

Sichere Handytickets und schnelle Kontrollen

Einführung des VDV-Barcodes im hvv

Daniel Ackers, Kerstin Dämon, Köln; Sebastian Heyna, Bad Oldesloe; Alain Leffin, Aachen; Martin Pfefferkorn, Hamburg

Die Nachfrage nach elektronischen Ticket-Angeboten steigt stetig. Um diese zu befriedigen, brauchen Verkehrsunternehmen und -verbünde skalierbare Sicherheitslösungen. Die Hamburger Hochbahn hat allein im Geschäftsjahr 2019 rund acht Millionen elektronische Fahrberechtigungen ausgegeben. Durch die Apps der Verkehrsunternehmen haben Fahrgäste auch während der Fahrt Zugriff auf diesen Vertriebskanal. Das erhöht das Betrugsrisiko. Fahrgäste können sich ihr Ticket in dem Moment kaufen, in dem das Kontrollteam in das Fahrzeug steigt. Außerdem können digitale Tickets leicht manipuliert oder vervielfältigt werden. Ein maßgeblicher Erfolgsfaktor bei digitalen Tickets ist daher ihre Sicherheit.

Die Sicherheit darf wiederum nicht zu Lasten der Performanz gehen, um Kontrollen nicht unnötig zu verkomplizieren und den Kaufprozess nicht zu verlangsamen. Wird ein kryptografisch abgesichertes Ticket gekauft oder kontrolliert, fließen viele hochkomplexe Daten zwischen Smartphone des Fahrgastes, Hintergrundsystem des Verkehrsunternehmens und Kontrollgerät des Servicepersonals hin und her. Das muss auch dann möglichst schnell geschehen, wenn beispielsweise wegen einer Großveranstaltung ungewöhnlich viele Menschen mit ihrem Smartphone Tickets kaufen oder kontrolliert werden. Deshalb müssen Performanz und Zuverlässigkeit der Sicherheitskomponenten immer der Last im Gesamtsystem entsprechen.

Der hvv und die Hamburger Hochbahn als dessen größter Partner, haben eine technische Lösung für diese Herausforderungen beim elektronischen Ticketing gesucht und gefunden: den von Worldline entwickelten SAM-Server in Verbindung mit dem VDV-Barcode zur Absicherung von Han-

dytickets. 2019 hat man sich zur Zusammenarbeit mit Worldline entschieden, 2021 wurde der VDV-Barcode eingeführt.

Einheitliche Lösungen für alle Vertriebskanäle

Weil Fahrgäste im hvv auf vielen verschiedenen Wegen Tickets kaufen können, gab es auch verschiedene technische Systeme hinter den Vertriebskanälen. Damit sollte Schluss sein. Gesucht wurde ein einheitlicher Standard, der wirtschaftlich, nachhaltig und skalierbar ist.

Bei rund acht Millionen statischen Berechtigungen, die bei der Hamburger Hochbahn allein im Geschäftsjahr 2019 ausgegeben wurden, musste die Durchlaufzeit für die Erzeugung und Produktion der Berechtigung bei unter 500 ms liegen. Selbst bei Großveranstaltungen wie dem Hamburg Marathon oder dem Hafengeburtstag, bei denen es zu deutlich mehr Anfragen im System kommt. Auch relevant: wie die elektronischen Fahrkarten codiert werden. Bisher hatten unterschiedliche Systeme die Tarifdaten importiert und entsprechend für die jeweiligen Zwecke aufbereitet. Im Rahmen der IT-Strategie der Hamburger Hochbahn sollte es hier ebenfalls eine Harmonisierung geben, um den Wartungs- und Pflegeaufwand zu

reduzieren. Daher musste ein zentraler Tarifserver bereitgestellt werden. Um auch hier Synergieeffekte zu nutzen, sollte es ein zentraler Tarifserver aus dem Kontext des Vertriebs von SPNV-Fahrkarten sein.

