Verkehrsverbund Rhein-Ruhr
Elektronisches Fahrgeldmanagement

Einsatz von
Chipkarten und Sicherheitsmodulen

Version 1_4
Stand: 23.01.02

Verkehrsverbund Rhein-Ruhr GmbH

0 Allgemeines

0.1 Inhaltsverzeichnis

Kapitel **Seite**

0 Allgemeines ... 2
0.1 Inhaltsverzeichnis ... 2
0.2 Änderungsverzeichnis ... 2
1 Vorbemerkungen ... 3
2 Richtlinien für die Nutzung von Chipkarten ... 3
2.1 Eindeutige Identifizierung ... 3
2.2 Datenmodell für ein Elektronisches Ticket ... 3
2.2.1 Felder für eine Anzeige im Taschenkartenleser ... 4
2.2.2 Felder ohne Anzeige im Taschenkartenleser ... 5
2.3 Speicherung eines Elektronischen Tickets in einer Chipkarte ... 6
2.4 Vorgaben für die optische Gestaltung der Chipkarten ... 9
3 Richtlinien für die Sicherheitsmodule ... 9
3.1 Eindeutige Identifizierung ... 9
3.2 Konfiguration von Sicherheitsmodulen ... 10
4 Anhang ... 11
4.1 Referenzen ... 11
4.2 Allgemeines zu Chipkarten ... 11
4.2.1 Bestellung/Produktion von Chipkarten ... 11
4.2.2 Eindeutige Identität einer Chipkarte ... 12
4.2.3 Eigenschaften einer Chipkarte bei ihrer Ausgabe ... 12
4.2.4 Anmerkungen zu den Versionen des ZKA-Betriebssystems ... 12
4.2.5 Anmerkungen zu der Währung einer Chipkarte ... 13
4.3 Funktionen für einen Zugriff auf ein Elektronisches Ticket ... 13
4.4 Allgemeines zu den Sicherheitsmodulen ... 15

0.2 Änderungsverzeichnis

Die Version 1_4 unterscheidet sich von der Version 1_3 durch die folgenden Änderungen:

Allgemein:	Titel und Inhalt sind 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 2.2.1 und 2.3, Ticketdaten:	Die Kapitel wurden hinsichtlich der Länge des Feldes Preisstufe und des neuen, im VRR nicht benutzten Feldes Bemerkungen überarbeitet, um eine mit dem VRS identische Struktur der Ticketdaten zu ermöglichen. Das Feld Name wurde auf eine größere maximale Länge erweitert, so dass keine komplizierten Regeln zur Abkürzung eines Namens erforderlich sind. Außerdem wurde die Beschreibung des Inhaltes in beiden Kapiteln verbessert.
Kapitel 4.5 (alt):	Das Kapitel entfällt und wird durch ein Dokument mit den jeweils aktuellen EFM-Daten ersetzt.

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 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.

In dem vorliegenden Dokument werden Richtlinien festgelegt, die für den Einsatz derartiger Chipkarten und der entsprechenden Sicherheitsmodule im Rahmen des Elektronischen Tickets des VRR verbindlich eingehalten werden müssen. In einem Anhang werden Erläuterungen gegeben, die die dabei benötigten Grundlagen der Chipkarten und der Zusatzanwendung für das Elektronisches Ticket beschreiben.

2 Richtlinien für die Nutzung von Chipkarten

Für die Speicherung der Elektronischen Tickets des VRR sollen auf Kundenseite als erstes ZKA-GeldKarten der Kreditwirtschaft und die PayCard der Firma card.etc zum Einsatz kommen. Diese bieten für die Speicherung der Elektronischen Tickets eine Zusatzanwendung nach [3] und [6] bzw. [9] an. In diesem Kapitel wird festgelegt, wie die Chipkarten mit dieser Zusatzanwendung im Rahmen des Elektronischen Tickets des VRR eingesetzt werden müssen.

2.1 Eindeutige Identifizierung

Jede Chipkarte, in die ein Elektronisches Ticket des VRR gespeichert wird, muss durch eine eindeutige Nummer im gesamten System identifizierbar sein. Diese Nummer wird für die Verwaltung der Elektronischen Tickets in Hintergrundsystemen und für die Einträge in Sperrlisten verwendet.

Im Rahmen des Elektronischen Tickets des VRR wird für diese Zwecke die weltweit eindeutige Nummer derartiger Chipkarten verwendet. Diese Nummer wird bei der Kartenproduktion vergeben und kann aus der Chipkarte einfach ausgelesen werden. Siehe dazu auch Abschnitt 4.2.2.

2.2 Datenmodell für ein Elektronisches Ticket

Ein Elektronisches Ticket des VRR besteht aus verschiedenen Feldern. In diesem Abschnitt wird (aus der Sicht der Anwendung) der Inhalt und die Codierung der einzelnen Felder beschrieben, wie sie bei dem Elektronischen Ticket des VRR zum Einsatz kommen. Die Umsetzung der Felder zu dem konkreten Aufbau eines Elektronischen Tickets, wie er (aus technischer Sicht) in einer Chipkarte gespeichert werden muss, wird im nächsten Abschnitt beschrieben.

Bei den Feldern wird zwischen solchen unterschieden, deren Inhalt dem Karteninhaber durch einen Taschenkartenleser angezeigt werden können, und solchen, die nur an den Kontrollgeräten bzw. den Verkaufsstellen angezeigt werden können.

Die Codierung einiger Felder ist durch [1] bereits festgelegt, bei anderen Feldern kann die Codierung durch den VRR festgelegt werden. Beide Arten von Feldern werden in diesem Dokument beschrieben.

Nicht jedes Feld ist Bestandteil von jedem Elektronischen Ticket.

2.2.1 Felder für eine Anzeige im Taschenkartenleser

Der Inhalt der folgenden Felder kann durch einen Taschenkartenleser angezeigt werden.

