Z E N T R A L E R K R E D I T A U S S C H U S S

MITGLIEDER: BUNDESVERBAND DER DEUTSCHEN VOLKSBANKEN UND RAIFFEISENBANKEN E.V. BERLIN • BUNDESVERBAND DEUTSCHER BANKEN E.V. BERLIN
BUNDESVERBAND ÖFFENTLICHER BANKEN DEUTSCHLANDS E.V. BERLIN • DEUTSCHER SPARKASSEN- UND GIROVERBAND E.V. BERLIN-BONN
VERBAND DEUTSCHER HYPOTHEKENBANKEN E.V. BERLIN

Einführung und Überblick

"Elektronischer Fahrschein und Marktplatz"

Version Entwurf 2.0

27.05.2004

Inhalt

Abbildungsverzeichnis

1 Einleitung

Dieses Dokument stellt eine Einführung in die Zusatzanwendungen "ZKA-Marktplatz" und "Elektronischer Fahrschein" dar und gibt einen Überblick über die beteiligten Systemkomponenten.

Das Dokument ist so konzipiert, dass es zunächst allgemeingültige Aspekte beschreibt, die für beide Zusatzanwendungen Gültigkeit haben.

Spezielle Aspekte, in denen sich die beiden Anwendungen stark voneinander abheben, sind in separaten Abschnitten behandelt.

2 Definitionen, Ziele und Hintergründe

2.1 Definition und Ziele von Zusatzanwendungen

Der ZKA[1] hat sich im Rahmen der Ausstattung von Chipkarten für kartengestützte Zahlungssysteme - im Folgenden ZKA-Chipkarte - dafür entschieden, interessierten Akzeptanten freien Speicherbereich auf den Karten für eigene Anwendungen zur Verfügung zu stellen. Ziel ist es, die chipgestützten Zahlungssysteme GeldKarte und electronic cash im Markt zu promovieren. Die Akzeptanten können die große Kartenbasis der Kreditwirtschaft nutzen und die Ausgabe eigener Karten oder von Papierbelegen einsparen, so dass sich eine attraktive Win-Win-Situation ergeben kann. Der Akzeptant kann sich auf die Gestaltung der Applikation konzentrieren, da die Qualitätssicherung und das Sicherheitsmanagement für die Chipkarten durch die Kreditwirtschaft erfolgt.

Die zentrale Anwendung ist die **Elektronische Geldbörse (GeldKarte)**, die auf jeder ZKA-Chipkarte vorhanden ist. Diese ermöglicht das bargeldlose Bezahlen, indem in einem dedizierten Datenfeld ein Betrag gespeichert ist, der an Ladeterminals hochgesetzt werden kann (Laden) und an Akzeptanzterminals verringert werden kann (Bezahlen).

Die Datenstrukturen, kryptographischen Schlüssel und Daten, die in die Chipkarte eingebracht werden müssen, damit der Speicherplatz durch den Anbieter nutzbar ist, werden als **Zusatzanwendungen** bezeichnet.[2]

Zusatzanwendungen sind in ZKA-Chipkarten immer in einem speziellen Administrationsverzeichnis enthalten. Dieses Verzeichnis und die darin enthaltenen

[1] Zentraler Kreditausschuss

[2] Der Begriff *Zusatz*anwendung wird deshalb verwendet, weil es sich aus Sicht der ZKA-Chipkarte um Anwendungen handelt, die *zusätzlich* zu den kreditwirtschaftlichen Anwendungen (z. B. elektronische Geldbörse, electronic cash) auf dem Chip gespeichert sind.

Datenfelder, Daten und Administrationsschlüssel werden auch als **Memory Organizer** bezeichnet.

Das Einbringen des Memory Organizer in die Chipkarte wird als **Vorstrukturierung** bezeichnet.

Beispiele für Zusatzanwendungen sind "Elektronische Rabattmarken" oder Homebanking-Anwendungen. Eine prädestinierte Zusatzanwendung ist der elektronische Fahrschein, weil dort der (bisherige) Wertträger, der (Papier-)Fahrschein, ähnlich verbreitet wie Bargeld ist und seinen Besitzer ähnlich schnell und oft wechselt. Da die Fahrscheine – im Gegensatz zu Banknoten – nach der Benutzung weggeworfen werden, ist ein ausreichender Fälschungsschutz jedoch schwieriger, da die Sicherungsmechanismen an die Laufzeit von Fahrscheinen gebunden sind. Aus dem elektronischen Fahrschein ergibt sich somit ein noch höherer Nutzen, da hier Sicherheitsmechanismen genutzt werden können , die nicht an die Laufzeit von Fahrscheinen gebunden sind.

Entwickelt wurde die Anwendung "**Elektronischer Fahrschein**" zusammen mit dem Verband deutscher Verkehrsunternehmen VDV. Über diesen Standard können verschiedene Fahrausweise unterschiedlicher Verkehrsunternehmen auf den Chipkarten gespeichert und ausgewertet werden. Damit kann deutschlandweit dasselbe Verfahren zur Speicherung elektronischer Fahrscheine angeboten und eingesetzt werden.

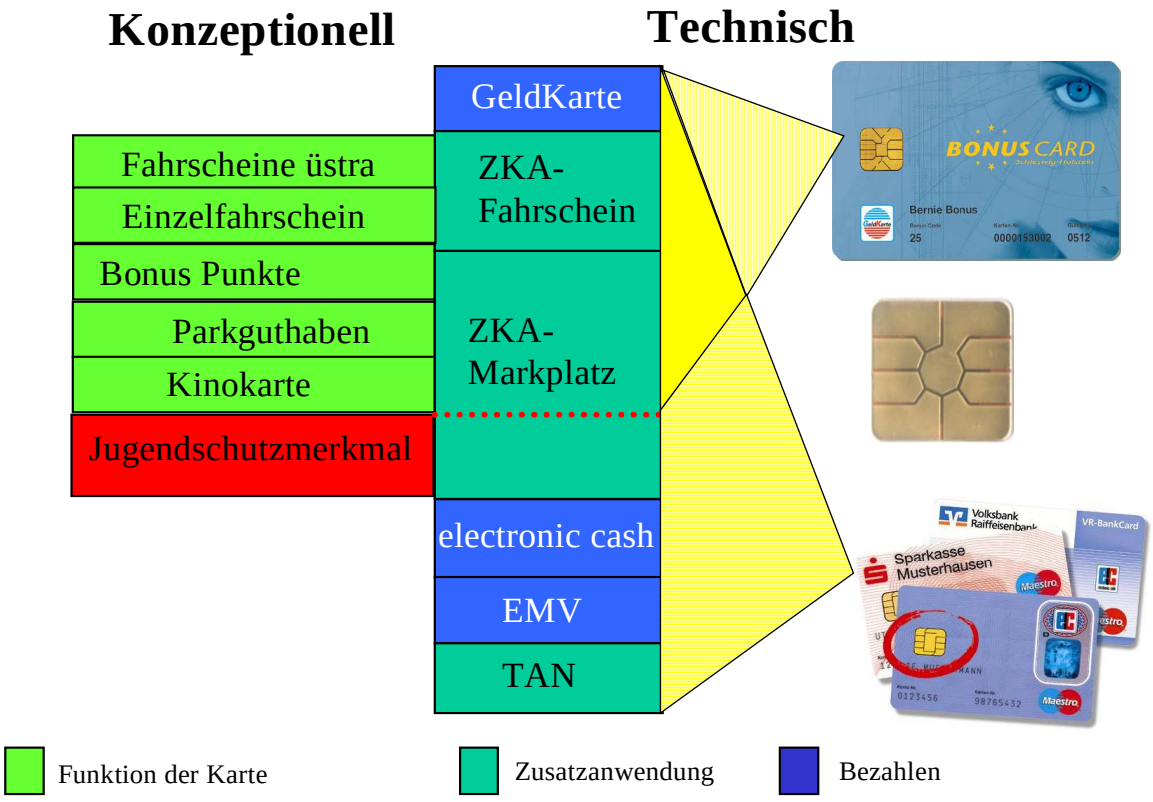


Abbildung 1: Aufbau der Karten

Der Standard "Elektronischer Fahrschein" legt nur die Bestandteile des elektronischen Fahrscheins fest, die für eine **deutschlandweite Einsatzfähigkeit** der ZKA-Chipkarte für den Öffentlichen Personenverkehr (ÖPV) absolut notwendig sind. Dem jeweiligen Verkehrsunternehmen soll maximale Freiheit zur Abbildung der örtlichen Tarifsysteme eingeräumt werden.

Da verschiedene Akzeptanten andere Berechtigungen, zum Beispiel Bonuspunkte, Gutscheine oder Ausweise, auf den Karten speichern wollen, wurde mit dem sog. "**ZKA-Marktplatz**" ein zweiter Standard im ZKA entwickelt, über den solche Anwendungen kartengestützt realisiert werden können.

Bei beiden Anwendungen handelt es sich um sogenannte **Pool-Anwendungen**. Das bedeutet, dass nicht jedem Anbieter dauerhaft eigener Speicher zur Verfügung gestellt wird, sondern dass der Speicher mehreren Anbietern zur gemeinsamen Nutzung zur Verfügung steht. In die Datenstruktur einer Pool-Zusatzanwendung kann somit nicht nur ein Anbieter sondern eine Gruppe von Anbietern Daten eintragen. So könnte beispielsweise zusammen mit einem elektronischen Theaterticket gleichzeitig ein elektronischer Fahrschein, der für den entsprechenden Abend gültig ist, auf der ZKA-Chipkarte angelegt werden.

Für die ZKA-Pool-Zusatzanwendungen sind technische Regeln festgelegt worden, die sicherstellen, dass Anbieter zwar miteinander dienstleistungs- oder warenrelevante Information austauschen können (z.B. Parkhausbetreiber und Kaufhäuser), dabei aber Dateninhalte der jeweils anderen Seite nicht unberechtigt verändert werden können. Die Einhaltung der Regeln für eine ZKA-Pool-Zusatzanwendung, insbesondere die richtige Interpretation von Dateninhalten wird technisch durch sog. Sicherheitsmodule garantiert.

2.2 Status quo „ZKA-Marktplatz“

2.2.1 Stand der Standardisierung und weitere Entwicklung

Die Applikation ZKA-Marktplatz ist eine Standard-Zusatzanwendung auf der ZKA-Chipkarte, die einen flexiblen Rahmen zur Gestaltung von anbieter-individuellen Zusatzanwendungen bietet. Der ZKA-Marktplatz stellt geeignete Datenstrukturen auf der Kundenkarte zur Verfügung, um alle notwendigen Anwendungsdaten für Gutscheine, Bonussysteme oder Ausweise kryptographisch gesichert speichern zu können.

Darüber hinaus zeichnet sich der ZKA-Marktplatz dadurch aus, dass die notwendigen Datenstrukturen auf der Chipkarte bereits bei der Kartenausgabe vorhanden sind. Die Karte ist damit bereits bei der Kartenausgabe für die Teilnahme an Zusatzanwendungen auf Basis des ZKA-Marktplatzes vorbereitet. Die Datensätze, die im Rahmen einer Zusatzanwendung auf die Karte gebracht werden, tragen jeweils die Kennung desjenigen Anbieters bzw. Akzeptanten, der den Datensatz in der Karte angelegt hat. Durch diese Zuordnung werden dem betreffenden Akzeptanten besondere Rechte an "seinem" Datensatz eingeräumt. Er allein ist in der Lage, die Inhalte des Datensatzes beliebig zu ändern, insbesondere auch den Datensatz zu löschen. Andere Akzeptanten können höchstens spezielle Felder des

Datensatzes bearbeiten und den Datensatz in ihren Terminals prüfen. Durch diese Vorkehrungen wird gewährleistet, dass der Zugriff auf Zusatzanwendungsdaten nach Akzeptanten separiert werden kann, obwohl diese Daten im gleichen Speicherbereich der ZKA-Chipkarte abgelegt sind.

Jedes Terminal eines Akzeptanten, das Zusatzanwendungsdaten auf der ZKA-Chipkarte bearbeitet, verfügt über ein Sicherheitsmodul, mit dem der Zugriff auf diese Daten abgesichert wird. Dieses Sicherheitsmodul garantiert insbesondere, dass der Akzeptant die Berechtigung zum Zugriff auf den Zusatzanwendungsdatensatz besitzt.

Des weiteren existieren Spezifikationen für die Akzeptanzterminals der Händler, in denen die Funktionen im Detail beschrieben sind, die ein Terminal zur Bearbeitung einer Zusatzanwendung auf der Kundenkarte ausführen kann.

Kreditwirtschaftliche Bereiche haben seit 2003 mit der verschlüsselten Einbringung eines Jugendschutzmerkmals des Karteninhabers in die ZKA-Chipkarte begonnen. Die Auswertung des Jugendschutzmerkmals ist an unbedienten Terminals (wie z.B. Selbstbedienungsautomaten) oder durch Internetanwendungen applikationsspezifisch möglich. Das Jugendschutzmerkmal wird auf Basis der ZKA-Standardanwendung Marktplatz realisiert, indem es verschlüsselt in die ZKA-Zusatzanwendung Marktplatz eingebracht wird. In die Kundenkarte wird nur das Kryptogramm eingebracht. Der eigentliche kartenindividuelle Schlüssel zum Ver- und Entschlüsseln wird nicht in der Kundenkarte gespeichert. Denjenigen Anbietern, die das Jugendschutzmerkmal verarbeiten dürfen, wird der Masterkey, aus dem die kartenindividuellen Schlüssel abgeleitet werden, in einem Sicherheitsmodul mit integrierter Ablaufkontrolle und weiteren Schutzmechanismen übergeben. Das erweitere Sicherheitsmodul der Zusatzanwendung Marktplatz (MSAM) enthält einen zusätzlichen Schlüssel zum Entschlüsseln des Jugendschutzmerkmals. (Detailliertere Informationen befinden sich im Anhang C.

Ab 2007 werden alle Tabakwarenautomaten nur nach erfolgreicher Verifikation dieses Jugendschutzmerkmals auf der ZKA-Chipkarte Zigaretten ausgeben. Die notwendigen Umrüstungen an den ca. 660.000 Terminals haben bereits begonnen.

2.2.2 Erfahrung aus Projekten

Seit Oktober 2001 gibt es eine Vielzahl von Projekten basierend auf dem ZKA-Marktplatz. Unter der Webadresse www.geldkarte.de befinden sich weitere Informationen und eine Liste mit Projekten.

2.3 Status quo „Elektronischer Fahrschein“

2.3.1 Stand der Standardisierung und weitere Entwicklung

Der Öffentliche Personenverkehr (ÖPV) in Deutschland ist heute durch eine Vielzahl unterschiedlicher Tarifsysteme gekennzeichnet. Die Bargeldent- und -versorgung an Automaten und für den Fahrer ist eine ebenso kostspielige wie zeitintensive Tätigkeit. Mit der Einführung des EURO und der zeitlich begrenzten Gültigkeit von zwei Währungen erhielt dieses Problem weitere Brisanz.