Nach einer Marktanalyse stand fest: Die Projektverantwortlichen bei der Hamburger Hochbahn mussten sich zwischen einem SAM-Cluster und einem SAM-Server entscheiden. Bei einem SAM-Cluster werden physische SAM in einer Ticket-Engine gleichzeitig betrieben, um diese an einer zentralen Stelle anzusprechen. Bei dem SAM-Server wird ein sogenanntes virtuelles SAM (vSAM) genutzt, bei dem der Schlüssel nicht mehr physisch eingebracht werden muss.

Eine rein wirtschaftliche Betrachtung bei einem Einsatz von circa 40 physischen SAM im Kontext der Anforderungen der Hochbahn ergab durchaus Vorteile. Die Aspekte der Antwortzeiten und die Strategie, möglichst viele Fahrscheine über die digitalen Vertriebskanäle App und Website zu verkaufen, hat schließlich den Ausschlag für den SAM-Server gegeben. Diese Lösung erschien nachhaltiger, langlebiger und hatte damit vor allem eine bessere Perspektive. Darüber hinaus ist der Wartungsaufwand deutlich geringer, da kein Handling

SAMs zur Authentifizierung von Nutzermedien und Terminals

Die marktgängigen eTicket-Systeme stützen sich auf ISO 14443-konforme kontaktlose Chipkarten. Passend zu diesen Chipkarten bietet die Halbleiterindustrie sogenannte SAM-Module an, die sich kontaktgebunden in ein entsprechendes ÖPNV-Kartenterminal einsetzen lassen. Ein SAM (Secure Application Modul) hat das Format einer Mobilfunk-SIM-Karte und wird unter anderem in Fahrkartenterminals und Kontrollgeräte eingebaut. Bei einer Kontrolle entschlüsselt, liest und kontrolliert das SAM das Ticket auf dem Nutzermedium (zum Beispiel Chipkarte oder Smartphone). Seine wesentliche Funktion ist die Authentifikation von Nutzermedium und Terminal, die bei einer Kontrolle miteinander kommunizieren.

mit physischen SAM notwendig ist. Weitere Vorteile sind die deutlich schnelleren Zeiten für die Signaturbildung sowie die Skalierbarkeit des Systems. Mit der Entscheidung für den SAM-Server ist die Hamburger Hochbahn, neben der Düsseldorfer Rheinbahn, das zweite Verkehrsunternehmen in Deutschland, das einen eigenen SAM-Server betreibt. Weitere SAM-Server befinden sich zurzeit in Abnahmetests. Seit 2021 ist der SAM-Server bei den Hamburgern im Einsatz und übernimmt den Großteil aller kryptographischen Operationen im hvv. Hierzu gehört vor allem das Signieren der statischen Berechtigung für Print- und Handyticket, Kombitickets für Messen, Theater oder sonstige Veranstaltungen. Zusätzlich wurde der SAM-Server mandantenfähig umgesetzt. Dadurch können mehrere Verkehrsunternehmen einen SAM-Server simultan nutzen.

Neben den beiden in Hamburg verwendeten Funktionen sind auch zusätzlich folgende Aktionen mit dem SAM-Server möglich:

- MAC-Prüfung: Absicherung der Partner-Kommunikation,
- Nutzermedium (NM)-Personalisierung: Einzel-, Batch- und Massenpersonalisierung,
- Ausgabe der Berechtigung auf NM: Automaten, Kundencenter, Großkunde, Zuhause,
- Ausführung von KA-Aktionslisten: Automaten.

Umstellung von UIC auf VDV-KA

Mit der Einführung des SAM-Servers stellte die Hochbahn zusammen mit dem hvv auf den VDV-Barcode um und löste damit das bestehende UIC-Barcode-Format (Standard des Internationalen Eisenbahnverbands) ab. Beide Standards basieren technologisch auf der Darstellung als Aztec-Code und unterscheiden sich vor allem in der Codierung. Für den VDV-Barcode sprach vor allem die vollständige elektronische Kontrolle und dass es sich um einen deutschlandweiten Standard handelt, der damit eine nachhaltigere Lösung darstellt, um weiterhin individuelle Ansätze für unterschiedliche Vertriebskanäle zu finden.

