



Verkehrsverbund Rhein-Ruhr Elektronisches Fahrgeldmanagement

Rahmenvorgaben für Kontrollgeräte



0 Allgemeines

0.1 Inhaltsverzeichnis

Kapitel	Seite
0 Allgemeines.....	2
0.1 Inhaltsverzeichnis.....	2
0.2 Änderungsverzeichnis	2
1 Vorbemerkungen.....	3
2 Rahmenvorgaben für Kontrollgeräte.....	3
2.1 Arbeitsweise eines Kontrollgerätes.....	3
2.1.1 Lese Kartendaten und Elektronisches Ticket (ET).....	4
2.1.2 Überprüfe Gültigkeit ET.....	6
2.1.3 Überprüfe Einträge in Sperrlisten	6
2.1.4 Markiere ET	7
2.1.5 Uhr/Datum.....	7
2.1.6 Eingabe Ticketwahl und Standortdaten	7
2.1.7 Sicherheitsmodul (SAM).....	7
2.1.8 Datei Ticket-/Tarifdaten	8
2.1.9 Datei Sperrlisten.....	8
2.1.10 Display	8
2.1.11 Ausgabedatei	8
2.2 Vorgaben für einzelne Komponenten	9
2.2.1 Chipkarten.....	9
2.2.2 Umgang mit Sicherheitsmodulen.....	9
2.2.3 Datei für Ticket-/Tarifdaten	10
2.2.4 Datei für Sperrlisten	10
2.2.5 Ausgabedatei	10
2.2.6 Eingabe Ticketwahl und Standortdaten	10
2.2.7 Display	11
2.2.8 Lese Kartendaten und Elektronisches Ticket, Markiere ET.....	11
3 Referenzen.....	11

0.2 Änderungsverzeichnis

Die Version 1_3 unterscheidet sich von der Version 1_2 durch die folgenden Änderungen:

- Allgemein: Der Inhalt ist nun neutral gestaltet, da zusätzlich die PayCard der Firma card.etc berücksichtigt wird. Die Verweise auf die Referenzen wurden überarbeitet und es wird einheitlich der Begriff „Elektronisches Ticket“ verwendet.
- Kapitel 1, dritter Absatz: Die Gültigkeit dieses Dokumentes wird auf die Einstiegskontrolle erweitert.
- Kapitel 2.1, Aufzählung 2. und 3. Punkt: Auf der Sperrliste befinden sich nur Fahrschein- und Terminalsperren aber keine Chipkartensperren.

1 Vorbemerkungen

Auf dem Gebiet des Verkehrsverbundes Rhein-Ruhr (VRR) soll (schrittweise) ein System für Elektronisches Fahrgeldmanagement eingeführt werden. In der ersten Stufe soll dabei ein Fahrausweis in der Form eines „Elektronischen Tickets“ in einer Chipkarte gespeichert werden. Als Chipkarten sollen dabei als erstes ZKA-GeldKarten der deutschen Kreditwirtschaft und die PayCard der Firma card.etc eingesetzt werden.

ZKA-GeldKarten und die Paycard sind bereits für die Speicherung von Elektronischen Tickets vorbereitet. Sie bieten dafür eine Zusatzanwendung, die kompatibel zu [1] ist. Zu dieser Zusatzanwendung gehören Datenstrukturen in den Chipkarten, die der Speicherung von Elektronischen Tickets dienen, und Sicherheitsmodule, die für den Zugriff auf die Chipkarten benötigt werden.

Für die Kontrolle von Elektronischen Tickets sollen sowohl sogenannte (mobile) Kontrollgeräte als auch (stationäre) am Fahrerplatz eingebaute Kontrollgeräte eingesetzt werden. Bei letzterem spricht man von der Einstiegskontrolle, für die dieses Dokument ebenfalls Gültigkeit besitzt. Wenn also im Folgenden von „Kontrolleur“ oder „Prüfer“ geredet wird, ist damit sowohl der Mitarbeiter bzw. die Mitarbeiterin eines Kontrollteams als auch der Fahrer bzw. die Fahrerin eines Fahrzeuges gemeint.