Im ÖPV hat man deshalb Strategien entwickelt, die beiden Problemen entgegen wirken sollen. In einer ersten Stufe möchte man durch Schaffung geeigneter Akzeptanzstellen den Einsatz von bargeldlosen Zahlungsmitteln wie z. B. der GeldKarte, der elektronischen Börse der deutschen Kreditwirtschaft, erhöhen.

In einer zweiten Stufe soll die Chipkarte auch zur Speicherung des Fahrscheins dienen. Es wird kein Papierfahrschein mehr ausgedruckt, sondern der Fahrschein wird elektronisch in der Chipkarte gespeichert. Dieses Modell wurde erstmals in einem Pilotversuch in Bremen seit Juni 1999 erfolgreich eingesetzt und soll nun auch im gesamten Verkehrsverbund Bremen Niedersachsen (VBN) unter Teilnahme der Deutschen Bahn AG zur Anwendung kommen. Das Verfahren basiert auf dem Standard "Elektronischer Fahrschein".

In der dritten Stufe soll eine automatische Fahrpreisberechnung stattfinden. Das System in den Fahrzeugen ermittelt über Informationen, die in einer Chipkarte des Kunden und in den Terminals gespeichert sind, automatisch die Höhe des Fahrpreises. Dabei unterscheidet man sog. prepaid-Systeme, bei denen dem Fahrgast spätestens unmittelbar nach Beendigung der Fahrt der ermittelte Fahrpreis aus einer elektronischen Börse der Chipkarte abgebucht wird, von sog. postpaid-Systemen, bei denen die Fahrpreisermittlung in einem zentralen Rechenzentrum auf Basis der von Terminals gesammelten Informationen erfolgt. Der Fahrpreis wird dem Kunden nach Beendigung der Fahrt auf einem interner Kundenkonto belastet, das z.B. monatlich ausgeglichen wird.

Für zukünftige Lösungen denken verschiedene Verkehrsverbünde heute über den Einsatz kontaktloser Chiptechnik nach. Hiervon versprechen sie sich eine Beschleunigung des Anlegevorgangs, des Ein- und Aussteigens, im Wesentlichen aber eine effiziente Möglichkeit der flexibleren Fahrpreisberechnung. Für den Kunden werden die Fahrstrecken insgesamt elektronisch beim Ein- und Aussteigen ermittelt und er erhält zu einem späteren Zeitpunkt eine Rechnung über die gesamte Fahrstrecke. (Anmerkung: Prinzipiell ist dieses Vorgehen auch mit kontaktbehafteter Technologie möglich, jedoch sollte das Verfahren den Kunden nicht bei jedem Ein- und Ausstieg zum aktiven Handeln zwingen). Diese Themen werden derzeit zwischen den Verkehrsverbünden noch kontrovers diskutiert. Federführend durch den VDV ist ein Projekt zur Entwicklung der so genannten Kernapplikation initiiert worden. Ziel ist es, eine deutschlandweit einheitliche Applikation zu entwickeln, die sowohl die zweite als auch die dritte Stufe umfasst. Die Applikation "elektronischer Fahrschein" soll ein Bestandteil dieser Kernapplikation sein.

Die Abläufe zum Anlegen eines elektronischen Fahrscheins werden auch von einem Internet-Kundenterminal unterstützt, so dass auch das Anlegen von Fahrscheinen über das Internet möglich ist.

2.3.2 Erfahrungen aus den ZKA-Piloten und umgesetzten Projekten

Mit Unterstützung der Kreditwirtschaft wurde die Anwendung "Elektronischer Fahrschein" von der Bremer Straßenbahn AG, BSAG, 1999 erfolgreich pilotiert. Für eine Straßenbahn- und eine Buslinie in Bremen wurde ein Fahrscheinkonzept auf Basis des Standards "Elektronischer Fahrschein" entwickelt, entsprechende Geräte implementiert und zusätzlich FunkLAN zur Entsorgung der in den Fahrzeugen getätigten Umsätze installiert. Der Pilot verlief ohne jedes technische Problem. Die intendierten positiven Wechselwirkungen zwischen steigenden Transaktionen für das GeldKarte-Zahlungsverfahren auf der einen Seite und steigenden Transaktionszahlen für die BSAG auf der anderen Seite sind voll eingetreten. So stiegen die Ladetransaktionen für GeldKarte im Rahmen des Piloten um 250%, die Bezahltransaktionen um über 400%. Umfragen haben belegt, dass der Bekanntheitsgrad des GeldKarte-Systems sich vor dem Hintergrund der Pilotierung erheblich steigern konnte. Bei einer Umfrage befürworteten 66% der Befragten die Ausdehnung des Piloten auf das Gesamtnetz. Zu Beginn des Jahres 2002 wurde der Ansatz flächendeckend von der BSAG umgesetzt. Im Jahr 2004 ist fast der gesamte Verkehrsverbund Bremen Niedersachsen (VBN) umgerüstet.

3 Systemkomponenten

3.1 Systemüberblick

Die ZKA-Chipkarte ist die Systemkomponente auf Seiten des Kunden, die benötigt wird, um eine Zusatzanwendung umzusetzen. Weitere Hardware-Komponenten, die beim Händler bzw. Anbieter vorgehalten werden müssen, sind das ÖPV-Terminal sowie das "Sicherheitsmodul Fahrschein" (FSAM) für die Zusatzanwendung "Elektronischer Fahrschein“ bzw. das Marktplatz-Terminal und das "Sicherheitsmodul Marktplatz" (MSAM) für die Zusatzanwendung "ZKA-Marktplatz".

Koordiniert durch das Terminal treten die ZKA-Chipkarte und das FSAM bzw. MSAM in Wechselwirkung miteinander. Hier findet der eigentliche Anwendungsablauf statt.

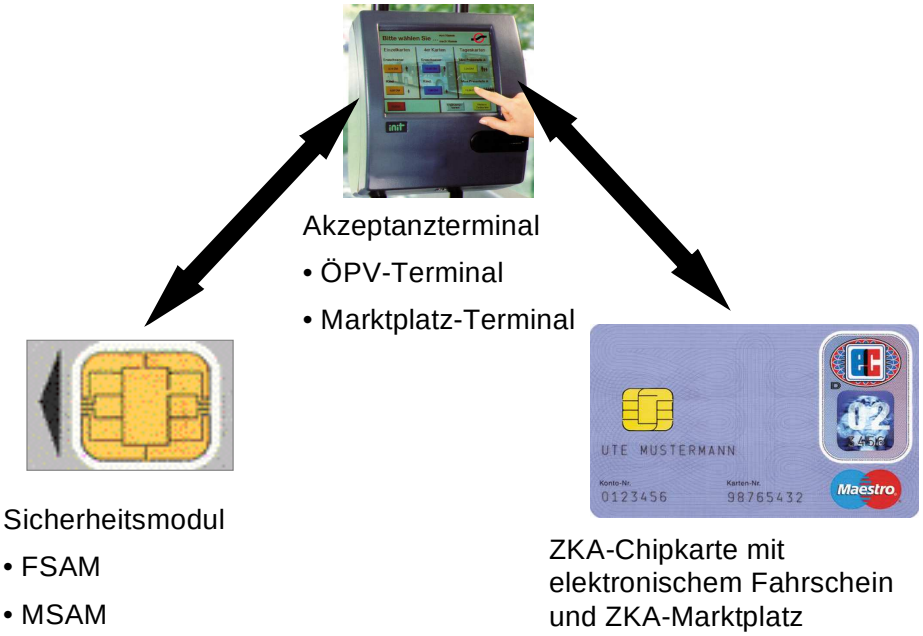


Abbildung 2: Zusammenspiel der Komponenten

Elektronischer Fahrschein

Ein **elektronischer Fahrschein** kann vom Kunden an einem Akzeptanzterminal eines Anbieters erworben und auf der ZKA-Chipkarte gespeichert werden. Über ein Anzeigegerät, z. B. den multifunktionalen Taschenkartenleser, können jederzeit alle gespeicherten Fahrscheine angezeigt werden. Fahrscheine können an ausgewählten Terminals entwertet bzw. gelöscht und auch angezeigt werden.

Der Standardisierungsprozess zwischen ZKA und VDV ist weitgehend abgeschlossen, und alle von der Kreditwirtschaft ab Mitte 1998 neu ausgegebenen ZKA-Chipkarten enthalten eine einheitliche Verzeichnisstruktur, die sie in die Lage versetzt, den Standard

"Elektronischer Fahrschein" zu nutzen. Im Auftrag des ZKA wurde die Schnittstellenspezifikation für die Zusatzanwendung Elektronischer Fahrschein erstellt. Sie beschreibt einen einheitlichen Aufbau von Datenstrukturen auf der ZKA-Chipkarte zur Ablage eines elektronischen Tickets, die den Anforderungen des Nah- und Fernverkehrs und den Sicherheitsanforderungen des ZKA genügen.

Ausführliche Informationen über den Aufbau von elektronischen Fahrscheinen finden sich in Anhang A.

Elektronischer Marktplatz

Bei der konkreten Ausprägung von Berechtigungen, die auf dem ZKA-Marktplatz basieren, auch *(ZKA-)Marktplatz-Anwendungen* genannt, wird unterschieden zwischen den beiden Berechtigungstypen **Ausweis** und **Gutschein**.

Ein **Ausweis** ist eine Berechtigung mit einem definierten, unveränderlichen Gültigkeitszeitraum. Er wird gelesen und ausgewertet, aber während seiner Gültigkeit nicht entwertet oder bezüglich seines Verfallzeitpunktes modifiziert. Während seiner Gültigkeitsdauer kann ein Ausweis beliebig oft zur Inanspruchnahme der mit ihm assoziierten Leistung eingesetzt werden. Beispiele für Ausweise sind Zeitkarten für Schwimmbäder, Zutrittsberechtigungen oder Rabattberechtigungen. Auch Marktplatz-Berechtigungen, die Bonuspunkte aufnehmen können oder allgemein als Speicher für Werteinheiten dienen, fallen im Standard "ZKA-Marktplatz" unter die Gruppe der Ausweise, da auch sie nicht entwertet oder bezüglich ihres Verfallzeitpunktes modifiziert werden können. Diese Ausweise verfügen über Zähler, die den Punktestand festhalten. Die Zählerstände in diesen Ausweisen werden im Falle der Ausstellung bzw. Einlösung von Bonuspunkten bei einem Akzeptanten erhöht bzw. verringert.

Während ein Ausweis während seiner Lebensdauer unverändert bleibt, wird ein **Gutschein** durch die Akzeptanten während der Dauer seiner potentiellen Gültigkeit bei Erbringung einer entsprechenden Leistung teilweise oder ganz entwertet. Ein Gutschein besitzt eine definierte, jedoch ggf. veränderbare Gültigkeitsdauer. Ein Gutschein stellt einen Geldwert, der bei einem Bezahlvorgang ganz oder teilweise verrechnet werden kann, oder einen Anspruch auf bestimmte Sachwerte oder Dienstleistungen dar.

Gutscheine können entweder innerhalb des Verbundes universell, d. h. bei jedem Akzeptanten für jede seiner Verbundleistungen, wie Bargeld zum Bezahlen eingesetzt werden oder zweckgebunden sein. Bei der Zweckbindung ist die Gruppe der Akzeptanten, die assoziierte Leistung oder beides eingeschränkt. In der Folge können Gutscheine hinsichtlich ihrer Akzeptanz einem sehr komplexen Modell unterliegen.

Beispiele der Zweckbindung von Gutscheinen sind

- Bezahlen nur beim Aussteller des Gutscheins,
- Bezahlen von definierten Warengruppen,
- Parkgutschein für die Parkgebühren in einem bestimmten Parkhaus und

- Sachwertgutschein zum Bezug einer Tasse Kaffee.

Beispiele für Gutscheine sind Parkgutscheine und entwertbare Tickets.

Im Auftrag des ZKA wurde die Schnittstellenspezifikation für die Zusatzanwendung Elektronischer Marktplatz erstellt. Sie beschreibt einen einheitlichen Aufbau von Datenstrukturen auf der ZKA-Chipkarte zur Ablage von Anwendungsdaten innerhalb einer Marktplatz-Anwendung, die den Anforderungen potentieller Anbieter und den Sicherheitsanforderungen des ZKA genügen. Alle ab Mitte 1998 herausgegebenen ZKA-Chipkarten sind mit diesem Standard ausgestattet.

Ausführliche Informationen über den Aufbau von elektronischen Berechtigungen finden sich in Anhang B.

3.2 Die ZKA-Chipkarte

Eine Chipkarte ist eine Plastikkarte, deren Abmessungen standardisiert sind (z. B. wie bei der eurocheque-Karte) und in die ein Chip eingebettet ist. In dem Chip können je nach Technik und Leistungsfähigkeit unterschiedliche Mengen an Daten gespeichert, verarbeitet und erzeugt werden. Außerdem enthält der Chip eine technische und funktionale Schnittstelle, über die Daten ein- und ausgegeben werden können.

Die ZKA-Chipkarte ist eine Prozessorchipkarte, die dadurch gekennzeichnet ist, dass sie neben Lese- und Schreibfunktionen zusätzlich mit einer CPU (Central Processing Unit) ausgestattet ist, die das selbständige Ausführen von Programmen ermöglicht. Aufgrund ihrer Speicherkapazität und Rechenleistung bietet die ZKA-Chipkarte somit wichtige Funktionen, die sie zu einem nahezu universellen Sicherheitswerkzeug machen:

- Die ZKA-Chipkarte dient als mobiler Datenspeicher für die unterschiedlichsten Anwendungsfelder, wobei der Zugriff auf dessen Inhalte einer Zugriffskontrolle unterliegen kann.

- In der ZKA-Chipkarte lassen sich sensible Daten, wie beispielsweise kryptographische Schlüssel, vertraulich und manipulationssicher speichern.

- Die ZKA-Chipkarte ist in der Lage, mathematische Operationen und komplexe kryptographische Algorithmen auszuführen.

Neben dem höheren Sicherheitsstandard ist ein weiterer Vorteil, dass die ZKA-Chipkarte dem Benutzer einen wesentlich größeren Grad an Flexibilität verleiht. Denn er ist für die Nutzung einer Anwendung nicht mehr an ein bestimmtes Endgerät gebunden.

Die deutsche Kreditwirtschaft hat ca. 50 Millionen ZKA-Chipkarten ausgegeben. Dabei handelt es sich hauptsächlich um kontogebundene Karten. Zusätzlich zu den Bezahlfunktionen steht auf diesen Chipkarten noch freier Speicherplatz zur Verfügung. Ein

Teil dieses Bereiches ist zur Aufnahme von Zusatzanwendungen reserviert, denen die Standards "Elektronischer Fahrschein" und "ZKA-Marktplatz" zugrunde liegen. Die Chipkarten fungieren damit als mobile Datenträger, die die Speicherung und den Austausch von Zusatzanwendungsdaten ermöglichen. Dazu werden Sicherheitsmodule benötigt, die ein gesichertes Schreiben und Lesen aus und in die Chipkarten erlauben.

