Certs on Rails

Studiengang: MAS Cyber Security

Weiterentwicklung Public-Key-Infrastruktur für Rollmaterial der Schweizerischen Bundesbahnen. Eine Reise in die Cloud zur automatisierten Public-Key-Infrastruktur für Maschinenzertifikate.

Matthias Ong

Umfeld

Die Digitalisierung hält auch in der Bahnwelt Einzug. Als erstes mag einem wohl die allseits bekannten Mobile Applikationen in den Sinn kommen. Bei keiner Pendlerin oder Pendler sind sie heute noch wegzudenken. Immer dabei zeigen sie den aktuellen Fahrplan, bieten eine bequeme Möglichkeit Billette zu lösen und vieles mehr. Doch die Rede ist nicht von den Mobile Applikationen, sondern von den Applikationen im Fahrzeug (APFZ). Die APFZ setzen sich aus Soft- und Hardwarekomponenten zusammen, die direkt im Zug verbaut sind und mit den zentralen Systemen landseitig über die Luft kommunizieren. Sie bestehen aus dem Kundeninformationssystem (aktustisch und visuell), der Videoüberwachung, der automatischen Fahrgastzählung, den Notsprechstellen, der elektronischen Sitzplatzreservation und der Belegungsanzeige. Sie alle tragen zur Erhöhung des Fahrkomforts bei. Sie geben unseren Fahrgästen Sicherheit und Informationen zur Fahrt.

Mit der zunehmenden Digitalisierung eröffnen sich ganz neue Möglichkeiten als auch Herausforderungen. Dieses Projekt setzt sich konkret mit dem Vertrauen in computergestützten Netzwerken in den Zügen zwischen seinen genannten Netzwerkteilnehmern auseinander. Dieses Vertrauen beruht auf digitalen Zertifikaten. Sie sind nichts anderes als digitale Ausweise für Maschinen. Sie dienen zur Authentisierung/Identifizierung an Diensten und Verifizierung von übertragenen Inhalten. Konkretes Beispiel: Alle Displays in den Zügen der Schweizerischen Bundesbahnen, welche die Fahrgäste über Zwischenhalte und Endbahnhof informieren, überprüfen die Vertrauenswürdigkeit der übertragenden Inhalte aufgrund des unterbreitenden Zertifikats.

Problemstellung

Digitale Zertifikate werden von einer zentralen Public-Key-Infrastruktur (PKI) ausgestellt und während seiner Gültigkeit auch von ihr betreut. Die bestehende PKI Architektur wird ihren aktuellen als auch künftigen Anforderungen nicht mehr gerecht. Die stark fortschreitende Modernisierung unserer Flotte und deren Anzahl an Zügen verlangt nach einer äusserts verfügbaren und skalierbaren PKI. Da es sich nicht um klassische IT handelt, sondern um ein stark von Industrieautomation geprägten Umfeld muss die PKI äusserst flexibel, modular und robust sein.

Lösungsansatz

Die bereits im Einsatz befindliche PKI Software hat sich bis anhin als sehr zuverlässig erwiesen und erfüllt die beschriebenen Anforderungen. Doch die Infrastruktur wurde an künftige Herausforderungen angepasst. Mit dem Re-Design erhalten die Schweizerischen Bundesbahnen eine hochverfügbare und skalierbare PKI für industrielle Applikationen im Zug. Erreicht wird dies durch Open Source Software und den Vorteilen der Cloud. Des Weiteren wurden Prozesse angepasst, die zu mehr Vertraulichkeit bei der initialen Ausstellung der digitalen Zertifikate führen. Durch Anwendung modernster Automatisierungswerkzeuge ist es innert kürzester Zeit nun möglich eine komplett neue PKI bereitzustellen.

Schlussbetrachtung

Die APFZ PKI ist nun bereit in Zukunft Zertifikate für weit über 100'000 national verteilte Endgeräte auszustellen und zu managen. Ohne eine robuste PKI Software, Beihilfe von Automatisierung, skalierbarer und flexibler Infrastruktur undenkbar. Es stellte sich deutlich heraus, dass die Cloud allein kein Garant für Hochverfügbarkeit ist. Sie wird nur in Zusammenarbeit mit Cloud Provider und dem Kunden erreicht. Mit der Ausstellung des ersten Zertifikats für ein Endgerät beginnt eine Reise bis zur dessen ordentlichen Ausserbetriebnahme. Daher nehmen Prozesse beim Design und Betrieb einer PKI eine wesentliche Stellung ein.