Kontrollgeräte überprüfen für eine Chipkarte, ob ein Elektronisches Ticket des VRR gespeichert ist, ob dieses gültig ist und ob das Elektronische Ticket auf einer Sperrliste vorhanden ist. Teile dieser Schritte werden kryptographisch abgesichert durchgeführt, wofür ein Sicherheitsmodul in dem Kontrollgerät vorhanden sein muss. Zusätzlich bietet ein Kontrollgerät eine Anzeige für den Kontrolleur und eine Verwaltung von Sperrlisten.

Kontrollgeräte werden durch ein Verkehrsunternehmen betrieben. Es ist Aufgabe der einzelnen Verkehrsunternehmen, die dabei zum Einsatz kommenden Geräte auszuschreiben und zu beschaffen.

Das vorliegende Dokument soll bei der Erstellung der Ausschreibungen für die Kontrollgeräte eine Hilfestellung bieten. Es enthält eine grobe Beschreibung der Funktionalität eines Kontrollgerätes und stellt aus funktionaler Sicht Vorgaben zusammen, die Kontrollgeräte erfüllen müssen.

Die Aufgaben eines Kontrollgerätes werden in diesem Dokument aus funktionaler Sicht beschrieben. Ein Kontrollgerät kann dabei als eigenständiges Gerät realisiert werden, es kann aber auch zusammen mit anderen Funktionen (z.B. EBE-Gerät) in einem Gerät realisiert werden.

In diesem Dokument werden nur die Funktionen eines Kontrollgerätes dargestellt, die für die eigentliche Prüfung eines Elektronischen Tickets in einer Chipkarte benötigt werden. Weitere (administrative) Funktionen wie den Datenaustausch mit einem Hintergrundsystem oder das An- bzw. Abmelden des Kontrolleurs werden nicht betrachtet.