Die ZKA-Chipkarten verfügen über ein Betriebssystem, das an die begrenzten Ressourcen und Ein-/Ausgabe-Schnittstellen der Chipkarten angepasst ist. Das Betriebssystem beinhaltet neben den Kommandos zur Datei-Verwaltung auch umfangreiche Sicherheitsmechanismen. Neben der Chipkarten-Hardware werden ebenso die Betriebssysteme weiter entwickelt. So sind ab Oktober 2000 die ZKA-Chipkarten mit einem in der Funktionalität umfangreich erweiterten Betriebsystem ausgegeben worden. Das aktuelle Betriebssystem SECCOS ermöglicht auch die Ausführung asymmetrischer Kryptoverfahren mit der ZKA-Chipkarte. Eine für die Bearbeitung von Zusatzanwendungen wesentliche Eigenschaft von SECCOS ist, dass Datenfelder auf der ZKA-Chipkarte angelegt werden können, die Records unterschiedlicher Länge enthalten.

Die Datei-Struktur einer Chipkarte ist vergleichbar mit dem Datei-System eines Standard-Betriebssystems für Home-PCs (z. B. UNIX oder MS-Windows). So gibt es einen Verzeichnisbaum, der in einem Root-Verzeichnis, dem sogenannten **MF** (= 'Master File'), beginnt und sich dann in weitere Verzeichnisse und darin enthaltene Datenfelder erstreckt. Die Verzeichnisse werden mit **DF** ('Dedicated File') und die Datenfelder, d. h. die "eigentlichen" Dateien, mit **EF** ('Elementary File') abgekürzt.

Alle EFs sind aus **Records** aufgebaut.[3] Die Records stellen die kleinste adressierbare Einheit eines EF dar. Ein Record kann eine Länge von 1 Byte bis 255 Byte haben, und ein EF kann bis zu 254 Records enthalten.

Da die Records eines EF unterschiedlich lang sein können, wird beim Anlegen eines EF auf der ZKA-Chipkarte die *maximale* Länge angegeben, den ein Record dieses EF haben darf. Das EF darf kürzere Records enthalten.

Das MF einer ZKA-Chipkarte enthält neben den kreditwirtschaftlichen Applikationen ein sogenanntes Zusatzanwendungshauptverzeichnis (**ZA_MF_NEU**). Das Verzeichnis ZA_MF_NEU ist das übergeordnete Verzeichnis für alle eingebrachten Zusatzanwendungen. Insbesondere enthält es die Verzeichnisse **DF_FAHRSCHEIN_NEU** und **DF_MARKTPLATZ_NEU** zur Aufnahme von Zusatzanwendungen, die auf den Standards "Elektronischer Fahrschein" bzw. "ZKA-Marktplatz" basieren. Zusätzlich kann das ZA_MF_NEU aber auch Verzeichnisse für weitere Zusatzanwendungen enthalten, z. B. für Rabattmarken-Anwendungen. So legen beispielsweise verschiedene Institutsgruppen bei der

[3] SECCOS unterstützt zusätzlich zu den recordorientierten auch sogenannte transparente Dateistrukturen, die aber nicht zur Speicherung von Zusatzanwendungsdaten nach den ZKA-Standards eingesetzt und daher hier nicht näher erläutert werden.

Produktion weitere Verzeichnisse zur Aufnahme von Zusatzanwendungsdaten auf der ZKA-Chipkarte an, die wie ZKA-Marktplatz-Anwendungen strukturiert sind, aber mit anderen kryptographischen Schlüsseln arbeiten.

Die Berechtigungen des Elektronischen Fahrscheins werden in dem Datenfeld **EF_FAHRSCHEIN** eingebracht. Dieses Datenfeld ist in dem Verzeichnis DF_FAHRSCHEIN_NEU enthalten. Berechtigungen, die auf dem ZKA-Marktplatz basieren, werden in das Datenfeld **EF_MARKTPLATZ** eingebracht. Dieses Datenfeld ist in dem Verzeichnis DF_MARKTPLATZ_NEU enthalten.

Die folgende Abbildung zeigt die Einbettung dieser Dateien innerhalb der bereits bei der Produktion erstellten Vorstrukturierung einer ZKA-Chipkarte.

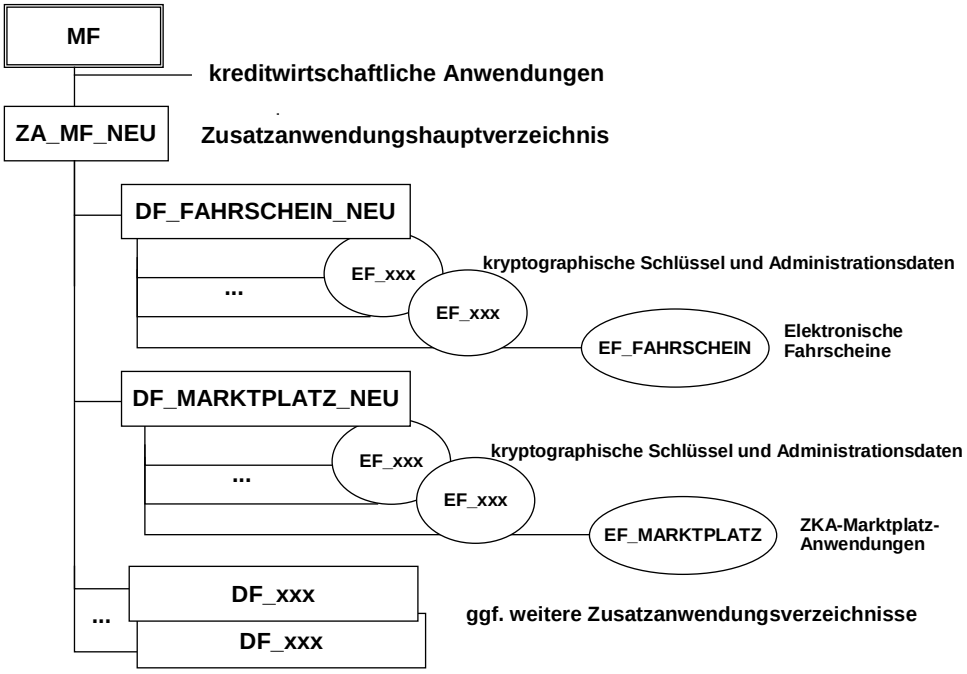


Abbildung 3: Verzeichnisstruktur auf der ZKA-Chipkarte

3.3 Die Sicherheitsmodule

3.3.1 Das Sicherheitsmodul der Applikation ZKA-Marktplatz

Zur Bearbeitung von Applikationen auf der ZKA-Chipkarte, die sich an die Vorgaben des Standards “ZKA-Marktplatz” halten, wurde im ZKA das Sicherheitsmodul der Applikation Marktplatz (**MSAM**) spezifiziert. Mit dem MSAM kann auf alle ZKA-Chipkarten zugegriffen werden, die sich bezüglich der Speicherung der Applikationsdaten an die Vorgaben des ZKA-Marktplatzes halten. Insbesondere können über dieses Modul nicht nur Marktplatz-Anwendungen in den Verzeichnissen DF_MARKTPLATZ_NEU der ZKA-Chipkarte bearbeitet werden, sondern auch solche in anderen Zusatzanwendungsverzeichnissen, sofern der Aufbau der Applikationsdaten den Vorgaben des ZKA-Marktplatzes entspricht.

Das MSAM wird bei einem Zusatzanwendungsanbieter oder seinen Akzeptanzpartnern zur Bearbeitung von Zusatzanwendungen eingesetzt, die dem Standard "ZKA-Marktplatz" folgen. Es wird dazu benötigt, Marktplatz-Anwendungsdaten auf der ZKA-Chipkarte gesichert anzulegen, auszulesen, zu verändern und zu löschen.

Das MSAM enthält mehrere Applikationsverzeichnisse, genannt **DF_MSAM1**, **DF_MSAM2**, ... Dadurch kann ein Akzeptant gleichzeitig an mehreren Zusatzanwendungen teilnehmen. Die Zusatzanwendungsdaten müssen zudem nicht notwendigerweise im Verzeichnis DF_MARKTPLATZ_NEU der ZKA-Chipkarte abgelegt sein, sondern können auch in anderen Zusatzanwendungsverzeichnissen, die Marktplatz-orientierte Datenstrukturen aufnehmen, auftreten. Insbesondere können die verschiedenen Verzeichnisse DF_MSAM1, DF_MSAM2, ... mit unterschiedlichen kryptographischen Schlüsseln ausgestattet sein.

Funktionen des Sicherheitsmoduls MSAM

Das MSAM hat die Aufgaben,

- das Überprüfen von Berechtigungen, die aus der ZKA-Chipkarte gelesen wurden,
- das Anlegen von Berechtigungen auf der ZKA-Chipkarte,
- das Modifizieren von Berechtigungen in der ZKA-Chipkarte,
- das Löschen von Berechtigungen in der ZKA-Chipkarte und
- die Auswertung des Jugendschutzmerkmals

zu unterstützen.

Bei der erstgenannten Aktivität, dem Überprüfen von Berechtigungen, wird das MSAM dazu eingesetzt, ein kryptographisches Merkmal, das von der Karte über die ausgelesenen Anwendungsdaten berechnet wurde, auf Korrektheit zu prüfen.

Für die drei Aktivitäten Anlegen, Modifizieren und Löschen ist ein Schreibzugriff auf das EF_MARKTPLATZ der ZKA-Chipkarte erforderlich. Aufgrund der Zugriffsbedingungen, die in der ZKA-Chipkarte kodiert sind, ist das Schreiben von Daten in das EF_MARKTPLATZ nur möglich, wenn das entsprechende Chipkartenkommando an die ZKA-Chipkarte mit einem kryptographischen Merkmal versehen ist, das die Integrität der übertragenen Daten bezeugt. Zur Berechnung solcher Integritätsmerkmale werden die Ergänzungskommandos des MSAM eingesetzt.

Das Akzeptanzterminal übergibt den Ergänzungskommandos die zur Berechnung des Integritätsmerkmals benötigten Daten. Das Sicherheitsmodul führt das Kommando nur nach erfolgreicher Prüfung der übergebenen Daten aus und generiert nur Integritätsmerkmale für Datensätze, die "korrekt" aufgebaut sind.

Ein wesentliches Merkmal des MSAMs ist die Unterstützung eines Gruppenkonzeptes, wodurch die Modifikation von Marktplatz-Anwendungen auf einer Kundenkarte kontrolliert wird. Beim Anlegen einer Marktplatz-Anwendung auf einer ZKA-Chipkarte legt der anlegende Akzeptant fest, welche weiteren Akzeptanten die Anwendungsdaten modifizieren dürfen. Diese Akzeptanten sind zu einer Gruppe zusammengefasst. Alle Gruppenmitglieder verfügen über eine einheitliche Gruppen_ID, die in die MSAMs ihrer Akzeptanzterminals eingebracht ist. Ein beliebiges Mitglied der Gruppe ist zwar nicht in der Lage, den Datensatz eines anderen Gruppenmitgliedes zu überschreiben oder zu löschen, kann aber bestimmte Datenfelder des Datensatzes modifizieren (z. B. einen Gutschein entwerten oder einen Bonuszählerstand verändern).

Im Unterschied zum Fahrschein-Sicherheitsmodul existiert für das Marktplatz-Sicherheitsmodul keine Ausprägung, die das Ausstellen von Berechtigungen fest an eine Bezahltransaktion mit der GeldKarte koppelt (vgl. Kapitel 3.3.2.1).

3.3.2 Das Sicherheitsmodul der Applikation Fahrschein

Um elektronische Fahrscheine in der ZKA-Chipkarte anzulegen, kommuniziert diese mit dem Sicherheitsmodul der Applikation Fahrschein (**FSAM**).

Das Sicherheitsmodul der Applikation Fahrschein ist logisch gesehen eine Erweiterung der Händlerkarte, die im GeldKarte-System als Sicherheitsmodul beim Händler zur sicheren Abwicklung von Bezahltransaktionen eingesetzt wird. Die Händlerkarte ist auf einer ZKA-Chipkarte realisiert. Die Parameter des FSAM werden im Anhang C erläutert.

Die Erweiterung der Händlerkarte besteht darin, dass der Dateistruktur der Händlerkarte ein weiteres Applikationsverzeichnis hinzugefügt wird, das als **DF_FSAM_NEU** bezeichnet wird. Das Verzeichnis enthält die kryptographischen Schlüssel, die zur Bearbeitung des Datenfeldes EF_FAHRSCHEIN auf der ZKA-Chipkarte benötigt werden. Außerdem verfügt die erweiterte Händlerkarte neben den Standardfunktionen des ZKA-Betriebssystems über weitere Funktionen, sogenannte Ergänzungskommandos, die speziell zur Verarbeitung von Fahrscheinen auf der ZKA-Chipkarte konzipiert wurden.

Funktionen des Sicherheitsmoduls

Das FSAM hat die Aufgaben,

- das Überprüfen von Fahrscheinen, die aus der ZKA-Chipkarte gelesen wurden,
- das Anlegen von Fahrscheinen auf der ZKA-Chipkarte,
- das Modifizieren von Fahrscheinen in der ZKA-Chipkarte und
- das Löschen von Fahrscheinen in der ZKA-Chipkarte

zu unterstützen.

Bei der erstgenannten Aktivität, dem Überprüfen von Fahrscheinen, wird das FSAM dazu eingesetzt, ein kryptographisches Merkmal, das von der Karte über die ausgelesenen Fahrscheindaten berechnet wurde, auf Korrektheit zu prüfen.

Für die drei letzten Aktivitäten (Anlegen, Modifizieren und Löschen) ist ein Schreibzugriff auf das EF_FAHRSCHEIN der ZKA-Chipkarte erforderlich. Aufgrund der Zugriffsbedingungen, die in der ZKA-Chipkarte kodiert sind, ist das Schreiben von Daten in das EF_FAHRSCHEIN nur möglich, wenn das entsprechende Chipkartenkommando an die ZKA-Chipkarte mit einem kryptographischen Merkmal versehen ist, das die Integrität der übertragenen Daten bezeugt. Zur Berechnung solcher Integritätsmerkmale werden die Ergänzungskommandos des FSAM eingesetzt.

Das ÖPV-Terminal übergibt den Ergänzungskommandos die zur Berechnung des Integritätsmerkmals benötigten Daten. Das Sicherheitsmodul führt das Kommando nur nach erfolgreicher Prüfung der übergebenen Daten aus und generiert nur Integritätsmerkmale für Datensätze, die "korrekt" aufgebaut sind. Was dies in Bezug auf die einzelnen Funktionen eines ÖPV-Terminals bedeutet, wird in Kapitel 3.4 erläutert.

