georg ebbing

Anlage 41 Datum: 12.08.2016

# Kontrolle des Semestertickets im Studienausweis der Martin-Luther-Universität

Version 1.10

## 1 Einleitung

An knapp 100 Universitäten und Hochschulen in Deutschland ist ein Chipkarten-System der Firma InterCard, Villingen-Schwennigen, im Einsatz, mit dem die Studienausweise erstellt werden. Typisch für dieses System ist, dass die Karten zu Beginn des Studiums und dann pro Semester nach jeder Rückmeldung in einem Automaten, der Validierungsstation, selbstbedient aktualisiert werden müssen. Dabei werden Datensätze in der Karte aktualisiert. Aber auch eine außen auf der Karte befindliche wiederbeschreibbare Folie (TRW-Folie) wird dabei gelöscht und neu beschrieben. Dort ist typischerweise das Semesterticket in Form des Logos des Verbundes aufgedruckt. Diese Lösung ist auch an der Martin-Luther-Universität (MLU) in Halle im Einsatz.

Seit dem Wintersemerster 2013/14 wird an der MLU das Semesterticket als Datensatz im Studienausweis (Chipkarte des Mifare DESfire EV1) gespeichert. Dabei kommt die statische Berechtigung der VDV-Kernapplikation zum Einsatz. Vorher bekamen die Studierenden eine extra Chipkarte der HAVAG, was sowohl für die Studierenden selbst aber auch für die HAVAG mit großen Nachteilen verbunden war.

Das Konzept ist im Detail im Dokument [SemTic Konz] dargestellt. Die Sicherheitsaspekte sind in [SemTic Sich] enthalten.

## 2 Speicherung und Kontrolle des eTickets

Das Konzept sieht vor, die statische Berechtigung in einer frei auslesbaren Datei (EF) in der Chipkarte zu speichern. Der Name des EF und der Zugriffspfad werden noch bekanntgegeben. Es kommt das in der [STB Spec] Kap. 2 definierte normale Format zum Einsatz, bei dem die statische Berechtigung eine Länge von ca. 360 Byte hat.

Um zu vermeiden, dass die statische Berechtigung in andere Karten übertragen werden kann, wird ein Teil der Seriennummer (UID) der DESfire-Karte, die eindeutig, einmalig und nicht veränderbar ist, mit in die eTicket-Daten geschrieben und verschlüsselt. Die Kontrollgeräte müssen dann prüfen, ob die UID der Karte und die im eTicket gespeicherte UID übereinstimmen.

Beim vorgeschlagenen Konzept kann die statische Berechtigung ohne besondere Sicherung aus dem EF ausgelesen und in den EF einer anderen Karte geschrieben werden. Ein solches Kopieren kann zwar nicht verhindert werden, der Angriff kann aber leicht offenbar gemacht werden. Dazu wird folgendes Verfahren angewendet:

- Bevor die Daten der statischen Berechtigung zusammengestellt werden, wird zunächst die UID aus der Karte gelesen, in die eine statische Berechtigung geschrieben werden soll. Die UID ist 7 Byte lang, konvertiert in eine Textkette ergibt dies eine Zahl mit 17 Ziffern. Davon werden aus Platzgründen die letz-

ten 9 Ziffern in die statische Berechtigung hineingeschrieben. Dass diesen 9 Ziffern an der MLU nicht mehrfach vorkommen können, wird durch organisatorische Maßnahmen sichergestellt.

- Liest nun ein Kontrollgerät die statische Berechtigung, wird der „Klartext" des eTickets erzeugt, indem der in der [STB Spec] in Kapitel 4.5 beschriebene Prozess durchlaufen wird. Außerdem wird die UID direkt aus der Karte gelesen. Die im eTicket gespeicherten Stellen der UID werden mit den korrespondierenden Stellen der aus der Karte direkt gelesenen UID verglichen. Stimmen sie überein, ist die statische Berechtigung mit sehr hoher Wahrscheinlichkeit nicht kopiert worden, stimmen sie nicht überein, liegt ein Betrugsversuch vor. Das Kontrollgerät muss eine entsprechende Meldung ausgeben.

Diese Lösung vermeidet, dass ein Desfire-SAM in den lesenden Geräten erforderlich ist.

Bei dem eTicket selbst handelt es sich um eine KA-konforme statische Berechtigung. Daher stimmen die für die weitere Kontrolle des eTickets erforderlichen Abläufe in den Kontrollgeräten mit denen überein, die für die Kontrolle eines 2D-Barcodes nach KA-Standard erforderlich sind. An die Stelle des Scannens und Decodierens des 2D-Barcodes tritt die Kommunikation des Kontrollgeräts mit der DESfire-Karte und das Auslesen des eTickets aus der Datei. Weiterhin ist die oben dargestellte Überprüfung der UID zusätzlich zu programmieren. Alle weiteren Abläufe sind dann identisch mit denen für die Kontrolle eines 2D-Barcodes.

Die Befehle zum Auslesen der UID aus der Chipkarte finden sich in **Anlage 2**.

# 3 Statische Berechtigung der HAVAG

**Anlage 1** zeigt die Struktur der statischen Berechtigung des MDV, die aus dem Referenz-EFS des MDV abgeleitet ist. Hier stehen die letzten 9 Ziffern der UID im Element efsKundeNameVorname (Zeile 32) in den ersten 9 Zeichen. Das gesamte Element hat eine Länge von 17 Zeichen und besteht aus

- letzte 9 Ziffern der UID
- Blank
- Vorname und Name des Kunden (7 Zeichen) in gekürzter Form

Es werden 2 statische Berechtigungen gespeichert für jeweils 2 aufeinanderfolgende Semester. Wie dies in der Dateistruktur der Karte im Detail geregelt wird, ist in der Spezifikationsphase festzulegen.