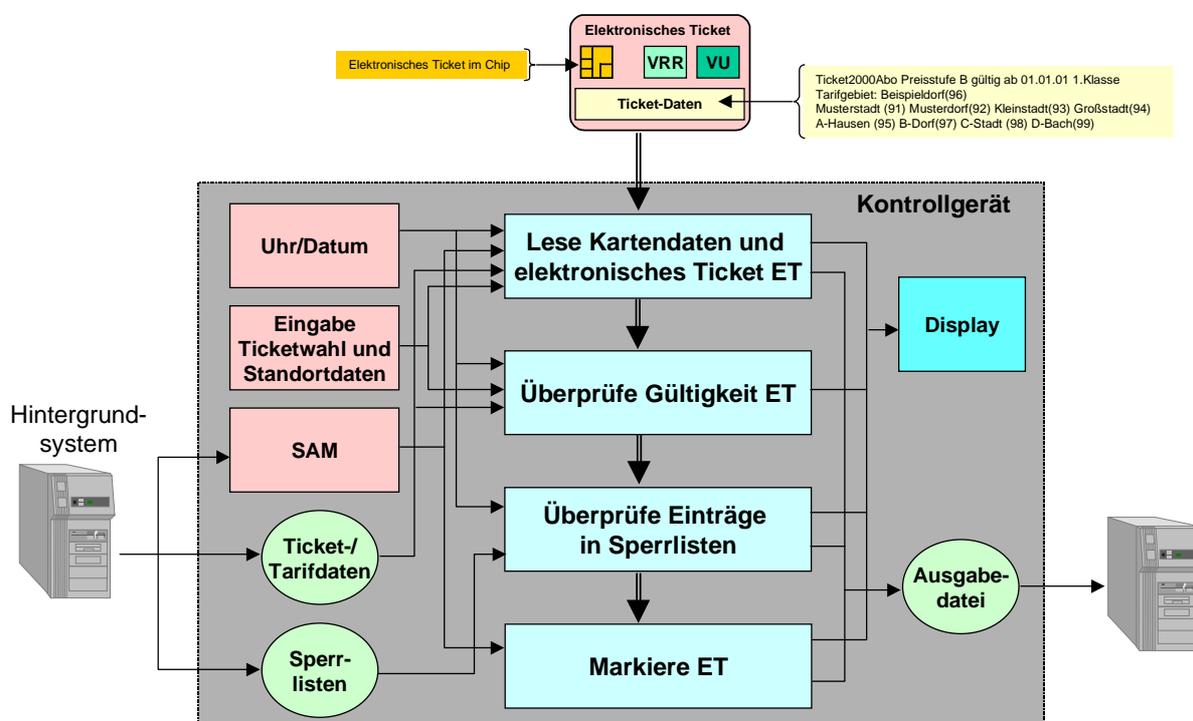
2 Rahmenvorgaben für Kontrollgeräte

2.1 Arbeitsweise eines Kontrollgerätes

Mit einem Kontrollgerät können Elektronische Tickets überprüft werden, die in einer Chipkarte gespeichert sind. Dabei sind die folgenden Arbeitsschritte in der angegebenen Reihenfolge durch ein Kontrollgerät durchzuführen:

1. Suchen eines Elektronischen Tickets des VRR in der Chipkarte. Wird ein entsprechendes Ticket gefunden, wird dieses „kryptographisch“ überprüft, wodurch sichergestellt wird, dass die beteiligte Chipkarte korrekt ist. Wenn ein Verkehrsunternehmen für mehrere Verbände Fahrleistungen erbringt und Tickets ausgibt, kann die Zugehörigkeit eines Tickets zu einem Verbund über die Servicekennung ermittelt werden.
2. Überprüfen, ob das gefundene Elektronische Ticket in einer Sperrliste gespeichert ist.
3. Markieren des gefundenen Elektronischen Tickets in der Chipkarte, falls das Ticket in einer Sperrliste gespeichert ist.
4. Überprüfen der Gültigkeit eines gefundenen Elektronischen Tickets. Dabei kann sowohl die zeitliche als auch die räumliche Gültigkeit untersucht werden.

Die folgende Abbildung gibt einen Überblick über die logischen Komponenten eines Kontrollgerätes und ihr Zusammenspiel:



Die Einteilung in die dargestellten logischen Komponenten stellt die verschiedenen Funktionsbereiche eines Kontrollgerätes dar. Im folgenden werden für die einzelnen logischen Komponenten die Aufgaben bei der Bearbeitung einer Chipkarte aus funktionaler Sicht kurz beschrieben.

2.1.1 Lese Kartendaten und Elektronisches Ticket (ET)

Diese Komponente liest alle benötigten Daten aus dem Chip der beteiligten Chipkarte. Sie muss dazu Zugriff über eine Chipkontaktiereinheit auf den Inhalt der Chipkarte haben. Zu den zu lesenden Daten gehören die Identifikationsdaten der Chipkarte und die Daten der in der Chipkarte gespeicherten Elektronischen Tickets.

In einer Chipkarte können mehrere Elektronische Tickets von verschiedenen Verkehrsunternehmen gespeichert sein. Das für die Speicherung verantwortliche Verkehrsunternehmen ist in dem Elektronischen Ticket gespeichert (Betreiber-ID).

Von den gespeicherten Elektronischen Tickets muss das für den aktuellen Kontrollvorgang benötigte Ticket ausgesucht werden. Dazu sind verschiedene Wege möglich, die sich im Komfort bei der Bedienung des Gerätes durch den Kontrolleur unterscheiden. Im folgenden werden vier mögliche Wege beschrieben:

- Die Komponente liest nacheinander die in der Chipkarte gespeicherten Elektronischen Tickets und zeigt diese in geeigneter Weise am Display an. Der Kontrolleur kann über Eingabetasten von einem zum nächsten Ticket „weiter blättern“, bis er ein geeignetes Ticket gefunden hat bzw. bis keine weiteren Tickets mehr in der Chipkarte gespeichert sind. Für diesen Weg müssen keine speziellen Daten in dem Kontrollgerät gespeichert bzw. verwaltet werden. Die Daten eines Elektronischen Tickets müssen nicht durch diese Komponente interpretiert werden.
- Wie vorher, jedoch werden nur die Elektronischen Tickets dem Kontrolleur angezeigt, bei denen der Verfallszeitpunkt (siehe [6] und [9]) noch nicht überschritten wurde. Für diesen Weg müssen keine speziellen Daten in dem Kontrollgerät gespeichert bzw. verwaltet werden. Die VRR-spezifischen Daten der Elektronischen Tickets müssen nicht durch diese Komponente interpretiert werden.
- Wie vorher, jedoch werden nur die Elektronischen Tickets dem Kontrolleur angezeigt, die durch bestimmte Verkehrsunternehmen erzeugt (gespeichert) wurden. Dazu muss eine Liste von möglichen Betreiber-IDs der Verkehrsunternehmen in dem Kontrollgerät gespeichert werden. Die VRR-spezifischen Daten der Elektronischen Tickets müssen nicht durch diese Komponente interpretiert werden.
- Wie vorher, jedoch werden nur die Elektronischen Tickets dem Kontrolleur angezeigt, die einen bestimmten Tickettyp haben. Dazu muss in dem Gerät eine Liste von möglichen Tickettypen gespeichert werden. Die VRR-spezifischen Daten der Elektronischen Tickets müssen bezüglich des Tickettyps bereits durch diese Komponente ausgewertet werden.

Die ersten beiden Wege haben den Vorteil, dass in dem Kontrollgerät keine für diesen Arbeitsschritt spezifischen Daten gespeichert werden müssen. Der Nachteil ist allerdings, dass der Kontrolleur „manuell“ durch alle in einer Chipkarte gespeicherten Tickets durchsuchen muss. In verschiedenen Kontrollgeräten können unterschiedliche Wege realisiert werden.

Wird ein geeignetes Elektronisches Ticket gefunden, muss es „kryptographisch überprüft“ werden. Dazu muss die Komponente auf das Sicherheitsmodul (SAM) zugreifen. Durch diese Überprüfung wird sichergestellt, dass die gelesenen Ticketdaten aus einer korrekten Chipkarte stammen und bei dem Lesen nicht verfälscht wurden. Ist die Überprüfung negativ, muss dies auf dem Display angezeigt werden und es muss ein entsprechender Eintrag in der Ausgabedatei gespeichert werden. Dieser Eintrag muss mindestens die Identifikationsdaten der Chipkarte und die Identifikationsdaten des SAM enthalten. Die Bearbeitung der Chipkarte muss in diesem Fall abgebrochen werden.

Ist die „kryptographische Überprüfung“ positiv, wird das gefundene Elektronische Ticket an den nächsten Arbeitsschritt übergeben. Es bleibt am Display angezeigt.

2.1.2 Überprüfe Gültigkeit ET

Diese Komponente unterstützt den Kontrolleur bei der Überprüfung, ob das gefundene Elektronische Ticket für die aktuelle Fahrt gültig ist. Bei der Überprüfung des Tickets wird zwischen der zeitlichen und der räumlichen Gültigkeit unterschieden. Diese Überprüfung kann nicht in jedem Fall mit absoluter Sicherheit alleine durch das Kontrollgerät durchgeführt werden. In einigen Fällen ist eine manuelle Entscheidung des Kontrolleurs notwendig.

Die genauen Vorschriften für die Überprüfung von Elektronischen Tickets werden in einem besonderen VRR-Dokument (EFM-Daten) beschrieben.

Verläuft die Überprüfung in dieser Komponente negativ, muss überprüft werden, ob in der Chipkarte noch weitere geeignete Elektronische Tickets vorhanden sind oder nicht.