Feld	Maximale Länge in Byte	Codierung	Beispiel	Feste Vorgabe durch [1]	Anzeige wie gespeichert
Tickettyp	15	ASCII	'T_1000_9h_Abo'	nein	ja
Preisstufe	29	ASCII	'A_010_110'	nein	ja
Gültigkeit	13	ASCII	'010100-310600'	nein	ja
Zusätze	8	ASCII	'1K_IR_XX'	nein	ja
Name	80 – Länge (Tickettyp) – Länge (Preisstufe) – Länge (Gültigkeit) – Länge (Zusätze) – Länge (Bemerkungen)	ASCII	'Musterfrau_Heike'	nein	ja
Bemerkungen	0	ASCII		nein	ja
Erstellungszeitpunkt	6	BCD	'200001010935'	ja	nein
Fahrpreis	4	BCD	'00001250'	ja	nein
Zähler (Entwertung, Blacklist-Flag)	1	Hex	'FE'	ja	nein

Anmerkungen:

1. Die Anschriften von Karteninhabern, Schulen bzw. Universitäten sollen nicht in einem Elektronischen Ticket gespeichert werden.

2. Innerhalb eines Feldes dürfen keine „Blanks“ vorkommen. Falls für die Lesbarkeit des Inhalts eines Feldes eine Trennung von Teilen notwendig ist, geschieht dies durch einen Unterstrich. Codiert wird der Unterstrich durch „5F“ (Hex).

3. Die Preisstufe besteht aus einem Zeichen „A“, „B“ bzw. „C“ gefolgt von maximal drei Nummern für Waben bzw. Tarifgebiet. Jede Nummer ist maximal drei Ziffern lang. Die einzelnen Angaben werden durch einen Unterstrich getrennt. Die dritte Nummer für eine Wabe existiert nur bei EinzelTicket und TagesTicket.

4. Die Gültigkeit wird „taggenau" angegeben.

5. Das Feld für die Zusätze kann maximal drei Zusätze enthalten, wobei jeder Zusatz durch zwei Zeichen codiert wird. Die einzelnen Angaben werden durch einen Unterstrich getrennt. Folgende Zusätze sind zur Zeit für die Codierung vorgesehen: „1K“ = 1. Klasse, „IR“ = InterRegio-Zuschlag. Die Codierung von weiteren Zusätzen wird in der Zukunft entschieden. (Anmerkung: Der Zusatz „Kind“ ist im Tickettyp codiert).

6. Die maximal mögliche Länge des Feldes Name ergibt sich aus dem angegebenen Wert abzüglich der konkreten Länge der Felder Tickettyp, Preisstufe, Gültigkeit, Zusätze und Bemerkungen.

7. Das Feld Bemerkungen wird z.Z. nicht benutzt.

8. Die Inhalte der Felder Tickettyp, Preisstufe, Gültigkeit, Zusätze, Name und Bemerkungen werden durch den Taschenkartenleser wie in dem Ticket codiert angezeigt.

9. Die Angabe von Erstellungszeitpunkt, Preis und Zähler (Anzahl der möglichen Entwertungen) durch den Taschenkartenleser ist eine Vorgabe durch [1]. Die Daten werden bei der Anzeige durch den Taschenkartenleser in eine lesbare Form umgewandelt.

10. Die Währung für den Fahrpreis richtet sich nach der Währung der Chipkarte, in der das Elektronische Ticket gespeichert wird. Siehe dazu 4.2.5.

11. Elektronische Tickets, die durch den Kunden im Rahmen eines Abonnements erworben wurden, erhalten den Fahrpreis „00000000“.

12. Für Tickets des VRR, die als Elektronische Tickets in einer Chipkarte gespeichert werden, sind keine Entwertungen vorgesehen. Der (Entwertungs-)Zähler wird stattdessen verwendet, um ein in einer Sperrliste entdecktes Ticket in der Chipkarte durch den Kontrolleur zu markieren. Bei der Erstellung eines Tickets erhält der Zähler den Wert „FE“ (eine Entwertung ist möglich, d.h. das Ticket ist OK). Entdeckt ein Kontrolleur ein Ticket in einer Sperrliste, „entwertet" er das Ticket, d.h. der Zähler erhält den Wert „FF“ (keine Entwertung mehr möglich, d.h. das Ticket ist nicht mehr OK). Werden im Rahmen von Test/Wartung eines Gerätes Elektronische Mustertickets erzeugt, wird der Entwertungszähler bei der Erzeugung dieser Mustertickets direkt auf „FF“ (d.h. Ticket nicht gültig) gesetzt.

2.2.2 Felder ohne Anzeige im Taschenkartenleser

Der Inhalt der folgenden Felder kann **nicht** durch einen Taschenkartenleser angezeigt werden (wohl aber durch ein Kontrollgerät).

Feld	Länge in Byte	Codierung	Beispiel	Feste Vorgabe durch [1]
Verfallszeitpunkt	6	BCD	'200012312359'	ja
Betreiber-ID	2	Hex	'F3 12'	ja
Servicekennung	3	Hex	'FF A1 25'	ja
SAM-ID	10	BCD	'11 22 ... 99 0D'	nein, noch nicht
Laufende Nummer	3	Hex	'FF A1 25'	nein, noch nicht
Haltestelle	4	Hex	'A1 B2 C3 D4'	nein
Geschlecht	1	ASCII	'W' bzw. 'M'	nein
Geburtstag	3	BCD	'191058'	nein

Anmerkungen:

1. Der Verfallszeitpunkt muss nach [1] Bestandteil von jedem Elektronischen Ticket sein. Er gibt an, ab wann ein Elektronisches Ticket ohne weitere Einschränkung in der Chipkarte überschrieben werden kann.

