



Systemkonzept Sicherheit im eTicketing

Den kontiki Themenschwerpunkten für 2007 folgend, stand die 29. kontiki Konferenz vom 14.-15. Juni 2007 in Erfurt im Zeichen des Systemkonzepts Sicherheit. 90 Teilnehmer aus sechs Ländern waren nach Erfurt gekommen, um sich mit den unterschiedlichen Aspekten der Sicherheit von eTicketing-Systemen und ihrer Realisierung als VDV-Kernapplikation auseinanderzusetzen.

In seiner Begrüßung spannte Dr. Ritschel den Bogen von der Technik über die Dienstleistung bis hin zu den Anforderungen an Hintergrundsysteme, die sowohl die Rolle als integrierender Faktor von eTicketing-Systemen zu übernehmen haben als auch deren zentrale Stütze sind.

Dipl.-Ing. Volker Krebs von der Erfurter Verkehrsbetriebe AG begrüßte die Teilnehmer der Konferenz mit einer kurzen, eindrucksvollen Darstellung von 124 Jahren ÖPNV in Erfurt, der mit der Pferdebahn begann, den Interzonenomnibusverkehr in der Zeit nach dem zweiten Weltkrieg unterstützte und heute, aufgrund einer klugen Entscheidung zur Erhaltung der Straßenbahn 1974, einen Schnellbahnverkehr in und um Erfurt herum gewährleistet. Mit einem hohen Anteil am gesamten Personenverkehr und einer innerstädtischen Reisegeschwindigkeit, die dem Individualverkehr nicht nachsteht, ist das moderne Erfurter Verkehrswesen auf die geplante Einführung des eTicketing bestens vorbereitet.

Dr. Annette G. Kersten, T-Systems GEI, Darmstadt, stellte in ihrem Vortrag zum Systemkonzept des Sicherheits- und Schlüsselmanagements der VDV-Kernapplikation neben den Grundprinzipien und Komponenten auch die Systemumgebung in einer verblüffend eingängigen und verständlichen Weise vor. An Beispielen aus verschiedenen Kartenanwendungsbereichen stellte sie den notwendigen Schutz aller Produktions- und Geschäftsprozesse der Anwendungen zur Verhinderung von Betrug und zur Einnahmesicherung dar. Am VDV-Kernapplikations-Konzept zeigte sie, wie das Konzept der kryptografischen Sicherung von der Erzeugung über die Verteilung, Speicherung bis zur Verwendung der Daten alle Bereiche gleichwertig schützt. Es beruht auf den drei Säulen Public Key Infrastructure [PKI], dem Schlüsselmanagement [KM] und den Secure Application Modules [SAM].



Von grundsätzlicher Bedeutung ist im Sicherheitskonzept ein Trustcenter, das gemäß dem Signaturgesetz akkreditiert sein muss. Es sichert mit Public Keys die Infrastruktur der gesamten Anwendung. Mit der zweiten Säule, dem Key Management, werden Komponenten, Rollen und Daten in der Anwendung gesichert. Das SAM ist am einfachsten als die zur SIM-Karte des Mobiltelefons analoge Sicherungsmethode zu verstehen.

Das Zusammenspiel der drei Säulen in dem insgesamt sehr komplexen Sicherheitssystem ist charakterisiert durch die Merkmale

- Modularer Aufbau
- Definierte Schnittstellen zwischen den Säulen
- Offenlegung der Schnittstellen zwischen den Säulen wie auch der externen Schnittstellen der Säulen
- Das Sicherheitsmanagement muss nicht zwingend von einem Dienstleister betrieben werden.

Das Konzept ist um ein weiteres Element für das Trustcenter ergänzt: die Sicherheit der Betriebsumgebung.

Das Dienstleistungsangebot der VDV-Kernapplikations GmbH, Köln, stellten Dr. Till Ackermann und Dr. Josef Lutgen vor. Auf der Grundlage von einem geprüften Datenstandard, einer gemeinsamen Kundenschnittstelle und einem integrierten Sicherheitskonzept ist die VDV-KA GmbH in der Lage, ihre Dienstleistungen mit einem umfassenden Sicherheitspaket anzubieten, das etwa 20 Komponenten von der technischen und organisatorischen Applikationssicherheit bis zur Verschlüsselungssicherheit umfasst. Damit werden die Risiken für den Betrieb eines dem KA-Standard entsprechenden eTicketing-Systems auf ein Minimum reduziert. Die Dienstleistungen der VDV-KA GmbH werden durch ein Standardwerk von Verträgen geregelt. Damit ist für alle Partner der GmbH eine Dienstleistung von gleichem Qualitätsstandard sichergestellt.