3.3.2.1 Kopplung / Entkopplung von der Bezahltransaktion

Das Sicherheitsmodul FSAM kann in zwei Modi betrieben werden.

Im sog. **gekoppelten Modus** gestattet das Sicherheitsmodul beim Anlegen eines Fahrscheins seine Speicherung in der ZKA-Chipkarte nur, wenn mit dieser ZKA-Chipkarte unmittelbar zuvor eine Bezahltransaktion über den Wert des anzulegenden Fahrscheins durchgeführt wurde, d. h. das Ausstellen des Fahrscheins ist an die Bezahltransaktion gekoppelt.

Um an dieser Stelle eine größere Flexibilität zu erreichen, kann das FSAM in einem zweiten Modus betrieben werden, der es gestattet, die beiden Transaktionen "Anlegen eines Fahrscheins auf der ZKA-Chipkarte" und "Bezahlen mit der GeldKarte" voneinander zu

entkoppeln. Solche Sicherheitsmodule ermöglichen es, Fahrscheine in einer ZKA-Chipkarte abzulegen, ohne dass zuvor eine Bezahltransaktion mit dieser GeldKarte durchgeführt wurde. Mit dieser Entkopplung wird das Ziel verfolgt, sowohl höherpreisige Fahrscheine auf der ZKA-Chipkarte anlegen zu können, als auch die Wahl des Zahlungsmittels dem Kunden zu überlassen. Im **entkoppelten Modus** autorisiert das Sicherheitsmodul im Rahmen von flexibel einstellbaren Randbedingungen (Maximalbetrag pro Fahrschein, Gesamtbetrag über alle Fahrscheine, etc.) jede Einbringung eines Fahrscheins in die ZKA-Chipkarte ohne eine konkrete Prüfung der Bezahlung. Der ordnungsgemäße Ablauf muss dann durch die Terminalsteuerung gewährleistet werden. Insbesondere muss die Terminalsteuerung sicherstellen, dass der entsprechende Betrag vor dem Einbringen des Fahrscheins in irgendeiner Form bezahlt worden ist (z.B. electronic cash, bar oder GeldKarte).

Bei einem Diebstahl könnte ein Sicherheitsmodul, das den entkoppelten Modus unterstützt, Fahrscheine bis zum Erreichen eines Maximalgesamtbetrages autorisieren. Dieser Maximalbetrag wird daher abhängig vom Terminalstandort und damit vom Diebstahlrisiko eingestellt, z. B. am Terminal in einer Service-Kundenhalle höher als am Automaten einer wenig frequentierten Haltestelle.

Da ein Sicherheitsmodul, das ausschließlich den gekoppelten Modus unterstützt, stets vor dem Autorisieren eines Fahrausweises für eine ZKA-Chipkarte prüft, dass der zu entrichtende Betrag mit derselben GeldKarte bezahlt worden ist, ist ein Missbrauch eines solchen Sicherheitsmoduls bei einem Diebstahl ausgeschlossen.

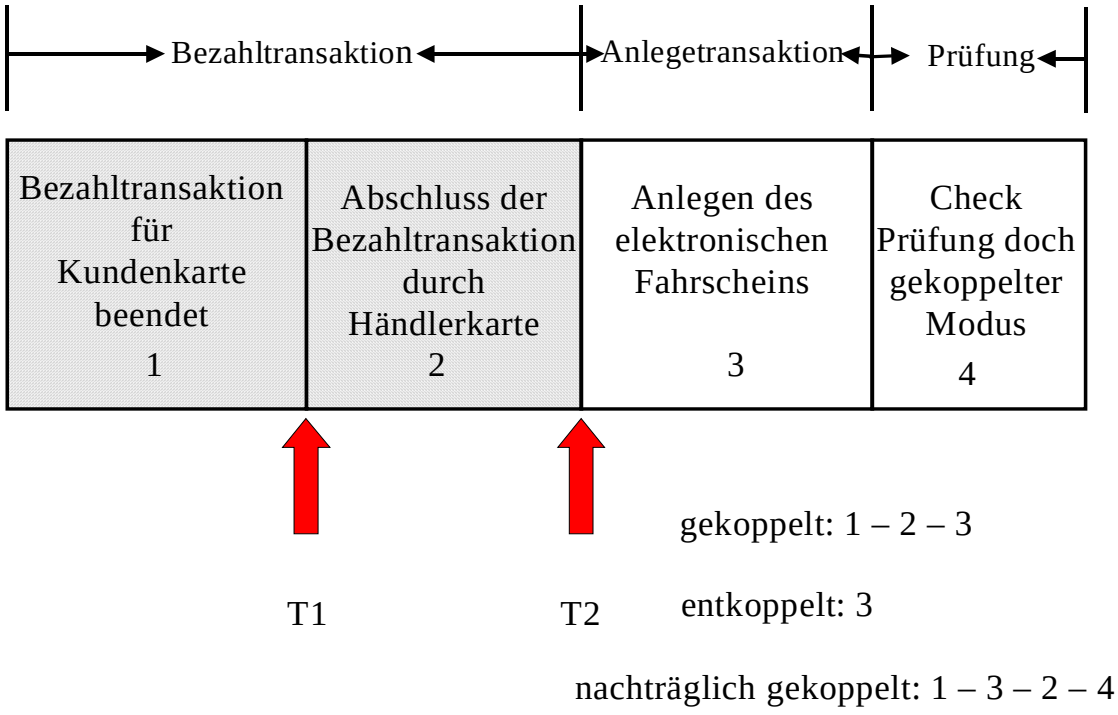


Abbildung 4: Anlege-Modi

In Abbildung 4 werden die unterschiedlichen Abläufe beim Anlegen von Fahrscheinen veranschaulicht. Dabei wird unterschieden zwischen dem Bezahlvorgang (Schritte 1 und 2), dem Anlegevorgang (Schritt 3) und der optionalen Überprüfung, ob die letzte Bezahltransaktion zu der letzten Anlegetransaktion passt. Zum Zeitpunkt T1 ist die Bezahltransaktion für die Kundenkarte abgeschlossen, kann also ohne sie beendet werden. Da Schritt 2 aber noch nicht durchgeführt ist, ist auch ein Rückbuchen des Bezahlbetrages in die Kundenkarte noch möglich. Nach Schritt 2 ist das Rückbuchen in die Kundenkarte nicht mehr möglich. Die Information über den Bezahlvorgang liegen aber erst nach Schritt 2 im Sicherheitsmodul vor, so dass ein Fahrschein gekoppelt angelegt werden kann. Erfolgt Schritt 2 erst nach der erfolgreichen Ausführung von Schritt 3, so kann mit Schritt 4 auch nachträglich noch festgestellt werden, dass es "eigentlich" ein gekoppelter Anlegevorgang war. Im Schritt 4 werden dann auch die im Sicherheitsmodul gepflegten Zähler entsprechend korrigiert.

Von einem entkoppelten Anlegen wird gesprochen, wenn nur Schritt 3 alleine ausgeführt wird bzw. wenn nicht mit der ZKA-Chipkarte bezahlt wird, in der der Fahrschein gespeichert wird.

Gekoppelt werden Fahrscheine angelegt wenn die Schritte 1, 2 und 3 nacheinander ausgeführt werden.

Bei einem nachträglich gekoppelten Anlegevorgang wird erst Schritt 1, dann Schritt 3 vor Schritt 2 und am Ende Schritt 4 ausgeführt.

3.3.3 Kombination von Sicherheitsmodulen

Wie in Kapitel 3.3.2 beschrieben, ist das FSAM stets mit einer Händlerkarte gekoppelt. Das MSAM kann entweder als eigenständiges Sicherheitsmodul existieren oder auf einer ZKA-Chipkarte wie folgt kombiniert werden:

- entweder zusammen mit einer Händlerkarte (ohne FSAM) oder
- zusammen mit FSAM und Händlerkarte.

Daneben ist es auch möglich, im gleichen Terminal die Sicherheitsmodule MSAM und FSAM auf unterschiedlichen ZKA-Chipkarten zu betreiben.

3.4 Akzeptanzterminals

3.4.1 ÖPV-Terminals

3.4.1.1 Anlegen eines Fahrscheins

Der Kunde hat z. B. am Automaten seinen Fahrschein ausgewählt. Das Terminal stellt den elektronischen Fahrschein zusammen und ermittelt die benötigte Anzahl von Records, wobei maximal 80 Byte pro Record aufgenommen werden können. Des weiteren prüft das Terminal, in welchen Record der ZKA-Chipkarte die neue Berechtigung eingebracht werden kann.

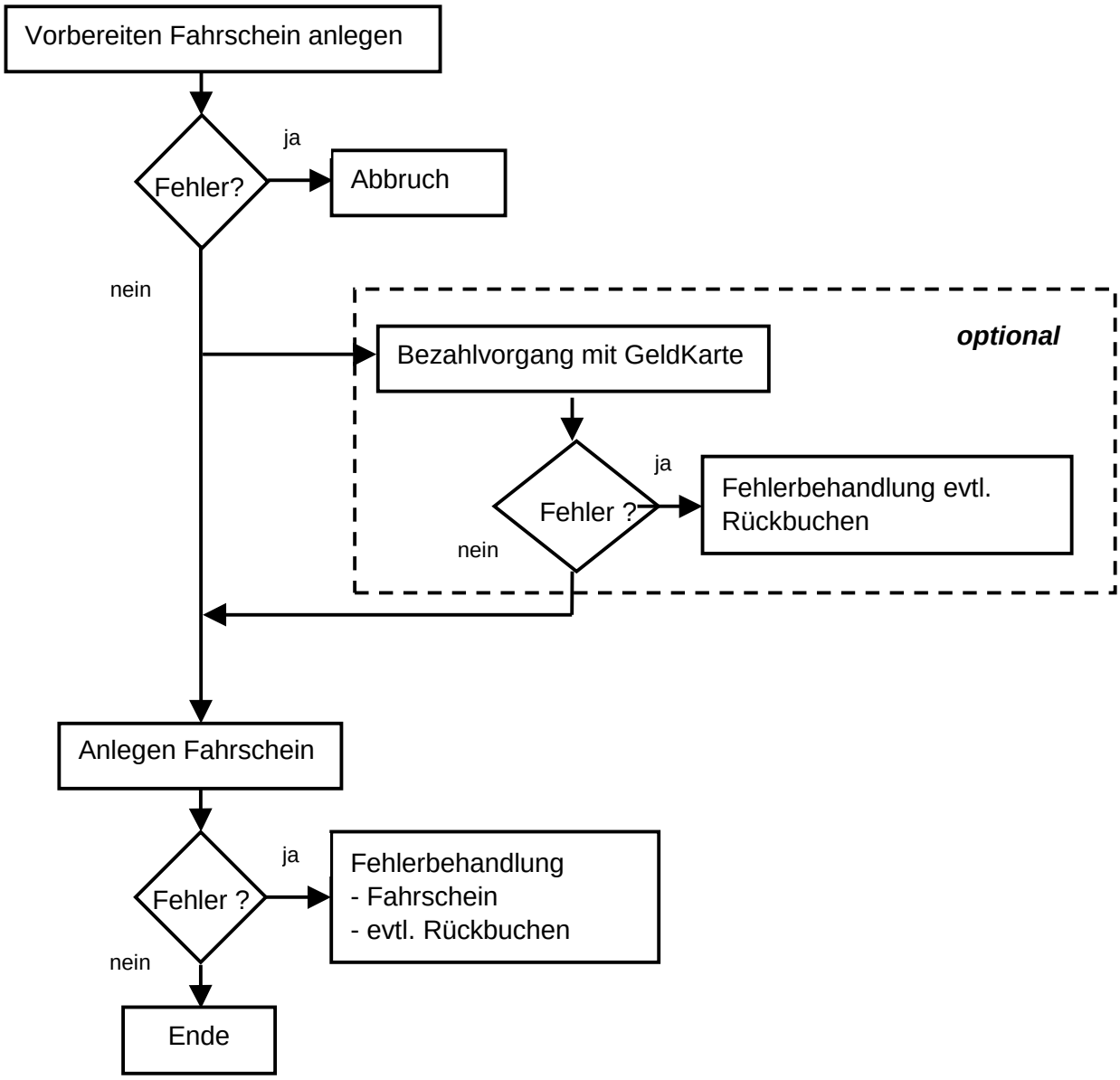


Abbildung 5: Ablauf Anlegen von Fahrscheinen

Der Kunde bezahlt seinen Fahrschein. Bei der Bezahlweise muss die Art der Kopplung des Bezahlvorgangs berücksichtigt werden. Falls der Bezahlvorgang aufgrund der Konfiguration des Sicherheitsmoduls gekoppelt erfolgt, muss der Fahrschein vollständig mit der elektronischen Geldbörse bezahlt werden, ansonsten autorisiert das Sicherheitsmodul das Anlegen nicht. Falls das Sicherheitsmodul einen entkoppelten Bezahlvorgang gestattet, kann eine andere Zahlungsweise, z. B. bar oder mit ec-Karte, gewählt werden. Dann muss das Terminal zuverlässig die Bezahlung des Fahrscheins prüfen.

Aufgrund der Zugriffsbedingungen der ZKA-Chipkarte kann ein Fahrschein-Record nur in die ZKA-Chipkarte geschrieben werden, wenn er mit einem Integritätsmerkmal (MAC) versehen ist. Dieser MAC muss vom Terminal bereitgestellt werden. Der kryptographische Schlüssel zur Berechnung des MAC ist ausschließlich in der ZKA-Chipkarte und im FSAM verfügbar. Daher übergibt das Terminal dem FSAM Daten des anzulegenden Fahrscheins sowie den Inhalt des Records, der in der ZKA-Chipkarte überschrieben werden soll. Das FSAM prüft, dass der zu überschreibende Record bereits verfallen ist, und berechnet den MAC für den anzulegenden Fahrschein. Für die MAC-Berechnung baut das FSAM den anzulegenden Fahrschein intern auf und kontrolliert dabei die Korrektheit des Aufbaus nach dem ZKA-Standard. Das FSAM übergibt nach erfolgreicher Kommandoausführung den berechneten MAC an das Terminal, das den Fahrschein-Record zusammen mit dem MAC an die ZKA-Chipkarte übergibt. Die ZKA-Chipkarte prüft den MAC und aktualisiert den Recordeintrag. Dieses Verfahren ist iteriert anzuwenden, wenn ein Fahrschein, der aus mehreren Records besteht, in die ZKA-Chipkarte geschrieben werden soll.

