KASPER OSWALD
Ingenieure für innovative Sicherheitslösungen

Voruntersuchung: Unerwünschtes Auslesen von elektronischen Fahrausweisen

06.03.2015

Kasper & Oswald GmbH
Mühlenweg 14 b
44809 Bochum

info@kasper-oswald.de

Tel: +49 234 5200 6267

Fax: +49 234 5200 6268

Geschäftsführer: Dr.-Ing. Timo Kasper, Dr.-Ing. David Oswald

Registergericht: Bochum, HRB 14184

Versionshistorie

Version	Date	Author	Comment
1	1.3.2015	David Oswald	Initiale Version
2	6.3.2015	David Oswald	Überarbeitung
3	30.5.2015	Timo Kasper	Final, nach Kommentaren von KCEFM

Einleitung

Im Öffentlichen Personen-Nahverkehr (ÖPNV) werden seit einigen Jahren verbreitet elektronische Fahrausweise auf Basis von Radio Frequenz Identifikation (RFID) bzw. NFC (Near Field Communication) eingesetzt, konkret kontaktlose Karten gemäß des ISO14443-Standards mit kryptografischen Funktionen. Die Einführung von Chipkarten als Träger von eTickets bringt für Fahrgäste eventuell eine Informationslücke mit sich. Das eigentliche Ticket ist mit bloßem Auge nicht zu überprüfen. Die Dateninhalte der Chipkarte sind damit für Kunden nicht im Klartext zu sehen und daher nicht überprüfbar.

Ziel der vorliegenden Voruntersuchung ist die Feststellung der möglichen Reichweiten zum Auslesen eines elektronischen Fahrausweises unter Verwendung des originalen Lesegerätes und eines (soweit möglich) mit einfachen Mitteln modifizierten Original-Lesegerätes. Zudem wird konzeptionell bewertet, inwiefern das Auslesen und die Modifikation der auf einem elektronischen Fahrausweis gespeicherten Daten möglich ist.

Dabei ist anzumerken, dass der für die Untersuchung zur Verfügung stehende Zeitrahmen äußerst begrenzt war (1,8 Projekttage). Damit decken die Ergebnisse nur einen kleinen Teil der möglichen Analysen und Bedrohungen ab.

Zur Durchführung standen die folgenden Geräte und Fahrausweise zu Verfügung:

- Zwei Mobile Datenerfassungsgeräte Casio DT-X11M10E
- eTicketInfo
- SchokoTicket

Auslesereichweiten mit Original-Lesegerät

Zunächst wurde die Reichweite zum Auslesen unter Verwendung des nicht modifizierten Original-Lesegeräts ermittelt. Die Plastikabdeckung über der Antenne des RFID-Moduls (auf der Rückseite des Lesegeräts) wurde dazu entfernt, um die tatsächliche Entfernung zwischen Antenne und Ticket zu bestimmen.

Wie in Abbildung 1 zu erkennen, ist das RFID-Lesemodul als aufgesteckte Platine realisiert. Die Platine ist beschriftet mit dem Namen des vermutlichen Herstellers „Inside Contactless“ und verfügt über eine relativ kleine Antenne (ca. 40 mm x 25 mm, 4 Windungen), die sich in einer der inneren Lagen befindet. In Abbildung 1 ist am unteren Rand zudem das in Form einer SIM-Karte ausgeführte Sicherheitsmodul für kryptographische Berechnungen (SAM) zu erkennen.

Abbildung 1: Geöffnetes Lesegerät, RFID-Modul in Bildmitte

Mit dem Original-Lesegerät ergab sich eine maximale Reichweite von ca. 2 cm (für beide Test-Fahrscheine und beide verfügbaren Lesegeräte). Bei größeren Distanzen war das Auslesen des Fahrausweises nicht mehr möglich. Diese Reichweite ist geringer als die üblicherweise anzutreffenden Ausleseentfernungen für ISO14443-System im Bereich von 5 … 10 cm. Dies ist vermutlich auf die geringe Größe der vorliegenden Antenne und den vergleichsweise hohen Stromverbrauch der Smartcard im Ticket zurückzuführen.