2. Die Betreiber-ID kennzeichnet den Verantwortlichen, der das Elektronische Ticket in eine Chipkarte geschrieben hat. Sie ist zwei Byte lang und wird vom VDV vergeben. Für den Bereich des VRR erhält jedes Verkehrsunternehmen eine eigene Betreiber-ID. Wenn andere Stellen Elektronische Tickets mit einer eigenen Betreiber-ID ausgeben sollen, müssen diese über eine Vertriebskomponente (Initialisierungsgerät, Front-End- und Back-Office-System) verfügen.

3. Die Servicekennung ist drei Byte lang und muss ebenfalls nach [1] Bestandteil von jedem Elektronischen Ticket sein. Jeder Tickettyp des VRR besitzt eine eindeutige Servicekennung, die in das Elektronische Ticket eingetragen wird.

4. Die SAM-ID kennzeichnet eindeutig das Sicherheitsmodul, das an der Speicherung des Elektronischen Tickets in eine Chipkarte beteiligt war. Sie wird durch das Sicherheitsmodul selbst im Elektronischen Ticket eingetragen. Wenn das Sicherheitsmodul dies jedoch nicht leisten kann, muss die SAM-ID bei der Erstellung durch das Initialisierungsgerät aus dem Sicherheitsmodul ausgelesen und im Elektronischen Ticket abgelegt werden. Damit bei den verschiedenen Sicherheitsmodulen keine unterschiedlichen Verhaltensweisen des Initialisierungsgerätes notwendig werden, wird die SAM-ID auf jeden Fall erst einmal durch das Initialisierungsgerät eingetragen. Das Hintergrundsystem trägt an dieser Stelle erst einmal als Platzhalter bei der Ticketerstellung „00 00 00 00 00 00 00 00 00 00“ ein.

5. Die laufende Nummer stellt eine zusätzliche Sicherheitsfunktion dar und wird durch das Sicherheitsmodul selbst bei der Erstellung eines Tickets eingetragen. Sicherheitsmodule, die über diese Funktion verfügen, beginnen mit einer 1 beim ersten Ticketeintrag und zählen diese Nummer dann selbst hoch. Das Hintergrundsystem trägt an dieser Stelle erst einmal als Platzhalter bei der Ticketerstellung „00 00 00“ ein.

6. Die Haltestelle wird in vier Byte hexadezimal codiert. Die genaue Codierung der Haltestellen muss noch entschieden werden. Enthält ein Elektronisches Ticket keine Angaben über eine Haltestelle, wird „00 00 00 00“ eingetragen.

7. Die Felder Geschlecht und Geburtstag existieren nur in Elektronischen Tickets, die auch das Feld Name enthalten.

8. In dem Feld Geschlecht wird weiblich durch „W“ (ASCII) und männlich durch „M“ (ASCII) codiert.

2.3 Speicherung eines Elektronischen Tickets in einer Chipkarte

Technisch gesehen werden innerhalb einer Chipkarte Elektronische Tickets in Records gespeichert. Je nach Speicherplatzbedarf kann ein Elektronisches Ticket dabei in einem oder auch in mehreren Records gespeichert werden.

Eine Chipkarte bietet heute 10 Records für die Speicherung von Elektronischen Tickets. Bei ZKA-GeldKarten mit dem neuen ZKA-Betriebssystem (Version 3.0) und bei der PayCard hat ein Record eine variable Länge mit einer maximalen Länge von 80 Byte. Im folgenden wird immer davon ausgegangen, dass nur diese Chipkarten eingesetzt werden. In diesem Falle benötigen die Elektronischen Tickets des VRR zur Zeit im Regelfall zwei Records. Dies kann sich jedoch in Zukunft ändern, welches bei der Programmierung der entsprechenden Terminals bzw. der Vertriebskomponenten zu berücksichtigen ist.

Für den Aufbau der Daten, die in einem Record gespeichert werden, gibt es feste Vorgaben aus der Spezifikation [1]. Die Daten sind TLV-codiert („TAG-Length-Value"). Im folgenden wird ein Überblick über den Aufbau der Recorddaten gegeben, wie sie für die Elektronischen

Tickets des VRR benötigt werden. Die Abläufe für die Speicherung eines Records in einer Chipkarte sind in [4] und [7] bzw. [8] und [9] beschrieben.

Kann ein Elektronisches Ticket in einem einzelnen Record gespeichert werden, hat dieser **Einzelrecord** den folgenden Aufbau:

TAG	Length	TAG	Length	Value	TAG	Length	Value	TAG	Length	Value	TAG	Length	Value
'E2'	L1	'C2'	'01'	RN	'C4'	'0B'	KD	'C5'	'0C'	HD	'C6'	L2	TD

Benötigt ein Elektronisches Ticket zwei (oder mehr) Records, wird er in einem Startrecord und einem (oder mehreren) Folgerecords gespeichert. Der letzte Folgerecord wird dabei auch als Schlussrecord bezeichnet. Diese haben den folgenden Aufbau:

Startrecord

TAG	Length	TAG	Length	Value	TAG	Length	Value	TAG	Length	Value	TAG	Length	Value
'E2'	L1	'C2'	'03'	RKD	'C4'	'0B'	KD	'C5'	'0C'	HD	'C6'	L2	TD

Folgerecord/Schlussrecord

TAG	Length	TAG	Length	Value	TAG	Length	Value	TAG	Length	Value
'E2'	L1	'C2'	'03'	RKD	'C4'	'06'	KD	'C6'	L2	TD

Die Abkürzungen bedeuten:

L1: Länge der folgenden Daten bis zum Recordende. L1 kann maximal den Wert 78 haben.

RN: Nummer des Records.

RKD: Recordkontrolldaten.

Bei einem Startrecord: „00 RN RNF“ mit RNF = Nummer des nächsten Folgerecords.

Bei einem Folgerecord: „RNV RN RNF“ mit RNV/RNF = Nummer des vorhergehenden/nächsten Folgerecords.