2.1.3 Überprüfe Einträge in Sperrlisten

In dieser Komponente wird überprüft, ob das zu kontrollierende Elektronische Ticket durch einen Eintrag in der Sperrliste gesperrt ist bzw. bereits vorher als gesperrt markiert wurde. Dazu sind die folgenden Tests durchzuführen:

1. Wurde das Elektronische Ticket bereits vorher als gesperrt markiert? Dies ist der Fall, falls der Entwertungszähler den Wert „FF“ (hex) statt „FE“ (hex) hat.
2. Wird ein einzelnes Ticket eines Verkehrsunternehmens gesperrt? Dies ist der Fall, falls in der Sperrliste ein entsprechender Eintrag (Typ „FAHRSCHEINSPERRUNG“) existiert.
3. Wurde das VRR-Ticket mit der Hilfe eines gesperrten Sicherheitsmoduls (SAM) gespeichert? Dies ist der Fall, falls in der Sperrliste ein Eintrag (Typ „TERMINALSPERRUNG“) existiert, in dem die Terminalnummer identisch ist mit der in dem Elektronischen Ticket gespeicherten SAM-ID und das Anfangsdatum der Sperrung in dem Eintrag vor und (sofern schon vorhanden) das Enddatum der Sperrung in dem Eintrag nach dem Ausgabezeitpunkt des Elektronischen Tickets liegt.

Siehe [9] für Informationen über den Aufbau eines Elektronischen Tickets und [10] für Informationen über den Aufbau der Einträge in der Sperrliste.

Sind alle durchgeführten Tests negativ, ist die Überprüfung abgeschlossen und das Elektronische Ticket wird an den nächsten Arbeitsschritt weitergegeben.

Ist einer der Tests positiv, ist das Elektronische Ticket gesperrt.

Der Kontrolleur muss über das Display in geeigneter Weise über eine erkannte Sperrung informiert werden.

Ist der Test 1 positiv, ist die Bearbeitung des Elektronischen Tickets abgeschlossen. In diesem Fall muss überprüft werden, ob in der Chipkarte noch weitere geeignete Elektronische Tickets vorhanden sind oder nicht.

Ist einer der Tests 2. oder 3. positiv, muss das Elektronische Ticket an die nächste Komponente zum markieren weitergegeben werden.

2.1.4 Markiere ET

Diese Komponente markiert das Elektronische Ticket als gesperrt. Dazu muss der Entwertungszähler in dem Elektronischen Ticket von „FE“ (hex) auf „FF“ (hex) gesetzt werden (siehe dazu [9]). Dies geschieht z.B. mit der Funktion „Entwerten eines Elektronischen Fahrscheins“ der Zusatzanwendung „Elektronischer Fahrschein“ der ZKA-GeldKarte (siehe [6] und [7]).

Das Markieren eines Elektronischen Tickets wird automatisch ausgeführt. Der Kontrolleur muß diesen Vorgang nicht vorher über eine Eingabe bestätigen.

Die Komponente muss für seine Aufgaben Zugriff über eine Chipkontaktiereinheit auf den Inhalt der Chipkarte und einen Zugriff auf das Sicherheitsmodul (SAM) haben.

Über den Ausgang des Markierens muss ein entsprechender Eintrag für die Ausgabedatei erzeugt werden.

Der Kontrolleur muss über das Display über den Ausgang des Markierens in geeigneter Weise informiert werden.

Die Bearbeitung des Elektronischen Tickets ist hiermit abgeschlossen. Es muss überprüft werden, ob in der Chipkarte noch weitere geeignete Elektronische Tickets vorhanden sind oder nicht.

2.1.5 Uhr/Datum

Das Kontrollgerät muss eine Komponente haben, die die anderen Komponenten mit der aktuellen Zeit und dem Tagesdatum versorgt.