Durch die Einführung des VDV-Barcodes im hvv konnte die erste von drei Sicherheitsstufen für Smartphone-Tickets vollständig umgesetzt werden. Das verbesserte die Sicherheit signifikant.



Zum Autor

Daniel Ackers (44) ist seit 2014 Pressesprecher beim VDV eTicket Service. Zusätzlich ist er für die Entwicklung strategischer Themen verantwortlich.



Zur Autorin

Kerstin Dämon (35) ist seit 2021 beim VDV eTicket Service als Referentin Online-Redaktion für die digitale Kommunikation zuständig.



Zum Autor

Sebastian Heyna (39) hat sich seit zehn Jahren in verschiedenen Rollen und Unternehmen der Digitalisierung von Vertriebssystemen in der Mobilitätsbranche verschrieben.



Zum Autor

Alain Leffin (61) ist Produkt- und Servicemanager bei Worldline, seit mehr als zehn Jahren mit dem Schwerpunkt Security-Lösungen für elektronisches Ticketing.



Zum Autor

Martin Pfefferkorn (40) arbeitet seit 2002 bei der Hamburger Hochbahn AG. Seit 2017 verantwortet er als Projektleiter verschiedene Projekte im Bereich Vertrieb und Verkehrswirtschaft.

Sicherheit und Performanz durch SAM-Server und VDV-KA

Durch die Einführung des KA-Standards profitiert der hvv von der Interoperabilität zwischen unterschiedlichen Ticketing-Systemen. Und seitdem der SAM-Server bei der Hamburger Hochbahn im Einsatz ist, sind die Ticketing-Geschäftsprozesse im hvv wei-

testgehend digitalisiert. Das bringt spürbare Vorteile für Verkehrsunternehmen, deren Mitarbeitende und die Fahrgäste.

Bei den Tickets, die jetzt via Onlineshop oder App gekauft werden, ist zum ersten Mal eine vollständige elektronische Prüfung möglich. Das erleichtert den Kontrollteams die Arbeit, weil sie die räumliche