Bei einem Schlussrecords: „RNV RN FF“ mit RNV = Nummer des vorhergehenden Folgerecords.

KD: Kennungsdaten.

Bei einem Einzelrecord und einem Startrecord enthalten die 11 Byte die Inhalte der Felder Verfallszeitpunkt (6 Byte), Betreiber-ID (2 Byte) und Servicekennung (3 Byte).

Bei einem Folge-/Schlussrecord enthalten die 6 Byte nur den Inhalt des Feldes Verfallszeitpunkt.

Für die Beschreibung der Felder siehe das Datenmodell.

HD: Headerdaten. Nur bei Einzelrecord und Startrecord. Die 12 Byte enthalten die Inhalte der Felder Fahrpreis (4 Byte), Erstellungszeitpunkt (6 Byte) und Zähler/Entwertung (1

Byte) gefolgt von einem Byte „00“, bei dem es sich um das in [1] beschriebene Feld ZD-Info mit der für den VRR z.Z. definierten Länge handelt.

L2: Länge der folgenden Ticketdaten. Bei einer Recordlänge von 80 Byte gelten die folgenden Maximalwerte für L2:

Einzelrecord: L2 = 46, Startrecord: L2 = 44, Folge-/Schlussrecord: L2 = 63.

TD: Ticketdaten. Die Ticketdaten enthalten die Inhalte der folgenden Felder:

Feld Tickettyp	maximal 15 Byte	
Blank	1 Byte	
Feld Preisstufe	maximal 29 Byte	
Blank	1 Byte	
Feld Gültigkeit	maximal 13 Byte	
Blank	1 Byte	
Feld Zusätze	maximal 5 Byte	optional
Blank	1 Byte	
Feld Name	maximal 80 Byte – Länge (Tickettyp) – Länge (Preisstufe) – Länge (Gültigkeit) – Länge (Zusätze) – Länge (Bemerkungen)	optional
Blank	1 Byte	
Feld Bemerkungen	0 Byte	z.Z. nicht benutzt
Sonderzeichen '@'	1 Byte	
Feld Terminal-Nr.	10 Byte	
Feld Laufende Nummer	3 Byte	
Feld Haltestelle	4 Byte	
Feld Geschlecht	1 Byte	optional, nur falls Feld Name vorhanden
Feld Geburtstag	3 Byte	optional, nur falls Feld Name vorhanden

Die als optional gekennzeichneten Felder können in den Daten eines Elektronischen Tickets fehlen. Das Feld Bemerkungen wird z.Z. im VRR nicht benutzt. Die Felder vor dem Sonderzeichen „@“ werden jeweils durch ein Blank (Hex „20“) getrennt. Die Blanks werden auch für ein fehlendes (leeres) Feld eingetragen, so dass immer fünf Blanks vorhanden sind. Diese Blanks ermöglichen eine generell variable Länge der Felder vor dem Sonderzeichen „@“, was bei der Programmierung der entsprechenden Terminals bzw. der Vertriebskomponenten zu berücksichtigen ist. Der gesamte Inhalt der Ticketdaten vor dem Sonderzeichen „@'“ kann durch einen Taschenkartenleser angezeigt werden.

Sind die Ticketdaten für ein Elektronisches Ticket länger als 44 Byte, werden (mindestens) zwei Records für seine Speicherung benötigt. Die maximale Länge der Ticketdaten beim VRR (inklusive der eingefügten Blanks und dem Sonderzeichen „@'“) beträgt z.Z. maximal 107 Byte, die zuzüglich der übrigen Daten in zwei Records untergebracht werden können.

Das Sonderzeichen „@“, die SAM-ID und die laufende Nummer müssen sich in einem Record befinden. Sie dürfen nicht auf zwei Records verteilt werden. D.h., sind die Ticketdaten vor dem Sonderzeichen „@“ inklusive der Blanks länger als 30 Byte, müssen das Sonderzeichen „@“, die SAM-ID und die laufende Nummer im nächsten Record untergebracht werden.

2.4 Vorgaben für die optische Gestaltung der Chipkarten

Bei der optischen Gestaltung der Chipkarten muss unterschieden werden zwischen Kundenkarten, die durch ein Kreditinstitut ausgegeben werden (z.B. ec-Karten, Bankkundenkarten) und sogenannten „White-Cards", die im Sinne eines Co-Brandings gemeinsam von einem Verkehrsunternehmen und einem Kreditinstitut oder ähnlichen Organisation ausgegeben werden. Siehe dazu auch Abschnitt 4.2.1.

Die optische Gestaltung von Chipkarten, die durch ein Kreditinstitut ausgegeben werden (z.B. ec-Karten, Bankkundenkarten), liegt alleine in der Verantwortung des Kreditinstituts. Im allgemeinen haben diese Chipkarten kein Logo, mit dem auf die Existenz des Elektronischen Tickets hingewiesen wird. Solche Chipkarten sollen für die Speicherung von Elektronischen Tickets des VRR erst nach der Übergangszeit ab Anfang 2003 zum Einsatz kommen.

Während der Übergangszeit für die Einführung des Elektronischen Tickets bis Ende 2002 sollen nur „White-Cards" zum Einsatz kommen. Die optische Gestaltung dieser Chipkarten kann gemeinsam von einem Verkehrsunternehmen und einem Kreditinstitut oder einer ähnlichen Organisation bestimmt werden. Im allgemeinen werden bei solchen Chipkarten die Vorderseite (d.h. die Seite, auf der der Chip sichtbar ist) durch das Kreditinstitut oder eine ähnlichen Organisation und die Rückseite durch das Verkehrsunternehmen gestaltet.

Für die Gestaltung gibt es eine einheitliche Vorgabe durch den VRR. Diese wird ergänzt durch das Logo des jeweiligen Verkehrsunternehmens.