2.1.6 Eingabe Ticketwahl und Standortdaten

Das Kontrollgerät benötigt eine Eingabemöglichkeit für den Kontrolleur. Im Rahmen der Überprüfung eines Elektronischen Tickets muss ein Kontrolleur dabei mindestens die folgenden Eingaben machen können:

- Bei dem Suchen eines geeigneten Elektronischen Tickets in einer Chipkarte muss der Kontrolleur zwischen den einzelnen in der Chipkarte gespeicherten Tickets "vorblättern" können. Optional kann auch die Möglichkeit eines „Rückblätterns“ angeboten werden.
- Soll durch das Kontrollgerät eine Überprüfung der räumlichen Gültigkeit eines Elektronischen Tickets unterstützt werden, muss der Kontrolleur die Möglichkeit haben, Informationen über die aktuelle Fahrt (Wabenummer, Linienummer, Richtung) einzugeben.
- Gegebenenfalls müssen manuelle Eingriffe bei der Überprüfung der Gültigkeit möglich sein.

2.1.7 Sicherheitsmodul (SAM)

Für die „kryptographische Überprüfung“ bzw. das Markieren eines Elektronischen Tickets müssen kryptographisch abgesicherte Daten überprüft bzw. erzeugt werden. Die dazu notwendigen Schlüssel sind in einem Sicherheitsmodul gespeichert. Die für die kryptographische Absicherung der Daten durchzuführenden Berechnungen finden ebenfalls im wesentlichen in dem Sicherheitsmodul statt. Ein Sicherheitsmodul ist dabei ebenfalls als Chipkarte (Plug-In, SIM-Format) realisiert.

In dem Sicherheitsmodul ist die Betreiber-ID des Verkehrsunternehmens manipulationssicher gespeichert, welches das Kontrollgerät betreibt.

2.1.8 Datei Ticket-/Tarifdaten

In dieser Datei werden Informationen gespeichert, die als Grundlage für die Überprüfung von Elektronischen Tickets benötigt werden. Dazu gehören:

- Eine Liste aller Betreiber-IDs der Verkehrsunternehmen, die überprüft werden sollen. Diese Liste wird benötigt, falls die Komponente „Lese Kartendaten und Elektronische Tickets“ bei der Suche eines geeigneten Tickets in einer Chipkarte eine entsprechende automatische Vorauswahl durchführen soll.
- Eine Liste aller Tickettypen. Diese Liste wird benötigt, falls die Komponente „Lese Kartendaten und Elektronische Tickets“ bei der Suche eines geeigneten Tickets in einer Chipkarte eine entsprechende automatische Vorauswahl durchführen soll.
- Listen mit Tarifdaten, die für die Überprüfung der räumlichen Gültigkeit eines Elektronischen Tickets benötigt werden.

Der Aufbau der Listen in dieser Datei kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

Das Kontrollgerät muss eine geeignete Schnittstelle zur Verfügung stellen, um diese Datei von einem Hintergrundsystem zu laden.

2.1.9 Datei Sperrlisten

In dieser Datei werden die Einträge über Sperrungen von Karten bzw. SAMs (Terminalspernung) gespeichert. Die einzelnen Einträge in dieser Datei sind gemäss [10] aufzubauen.

Das Kontrollgerät muss eine geeignete Schnittstelle zur Verfügung stellen, um diese Datei von einem Hintergrundsystem zu laden.

2.1.10 Display

Das Kontrollgerät benötigt ein Display, auf dem Elektronische Tickets in geeigneter Weise dem Kontrolleur angezeigt werden. Dabei werden auf diesem Display alle Daten eines Elektronischen Tickets angezeigt und nicht nur die Daten, die auch durch einen Taschenkartenleser anzeigbar sind.

Über das Display muss der Kontrolleur in geeigneter Weise über die durchgeführten Arbeitsschritte und ihren Ergebnissen informiert werden.

Der genaue Aufbau der Anzeige der Daten kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

2.1.11 Ausgabedatei

Werden bei der Überprüfung eines Elektronischen Tickets Probleme erkannt, die für die Sicherheit des Gesamtsystems relevant sein können, müssen darüber Informationen an das Hintergrundsystem des Verkehrsunternehmens geleitet werden. Solche Probleme sind:

- Die kryptographische Überprüfung eines Elektronischen Tickets war negativ.
- Ein Elektronisches Ticket wurde durch das Kontrollgerät markiert.