Die Dateistruktur in der DESFire-Karte sieht folgendermaßen aus:

AID 0x85845F

WriteLog:
FID 0
CR FILE
PLAIN
SIZE: 4x32 Byte
ACC: C: 0, R: 3, W: 4, RW: 1

eTicket-1:
FID 1
STD DATA FILE

PLAIN
SIZE: 384 Byte
ACC: C: 0, R: free, W: 1, RW: 2

eTicket-2:
FID 2
STD DATA FILE
PLAIN
SIZE: 384 Byte
ACC: C: 0, R: free, W: 1, RW: 2

Das File „Write-Log" enthält die Zeitstempel der letzten 4 Schreibvorgänge.

Die Files eTicket-1 und eTicket-2 sind mit den 362 Byte langen Daten der STB beschrieben. Die restlichen 22 Byte sind mit 0x00 gefüllt. Leere eTicket-Files sind mit 0x00 gefüllt.

# 4 Anzeige der statischen Berechtigung

Es werden immer beide vorhandene eTickets aus den EFs gelesen und decodiert. Das eTicket mit dem passenden zeitlichen Gültigkeitsbereich wird angezeigt. Findet sich kein zeitlich gültiges Ticket, wird die Meldung wie bei der Kontrolle einer KA-Chipkarte angezeigt.

Nach dem Lesen und Entschlüsseln des eTickets muss der Inhalt Name im Element KundeNameVorname der Form angepasst werden, wie sie bisher üblich ist. Aus z.B.

- 987654321 G3g@E4g muss
- Exxxxg, Gxxxg

werden. Dazu sind folgende Schritte anzuwenden:

- Die ersten 10 Zeichen (UID-Teil und Blank) werden entfernt
- Die Zeichen hinter dem @ werden genommen und zwischen die Buchstaben werden soviel x eingefügt wie es dem Wert der Ziffer entspricht. Ist keine Ziffer zwischen den Buchstaben, wird kein x eingefügt. Ist die Ziffer eine 0, werden 10 x eingefügt.
- Der so erhaltene Textkette werden ein Komma und ein Blank angehängt.
- Die Zeichen vor dem @ werden genommen und zwischen die Buchstaben werden soviel x eingefügt wie es dem Wert der Ziffer entspricht. Ist keine Ziffer zwischen den Buchstaben, wird kein x eingefügt. Ist die Ziffer eine 0, werden 10 x eingefügt.
- Diese Zeichen werden an den Nachnamen angehängt.

# 5 Kontrollablauf

In dem Studierendenausweis der MLU stehen in der Regel 2 eTickets. Sie müssen beide gelesen und entschlüsselt werden nach dem in Kapitel 4.5 der [STB Spec] beschriebenen Verfahren. Die Berechtigung, deren Gültigkeitsbeginn und -ende zum aktuellen Datum passt, wird kontrolliert.

In Bezug auf die übrigen Kontrollschritte, die Meldungen und wie z.B. das Schreiben des Kontrollnachweises wird mit dieser Berechtigung dann genauso verfahren, als

wenn sie aus einer Chipkarte gelesen wurde. Beim Element efsKundeNameVorname ist zu berücksichtigen, dass es nicht 40 sondern nur 17 Zeichen lang ist.

# 6 Anfrage des eTicket-Inhalts beim MDV-BerSy

Wie bei den klassischen KA-Karten auch, schickt das BerSyTicketCheck eine Kartennummer an das BerSy. Im Falle des Semestertickets muss diese Nummer im Gerät erst noch gebildet werden, bevor sie an das BerSy geschickt werden kann.

Da die DESFire-Karte kein Applikationsverzeichnis hat, das mit dem Befehl „Select File" gelesen werden könnte, wird stattdessen die UID zur Bildung einer app-Instanz_ID herangezogen. Deren letzten 9 Stellen dienen zur Bildung der Applikationsnummer. Sie beginnt immer mit einer 3, die den 9 Stellen vorangestellt wird, d.h. die 10. Stelle von rechts (erste Stelle von links) ist immer eine 3. Damit lassen sich die Applikationsnummern von den anderen abgrenzen.

Die Org_ID ist immer die 6053.

Beispiel für die Bildung der appInstanz_ID aus der UID

| | |
|---|---|
| Nummer auf der Karte (UID): | 36066996075722244 |
| letzte 9 Ziffern: | 075722244 |
| Org_ID: | 6053 (festgelegt) |
| Applikationsnummer: | **3**075722244 (um die 3 ergänzt) |
| um Prüfziffer ergänzt: | -1 (immer -1) |
| in klassischer Schreibweise: | 6.053-3.075.722.244-1 |

Diese Nummer wird an das BerSy gesendet.

Die Antwortdaten des BerSy sind genauso aufgebaut wie bei einer klassischen Chipkarte, so dass die Anzeige nicht verändert werden muss.

# 7 Referenzierte Dokumente

[STB Spec] KA_Technische Spezifikation für elektronisches Fahrgeldmanagement, Verwendung von Statischen Berechtigungen auf der Grundlage des KA-Referenz_EFS/KA-TLV-Referenz- EFS für 2D Barcode

[SemTic Konz] Konzept für die Realisierung des Semestertickets der Halleschen Verkehrs-AG

[SemTic Sich] Aussagen zur Sicherheit des Semestertickets der Halleschen Verkehrs-AG

# Anlagen:

Anlage 1: Statische Berechtigung des MDV

Anlage 2: Mail zu APDU-Kommandos