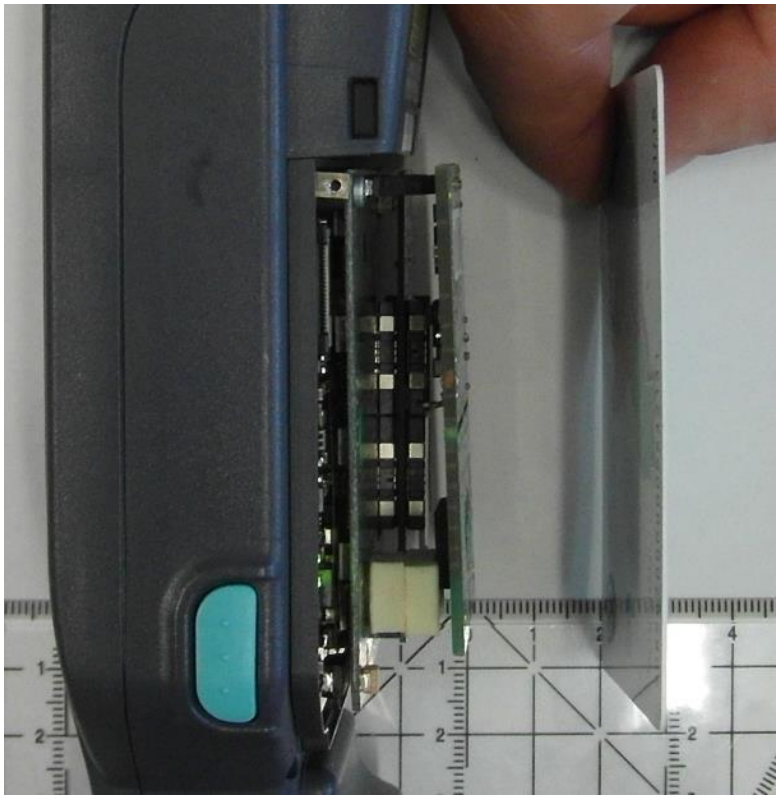

Abbildung 2: Bestimmung der Auslesereichweite

Möglichkeiten zur Erhöhung der Auslesereichweite des Original-Lesegeräts

Da im Rahmen des vorliegenden Projekts nur 1,8 Personentage für die Untersuchung zur Verfügung standen, wurde in Abstimmung mit dem KCEFM festgelegt, dass lediglich Möglichkeiten zur Reichweitenerhöhung des Original-Lesegeräts betrachtet werden. Die Betrachtung von weitergehenden Ansätzen (z.B. Verwendung von Leistungsverstärkern etc.) blieb daher außen vor.

Zunächst wurde die vorhandene Beschaltung zur Abstimmung und Anpassung der Antenne untersucht. Dabei zeigte sich, dass eine recht komplizierte Schaltung (Abbildung 3) Anwendung findet, um die Impedanz der Antenne auf den auf der Platine befindlichen Reader-Chip („PicoRead“) anzupassen.

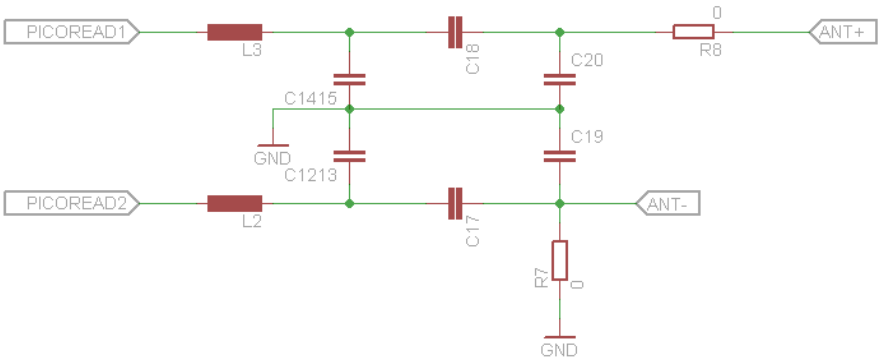

Abbildung 3: Anpassnetzwerk für RFID-Antenne

Im Umfang des vorliegenden Projektes war die genaue Bestimmung aller Komponenten-Werte im Anpassnetzwerk nicht möglich. Als einzige Möglichkeit zum Anschluss einer zusätzlichen Antenne ergab sich damit die Verwendung einer Antenne mit ähnlicher Induktivität. Die Induktivität der Original-Antenne ergab sich zu ca. 1 µH, festgestellt mit einem Netzwerkanalysator.