Über jeden dieser Fälle muss ein Eintrag in der Ausgabedatei erzeugt werden. Der Aufbau dieser Einträge kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

Das Kontrollgerät muss eine geeignete Schnittstelle zur Verfügung stellen, um diese Datei an ein Hintergrundsystem zu übermitteln.

2.2 Vorgaben für einzelne Komponenten

2.2.1 Chipkarten

Als Chipkarten für die Speicherung der Elektronischen Tickets des VRR werden ZKA-GeldKarten der deutschen Kreditwirtschaft und die PayCard der Firma card.etc eingesetzt. Zugriffe auf den Chip müssen über das Protokoll T=1 gemäß ISO 7816 erfolgen. Die benötigten Grundlagen des ZKA-Betriebssystems sind in [2] beschrieben.

Jede Chipkarte mit einem Elektronischen Ticket muss im gesamten System des VRR eindeutig identifizierbar sein. Hierfür wird die durch den Kartenherausgeber vergebene eindeutige Nummer (10 Byte) der Chipkarte verwendet. Diese steht in der Chipkarte in einer Datei (z.B. EF_ID im Verzeichnis MF der ZKA-GeldKarte, der Inhalt dieser Datei ist in [8] beschrieben).

Für den Aufbau der Daten, die für ein Elektronisches Ticket in einer Chipkarte gespeichert werden, gelten verbundweite Richtlinien des VRR. Siehe dazu [9].

Für die Speicherung eines Elektronischen Tickets des VRR in der ZKA-Geldkarte der Kreditwirtschaft wird die Zusatzanwendung „Elektronischer Fahrschein“ verwendet. Die zu berücksichtigenden Strukturen für diese Zusatzanwendung in den ZKA-GeldKarten sind in [6] beschrieben. Bei den Zugriffen auf diese Zusatzanwendung in den ZKA-Chipkarten sind die Vorgaben aus [7] einzuhalten.

2.2.2 Umgang mit Sicherheitsmodulen

Damit ein Kontrollgerät ein Elektronisches Ticket in einer Chipkarte markieren bzw. kryptographisch überprüfen kann, muss es ein entsprechendes Sicherheitsmodul haben.

Der Aufbau des derzeit verfügbaren Sicherheitsmoduls der Kreditwirtschaft ist in [5] beschrieben. Vorgaben für die Abläufe bei den Zugriffen auf dieses Sicherheitsmodul stehen in [7]. Sicherheitsmodule sind als Chipkarte (Plug-In, SIM-Format) realisiert. Der Zugriff geschieht ebenfalls über das Protokoll T=1 gemäß ISO 7816.

Anmerkung: Zur Zeit existiert das Sicherheitsmodul der Kreditwirtschaft für die Zusatzanwendung „Elektronischer Fahrschein“ nur als Erweiterung der Händlerkarte des ZKA-GeldKarte-Systems. Es wird jedoch an einer neuen Version des Sicherheitsmoduls gearbeitet, bei der dann das Sicherheitsmodul auch getrennt von einer Händlerkarte existieren kann. Im Rahmen des Systems des VRR soll diese neue Version des Sicherheitsmoduls zum Einsatz kommen. Dadurch wird es zu Erweiterungen der Vorgaben aus [5] und [7] kommen, deren Spezifikation zur Zeit noch nicht vorliegt.

In einem Sicherheitsmodul wird bei der Produktion eine Betreiber-ID eingetragen. Dabei ist die Betreiber-ID des Verkehrsunternehmens zu verwenden, welches das Kontrollgerät betreibt, in das das Sicherheitsmodul eingesetzt werden soll.

Sicherheitsmodule haben eine begrenzte Gültigkeitsdauer. Sie müssen daher so in die Geräte eingesetzt werden, dass sie nach Ablauf ihrer Gültigkeit einfach austauschbar sind. Das Kontrollgerät muss über das Display über den nächsten notwendigen Austausch des Sicherheitsmoduls informieren.