Im zweiten Teil des Vortrages erläuterte Dr. Lutgen die Struktur der fünf unterschiedlichen Verträge und ging im Einzelnen auf ihre Bedeutung ein. Neben allen Aufgaben, die für PKI, KM und SAM's zu erbringen sind, unterstützt die VDV-KA GmbH auch die Verkehrsunternehmen massiv beim Testen und Umsetzen des Sicherheitskonzepts. Mit den Dienstleistungen der VDV-KA GmbH werden nicht nur die Sicherheitsdienstleistungen angeboten, sondern auch Betrieb und Weiterentwicklung des Systems. Vorteile für alle Verkehrsunternehmen ergeben sich damit aus einer Verteilung der Entwicklungslasten auf eine große Anzahl von Beteiligten.



Anforderungen an Hintergrundsysteme aus der Sicht der VDV-Kernapplikation machte Dipl.-Ing. Helge Lorenz, GWT, Dresden, zum Gegenstand seiner Ausführungen. Mit der VDV-KA ist der höchste Anspruch an EFM (Elektronisches Fahrgeld-Management) in Europa entwickelt worden. Es bleibt die Aufgabe zu lösen, die Interpretationsbreite von Begriffen zu Hintergrundsystemen [HGS] einzuschränken. Bisher wurde noch kein vollständiges KA-konformes Hintergrundsystem realisiert. Es besteht das Risiko, dass Hintergrundsysteme zum Flaschenhals bei der Realisierung von elektronischen Fahrgeld-Management-Systemen werden. Der vorgetragene Anforderungskatalog kann hier nur mit einigen Beispielen wiedergegeben werden.

Es bleibt das Problem zu lösen, dass Hintergrundsysteme alle Formen des Ticketing vom konventionellen bis zu den aktuellen Ausprägungen des eTicketing integrieren müssen. Zusätzlich wird verlangt, dass HGS auch die Rollen der KA abbilden. Anforderungen an HGS zum Investitionsschutz und zur Finanzierbarkeit, wie z. B. langfristige Migrationskonzepte der KA-Phasen 2 und 3, Modularität, geeignete Betreibermodelle, Unabhängigkeit von eTechniken [CiCo, BiBo,...] führen zu einer komplexen Architektur der HGS. Die Organisationsstrukturen der Unternehmen müssen ebenfalls im jeweiligen HGS abgebildet werden. Die KA definiert die Schnittstellen zwischen Komponenten, die sich aus den Modellen ergeben. Die Inhalte der Komponenten sind aber noch zu definieren.

In der lebhaften Podiumsdiskussion wurde eine Vielzahl von Fragen erörtert, die im Zusammenhang mit den Plenumsvorträgen standen. Hier einige Beispiele:

- Sollte man Finanzdienstleistungen outsourcen?
- Sind Mandantensysteme vertrauenswürdig?
- Sollten HGS einzeln betrieben oder als gemeinsame Dienstleistung in Anspruch genommen werden?
- Soll ein Verkehrsunternehmen Schlüsselmanagement selbst betreiben? Steht PKI nur von einem Anbieter zur Verfügung?

Die Arbeitsgruppen haben in Erfurt an folgenden Schwerpunkten gearbeitet:

AG Migration - Wie in allen Vorträgen stand auch Sicherheit im Fokus der AG Migration. Die Detailfragen der Sicherheit wurden strukturiert und ein Verfahren zum Ableiten von Sicherheitsmassnahmen sowie zur Abschätzung des Restrisikos aufgestellt.

WG Interoperability hat Requirements on Interoperability, Rules and Regulations, Media, Man-Machine-Interface vertieft.

AG Mobilität hat sich mit der Kombination von eTicketing und anderen verkehrsorientierten Anwendungen befasst. Ein



Status wurde erhoben, Multiapplikationen und Co-Branding beleuchtet.

In seinem Schlusswort machte Hansjörg Röhrich deutlich, dass zur Anwendung der Kernapplikation ein gutes Gerüst vorhanden ist, aber für Verkehrsunternehmen und Verkehrsverbände noch ein ganzes Stück Arbeit erforderlich ist. Die Frage- und Aufgabenstellungen zur VDV-Kernapplikation werden kontiki sicher noch einige Konferenzen beschäftigen. Dem Ziel, die KA-Thematik im Detail in die Verkehrsunternehmen zu tragen, bleibt kontiki weiterhin verpflichtet.

Die nächsten Konferenzen:

Brüssel – 13. – 14. September 2007

Stuttgart - 28. – 29. Februar 2008

Oslo / Schiffsreise - 12. – 14. Juni 2008

Bremen - 11. – 12. September 2008