3.4.1.2 Ändern und Entwerten eines Fahrscheins

Die Entwertung eines Fahrscheins erfolgt, indem der Entwertungszähler inkrementiert und die zusätzlichen Datenheader-Informationen (ZD_INFO) aktualisiert werden. Dabei ist der Record in der ZKA-Chipkarte mit den neuen Werten zu überschreiben. Auch für diesen Schreibvorgang muss das Terminal einen MAC bereitstellen, der vom FSAM zu berechnen ist.

3.4.1.3 Löschen eines Fahrscheins

Ein Fahrschein wird gelöscht, indem der Verfallzeitpunkt des Einzelrecords bzw. aller verknüpften Records auf den Erstellzeitpunkt zurückgesetzt und anschließend der erste Record mit einem Initialrecord überschrieben wird. Auch für diesen Schreibvorgang muss das Terminal einen MAC bereitstellen, der vom FSAM zu berechnen ist. Die Funktion ist nur auf Fahrscheine anwendbar, die vom Zusatzanwendungsanbieter ausgestellt wurden. Dies wird über die Betreiber_ID kontrolliert, die in den Fahrscheindaten und im FSAM identisch sein muss.

3.4.1.4 Kontrollieren eines Fahrscheins

Bei einer Fahrscheinkontrolle muss der Inhalt eines Fahrschein-Records bestimmt und dessen Echtheit durch ein Sicherheitsmodul verifiziert werden.

Das Terminal (z. B. ein Kontrolleur-Lesegerät) liest den Record der ZKA-Chipkarte aus, in dem sich die zu überprüfende Berechtigung befindet. Bei diesem Lesezugriff berechnet die ZKA-Chipkarte einen MAC, den sie ebenfalls ausgibt. Das Terminal schickt die Recorddaten samt MAC an das FSAM, welches den korrekten Aufbau (nicht den Inhalt) des Fahrscheins und dessen MAC prüft. Nach positiver Verifikation ist sichergestellt, dass ein echter Fahrschein in der ZKA-Chipkarte enthalten ist.

3.4.1.5 Ungesichertes Lesen eines Fahrscheins

Bei dieser Transaktion werden Fahrscheindaten aus der Karte ungesichert ausgelesen, d. h. von der ZKA-Chipkarte wird *kein* MAC über die gelesenen Daten angefordert. Dies geschieht beispielweise im Taschenkartenleser mit einem standardisierten Kommando. Die Chipkarte gibt daraufhin den entsprechenden Recordinhalt aus, welcher vom Taschenkartenleser ausgewertet wird, der dann z.B. die Ticketdaten und den Fahrpreis ausgibt.

Diese Transaktion wird *ohne* Sicherheitsmodul ausgeführt.

3.4.2 Marktplatz-Terminal

Im Folgenden werden Funktionen eines Marktplatz-Terminals beschrieben, die geeignet sind, Marktplatz-Anwendungen im Verzeichnis DF_MARKTPLATZ_NEU der ZKA-Chipkarte zu bearbeiten. Für die Bearbeitung von Marktplatz-Anwendungen in anderen Zusatzanwendungsverzeichnissen einer ZKA-Chipkarte können davon abweichende Funktionen erforderlich sein. So ist es beispielsweise möglich, dass der Zugriff auf solche Anwendungsdaten erst nach einer Benutzerauthentikation mittels einer applikationsspezifischen PIN möglich ist. Im Folgenden wird aber nur der "Standardfall" betrachtet.

3.4.2.1 Anlegen einer Marktplatz-Berechtigung

Daten einer ZKA-Marktplatz-Anwendung können an einem Terminal in die ZKA-Chipkarte geschrieben werden, sofern im Terminal die entsprechenden Datensätze vorliegen und es über ein Sicherheitsmodul MSAM verfügt. Dabei können die Daten im Terminal fest gespeichert, von einem Benutzer eingegeben worden oder auch auf andere Weise, z. B. über eine Kassenschnittstelle, an das Terminal übertragen worden sein.

Das Terminal stellt den bzw. die in der ZKA-Chipkarte anzulegenden Datensätze der Marktplatz-Anwendung zusammen und ermittelt die benötigte Anzahl von Records. Zur Zeit

können im Verzeichnis DF_MARKTPLATZ_NEU pro Record Zusatzanwendungsdaten mit maximal 60 Byte aufgenommen werden.[4] Des weiteren prüft das Terminal, in welchen Record bzw. welche Records der ZKA-Chipkarte die neue Berechtigung eingebracht werden kann.

Aufgrund der Zugriffsbedingungen der ZKA-Chipkarte kann eine Markplatz-Berechtigung nur in die ZKA-Chipkarte geschrieben werden, wenn sie mit einem Integritätsmerkmal (MAC) versehen ist. Dieser MAC muss vom Terminal bereitgestellt werden. Der kryptographische Schlüssel zur Berechnung des MAC ist ausschließlich in der ZKA-Chipkarte und im MSAM verfügbar. Daher übergibt das Terminal dem MSAM Daten der anzulegenden Berechtigung sowie den Inhalt des Records, der in der ZKA-Chipkarte überschrieben werden soll. Das MSAM prüft, dass der zu überschreibende Record bereits verfallen ist, und berechnet den MAC für die anzulegende Berechtigung. Für die MAC-Berechnung baut das MSAM die anzulegende Berechtigung intern auf und kontrolliert dabei die Korrektheit des Aufbaus nach dem ZKA-Standard. Das MSAM übergibt nach erfolgreicher Kommandoausführung den berechneten MAC an das Terminal, das den Marktplatz-Record zusammen mit dem MAC an die ZKA-Chipkarte übergibt. Die ZKA-Chipkarte prüft den MAC und aktualisiert den Recordeintrag. Dieses Verfahren ist iteriert anzuwenden, wenn eine Berechtigung, die aus mehreren Records besteht, in die ZKA-Chipkarte geschrieben werden soll.

Insbesondere kann beim Anlegen einer Marktplatz-Berechtigung eine Gruppen_ID in den Datensatz eingetragen werden, die das spätere Modifizieren der Berechtigung neben dem ausstellenden Akzeptanten auch anderen Gruppenmitgliedern erlaubt.

Der Standard "ZKA-Marktplatz" gestattet es, anwendungsspezifische vertrauliche Daten in einer Marktplatz-Berechtigung verschlüsselt zu speichern. Der Verschlüsselungsschlüssel ist nicht in der ZKA-Chipkarte, sondern ausschließlich im MSAM gespeichert. Die Sicherheitsmechanismen des MSAMs garantieren, dass eine spätere Entschlüsselung der Daten nur an Terminals des Akzeptanten möglich ist, der die Marktplatz-Berechtigung angelegt hat.

3.4.2.2 Einlösen einer Marktplatz-Berechtigung

Eine Marktplatz-Berechtigung wird bei einem Akzeptanten eingelöst, indem sie

- vom Akzeptanten erfolgreich auf Echtheit überprüft wird (im Fall eines Ausweises) bzw.
- vom Akzeptanten erfolgreich auf Echtheit überprüft und (teilweise oder vollständig) entwertet wird (im Fall eines Gutscheins).

[4] In spezifischen Zusatzanwendungsverzeichnissen einzelner Institutsgruppen sind auch davon abweichende Recordlängen möglich.

Die Entwertung eines Gutscheins erfolgt, indem der Entwertungszähler in den Gutscheindaten inkrementiert wird. Zur Entwertung des Gutscheines sind neben dem ausstellenden Akzeptanten auch seine Verbundpartner berechtigt, sofern der Gutschein eine Gruppenkennung enthält. Im Rahmen der Entwertung ist der Record in der ZKA-Chipkarte mit einem Record zu überschreiben, der den neuen Zählerwert enthält. Auch für diesen Schreibvorgang muss das Terminal einen MAC bereitstellen, der vom MSAM zu berechnen ist.

Die Entwertung eines Gutscheines wie auch die Prüfung eines Ausweises setzt voraus, dass die Integrität der aus der ZKA-Chipkarte ausgelesenen Marktplatz-Anwendungsdaten überprüft wird. Bei dem Lesezugriff berechnet die ZKA-Chipkarte einen MAC, den sie zusammen mit den Anwendungsdaten ausgibt. Das Terminal schickt diese Daten inklusive MAC an das MSAM, welches den korrekten Aufbau (nicht den Inhalt) der Anwendungsdaten und deren MAC prüft. Nach positiver Verifikation ist sichergestellt, dass eine echte Marktplatz-Anwendung in der ZKA-Chipkarte enthalten ist.

Sind in der zur Prüfung ausgelesenen Marktplatz-Berechtigung verschlüsselte Daten enthalten, so werden diese am Terminal entschlüsselt, sofern es sich um ein Terminal des Akzeptanten handelt, der die Berechtigung auf der ZKA-Chipkarte angelegt hat.

3.4.2.3 Modifizieren einer Marktplatz-Berechtigung

Spezielle anwendungsspezifische Felder einer Marktplatz-Berechtigung können vom ausstellenden Akzeptanten modifiziert werden. Dazu zählen insbesondere die Punktestände in Bonusberechtigungen. Enthält die Berechtigung eine Gruppen_ID, so sind zusätzlich die Verbundpartner des Ausstellers, die dieser Gruppe zugeordnet sind, autorisiert, diese Modifikationen durchzuführen. Der Record in der ZKA-Chipkarte wird mit einem Record überschrieben, der die veränderten Daten enthält. Auch für diesen Schreibvorgang muss das Terminal einen MAC bereitstellen, der vom MSAM zu berechnen ist.

3.4.2.4 Löschen einer Marktplatz-Berechtigung

Eine Marktplatz-Berechtigung auf der ZKA-Chipkarte wird gelöscht, indem der entsprechende erste Record mit Initialdaten überschrieben wird. Das Überschreiben der Berechtigung ist ausschließlich dem ausstellenden Akzeptanten möglich. Auch für diesen Schreibvorgang muss das Terminal einen MAC bereitstellen, der vom MSAM zu berechnen ist.

3.4.2.5 Ungesichertes Lesen einer Markplatz-Berechtigung

Bei dieser Transaktion werden Daten einer Marktplatz-Anwendung aus der Karte ungesichert ausgelesen, d. h. von der ZKA-Chipkarte wird *kein* MAC über die gelesenen Daten angefordert. Dies geschieht beispielweise im Taschenkartenleser mit einem standardisierten Kommando. Die Chipkarte gibt daraufhin den entsprechenden Recordinhalt aus, welcher vom Taschenkartenleser ausgewertet wird, der dann z.B. bei einer Bonusberechtigung den aktuellen Punktestand ausgibt. Diese Transaktion wird *ohne* Sicherheitsmodul ausgeführt.

3.4.3 Kontrollgeräte und Infoterminals für Zusatzanwendungen

Infoterminals, die Kunden zu Informationszwecken dienen, zeigen allgemeine Daten aus den ZKA-Zusatzanwendungen an. Hierunter fallen beispielsweise Taschenkartenleser für Fahrscheine und andere Tickets oder für ein Bonussystem, die dem Kunden seinen aktuellen Bonusstand anzeigen. Die Spezifikation dieser multifunktionalen Taschenkartenleser liegen vor.

Zusätzlich zur Anzeige der allgemeinen Daten können Kontrollgeräte spezielle Daten aus den individuellen Teilen der Fahrscheine und Berechtigungen anbieterspezifisch anzeigen und auswerten. In der Regel sind diese Geräte auf eine Zusatzanwendung beschränkt. Ihre individuelle Ausgestaltung hängt somit sehr stark von der jeweiligen Zusatzanwendung ab.

3.5 Übersicht über die Spezifikationen

Die folgende Abbildung enthält eine Übersicht über die Spezifikationen der Sicherheitsmodule, der Applikationen auf der Chipkarte und der Abläufe an den Terminals sowie deren Zusammenhänge.

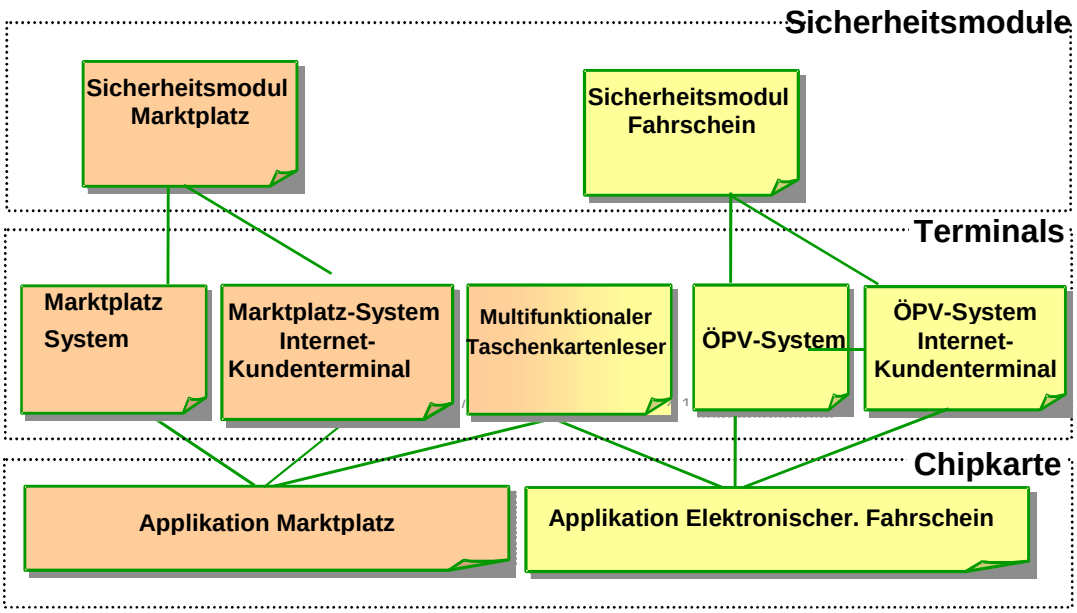


Abbildung 6: Übersicht über die Schnittstellenspezifikationen

3.6 Sicherheit

Das auf der ZKA-Chipkarte befindliche Betriebssystem wurde in seinem Entwurf auf hohe Sicherheit hin ausgelegt. Ein wichtiges Ziel ist es, das Lesen von Daten aus dem Chip der ZKA-Chipkarte oder das Schreiben von Daten in den Chip nur unter genau vorgegebenen Bedingungen zuzulassen und somit auch beim Einsatz der ZKA-Chipkarte in unsicherer Umgebung eine möglichst hohe Sicherheit zu gewährleisten. Eine solche Bedingung kann beispielsweise sein, dass ein Benutzer sich gegenüber seiner Chipkarte zunächst mit einer PIN als rechtmäßiger Karteninhaber ausweisen muss, bevor er Daten auslesen kann, oder dass ein Terminal der ZKA-Chipkarte die Kenntnis eines bestimmten, auch in der ZKA-Chipkarte vorhandenen kryptographischen Schlüssels nachweisen muss, um Daten in der ZKA-Chipkarte verändern zu dürfen. Letzteres kann dadurch geschehen, dass das Terminal mit dem fraglichen Schlüssel eine Verschlüsselungsoperation ausführt, der ZKA-Chipkarte das Ergebnis dieser Operation übermittelt und die ZKA-Chipkarte dieses Ergebnis mit ihrem Schlüssel überprüft.