Der Verlust eines Sicherheitsmoduls während seiner Gültigkeit ist ein Sicherheitsrisiko, da mit dem Sicherheitsmodul in diesem Fall nicht autorisierte elektronische Tickets in Chipkarten gespeichert werden können. Um dieses Risiko zu verringern, sollten Sicherheitsmodule für ein Kontrollgerät so konfiguriert werden, dass mit ihnen nur das Markieren und das kryptographische Überprüfen eines elektronischen Tickets unterstützt werden kann.

Jedes Sicherheitsmodul muss eindeutig identifizierbar sein. Hierfür wird die durch den Kartenherausgeber vergebene eindeutige Nummer (10 Byte) des Sicherheitsmoduls verwendet. Diese steht in dem Sicherheitsmodul in einer Datei (z.B. EF_ID im Verzeichnis MF des SAMS der Kreditwirtschaft).

Bei der Konfiguration des Sicherheitsmoduls müssen verbundweite Vorgaben eingehalten werden. Der VRR hat dafür in [9] Richtlinien aufgestellt. Die Konfiguration muss dabei im wesentlichen vor der Produktion bereits bei der Bestellung des Sicherheitsmoduls festgelegt werden.

2.2.3 Datei für Ticket-/Tarifdaten

Der Aufbau dieser Datei kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

2.2.4 Datei für Sperrlisten

Der Aufbau der Einträge in dieser Datei muss [10] berücksichtigen.

2.2.5 Ausgabedatei

Der Aufbau dieser Dateien kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

Die Ausgabedatei muss für jeden Eintrag mindestens die folgende Information enthalten:

- Nummer der beteiligten Chipkarte.
- Nummer des Sicherheitsmoduls des Kontrollgerätes.
- Information über den Grund für den Eintrag.

2.2.6 Eingabe Ticketwahl und Standortdaten

Die Gestaltung der Eingabemöglichkeit kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

2.2.7 Display

Die Gestaltung der Anzeige eines Elektronischen Tickets und zusätzlicher Informationen auf dem Display kann durch den jeweiligen Betreiber des Kontrollgerätes festgelegt werden.

2.2.8 Lese Kartendaten und Elektronisches Ticket, Markiere ET

Hier sind die Vorgaben für die Bearbeitung einer Chipkarte bei einem Zugriff auf den Chip einzuhalten. Siehe dazu den entsprechenden Abschnitt oben.

3 Referenzen

- [1] Elektronische Tickets auf Chipkarten des deutschen Kreditgewerbes, Version 1.1, November 1999, VDV-Mitteilung
- [2] Schnittstellenspezifikation für die ZKA-Chipkarten, Datenstrukturen und Kommandos, Version 4.1, 01.07.1999, ZKA
- [3] Schnittstellenspezifikation für die ec-Karte mit Chip, Zusatzanwendungen, Elektronischer Fahrschein, Version 3.0, 02.04.1998, ZKA
- [4] Schnittstellenspezifikation für die ec-Karte mit Chip, ÖPV-Systeme, Version 1.0, 03.12.1998, ZKA
- [5] Schnittstellenspezifikation für die ec-Karte mit Chip, GeldKarte, Erweiterung der Händlerkarte Typ 1, Version 1.1, 20.07.1999, ZKA
- [6] Schnittstellenspezifikation für die ZKA-Chipkarte, Zusatzanwendungen, Applikation Elektronischer Fahrschein, Version 4.0, 10.12.1999, ZKA
- [7] Schnittstellenspezifikation für die ZKA-Chipkarte, Zusatzanwendungen, ÖPV-System, Version 2.0 (Entwurf), 04.02.2000, ZKA
- [8] Schnittstellenspezifikation für die ec-Karte mit Chip, Dateien des MF, Version 4.0, 06.09.1999, ZKA
- [9] Einsatz von Chipkarten und Sicherheitsmodulen, VRR-Richtlinie, Version 1.4, 23.01.2002, VRR GmbH
- [10] Austausch von Daten zwischen den Verkehrsunternehmen und dem Verbund, VRR-Richtlinie, Version 1.10, 27.08.2004, VRR GmbH