Für die Übergangszeit sollen die für eine Kontrolle eines Elektronischen Tickets relevanten Daten auch auf der Chipkarte lesbar aufgedruckt werden. Dazu muss es auf der Chipkarte (Seite des Verkehrsunternehmens) ein Feld geben, das mehrfach bedruckt werden kann. Dieses Feld muss mindestens eine Kapazität von 4 Zeilen mit jeweils 70 Zeichen haben. Für die Realisierung und das Bedrucken dieses Feldes wird das Thermodruckverfahren eingesetzt.

3 Richtlinien für die Sicherheitsmodule

Für die Speicherung der Elektronischen Tickets des VRR in Chipkarten werden entsprechende Sicherheitsmodule benötigt. Für den Zugriff auf die Zusatzanwendung für das Elektronische Ticket muss dabei bei der Kreditwirtschaft das Sicherheitsmodul FSAM entsprechend [5] eingesetzt werden. Zur Zeit wird an der Spezifikation einer neuen Version für das FSAM gearbeitet, die für das Elektronische Ticket des VRR eingesetzt werden soll. Bei der PayCard muss das Sicherheitsmodul entsprechend [10] eingesetzt werden. In diesem Kapitel wird festgelegt, wie die Sicherheitsmodule im Rahmen des Elektronischen Tickets des VRR eingesetzt werden müssen.

3.1 Eindeutige Identifizierung

Jedes Sicherheitsmodul muss durch eine eindeutige Nummer im gesamten System identifizierbar sein. Diese Nummer wird für die Verwaltung der Sicherheitsmodule in Hintergrundsystemen und für die Einträge in Sperrlisten verwendet. Wird mit dem Sicherheitsmodul ein Elektronisches Ticket in einer Chipkarte gespeichert, wird diese Nummer des Sicherheits-

moduls in das Elektronische Ticket eingetragen. Siehe dazu das Datenmodell in Abschnitt 2.2.

Im Rahmen des Elektronischen Tickets des VRR wird für diese Zwecke die eindeutige Nummer des Sicherheitsmoduls verwendet. Diese Nummer wird bei der Produktion des Sicherheitsmoduls vergeben und kann aus dem Sicherheitsmodul einfach ausgelesen werden. Siehe dazu auch Abschnitt 4.4.

3.2 Konfiguration von Sicherheitsmodulen

Für die Sicherheitsmodule muss bei der Produktion eine Konfiguration festgelegt werden. Siehe Abschnitt 4.4 für die Einzelheiten. Im Rahmen der Elektronischen Tickets des VRR sind dabei die folgenden Richtlinien einzuhalten:

1. In jedes Sicherheitsmodul muss die Betreiber-ID des Verkehrsunternehmens eingesetzt werden, welches das Sicherheitsmodul in eines seiner Terminals einsetzt.

2. Das Speichern eines Elektronischen Tickets in eine Chipkarte ist nicht an einen Bezahlvorgang mit der gleichen Chipkarte gekoppelt.

3. Die Anzahl der ohne Bezahlvorgang durch ein Sicherheitsmodul speicherbaren Elektronischen Tickets sowie der maximale Einzelwert eines Tickets und die Summe der Werte aller Tickets muss durch das Verkehrsunternehmen festgelegt werden. Dabei ist auf einen Ausgleich zwischen der möglichst einfachen Administration des Sicherheitsmoduls und dem maximalen Schaden durch Mißbrauch bei dem Verlust eines Sicherheitsmoduls durch Diebstahl zu achten.

4. Die eindeutige Nummer eines Sicherheitsmoduls (10 Byte) muss in jedes Elektronische Ticket geschrieben werden, das mit dem Sicherheitsmodul in einer Chipkarte gespeichert wird.

5. Ein Sicherheitsmodul darf von seiner Konfiguration her nur die Funktionen ausführen können, die in dem Terminal benötigt werden, in welches das Sicherheitsmodul eingesetzt werden soll. Siehe dazu auch Abschnitt 4.3.

4 Anhang

4.1 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-Systeme, 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] Functional Specification of the PayCard on ISO Card Operating Systems, Version 3.1, 23.11.2001, card.etc AG

[10] PayCard, Security Application Module (SAM), Interface Specification, Version 3.1, 30.11.2001, card.etc AG

[11] Administrierung der PayCard-Sicherheitsmodule, VRR-Richtlinie, Version 1.0, 23.01.2002, VRR GmbH

4.2 Allgemeines zu Chipkarten

4.2.1 Bestellung/Produktion von Chipkarten

Eine Chipkarte wird grundsätzlich nur im Auftrag eines Kreditinstitutes oder einer ähnlichen Organisation produziert. Die eigentliche Produktion der Chipkarten wird im Auftrag dieser Kreditinstitute/Organisationen durch entsprechende Fachfirmen durchgeführt.

Ein Verkehrsunternehmen kann in eine Chipkarte ein Elektronisches Ticket einbringen. Bezüglich des Weges, wie ein Kunde in den Besitz einer Chipkarte mit Elektronischem Ticket gelangt, ist zwischen Kundenkarten der Kreditinstitute oder ähnlichen Organisation und sogenannten „White-Cards" zu unterscheiden.

Eine Kundenkarte eines Kreditinstituts (z.B. ec-Karte, Bankkundenkarte) enthält in der Regel eine kontogebundene Geldbörse. Diese Karten werden direkt durch das Kreditinstitut an seine Kunden gegeben. Die Karten werden regelmäßig alle 3-5 Jahre ausgetauscht. Die optische Gestaltung der Kundenkarten liegt alleine in der Verantwortung des ausgebenden Kre-

ditinstituts. Ein Kunde kann mit seiner Kundenkarte zu einer Verkaufsstelle eines Verkehrsunternehmens gehen und ein Elektronisches Ticket in seine Karte laden lassen.

