DIGITALE VERNETZUNG im ÖFFENTLICHEN PERSONENVERKEHR

Bundesministerium für Verkehr und digitale Infrastruktur

eTicketing und digitale Vernetzung
Steckbrief zu den Projektergebnissen (Stand 30.09.2018)

Langtitel / Kurztitel

Sicherheitsinfrastruktur der zweiten Generation für die VDV-Kernapplikation
Kurztitel 2GSI

Partner / Zuwendungsempfänger + assoziierte Partner

Keine, nur Unterauftragnehmer

Kernziele und –thema des Projektes

Ziel des Vorhabens war es, die inhaltliche und planerische Grundlage für eine zukunftssichernde Erneuerung der Sicherheitsinfrastruktur der VDV-Kernapplikation – die sogenannte zweite Generation Sicherheitsinfrastruktur (2GSI) – zu erschaffen. Die VDV-Kernapplikation ist der offene Standard für elektronisches Ticketing im öffentlichen Verkehr in Deutschland (eTicket Deutschland), der auch anderen Ländern zur Verfügung steht und bereits in anderen europäischen Ländern verwendet wird, z.B. Luxemburg. Auf Basis der Ergebnisse dieses Vorhabens sollen der Aufbau der zweiten Generation und die Migration der ersten Generation vorgenommen werden können.
Das Gesamtziel der Konzipierung und Spezifikation einer zukunftssichernden Erneuerung der Sicherheitsinfrastruktur der VDV-Kernapplikation setzt sich aus den folgenden beiden Teilzielen zusammen:

(1) Ein hohes Niveau im Bezug auf IT-Sicherheit und Datenschutz langfristig sichern.

(2) Die Attraktivität der VDV-Kernapplikation für Anwender erhöhen.

Die derzeitige Sicherheitsinfrastruktur der Kernapplikation bildet eine wesentliche Basis für das Vertrauen in eTicket Deutschland und ermöglicht die Interoperabilität zwischen allen teilnehmenden Unternehmen bei gleichzeitigem Schutz der Integrität und Autonomie der Geschäftsprozesse dieser Teilnehmer. Ein wesentlicher Aspekt dabei ist das hohe Sicherheitsniveau sowie aus Sicht der Nutzer den Datenschutz.
Es ist also von außerordentlicher Wichtigkeit für die Zukunftsfähigkeit des eTicket Deutschland das Sicherheitsniveau auch langfristig zu erhalten. Dazu bedarf es eines Updates bzgl. der in der Sicherheitsinfrastruktur verwendeten Krypto-Verfahren und Schlüssellängen sowie Technologien.
Aus der Betriebserfahrung der letzten Jahre ist erkennbar, dass die bislang notwendigen Komplexität den Betriebsaufwand erhöht und die Flexibilität beschränkt, so dass für eine langfristige deutschlandweite Umsetzung zusätzliche Anstrengungen zur Reduzierung der Komplexität wesentlich sind.
Zur Erreichung der Ziele wurden daher im Vorhaben 2GSI folgende Maßnahmen konzeptuell und planerisch umgesetzt:

- Die Erneuerung der verwendeten Krypto-Verfahren und Schlüssellängen.
- Die Verfolgung eines neuen Konzepts ohne Verwendung von Masterkeys, wodurch das mit der Speicherung solcher Schlüssel in SAMs verbundene hohe Risiko sowie das entsprechende Keymanagement-System entfallen.
- Die Ermöglichung des Ladens und Initialisierung der Applikationen (für SAM und Nutzermedien) über offenen Netzwerken in Standardkomponenten (z.B. in mobilen Handsets und anderen Geräten). Durch die resultierende schnelle Updatefähigkeit wird die Sicherheit des Systems gesteigert und die Kosten für Rollouts und Fehlerkorrekturen reduziert.
- Konsolidierung von Daten und Prozessen in den Applikationen, Reduzierung der mit dem applikationsspezifischen Charakter bedingten Komplexität. Dadurch können Kosten für Implementierung und Tests reduziert und Ressourcen im Einsatz geschont werden. Als Begleiterscheinung wird die

Wahrscheinlichkeit von Fehlern reduziert, was auch die Sicherheit erhöht.