Die Bedingungen, die den Zugriff auf Daten der ZKA-Chipkarte festlegen und die Ausführung von Kommandos in der ZKA-Chipkarte steuern, sind als Zugriffsregeln in der ZKA-Chipkarte kodiert. Diese Regeln werden vom Betriebssystem beim Einsatz der ZKA-Chipkarte ausgewertet. Wesentlicher Bestandteil der Zugriffsregeln sind Referenzen auf kryptographische Schlüssel, PINs und Passwörter, die in der ZKA-Chipkarte sicher gespeichert sind.

Solche Zugriffsregeln können individuell auf die verschiedenen Anwendungen der ZKA-Chipkarte zugeschnitten werden. Für die kreditwirtschaftlichen Anwendungen sind die Zugriffsregeln fest vorgegeben, ebenso für die Standards "Elektronischer Fahrschein" und "ZKA-Marktplatz" im Bereich der Zusatzanwendungen. Insbesondere kann also ein Zusatzanwendungsanbieter, der seine Anwendung auf einem von der ZKA-Chipkarte unterstützten Standard aufbaut, auf die Sicherheitsinfrastruktur der Chipkarte zurückgreifen.

4 Rollenmodell

Ein Anbieter meldet bei seinem Kreditinstitut eine Anwendung an (z. B. ein System zur Verarbeitung elektronischer Fahrscheine oder von Bonuspunkten), die er auf Basis vorgegebener Rahmenbedingungen entwickelt hat.

Damit der Anbieter auf den freien Speicherbereich der ZKA-Chipkarte zugreifen kann, um seine Zusatzanwendungsdaten dort einbringen und bearbeiten zu können, benötigt er ein geeignetes Sicherheitsmodul. Dieses FSAM oder MSAM muss in der Lage sein, die kryptographischen Funktionen auszuführen, die zur Bearbeitung der Zusatzanwendung auf der ZKA-Chipkarte notwendig sind. Der Anbieter bestellt solche Sicherheitsmodule über sein Kreditinstitut, die so genannte Händlerbank.

Die Sicherheitsmodule sind individuell so konfigurierbar, dass sie die Zugriffe verschiedener Anbieter auf die ZKA-Chipkarte voneinander separieren. Damit wird verhindert, dass ein Anbieter Berechtigungen, die ein anderer Anbieter auf der ZKA-Chipkarte angelegt hat, unberechtigterweise modifizieren oder löschen kann.

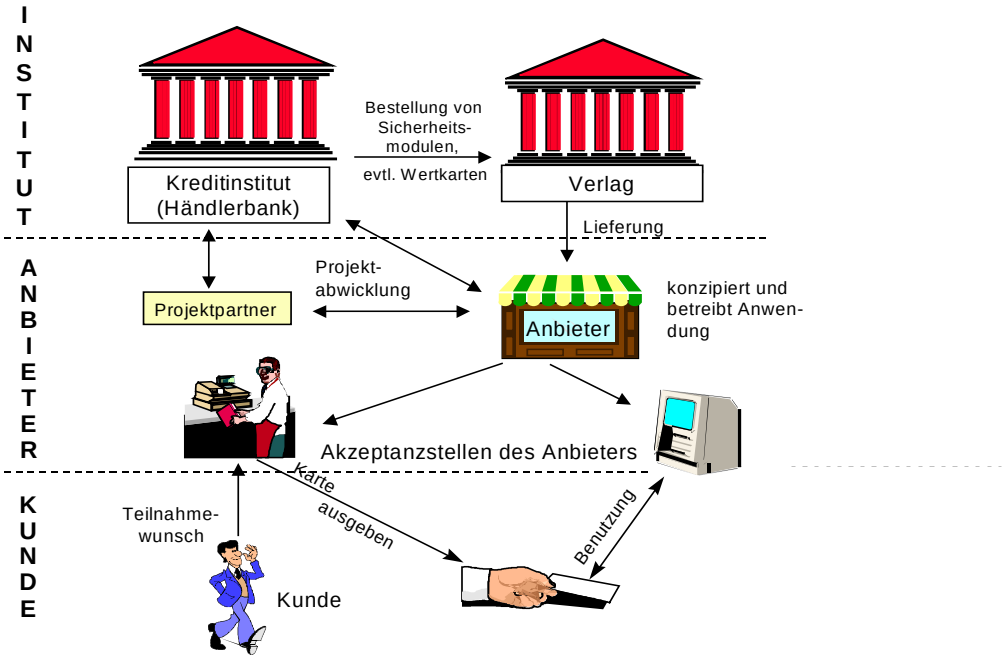


Abbildung 7: Rollenmodell

Die Händlerbank leitet die Bestellung der Sicherheitsmodule an einen Verlag weiter. Dort werden die Sicherheitsmodule mit den anbieterspezifischen Daten konfiguriert und an den Anbieter ausgeliefert.

Der Anbieter rüstet seine Akzeptanzterminals und die seiner Akzeptanzpartner mit den gelieferten Sicherheitsmodulen aus und erstellt eine Terminalablaufsteuerung für seine Zusatzanwendung. Betreiber des Terminals ist der Anbieter oder ggf. ein Vertragspartner, z. B. ein Verkehrsunternehmen oder ein Einzelhändler.

Soll die Anwendung auf kontoungebundene ZKA-Chipkarten, sog. Wertkarten, aufgebracht werden, so werden diese ggf. ebenfalls über das Kreditinstitut bestellt und vom Verlag an den Anbieter ausgeliefert.
Der Kunde erhält auf seinen Wunsch vom Anbieter an dessen Akzeptanzstellen Zugang zu einer Zusatzanwendung über seine ZKA-Chipkarte oder eine ZKA-Chipkarte des Anbieters. Allein der Kunde entscheidet, an welcher Zusatzanwendung er teilnehmen möchte. Standardmäßig enthält jede ZKA-Chipkarte bei der Kartenausgabe bereits die Datenstrukturen, die sie befähigen, Zusatzanwendungen aufzunehmen, die auf den Standards "Elektronischer Fahrschein" und "ZKA-Marktplatz" basieren.

4.1 Schritte zur Nutzung der ZKA-Zusatzanwendungen

4.1.1 Antrag des Leistungsanbieters bei der Hausbank

Soweit ein Leistungsanbieter sich zur Nutzung der Applikation entschließt, wendet er sich an seine Hausbank. Hier beantragt er im Falle des ZKA-Marktplatzes die Vergabe einer sog. Anbieter_ID sowie die Erstellung der für seine Zusatzanwendung notwendigen Sicherheitsmodule (MSAM). Die Vergabe der Anbieter_ID erfolgt über den jeweiligen Verlag, wobei die bundesweite Eindeutigkeit sichergestellt wird. Für den elektronischen Fahrschein wird eine Betreiber_ID und Servicekennungen vom VDV benötigt, die an den Verlag zu übermitteln ist.

Voraussetzung hierfür ist die Anerkennung der einheitlichen Bedingungen für Leistungsanbieter im Rahmen der Applikation durch den Leistungsanbieter sowie die Definition der Anforderungen an das vom jeweiligen Verlag zu erstellende Sicherheitsmodul.

Für die Produktion eines MSAM sind weitere Daten erforderlich. Die im EF_Kennung des MSAM zu speichernde Terminal-Kennung kann vom Leistungsanbieter vorgegeben werden. Erfolgt keine Vorgabe durch den Leistungsanbieter nimmt der das MSAM produzierende Verlag die Vergabe im Rahmen einer fortlaufenden Nummerierung vor. Zur Vergabe der Terminal-Kennung durch die Verlage ist eine entsprechende Verwaltung der Kennungen und deren Einbindung in die Personalisierungssysteme für MSAMs in den Verlagen vorzusehen. MSAMs werden prinzipiell "abgeschlossen" ausgeliefert. Die Nutzung der "Lock/Unlock"-Funktion erfolgt mit Hilfe einer vom Verlag zu produzierenden PIN. Nach dreimaliger Fehleingabe der PIN kann die PIN nicht mehr verwendet werden. Um den Fehlbedienungszähler zurückzusetzen, kann ein spezieller PUK (PIN-Unblock-Key) verwendet werden, der ebenfalls vom Verlag bei der Produktion des MSAM generiert wird und zusammen mit dem MSAM an den Leistungsanbieter ausgeliefert wird.

Die möglichen Parameter des FSAM befinden sich im Anhang C.

Auf Wunsch des Leistungsanbieters kann auch eine Limitierung der Schreibvorgänge pro Sicherheitsmodul vorgesehen werden.

Alle Informationen werden von der Hausbank an den jeweils zuständigen Verlag geleitet, der die Unterlagen prüft und die Erstellung der Sicherheitsmodule übernimmt.

4.1.2 Auslieferung Sicherheitsmodule

Der produzierende Verlag liefert im Auftrag der Hausbank des Leistungsanbieters die bestellten Sicherheitsmodule entweder direkt an den Leistungsanbieter oder über die Hausbank an den Leistungsanbieter aus. Zusammen mit den Sicherheitsmodulen erhält der Leistungsanbieter die evtl. benötigten PIN- und PUK-Briefe (auf Standard-PIN-Briefen) sowie seine weiteren Daten, wie z. B. die Anbieter_ID und – soweit beantragt – seine Gruppen_ID.

Soweit Zusatzanwendungen die gesicherte Auswertung von Datensätzen in Hintergrundsystemen erforderlich machen, ist hierzu der Zugriff auf den kryptographischen Schlüssel KGK_{LOG} des jeweiligen Anbieters notwendig. Der KGK_{LOG} wird von den Verlagen ebenfalls ausschließlich in Sicherheitsmodulen ausgeliefert.

4.1.3 Zulassung von Terminals

Die für Zusatzanwendungen vom Typ "Marktplatz" oder "Fahrschein" genutzten Terminals müssen den Anforderungen der ZKA-Spezifikation an die elektromechanischen Eigenschaften sowie an das Übertragungsprotokoll T=1 von Bezahl-Terminals genügen. Zum Nachweis der Einhaltung dieser Anforderungen ist eine ZKA-Zulassung erforderlich.

Bezahl- und Lade-Terminals, für die bereits die Einhaltung der Anforderungen an die elektromechanischen Eigenschaften und das Übertragungsprotokoll T=1 mit positivem Ergebnis untersucht worden ist, benötigen keine weitere Zulassung. Die reduzierten Anforderungen der elektromechanischen Eigenschaften und des Übertragungsprotokolls bei Taschenkartenlesern sind nicht ausreichend für die Verwendung von Terminals im Rahmen von Zusatzanwendungen. Für die Terminals, die noch nicht über einen hinreichenden Nachweis der Einhaltung der Anforderungen an die elektromechanischen Eigenschaften und das Übertragungsprotokoll T=1 verfügen, ist ein gesonderter Funktionstest durch ein ZKA-Testlabor durchzuführen. Weiterführende Informationen sind über www.zka.de und zulassungsstelle@voeb.de erhältlich.

Darüber hinaus müssen sich die für Zusatzanwendungen vom Typ "Fahrschein" oder "Marktplatz" genutzten Terminals der Mechanismen, wie sie in der Spezifikation für das Marktplatz-Terminal bzw. der Spezifikation des ÖPV-Terminal niedergelegt sind, bedienen (vgl. Abschnitt 3.5).

Eine gesonderte Abnahme zur Einhaltung der Spezifikationen "Marktplatz-System“ bzw. "ÖPV-System" sowie eine hierauf beruhende Zulassung erfolgt nicht.

Für Zusatzanwendungsterminals werden dementsprechend keine eigenständigen Zulassungszertifikate ausgestellt.

4.1.4 Einrichtung von Gruppen im ZKA-Marktplatz

4.1.4.1 Vergabe Gruppen_ID

Leistungsanbieter können sich zu Gruppen zusammenschließen, um sich gegenseitig Zugriff auf die von den an der Gruppe beteiligten Leistungsanbietern gespeicherten Daten einzuräumen. Voraussetzung hierfür ist die Bestimmung eines Gruppenführers sowie die Vergabe einer eindeutigen Gruppen_ID.

Zur Vergabe einer Gruppen_ID wendet sich der Gruppenführer an seine Hausbank. Diese leitet den Antrag weiter an ihren zuständigen Verlag, der dann die Vergabe einer Gruppen_ID vornimmt.

Die Gruppen_ID ist in die MSAMs aller beteiligten Gruppenmitglieder einzubringen. Hierzu stehen prinzipiell zwei unterschiedliche Wege zur Verfügung. Zum einen besteht die Möglichkeit, bestehende MSAMs ohne Gruppen_ID gegen neue MSAMs mit Gruppen_ID auszutauschen. In einer weiteren Ausbaustufe besteht die Möglichkeit, dass der Verlag ein Kommando zum Einbringen der neuen Gruppen_ID in ein bestehendes MSAM generiert, das per DFÜ oder per Datenträger an den Leistungsanbieter weitergeleitet wird, um so die Gruppen_ID nachträglich in bereits ausgegebene MSAMs einzubringen. Dies setzt allerdings die Verfügbarkeit entsprechender Mechanismen beim Leistungsanbieter voraus.

4.1.4.2 Einbeziehung von neuen Gruppenmitgliedern in eine Gruppe

Um Gruppenmitglieder in eine Gruppe einzubeziehen, gibt der Gruppenführer die Gruppen_ID der Gruppe an die einzubeziehenden Gruppenmitglieder weiter. Umgekehrt informieren diese den Gruppenführer über ihre eigene Anbieter_ID. Um sicherzustellen, dass nur berechtigte Gruppenmitglieder MSAMs mit der Gruppen_ID einer bestimmten Gruppe erhalten, gibt der Gruppenführer die Anbieter_IDs der einzubeziehenden Gruppenmitglieder über seine Hausbank an den Verlag weiter, der die Gruppen_ID vergeben hat.

Die einzubeziehenden Gruppenmitglieder wenden sich mit der vom Gruppenführer erhaltenen Gruppen_ID an ihre jeweilige Hausbank, um MSAMs mit der Gruppen_ID der Gruppe zu erhalten. Die Anträge werden von den Hausbanken an ihre jeweiligen Verlage weitergeleitet, die bei dem die Gruppen_ID generierenden Verlag prüfen, inwieweit die beantragenden Leistungsanbieter (Anbieter_ID) berechtigt sind, an der Gruppe teilzunehmen. Nach erfolgreicher Prüfung werden MSAMs mit Gruppen_ID der Gruppe produziert und ausgeliefert. Alternativ steht – in Abhängigkeit von den technischen Voraussetzungen beim Leistungsanbieter – die Möglichkeit zur Weiterleitung eines

Kommandos zum Einbringen der Gruppen_ID in bereits ausgegebene MSAMs zur Verfügung. Dabei besteht die Möglichkeit, dass Leistungsanbieter gleichzeitig an mehreren Gruppen teilnehmen.