WORDLINE SAM-SERVER: AUFBAU & EINBINDUNG

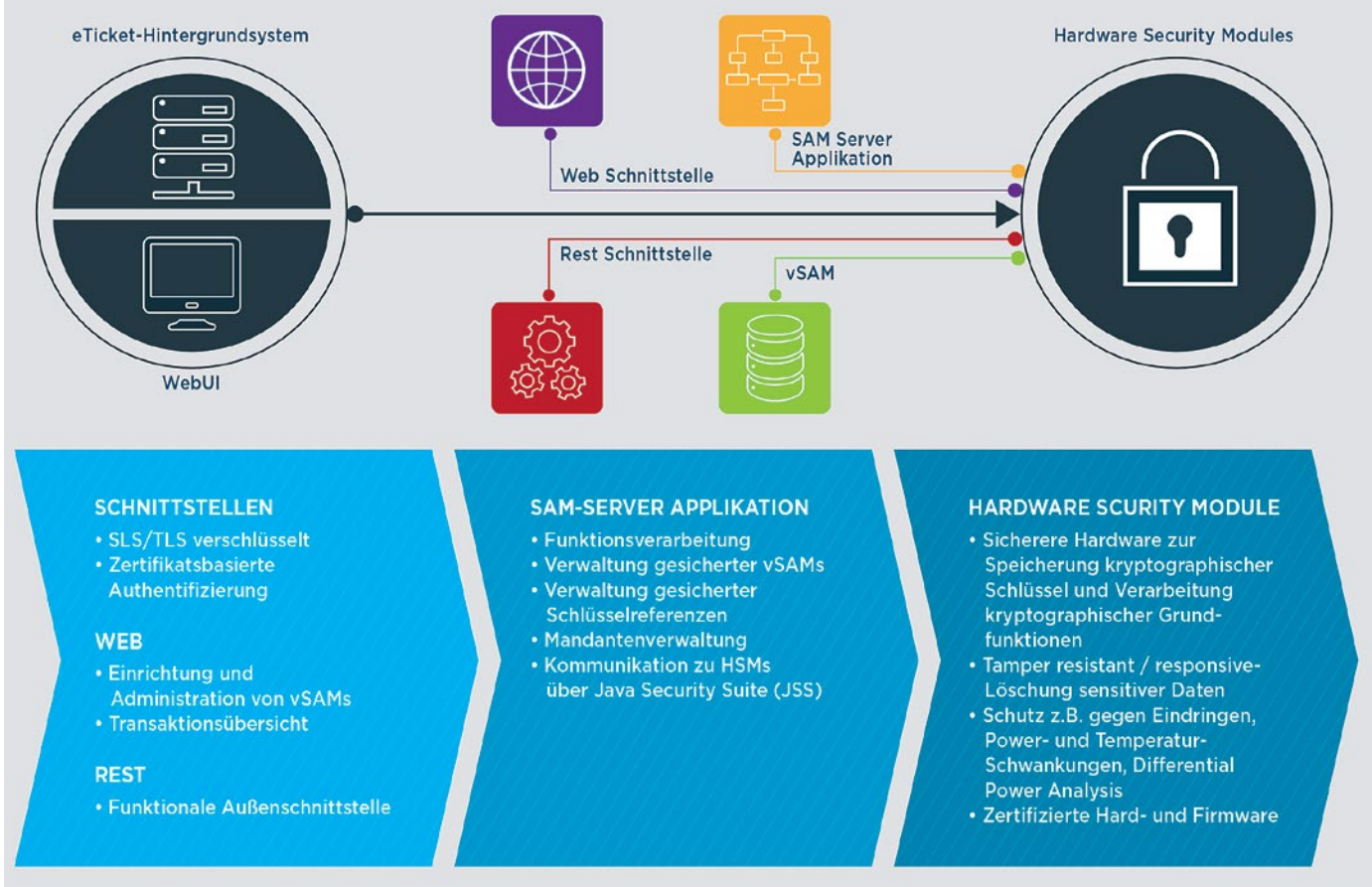


Abb. 1: Der von Worldline entwickelte SAM-Server nutzt als Fundament sogenannte HSM (Hardware Security Module). Dies sind hochleistungsfähige und hochsichere Kryptographie-Rechner, die in der Absicherung des elektronischen Zahlungsverkehrs ihren Ursprung haben. Um den Einsatz in eTicket-Systemen SAM-kompatibel zu ermöglichen, entwickelte Worldline eine VDV-KA-konforme und zugelassene Sicherheitssoftware, die sich durch folgende Eigenschaften auszeichnet:

- Skalierbarkeit und Redundanz bis hin zur Hochverfügbarkeit,
- Lastverteilung und Erweiterbarkeit bei wachsendem Bedarf,
- digitaler Workflow, durchgängig digitales Schlüsselmanagement und Provisioning,
- Unterstützung flexibler Applikationsentwicklung.

Grafik: Yvonne Tamme

Sicherheitsstufen für Tickets auf dem Smartphone

Sicherheitsstufe 1

- VDV-einheitliches Ticketlayout,
- Lichtbildeinführung,
- dynamische Effekte, die einen Nachbau der App erschweren sollen.

Sicherheitsstufe 2

- anspruchsvolle dynamische Elemente mit der Übertragungsmöglichkeit auf elektronische Prüfgeräte,
- Selbstüberprüfung der App bei Manipulationen.

Sicherheitsstufe 3

- Fahrkartenbindung an ein festgelegtes Endgerät („Client-Id“ als Barcode Mobile + und Motics in Umsetzung),
- Onlineprüfung des Barcodes mit dem Hintergrundsystem,
- Meldung von Manipulationsversuchen der App.

und zeitliche Gültigkeit der Tickets nicht mehr selbst überprüfen müssen. Dadurch werden Fahrkartenkontrollen schneller und effizienter.