Eine White-Card enthält in der Regel eine kontoungebundenen Geldbörse. Eine solche Karte kann im Sinne eines Co-Brandings gemeinsam von einem Verkehrsunternehmen und einem Kreditinstitut oder einer ähnlichen Organisation ausgegeben werden. Das Verkehrsunternehmen bestellt die Karten bei der Organisation, welches wiederum die Produktion der Karten bei einer Fachfirma veranlasst. Die produzierten Karten werden an das Verkehrsunternehmen ausgeliefert, welches wiederum die Karten an seine Kunden ausgibt. Die optische Gestaltung dieser Karten wird im allgemeinen gemeinsam durch das ausgebende Kreditinstitut oder einer ähnlichen Organisation und dem Verkehrsunternehmen festgelegt. Vor der Ausgabe dieser Karten an den Kunden bringt das Verkehrsunternehmen das gewünschte Elektronische Ticket in die Karte ein.

4.2.2 Eindeutige Identität einer Chipkarte

Jede für das Elektronische Ticket eingesetzte Chipkarte besitzt eine eindeutige Nummer. Dies gilt sowohl für die ZKA-GeldKarten und die PayCard als auch für die entsprechenden Sicherheitsmodule. Diese Nummer ist 10 Byte lang und besteht aus einer 4 Byte langen Kennung des ausgebenden Kreditinstituts oder einer ähnlichen Organisation, einer 5 Byte langen laufenden Nummer und einer ein Byte langen Prüfziffer. Diese Nummer wird bei der Produktion in die Karten eingebracht und ist danach nicht mehr veränderbar. Die Nummer steht in einer Datei der Karte (z.B. EF_ID in dem Verzeichnis MF der ZKA-GeldKarte), deren Inhalt einfach aus der Karte ausgelesen werden kann.

Für den Aufbau dieser Datei und der Nummer siehe auch [8], [9] und [10].

4.2.3 Eigenschaften einer Chipkarte bei ihrer Ausgabe

Bei der Ausgabe einer Chipkarte durch ein Kreditinstitut oder eine ähnlichen Organisation (entweder direkt an den Kunden oder bei White-Cards an ein Verkehrsunternehmen) ist die Karte bereits für die Aufnahme von Elektronischen Tickets nach der Spezifikation [3] und [6] oder [8] vorbereitet. Dies bedeutet, dass vor dem Einbringen eines Elektronischen Tickets in diese Chipkarten keine weiteren Schritte (wie z.B. das Laden von neuen Schlüsseln oder das Reservieren von Speicherplatz) durchgeführt werden müssen.

Der Speicherplatz für Elektronische Tickets ist in diesen Chipkarten beschränkt. Zur Zeit können maximal 10 Elektronische Tickets in einer Karte gespeichert werden. Die Anzahl der speicherbaren Tickets hängt dabei jedoch von dem Speicherplatzbedarf der einzelnen Tickets ab.

4.2.4 Anmerkungen zu den Versionen des ZKA-Betriebssystems

Jede ZKA-GeldKarte basiert auf dem ZKA-Betriebssystem für Chipkarten. Im Jahre 1999 wurde die Spezifikation [2] einer vollständig neuen Version dieses Betriebssystems abgeschlossen. Zur Zeit wird an der Realisierung dieses neuen Betriebssystems gearbeitet (Stand März 2000).

Alle ZKA-GeldKarten mit einer Ausgabe ab 10.2000 werden das neue Betriebssystem enthalten. ZKA-GeldKarten, die bereits mit dem bisherigen Betriebssystem ausgegeben wurden (bzw. noch ausgegeben werden), verlieren ihre Gültigkeit spätestens Ende 2002.

Durch die Einführung des neuen Betriebssystems ergeben sich auch wesentliche Änderungen für die Speicherung und das Einbringen von Elektronischen Tickets in ZKA-GeldKarten gegenüber dem bisherigen System. Siehe dazu auch [6] und [7].

Für die Speicherung von Elektronischen Tickets des VRR sollen ausschließlich ZKA-GeldKarten mit dem neuen Betriebssystem zum Einsatz kommen. Dies bedeutet, dass für eine Übergangszeit bis Ende 2002 nur White-Cards für das Elektronische Ticket des VRR eingesetzt werden können. Durch ein Kreditinstitut ausgegebene Kundenkarten (z.B. ec-Karte, Bankkundenkarte) können im allgemeinen erst ab Januar 2003 eingesetzt werden.

4.2.5 Anmerkungen zu der Währung einer Chipkarte

Jede Chipkarte hat eine Währung für die in ihr gespeicherten Einheiten der Elektronischen Geldbörse. Bei allen ZKA-GeldKarten, die ab 10.2000 basierend auf dem neuen ZKA-Betriebssystem ausgegeben werden, ist die Währung EURO. Alle bereits (basierend auf dem bisherigen Betriebssystem) ausgegebenen ZKA-GeldKarten bzw. noch vor 10.2000 auszugebenden ZKA-GeldKarten haben die Währung DM. Die für die Elektronischen Tickets eingesetzte PayCard hat die Währung EURO.

ZKA-GeldKarten mit der Währung DM verlieren spätestens Ende 2002 ihre Gültigkeit.

Die konkrete Währung einer ZKA-GeldKarte ist in dem Währungskennzeichen in der Datei EF_ID (im Verzeichnis MF) angegeben. Siehe dazu auch [8].

4.3 Funktionen für einen Zugriff auf ein Elektronisches Ticket

In diesem Abschnitt werden die Funktionen beschrieben, die für das Einbringen, die Kontrolle und das Ändern von Elektronischen Tickets in einer Chipkarte benötigt werden. Die Funktionen werden aus der Anwendungssicht beschrieben. Für ihre technische Umsetzung in den verschiedenen Terminals wird auf die Spezifikation [4], [7] und [9] verwiesen.