Die Original-Antenne wurde dazu abgetrennt (an R8 und C17) und durch eine Spule mit 2 Windungen Kupferdraht ersetzt (Abbildung 4). Obwohl mit dem Netzwerkanalysator eine ähnliche Induktivität gemessen wurde, war ein Auslesen von Fahrausweisen mit dem modifizierten Lesegerät nicht möglich. Dies könnte z.B. auf eine Fehlanpassung der neuen Antenne zurückzuführen sein. Aufgrund des verfügbaren Zeitrahmens konnte eine genauere Untersuchung nicht vorgenommen werden.

Ein analoger Versuch wurde mit einer Rahmenantenne aus Kupferrohr durchgeführt (ca. 290 mm x 290 mm). Auch hier funktionierte das modifizierte Lesegerät nicht, eine Reichweitenerhöhung auf diese Weise war daher im Rahmen des vorliegenden Projektes nicht möglich. Die Chipkarten konnten mit dem Original Lesegerät aus max. 50 mm Entfernung ausgelesen werden. In der Literatur gibt es jedoch Hinweise, dass weitaus größere Reichweiten über 200 mm möglich sind. Zur genauen Feststellung ist jedoch eine detaillierte Literaturrecherche und anschließende Fortführung der Untersuchungen notwendig.

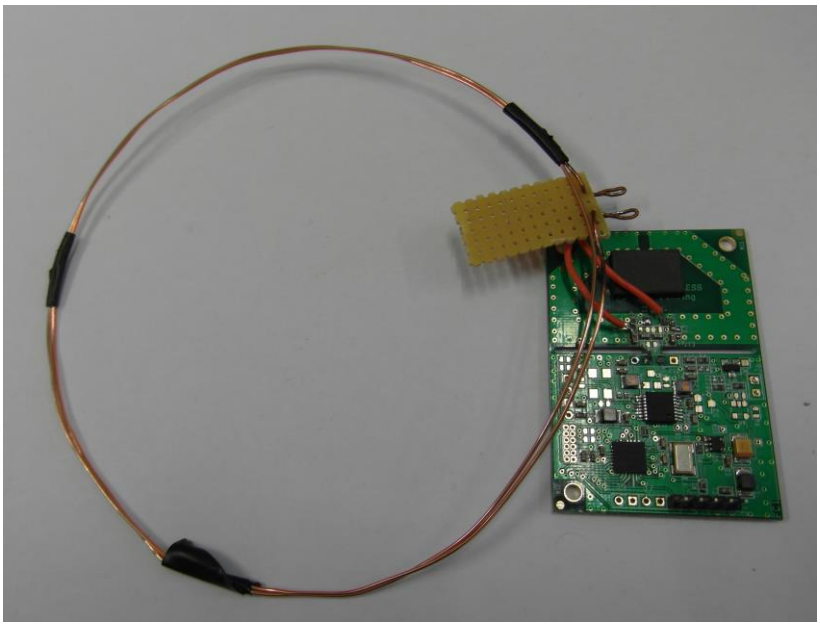

Abbildung 4: Angeschlossene Ersatzantenne

Auslesen und Modifikation der auf dem elektronischen Fahrausweis gespeicherten Daten

Aus der Spezifikation der VDV-Kernapplikation (Spec_NM_V130, 1.5.2013) ergibt sich, dass die folgenden auf der Karte gespeicherten Daten über die RFID-Schnittstelle ohne Authentifizierung frei auslesbar sind, z.B. unter Nutzung der Applikation „eTicketinfo“:

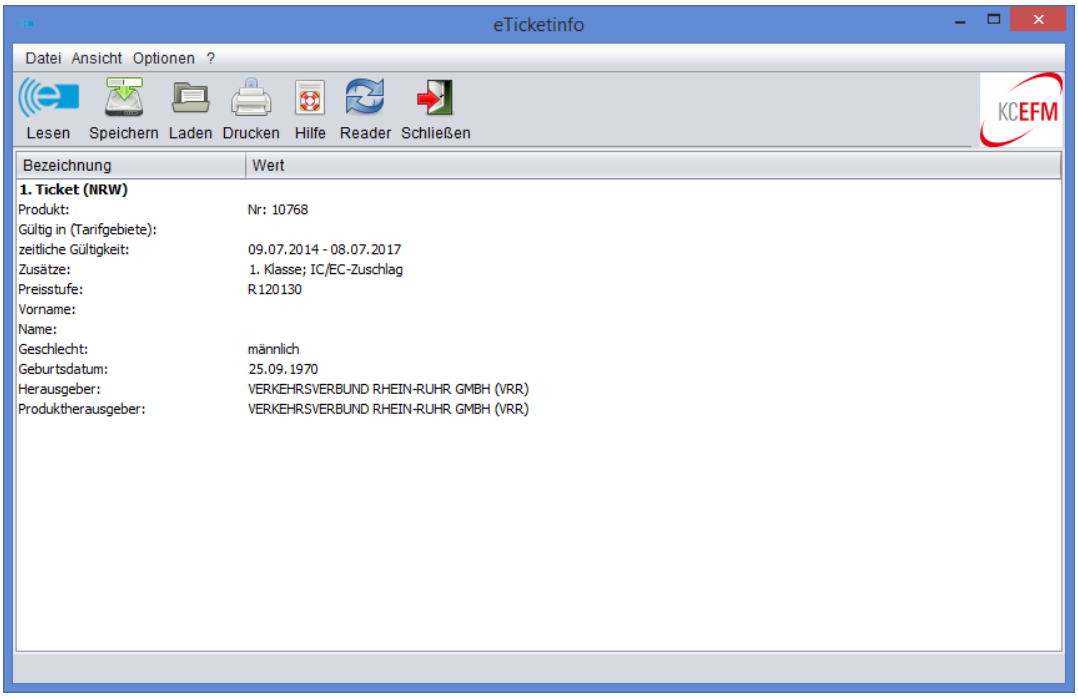

Abbildung 5: Kundendaten auf Fahrschein, Auszug

Vgl. dazu auch Abschnitt 2.2.1.4 „Datenstruktur der Kundendaten“ und Anhang A.7 der Spezifikation Nutzermedium. Weitere Daten erfordern u.U. die Authentifizierung mit der PIN des Nutzers. Es ist nicht ausgeschlossen, dass weitere Kundendaten ungeschützt auf der Karte gespeichert sind – dies wurde in dieser Voruntersuchung nicht geprüft. Zur Änderung von auf dem Fahrschein gespeicherten Daten ist hingegen lt. Spezifikation immer eine Authentifizierung mittels RSA (realisiert mit einer Zertifizierungs-Hierarchie) erforderlich:

2.1.2 Allgemeines zu den Lebenszyklen von Applikation und Berechtigung

Jeder KVP besitzt ein zertifiziertes Schlüsselpaar, mit dem er sich gegenüber einer initialisierten Applikation (siehe Kapitel 2.1.4) authentisieren kann. Nach der erfolgreichen Authentisierung kann ein KVP

- die Ausgabe (Personalisierung) der Applikation (sofern noch nicht erfolgt) durchführen,
- die Ausgabe (Personalisierung) des WES entfällt in der weiteren Anwendung,
- das Schreiben der Kundendaten (sofern noch nicht erfolgt) durchführen,
- die Ausgabe von Berechtigungen durchführen,
- das Löschen von Berechtigungen durchführen und
- die Änderung der Prioritäten durchführen.

Abbildung 6: Auszug aus Spezifikation zum Schreiben von Daten

Die entsprechenden privaten RSA-Schlüssel liegen auf dem Lesegerät in einem SAM-Modul (s.o.) vor und sind damit vermutlich gegen bestimmte Angriffsklassen (z.B. Seitenkanal und Fehlerinjektion) geschützt. Eine genauere Bewertung der kryptographischen Qualität der verwendeten Protokolle und Implementierungen konnte im Rahmen der Voruntersuchung nicht erfolgen.