Das Rechtsverhältnis der Gruppenmitglieder zueinander ist nicht Gegenstand der im Zentralen Kreditausschuss zu treffenden Regelungen und muss gesondert zwischen den Gruppenmitgliedern vereinbart werden.

4.1.4.3 Ausscheiden von Gruppenmitgliedern

Möglichkeiten und Konsequenzen des Ausscheidens von Gruppenmitgliedern sind im Rahmen der internen Vereinbarung zwischen den Gruppenmitgliedern zu regeln. Dies gilt insbesondere für die Verpflichtung des ausscheidenden Gruppenmitglieds, die Gruppen_ID der Gruppe nach Ausscheiden aus der Gruppe nicht mehr zu nutzen.

Seitens der Kreditwirtschaft besteht keine technische Möglichkeit, ein Gruppenmitglied an der Verwendung einer Gruppen_ID vor dem Ablauf der Gültigkeit eines MSAMs mit Gruppen_ID zu hindern.

Die Produktion neuer MSAMs mit der ID einer Gruppe, zu der ein Leistungserbringer nicht mehr gehört, kann vom Gruppenführer verhindert werden durch eine entsprechende Meldung an seine Hausbank, die diese Information an ihren zuständigen Verlag weiterleitet und die Anbieter_ID des ausgeschiedenen Gruppenmitglieds aus der Liste der an der Gruppe teilnehmenden Anbieter streicht. Gleichzeitig informiert der Verlag den Verlag des ausscheidenden Gruppenmitglieds über die Änderung der Gruppenzugehörigkeit.

4.1.4.4 Übertragen der Gruppenführung auf andere Gruppenmitglieder

Scheidet der Gruppenführer einer Gruppe aus, so können die Gruppenmitglieder gleichwohl an einer Fortführung der Gruppe interessiert sein. Insbesondere bei einer großen Zahl von MSAMs kann es sinnvoll sein, die bisherige Gruppen_ID fortzuführen.

Um auch in diesen Fällen eine einfache Abwicklung der Abfragen zwischen den Verlagen bei Neuzugängen zu ermöglichen, verbleibt die Verwaltung der Gruppe immer bei dem Verlag, der die Gruppen_ID vergeben hat. Die Übertragung einer Gruppen_ID von einem Gruppenführer auf einen neuen Gruppenführer setzt einen Vertrag voraus, aus dem hervorgeht, dass der neue Gruppenführer Rechtsnachfolger des bisherigen Gruppenführers in bezug auf die Gruppe werden soll. Der übertragende Gruppenführer meldet den neuen Gruppenführer an seine Hausbank. Dem neuen Gruppenführer steht es frei, sich zur Verwaltung seiner Gruppe unmittelbar an die Hausbank des bisherigen Gruppenführers zu wenden oder seine eigene Hausbank um Weiterleitung aller die Gruppe betreffenden Informationen zu bitten.

5 Literaturliste

Applikation	**Stand**
Applikation Elektronischer Fahrschein	Vers. 5.0 vom 01.10.03
Sicherheitsmodul Fahrschein (FSAM)	Vers. 5.0 vom 03.06.03
ÖPV-System (Terminalablauf)	Vers. 5.0 vom 16.03.04
ÖPV-System: Internet Kundenterminal	Vers. 4.0 vom 01.04.04
Applikation Marktplatz	Vers. 5.0 vom 01.10.03
Sicherheitsmodul Marktplatz (MSAM)	Vers. 5.0 vom 03.06.03
Marktplatz-System (Terminalablauf)	Vers. 5.0 vom 16.03.04
Marktplatz -System: Internet Kundenterminal	Vers. 4.0 vom 01.04.04
Multifunktionaler Taschenkartenleser	Vers. 3.1 vom 06.09.01

Anhang A Aufbau von elektronischen Fahrscheinen

Ein elektronischer Fahrschein besteht aus einem oder mehreren verknüpften Datensätzen, die einen einheitlichen Aufbau haben. Die Spezifikation der gemeinsamen VDV-ZKA-Arbeitsgruppe beschränkt sich darauf, den Aufbau der Kennung, des Datenheader und des Ticketteiles festzulegen. Die Kennung und der Datenheader sind fest vorgegeben, der Ticketteil wird vom Anbieter definiert. Die folgende Tabelle beinhaltet die standardisierten Felder des elektronischen Fahrscheins:

Länge	Kodierung	Feld	
6	JJJJMMTTHHMM	Kennung	Verfallzeitpunkt
2	'XX XX'		Betreiber_ID
3	'XX XX XX'		Servicekennung
4	'nn..nn'	Datenheader	Fahrpreis
6	JJJJMMTTHHMM		Erstellungszeitpunkt
1	'XX'		Entwertungszähler
var.	'XX..XX'		ZD_INFO
var.	'XX..XX'	Ticketteil	

Elektronische Fahrscheine können von verschiedenen (Zusatzanwendungs-)Anbietern oder deren Akzeptanzpartnern in die ZKA-Chipkarte des Kunden eingebracht werden. Jeder berechtigte Akzeptanzpartner hat eine eigene Kennung, die **Betreiber_ID**, durch die das jeweilige Verkehrsunternehmen deutschlandweit eindeutig identifiziert wird. Diese Betreiber_ID wird vom VDV verwaltet.

Der Verfallzeitpunkt (**VZP**) gibt im Format 'JJJJMMTTHHMM' das Datum (und die Uhrzeit an), an dem eine Berechtigung überschrieben werden darf. Dies ist nicht notwendigerweise der gleiche Zeitpunkt, an dem die Berechtigung ungültig wird. Das Überschreiben kann auch erst zu einem späteren Zeitpunkt zugelassen werden. So kann beispielsweise vereinbart werden, dass ein Einzelfahrschein frühestens 48 Stunden nach seiner Erstellung überschrieben werden kann. Anhand der **Servicekennung** kann ein Terminal die Art des Fahrscheins (z.B. Kurzstrecke, Tages-Ticket, etc.) erkennen. Sie charakterisiert ein bestimmtes tarifliches Angebot, wie z. B. eine Fahrscheingattung. Die Kodierung von tariflichen Leistungen in der Service-Nummer erfolgt einheitlich durch das im Sinne der Tarifhoheit jeweils zuständige Unternehmen in eigener Regie. Der **Fahrpreis** wird in 4 Byte kodiert, z.B. '00 00 12 50' für EURO 12,50. Der Erstellungszeitpunkt (**EZP**) der Berechtigung wird beim Einbringen mit dem aktuellen Datum und der Uhrzeit gefüllt. Der **Entwertungszähler** gibt an wie oft ein Fahrschein noch entwertet werden kann. Beim Anlegen des Fahrscheins wird dieser Wert vom Betreiber festgelegt und kann bis zu einem Wert von 255 inkrementiert werden.

In Feld **ZD_INFO** stehen zusätzliche Datenheader Informationen mit variabler Länge, die vom Betreiber festgelegt wird und bei einer Entwertung des Fahrscheins modifiziert werden kann. Der **Ticketteil** kann vom Betreiber frei gestaltet werden. Innerhalb dieses

Datenobjektes befinden sich die Informationen, die dem Kunden im Klartext z.B. am Taschenkartenleser angezeigt werden. Der Ticketteil und das ZD_INFO Feld werden daher gemäß dem ASCII-Zeichensatz kodiert. Optional vorhandene zusätzliche Informationen in beiden Feldern, die nicht ASCII-kodiert sind, werden mit dem "@" Zeichen abgetrennt.

Der **Ticketteil** kann vom Anbieter frei gestaltet werden. Wenn der Ticketteil hinreichend kurz ist, um in einen Record zu passen, dann befindet sich der Fahrschein in einem Einzelrecord. Folgende Tabelle zeigt einen Fahrschein, der in einem Einzelrecord abgelegt ist. Die Inhalte der vom Anbieter zu belegenden Felder sind darin zur Illustration mit Beispielwerten gefüllt.

Tag	Länge	Wert (Beispiel)	Erläuterung
'E2'	'39'		Tag und Länge der Recorddaten
'C2'	'01'		Tag und Länge der Kontrolldaten
	1	'02'	Kontrolldaten (Recordnummer)
'C4'	'0B'		Tag und Länge der Kennungsdaten
	6	'20 00 12 05 14 55'	VZP (5. Dezember 2000)
	2	'00 29'	Betreiber_ID
	3	'23 44 56'	Servicekennung
'C5'	'0C'		Tag und Länge der Headerdaten
	4	'00 00 03 20'	Fahrpreis (EUR 3,20)
	6	'20 00 12 03 14 55'	Erstellungszeitpunkt (3. Dezember 2000)
	1	'FF'	Entwertungszähler
	1	'00'	ZD_INFO
'C6'	'19'		Tag und Länge des Ticketteiles
	25	"Einzel-Erwachsener@" + '01 02 03 04 05 06'	Ticketteil für einen Einzelfahrschein für einen Erwachsenen

Die Längen werden binär kodiert, so steht '19' in der Länge des Ticketteils für den dezimalen Wert 25. Konkret befindet sich die Aneinanderreihung der grau unterlegten Felder für dieses Beispiel im Record 2 des EF_FAHRSCHEIN.

Der Entwertungszähler wurde hier auf 'FF' gesetzt, um in diesem Beispiel die Gültigkeit des Fahrscheins zu kennzeichnen. In ZD_INFO soll keine spezifische Information enthalten sein. Das Feld wird deshalb auf '00' gesetzt.

Im Ticketteil steht zur Information des Kunden "Einzel-Erwachsener". Diese Information ist im ASCII-Format kodiert. Das '@'-Zeichen ist ein vordefiniertes Trennzeichen. Dadurch wird gekennzeichnet, dass die vor dem Trennzeichen stehende Information von einem Taschenkartenleser angezeigt werden kann. Die Information hinter dem '@'-Zeichen wird dagegen nur von Kontrolleur-Geräten oder anderen Terminals angezeigt. Hier kann beispielsweise die Einstiegshaltestelle, Zielhaltestelle oder die Streckenlinie kodiert werden.

Ist der Ticketteil zu lang, um die Berechtigung in einem Record des EF_FAHRSCHEIN speichern zu können, so werden mehrere Records des EF_FAHRSCHEIN verknüpft. Der erste Record dieser Verknüpfung wird **Startrecord** genannt. Er enthält alle Datenobjekte, die auch in einem Einzelrecord enthalten sein können. Die nachfolgenden Records werden **Nachfolgerrecords** genannt. Diese enthalten neben den Ticketdaten, die nicht mehr in den vorigen Record passen, lediglich das Verfallsdatum und die Nummern der Vorgänger- und Nachfolgerrecords sowie des eigenen Records.

Es folgt ein Beispiel einer verknüpften Berechtigung, die 2 Records beansprucht.

Der Startrecord hat folgenden Aufbau:

Tag	Länge	Wert (Beispiel)	Erläuterung
'E2'	'4D'		Tag und Länge der Recorddaten
'C2'	'03'		Tag und Länge der Kontrolldaten
	3	'02 00 06'	Recordnummer + Vorgänger + Nachfolger
'C4'	'0B'		Tag und Länge der Kennungsdaten
	6	'20 00 12 05 14 55'	VZP
	2	'00 29'	Betreiber_ID
	3	'23 44 56'	Servicekennung
'C5'	'0C'		Tag und Länge der Headerdaten
	4	'00 00 03 20'	Fahrpreis (EUR 3,20)
	6	'20 00 12 03 14 55'	Erstellungszeitpunkt
	1	'FF'	Entwertungszähler
	1	'00'	ZD_INFO
'C6'	'2B'		Tag und Länge des Ticketteiles
	43	"Einzelfahrschein-Erwachsener Tarifgebiet 1@"	Ticketteil für einen Einzelfahrschein für einen Erwachsenen

Der Nachfolgerrecord hat folgenden Aufbau:

Tag	Länge	Wert	Erläuterung
'E2'	'15'		Tag und Länge der Recorddaten
'C2'	'03'		Tag und Länge der Kontrolldaten
	3	'06 02 FF'	Recordnummer + Vorgänger + Nachfolger
'C4'	'06'		Tag und Länge der Kennungsdaten
	6	'20 00 12 05 14 55'	VZP
'C6'	'06'		Tag und Länge des Ticketteiles
	6	'01 02 03 04 05 06'	Ticketteil

In diesem Beispiel handelt es sich im Prinzip um den gleichen Fahrschein wie beim Einzelrecord, jedoch ist der Ticketteil länger, da das vom Taschenkartenleser anzuzeigende

Datenelement "Einzelfahrschein-Erwachsener Tarifgebiet 1" länger ist als im vorherigen Beispiel.

Die Berechtigung soll auf eine Karte aufgebracht werden, deren EF_FAHRSCHEIN eine maximale Recordlänge von 80 Byte hat. Der entsprechende Ticketteil wird nach Erreichen des Recordendes abgeschnitten und unmittelbar im Ticketteil des Nachfolgerrecords fortgeführt. Der Verfallzeitpunkt ist in allen Records einer Berechtigung identisch. Da es für einen Startrecord keinen Vorgängerrecord gibt, wird dieser mit '00' bezeichnet; für den Nachfolgerrecord des letzten Records einer Verknüpfung wird 'FF' gewählt.

Anhang B Aufbau der Marktplatz-Anwendungen

Eine Marktplatz-Anwendung besteht ähnlich wie ein elektronischer Fahrschein aus einem oder mehreren verknüpften Datensätzen, die einen standardisierten Aufbau haben. Sie kann von verschiedenen (Zusatzanwendungs-)Anbietern oder Akzeptanzpartnern in die ZKA-Chipkarte des Kunden eingebracht werden. Jeder berechtigte Akzeptanzpartner hat eine eigene Kennung, die **Anbieter_ID**, durch die er eindeutig identifiziert wird. Darüber hinaus können sich Akzeptanten zu sogenannten Akzeptantengruppen zusammenschließen, z. B. um gemeinsame Bonusprogramme herauszugeben. Der ZKA-Marktplatz unterstützt dieses Konzept durch die Vergabe von Gruppenkennungen, sogenannte Gruppen_IDs. Allen Akzeptanten, die beispielsweise an einem Bonusprogramm teilnehmen, wird die gleiche Gruppen_ID zugeteilt. Zudem kann jeder Akzeptant mehreren Gruppen zugeordnet sein.

Die Datei EF_MARKTPLATZ kann bis zu zehn Records mit Daten von ZKA-Marktplatz-Anwendungen aufnehmen. Die Records haben eine variable Länge von maximal 60 Byte. In diesen Records sind die Anwendungsdaten gespeichert, die sich für eine einzige Marktplatz-Anwendung auch über verknüpfte Records erstrecken können.