Für die Festlegung der Funktionen sind die beiden folgenden Vorgaben des VRR von Bedeutung:

Elektronische Tickets des VRR sollen nach ihrem Einbringen in eine Chipkarte nicht entwertet werden. Mehrfahrtenkarten (4er-Ticket bzw. 10er-Ticket) werden nicht als Elektronisches Ticket realisiert. Dies bedeutet, dass der Inhalt eines Elektronischen Tickets des VRR vom Zeitpunkt seines Einbringens in eine Chipkarte bis zum Ende seiner Gültigkeit nicht mehr geändert werden soll. Das Ticket kann lediglich markiert werden, d.h. die noch vorhandene Gültigkeit kann storniert werden. Damit ist das Ticket ungültig.

Ein Kontrolleur soll ein Elektronisches Ticket in einer Chipkarte „markieren" können, falls die Chipkarte auf der Sperrliste des Kontrolleurs steht. Dadurch wird bei späteren Kontrollen auch ohne Vergleich mit einer Sperrliste erkennbar, dass ein Elektronisches Ticket nicht (mehr) gültig ist.

Für das Elektronische Ticket des VRR werden die folgenden Funktionen mit einem Zugriff auf die Chipkarten benötigt:

- Einbringen eines neuen Elektronischen Tickets.
- Löschen eines gültigen Elektronischen Tickets.
- Kontrolle eines Elektronischen Tickets.
- Markieren eines Elektronischen Tickets.
- Anzeige des Elektronischen Tickets am Taschenkartenleser.

Die Funktion „Einbringen eines neuen Elektronischen Tickets" wird durch die entsprechende technische Funktion der Spezifikationen [4], [7] und [9] realisiert. Sie muss dabei auch ohne vorherigen Bezahlvorgang mit der Chipkarte ausführbar sein.

Die Funktion „Löschen eines gültigen Elektronischen Tickets" wird durch Rückdatieren des Tickets in der Chipkarte und/oder Überschreiben des Tickets in der Chipkarte durch einen Initialrecord realisiert. Diese Funktion bezieht sich dabei nur auf das Überschreiben von Elektronischen Tickets, deren Verfallszeitpunkt noch nicht überschritten wurde. Die Funktion kann nur unter bestimmten Umständen oder nur durch das Verkehrsunternehmen ausgeführt werden, welches das Elektronische Ticket auch in die Karte geschrieben hat. Siehe dazu auch [1], [4], [7] und [9].

Die Funktion „Kontrolle eines Elektronischen Tickets" beinhaltet das Anzeigen der Inhalte aller Felder des Elektronischen Tickets (siehe Kapitel 2.2) und die kryptographische Überprüfung der aus der Karte gelesenen Daten.

Die Funktion „Markieren eines Elektronischen Tickets" wird durch die Funktion Entwerten der Spezifikation [4], [7] und [9] realisiert. Bei dem Einbringen eines Elektronischen Tickets in eine Chipkarte wird der Entwertungszähler (siehe Kapitel 2.2) auf den Wert „FE“ gesetzt. Dies kennzeichnet ein gültiges Ticket. Wird eine Karte bei einer Kontrolle in einer Sperrliste entdeckt, wird durch die Funktion „Markieren eines Elektronischen Tickets" der Entwertungszähler auf den Wert „FF“ gesetzt, wodurch das Ticket als ungültig gekennzeichnet wird.

Bei der Funktion „Anzeige eines Elektronischen Tickets an einem Taschenkartenleser" werden die Inhalte der anzeigbaren Felder (siehe Kapitel 2.2) auf dem Display eines (für die Zusatzanwendung Elektronisches Ticket erweiterten) Taschenkartenlesers angezeigt.

Die folgende Tabelle gibt einen Überblick, mit welchen Funktionalitäten die benötigten Terminals ausgestattet sein müssen.

Funktion	Terminal in Verkaufsstellen	Terminal für Kontrolleure	Taschen-kartenleser
Einbringen	X		
Löschen	X		
Kontrolle	X	X	
Markieren	X	X	
Anzeige Taschenkartenleser			X

Für die Ausführung aller Funktionen mit der Ausnahme von „Anzeige eines Elektronischen Tickets an einem Taschenkartenleser" wird ein Sicherheitsmodul gemäß [5] oder [10] benötigt.

Anmerkung: Neben den hier aufgeführten Terminals kann es in der Zukunft weitere geben, z.B. in Form von Automaten oder Ticketdruckern. Der Funktionsumfang dieser Geräte ist eine (nicht notwendigerweise echte) Untermenge der Funktionen der Verkaufsstelle. Damit ist diese Richtlinie auch auf derartige zukünftige Geräte anwendbar.

4.4 Allgemeines zu den Sicherheitsmodulen

Für alle Funktionen, bei denen in einer Chipkarte die für ein Elektronisches Ticket gespeicherte Daten geändert werden sollen, wird ein Sicherheitsmodul benötigt. Zusätzlich wird ein Sicherheitsmodul für die kryptographische Überprüfung der Integrität der Daten eines Elektronischen Tickets benötigt, die aus einer Chipkarte gelesen wurden. Ein Sicherheitsmodul wird daher für alle im letzten Abschnitt genannten Funktionen mit der Ausnahme der Funktion „Anzeige eines Elektronischen Tickets an einem Taschenkartenleser" benötigt. Jedes Terminal des Systems mit der Ausnahme eines Taschenkartenlesers muss mit einem Sicherheitsmodul ausgestattet werden.

Das Sicherheitsmodul der Kreditwirtschaft für den Zugriff auf Elektronische Tickets wird auch als FSAM bezeichnet und ist in [5] spezifiziert. Realisiert wird ein FSAM ebenfalls als Chipkarte (SIM-Format) basierend auf dem ZKA-Betriebssystem. Zur Zeit wird an einer neuen Version des FSAM gearbeitet. Diese neue Version des FSAM soll ab Ende 2000 verfügbar sein. Im Rahmen des Elektronischen Tickets des VRR soll die neue Version von FSAM eingesetzt werden. Das Sicherheitsmodul der PayCard muß [10] entsprechen.