Mit diesem Vorhaben wird die bestehende Grundlage der zentralen KA-Infrastruktur ausgebaut, um die Zukunftsfähigkeit von (((eTicket Deutschland langfristig zu sichern.
Die vorgesehenen Arbeiten werden die Grundlage für die Sicherheitsinfrastruktur für voraussichtlich 15 bis 20 Jahre bilden. In diesem Vorhaben wurden Positionen bzgl. relevanter technischen und wissenschaftlichen Entwicklungen der letzten Jahre erarbeitet. Die Entwicklungen wurden nach ihrem Nutzen für die Sicherheitsinfrastruktur der VDV-Kernapplikation beurteilt und in ein innovatives Konzept für die künftige Sicherheitsinfrastruktur integriert. Es handelte sich dabei sowohl um die Verwertung neuer Ideen als auch um früher bereits vorliegender Ideen, die aber erst durch die Entwicklungen der letzten Jahre für Anwendungen in diesem Bereich zugänglicher geworden sind. Insbesondere wurden innovativen Ergebnisse in den Bereichen neue Krypto-Verfahren und neue technische Plattformen (insbesondere Smartphones und Cloud-Services) erzielt.

Erzielte Ergebnisse zum Projektabschluss Ende September 2018

Eine Anforderungsanalyse (AP110) wurde durchgeführt und daraufhin wurden entsprechende technische Lösungen und Maßnahmen (AP110) entworfen und die Ergebnisse in Konzeptpapieren dokumentiert.
Die Erkenntnisse aus der Validierungsarbeit bzw. der Durchführung des Proof-of-Concept (PoC) (AP120) wurden in den Konzeptarbeiten berücksichtigt. Im Rahmen des PoC wurden folgende Komponenten implementiert, die nach dem Projekt noch vorgehalten werden: PoC-PTO-App und PoC-User-App auf Android implementiert; PoC-PKI und PoC-SAM in Google Cloud realisiert.
Darüber hinaus wurden für kritische Aspekte Detailspezifikationen ausgearbeitet und dokumentiert (AP200).
Ein Gesamtplan für die Einführung von 2GSI wurde unter Berücksichtigung aller betroffenen Systeme und Komponenten ausgearbeitet (AP300 Umsetzungskonzept) und in Workshops mit Kollegen sowie mit Herstellern und Verkehrsunternehmen abgestimmt und validiert. Für alle relevanten Systeme und Komponenten koordiniert der Gesamtplan die Detailspezifikation, Aufbau und Inbetriebnahme, Einzelkomponenten- sowie Integrationstests, Systemmigrationen sowie CR-Verfahren.

Die Ergebnisse des Vorhabens bilden die technische und planerische Grundlage für die Einführung von 2GSI und tragen wesentlich zur Erneuerung der wirtschaftlichen Grundlage von eTicket Deutschland bei.
Diese Arbeit beginnt jetzt mit den ersten Aufgaben aus dem erarbeiteten Gesamtplan. Die Erstellung der Feinspezifikationen SAM, PKI und KM stehen auf dem Plan für 2019, damit diese dann im Frühjahr 2020 in die Teilnehmerversammlung gehen können. Im Jahr darauf folgen weitere CRs.
Für VDV-Barcode mobile+ wird noch in 2018 die VDV-PKI um eine Sub-CA erweitert, die nach den Vorgaben aus diesem Projekt für 2GSI bereits gebaut wird. Ferner werden die in diesem Vorhaben gewonnenen Kenntnisse zu Software Security eine Schlüsselrolle in der Etablierung des Services „Motics“ als zentraler Baustein für VDV-Barcode mobile+ im kommenden Jahr spielen.
Mit VDV-Barcode mobile+ wird die Integration von Smartphone-Anwendungen in eTicket Deutschland stark vorangetrieben und somit auch die wirtschaftliche Grundlage von eTicket Deutschland entsprechend erweitert.
Es gilt nun die in 2GSI erarbeiteten und erprobten Konzepte in 3 weiteren Phasen zu vertiefen und ins Feld zu bringen. Diese drei Phasen wurden im Vorhaben in Detail geplant und sind wie folgt:

- Die Konzepte und Ergebnisse des Vorhabens in die Spezifikationen der betroffenen Komponenten und Systeme in Detail vollständig umzusetzen
- Implementierung und Aufbau zentraler Systeme
- Migration der Systeme und Terminals der Teilnehmer

Gerade in der zweiten Phase erwarten wir durch die intensivere Ausnutzung neuer Technologien weitere Innovationsmöglichkeiten.