anspruchsvoller IT-Sicherheit. Im engen Dialog mit seinen nationalen und internationalen Kunden aus Privatwirtschaft sowie öffentlichen Institutionen entwickelt secunet leistungsfähige Produkte und fortschrittliche IT-Sicherheitslösungen. Damit schützt secunet nicht nur die IT-Prozesse und -Systeme seiner Kunden, sondern erzielt intelligente Prozessoptimierungen und schafft nachhaltige Mehrwerte.

Bei secunet konzentrieren sich mehr als 380 Experten auf Themen wie Kryptographie (SINA), E-Government, Kritische Infrastrukturen sowie Business- und Automotive-Security – mit dem Anspruch, in Qualität und Technik immer einen Schritt voraus zu sein. Unser Ziel ist der effiziente und effektive Schutz der Daten und IT-Infrastrukturen bis hin zur Absicherung des geistigen Eigentums und der Reputation unserer Kunden.

secunet Security Networks AG
Kurfürstenstraße 58
45138 Essen
Tel.: +49-201-5454-0
Fax: +49-201-5454-1000
E-Mail: info@secunet.com
www.secunet.com

04/2016