Ein Sicherheitsmodul kann wie eine Chipkarte nur im Auftrage eines Kreditinstitutes oder einer ähnlichen Organisation produziert werden. Ein Verkehrsunternehmen muss daher die für seine Terminals benötigten Sicherheitsmodule über ein Kreditinstitut oder eine ähnliche Organisation bestellen.

Die Sicherheitsmodule der Kreditwirtschaft haben wie die Chipkarten eine beschränkte Gültigkeitsdauer. Sie müssen daher regelmäßig (ca. alle drei Jahre) ausgetauscht werden. Für die Sicherheitsmodule der PayCard ist dies nicht zwingend vorgeschrieben und kann somit flexibler geregelt werden.

Heute werden Sicherheitsmodule FSAM nur in Verbindung mit einer Händlerkarte für die ZKA-GeldKarte produziert. Das Einbringen eines neuen Elektronischen Tickets in eine ZKA-GeldKarte ist dabei eng an einen vorher stattfindenden Bezahlvorgang mit der gleichen GeldKarte gekoppelt. Der Betrag des Bezahlvorgangs wird dabei automatisch als Preis in das Elektronische Ticket eingetragen. Bei der neuen Version des FSAM kann die enge Kopplung zwischen Bezahlvorgang und Einbringen eines neuen Elektronischen Tickets aufgehoben werden (siehe weiter unten). Bei den Sicherheitsmodulen der PayCard kann dies auch nachträglich konfiguriert werden.

Die Sicherheitsmodule können bei der Produktion so konfiguriert werden, dass sie nur bestimmte Funktionen unterstützen. Aus Sicherheitsgründen ist es dabei sinnvoll, dass ein Sicherheitsmodul immer nur die Funktionen unterstützen kann, die das Terminal ausführen soll, in dem das Sicherheitsmodul eingesetzt wird.

In einem Sicherheitsmodul wird die Betreiber-ID (siehe Kapitel 2.2) des Verkehrsunternehmens gespeichert, das das Sicherheitsmodul bestellt und in seinen Terminals einsetzt. Die Betreiber-ID wird dabei automatisch in jedes Elektronische Ticket eingetragen, das mit der Hilfe des Sicherheitsmoduls in eine Chipkarte eingebracht wird. Dadurch ist für jedes Elektronische Ticket erkennbar, welches Verkehrsunternehmen es erzeugt hat.

Jedes Sicherheitsmodul besitzt (wie die Chipkarten auch) eine eindeutige Nummer. Diese Nummer ist 10 Byte lang und besteht aus einer 4 Byte langen Kennung des ausgebenden Kreditinstituts oder ähnlichen Organisation, einer 5 Byte langen laufenden Nummer und einer ein Byte langen Prüfziffer. Diese Nummer wird bei der Produktion in das Sicherheitsmodul eingebracht und ist danach nicht mehr veränderbar. Die Nummer steht in einer Datei der Karte (z.B. EF_ID im Verzeichnis MF des SAMs der Kreditwirtschaft), deren Inhalt einfach aus dem Sicherheitsmodul ausgelesen werden kann.

Bei einem FSAM der neuen Version der Kreditwirtschaft und dem Sicherheitsmodul der PayCard können bereits bei der Produktion verschiedene Konfigurationen eingestellt werden. Für diese Konfiguration müssen dabei die folgenden Fragen (vor der Produktion) beantwortet sein:

1. Soll das Einbringen eines neuen Elektronischen Tickets in eine Chipkarte an einen Bezahlvorgang mit der gleichen Chipkarte gekoppelt werden?

2. Wie viele neue Elektronische Tickets können ohne gekoppelten Bezahlvorgang in eine Chipkarte eingebracht werden?

3. Was ist der maximale Wert eines neuen Elektronischen Tickets, das ohne gekoppelten Bezahlvorgang in eine Chipkarte eingebracht werden kann?

4. Was ist die maximale Summe der Werte der Elektronischen Tickets, die ohne gekoppelten Bezahlvorgang in eine Chipkarte eingebracht werden können?

5. Soll die eindeutige Nummer des Sicherheitsmoduls in die Daten eines Elektronischen Tickets eingetragen werden?

6. Welche Funktionen können mit dem Sicherheitsmodul ausgeführt werden?

Durch die Beantwortung dieser Fragen wird eine Konfiguration für ein Sicherheitsmodul festgelegt. Die Fragen 2 bis 4 sind dabei nur dann von Bedeutung, falls Frage 1 mit „Nein“ beantwortet wurde. In Kapitel 3 werden Richtlinien für die Beantwortung der Fragen für den Einsatz von Sicherheitsmodulen im Rahmen des Elektronischen Tickets des VRR gegeben.

Die Konfiguration eines Sicherheitsmoduls wird im wesentlichen bei der Produktion festgelegt. Einige der Werte einer Konfiguration lassen sich aber auch nachträglich administrieren. Wurde zum Beispiel oben unter Frage 2 eine bestimmte Anzahl von Elektronischen Tickets festgelegt, die mit einem Sicherheitsmodul in Chipkarten gespeichert werden können, und wurde diese Anzahl nach einer gewissen Zeit aufgebraucht, kann in das Sicherheitsmodul eine neue Anzahl von speicherbaren Elektronischen Tickets geladen werden. Für diese Administrationsaufgaben muss auf das Sicherheitsmodul kryptographisch abgesichert zugegriffen werden. Das genaue Vorgehen dabei wird bei dem Sicherheitsmodul der Kreditwirtschaft zur Zeit spezifiziert. Bei dem Sicherheitsmodul der PayCard siehe dazu auch [11]. Benötigt wird aber eine (zeitweise bestehende) Online-Verbindung zu einem Hintergrundsystem des Verkehrsunternehmens, das das Sicherheitsmodul (in einem seiner Terminals) betreibt.