Die gestiegene Performanz der Hardware erlaubt die Ausgabe zahlreicher statischer Berechtigungen innerhalb kürzester Zeit, weshalb die Erstellung von Kombitickets für Veranstaltungen wie Fußballspiele, Konzerte oder Messen möglich ist. Die Barcodes für ein ÖPNV-Ticket können als Batch an die jeweiligen Veranstaltungspartner ausgegeben werden, die diese wiederum auf ihre Tickets drucken beziehungsweise per App ausgeben können. Letztlich sorgt der SAM-Server auch für eine bessere Absicherung der elektronischen Ticketarten. Damit wird die Tür für höherpreisige

Zeitkarten als Ticket auf dem Smartphone ein wenig weiter geöffnet.

Aktuell sorgt der VDV-Barcode dafür, dass Handytickets fälschungssicher sind. Mit dem Motics („Barcode Mobile+“) des VDV eTicket Service erhalten sie auch einen Kopierschutz: Im Hintergrundsystem wird ein Ticket generiert, das mit einer eindeutigen ID des anfordernden Smartphones versehen ist. Im zweiten Schritt wird die-

se statische Berechtigung dann bei erfolgreicher Kontrolle mit einem dynamischen Element versehen und als Aztec-Barcode ausgegeben. Hierdurch ist ein Kopieren des Barcodes zwecklos. Dann können auch Jahreskarten, Jobtickets und andere höherpreisige Tarifprodukte guten Gewissens via App ausgegeben werden. Entsprechend sind die Motics-Kompatibilität und Unterstützung von „VDV-Barcode Mobile+“ bei statischen Berechtigungen

bereits als Funktionen im SAM-Server umgesetzt. Genau wie die Ausgabe von Multi-Berechtigungen (Performancesteigerung durch optimiertes Schlüsselhandling), die Ticketkontrolle (bei Fahrzeugen mit Internetverbindung) sowie ein Plug-In für SAM-PE (Vereinfachung der Integration) stehen zur Verfügung. Damit das elektronische Ticketing für Fahrgäste und Verkehrsunternehmen in Zukunft einfach und sicher ist.

Zusammenfassung/Summary

Sichere Handytickets und schnelle Kontrollen

Im Hamburger ÖPNV stehen die Weichen seit November 2021 auf Hochgeschwindigkeit: Ein SAM-Server bei der Hamburger Hochbahn sorgt dafür, dass Fahrgäste, die mobile Tickets erwerben, diese blitzschnell auf ihrem Smartphone haben. Selbst wenn die Mobilfunknetze wegen Großveranstaltungen ausgelastet sind.

Secure mobile tickets and fast controls

Since November 2021 Hamburg's public transportation system has been set on high speed: A SAM server at Hamburger Hochbahn ensures that passengers who purchase tickets on the move have them on their smartphones at lightning speed. Even when the mobile networks are busy because of major events.

ANZEIGE

Jetzt würz' kundenorientiert:
Vertriebsstrategie schärfen, Stammkunden gewinnen

HanseCom
Ein Unternehmen der INIT Gruppe

Wie kann der ÖPNV heute noch Stammkunden gewinnen?

Antworten geben Mobilitätsexperten in **kostenlosen Webinaren:**

➤ Kunden erreichen: Mobilitätsapp als digitaler Kundenkontaktpunkt

15. November, 14 Uhr & 22. November, 11 Uhr

ÖPNV-Experte Frank Niggemeier-Oliva, Geschäftsführer der Bahnen der Stadt Monheim, berichtet über eine App, die ihre Nutzer mit besonders wenigen Klicks zu mobilen Tickets führt.

➤ Kunden (mehr) Auswahl bieten: Mobilitäts- und Freizeitangebote zu neuen Produkten kombinieren

6. Dezember, 10 Uhr

Mobilitätsexperte Markus Pellmann-Janssen, Head of Sales bei ioki beleuchtet, welche Rolle die Integration von On-Demand-Verkehren für die Abdeckung der „letzten Meile“ spielen kann.



Weitere Themen & Termine: www.hansecom.com/stammkunden-gewinnen