Die Records haben einen weitgehend einheitlichen Aufbau. Unterschiede ergeben sich durch unterschiedliche Anwendungen (beispielsweise Gutscheine oder Ausweise), die verschiedenartige Datengruppen benötigen. Innerhalb der Records sind die Daten in sogenannten Datenobjekten organisiert. Dabei enthält jedes Datenobjekt Daten einer bestimmten Bedeutung. Einige Datenobjekte finden sich dabei in jedem Record, andere sind spezifisch für ein konkretes Anwendungsbeispiel. Im Folgenden werden die einzelnen Datenobjekte vorgestellt:

Der Standard "ZKA-Marktplatz" legt folgende Datenobjekte als Bestandteile der Anwendungsdaten im ZKA-Marktplatz fest:

- Anwendungsfall-unabhängige Daten
- Anwendungsfall-abhängige Daten

Die **anwendungsfall-unabhängigen Daten** umfassen die Record-Kontrolldaten, die UPDATE_ID des Datensatz-Erzeugers und die Datensatz-Kontrolldaten.

Die **Record-Kontrolldaten** regeln die eventuelle Verknüpfung verschiedener Records, falls die Anwendungsdaten für einen einzigen Record zu groß sind, und geben die Recordnummer an.

Die **UPDATE_ID des Datensatz-Erzeugers** enthält eine Anbieter_ID, die für jeden an der Anwendung teilnehmenden Anbieter bzw. Akzeptanten eindeutig ist.

Durch die **Datensatz-Kontrolldaten** wird festgelegt, ob die folgenden Daten des Records verändert oder gelöscht werden dürfen. Die Kontrolldaten beinhalten deshalb einen Verfallzeitpunkt und eine Kennung der folgenden Daten. Über die Kennung kann auch

vorgegeben werden, wie oft der folgende Datensatz verändert werden darf. Dies lässt sich beispielsweise für die Realisierung eines Gutschein-Heftes nutzen.

Anwendungsfall-abhängige Daten, die in Anwendungsdaten von ZKA-Marktplatz-Anwendungen enthalten sind und auf passende Weise kombiniert werden, sind im Folgenden beschrieben:

Anwendungsbeschreibungsdaten enthalten vom Anbieter frei wählbare Informationen, die er entsprechend seiner Anwendung ändern und auswerten kann. Die **Anbieter_ID des Datensatz-Entwerters** kann dazu genutzt werden, bei der Entwertung von Gutscheinen zu Protokollierungszwecken die ID des Datensatz-Entwerters aufzunehmen.

Das Datenobjekt für **verschlüsselte Daten** dient zur Aufnahme vertraulicher Daten. Dabei kann es sich beispielsweise um personenbezogene Daten handeln, die bei einer Zugangskontrolle ausgewertet werden. Solche Daten lassen sich generell zur Realisierung eines Ausweises nutzen.

Das Datenobjekt **Zähler** enthält einen Zählerstand, der verändert werden kann. Dabei kann die Möglichkeit, diesen Zähler zu verändern, durch zwei weitere Datenobjekte zeitlich befristet werden. Das Datenobjekt **Gültigkeitsdatum vergrößern** enthält das Datum, bis zu dem der Zählerstand erhöht werden kann, das Datenobjekt **Gültigkeitsdatum verringern** entsprechend jenes für ein Verringern des Zählerstandes. Über diese Datenobjekte lassen sich beispielsweise Bonuspunktezähler realisieren.

Die **Gruppenkennung** gibt an, ob die Anwendung zu einer Gruppe mehrerer Anbieter bzw. Akzeptanten gehört. Ist dies der Fall, so kann jeder dieser Anbieter bzw. Akzeptanten die Daten verändern. Fehlt dieses Datenobjekt, so ist die Modifikation der Daten nur dem Anbieter bzw. Akzeptanten möglich, der die Anwendung auf der ZKA-Chipkarte angelegt hat.

Als Beispiel für eine Marktplatz-Berechtigung ist in der folgenden Tabelle der Aufbau eines Ausweises dargestellt, der aus einem Einzelrecord besteht.

Tag	Länge	Wert (Beispiel)	Erläuterung
'E3'	'39'		Tag und Länge für Marktplatz-Recorddaten
'C2'	'01'		Tag und Länge für Kontrolldaten
	1	'01'	Recordnummer
'C4'	'03'		Tag und Länge für Kennungsdaten
	3	'00 00 0A'	UPDATE_ID des Datensatz-Erzeugers
'C5'	'07'		Tag und Länge für Datensatz-Kontrolldaten
	6	'20 03 12 31 23 59'	Verfallzeitpunkt für den Record
	1	'00'	Kennung für einen Ausweis
'E6'	'26'		Tag und Länge für Anwendungsdaten
'CB'	'02'		Tag und Länge für Zähler
	2	'00 35'	Zählerstand

Tag	Länge	Wert (Beispiel)	Erläuterung
’C9’	’04’		Tag und Länge für Gültigkeitsdatum Vergrößerung des Zählerstandes
	4	'20 02 12 31'	Gültigkeitsdatum vergrößern
'CA'	'04'		Tag und Länge für Gültigkeitsdatum Verringerung des Zählerstandes
	4	'20 03 03 31'	Gültigkeitsdatum verringern
'C6'	'14'		Tag und Länge für Anwendungsbeschreibungsdaten
	20	"Dies ist ein Ausweis"	Informationen für den Kunden (ASCII-Text)

Die Längen werden wiederum binär kodiert, so steht '14' in der Länge der Anwendungsbeschreibungsdaten für den dezimalen Wert 20. Konkret befindet sich für dieses Beispiel im Record 1 des EF_MARKTPKLATZ die Aneinanderreihung der grau unterlegten Felder.

Der Verfallzeitpunkt, in diesem Beispiel der 31.12.2003, 23 Uhr 59, gibt an, wann dieser Record überschrieben werden darf. Zusätzlich gibt die Kennung in den Datensatz-Kontrolldaten an, um welchen Berechtigungstyp es sich handelt. '00' steht für einen Ausweis. 'FX' kodiert einen Gutschein, der X-mal (maximal 15 mal) entwertet werden darf. Ein Gutschein ist im folgenden Beispiel beschrieben.

Die UPDATE_ID des Erzeugers enthält in diesem Beispiel die Anbieter_ID, die jedem teilnehmenden Anbieter zugewiesen wird und ihn innerhalb einer Anwendung eindeutig identifiziert. Für die UPDATE_ID sind neben der Angabe der Anbieter_ID auch die Angabe von Anbieter_ID | Terminal_ID bzw. Anbieter_ID | Terminal_ID | SEQ möglich. Die Terminal_ID wird vom Anbieter an seine Terminals vergeben, SEQ ist eine Sequenznummer, die in den Sicherheitsmodulen beim Anlegen einer Berechtigung inkrementiert wird. Durch die zusätzliche Angabe der Terminal_ID kann das Terminal identifiziert werden, an dem die Berechtigung ausgestellt wurde, die zusätzliche Aufnahme der Sequenznummer SEQ ermöglicht darüber hinaus die eindeutige Identifizierung der Berechtigung in den Systemen des Zusatzanwendungsanbieters.

Die Tags 'C9' und 'CA' geben das Datum an, bis zu dem der Zähler aus Tag 'CB' vergrößert (hier: 31.12.2002) bzw. verringert (hier: 31.03.2003) werden darf. Mit diesem Beispiel kann also ein Bonuspunkteprogramm umgesetzt werden, in dem bis zum 31.12.2002 Bonuspunkte vergeben werden, die bis zum 31.03.2003 eingelöst werden müssen und danach verfallen. Der aktuelle Bonuspunktestand auf der ZKA-Chipkarte ist 53 (dezimal).

Als weiteres Beispiel für eine Marktplatz-Berechtigung ist in der folgenden Tabelle der Aufbau eines Gutscheins dargestellt.

Tag	Länge	Wert (Beispiel)	Erläuterung
'E3'	'33'		Tag und Länge für Marktplatz-Recorddaten
'C2'	'01'		Tag und Länge für Kontrolldaten
	1	'04'	Recordnummer
'C4'	'06'		Tag und Länge für Kennungsdaten
	6	'00 00 0A 01 01 01'	UPDATE_ID des Datensatz-Erzeugers
'C5'	'07'		Tag und Länge für Datensatz-Kontrolldaten
	6	'20 03 12 31 23 59'	Verfallzeitpunkt für den Record
	1	'F3'	Kennung für einen Gutschein
'E6'	'1D'		Tag und Länge für Anwendungsdaten
'CC'	'03'		Tag und Länge für Gruppenkennung
	3	'00 00 01'	Gruppenkennung
'C6'	'16'		Tag und Länge für Anwendungsbeschreibungsdaten
	22	"Dies ist ein Gutschein"	Informationen für den Kunden

Die Längen werden wiederum binär kodiert, so steht '16' in der Länge der Anwendungsbeschreibungsdaten für den dezimalen Wert 22. Konkret befindet sich für dieses Beispiel im Record 4 des EF_MARKTPKLATZ die Aneinanderreihung der grau unterlegten Felder.

Der Verfallzeitpunkt, in diesem Beispiel der 31.12.2003, 23 Uhr 59, gibt an, wann dieser Record überschrieben werden darf. Zusätzlich gibt die Kennung mit 'F3' an, dass es sich hierbei um einen Gutschein handelt, der noch dreimal entwertet werden darf.

Die UPDATE_ID des Erzeugers enthält in diesem Beispiel die Anbieter_ID | Terminal_ID. Die Terminal_ID wird vom Anbieter an seine Terminals vergeben.

Anhang C Jugendschutzmerkmal in der ZKA-Chipkarte

C.1 Randbedingungen für die Nutzung

Generell gilt, dass die Prüfung eines im ZKA-Marktplatz auf der Karte gespeicherten Jugendschutzmerkmals ohne gleichzeitige Karteninhaberverifikation nicht eindeutig darüber Auskunft geben kann, ob das Jugendschutzmerkmal tatsächlich dem berechtigten Karteninhaber zugeordnet werden kann. Bei kontogebundenen Karten ist allerdings die Wahrscheinlichkeit einer Weitergabe an Dritte relativ gering, so dass bei diesen Karten i.d.R. davon ausgegangen werden kann, dass sie vom berechtigten Karteninhaber verwendet werden.

Im Gegensatz dazu besitzen kontoungebundene Karten keine kundenspezifischen Daten. Diese Karten sind frei übertragbar und werden an beliebigen Orten u.a. auch durch Automaten ausgegeben. Die fehlende Bindung der kontoungebundenen Karte an ein Kundenkonto erlaubt die Weitergabe der Karte, und somit den missbräuchlichen Einsatz des Jugendschutzmerkmals. Das Jugendschutzmerkmal muss daher einer Person zugeordnet werden, um im beabsichtigten Sinne wirksam zu werden. Mit der Speicherung des Jugendschutzmerkmals in der Karte muss somit immer auch eine entsprechende kundenspezifische Bindung in der Karte abgelegt werden. Der Charakter der kontoungebundenen Karte als übertragbares Zahlungsmedium steht dieser Anforderung konzeptionell entgegen.

C.2 Aufbau des Datensatzes in der Kundenkarte

In der Marktplatz-Applikation werden die einzelnen Anbieter über eine 3 Byte lange Anbieter_ID identifiziert, die bei der Produktion in das Sicherheitsmodul eingebracht wird und dann nicht mehr vom Anbieter verändert werden kann. Hierbei hat die Anbieter_ID '00 00 00' eine besondere Rolle und ist für Systeme der Kreditwirtschaft reserviert. Das Jugendschutzmerkmal wird bei der Produktion mit der Anbieter_ID '00 00 00' in die Kundenkarten eingebracht.

Der Verfallszeitpunkt einer Berechtigung im Marktplatz legt fest, ab wann der Speicherplatz, der von der Berechtigung belegt wird, wieder allen Anbietern zur Verfügung steht. Hierbei hat das Datum 31.12.9999 23:59 Uhr eine besondere Bedeutung und legt fest, dass unabhängig vom aktuellen Datum nur der Anbieter selbst die Berechtigung verändern darf. Der Verfallszeitpunkt der Berechtigung mit dem Jugendschutzmerkmal wird auf den 31.12.9999 23:59 Uhr festgelegt.

Prinzipiell hat bis zum Verfallszeitpunkt einer Berechtigung nur der Anbieter die Rechte an der Berechtigung in der Kundenkarte. Mittels des Gruppenkontextes in der Applikation Marktplatz kann der anlegende Anbieter anderen Anbietern Rechte an der Berechtigung einräumen. Die Gruppenzugehörigkeit wird bei der Produktion in das Sicherheitsmodul des Anbieters eingebracht und kann dann nur durch die Verlage der Kreditwirtschaft administriert werden. In den Datensatz in der Kundenkarte wird eine noch nicht vergebene Gruppenkennung eingebracht, die dann auch in die Sicherheitsmodule derjenigen Anbieter eingebracht wird, denen die Auswertung des Jugendschutzmerkmals erlaubt wird. Dadurch

benötigt ein Anbieter kein zusätzliches Sicherheitsmodul, welches nur für die Verarbeitung des Jugendschutzmerkmals genutzt werden kann.

Zur Speicherung des Jugendschutzmerkmals wird ein neuer Tag 'CE' definiert. Dieser Tag wird bisher nicht vom Sicherheitsmodul interpretiert und führt bei der Verarbeitung im Sicherheitsmodul in der jetzigen Version zu einem Fehler bei der Konsistenzprüfung der Daten. Somit ist eine Verarbeitung der Daten im jetzigen Sicherheitsmodul ausgeschlossen. Ein Terminal kann den Datensatz mit dem neuen Tag 'CE' aus der Kundenkarte lesen und erkennen, dass aufgrund des Verfallszeitpunkts ein Überschreiben der Berechtigung nicht erlaubt ist.

Die folgende Tabelle enthält den Aufbau des kompletten Datensatzes in der Kundenkarte. Es wird empfohlen, den Datensatz im letzten Record des EF_MARKTPLATZ abzuspeichern, da dadurch bis zu dessen eigentlicher Nutzung die geringsten Auswirkungen auf die Marktplatz-Applikation entstehen.

	Länge (in Byte)	**Wert**	**Erläuterung**
Tag	1	'E3'	Tag für Recorddaten
Length	1	'3A'	Länge der Recorddaten
Tag	1	'C2'	Tag für Record-Kontrolldaten
Length	1	'01'	Länge der Record-Kontrolldaten
	1	'0A'	Kontrolldaten (Recordnummer)
Tag	1	'C4'	Tag für UPDATE-ID des Datensatz-Erzeugers
Length	1	'03'	Länge der UPDATE-ID des Datensatz-Erzeugers
	3	'00 00 00'	UPDATE-ID des Datensatz-Erzeugers
Tag	1	'C5'	Tag für Datensatz-Kontrolldaten
Length	1	'07'	Länge der Datensatz-Kontrolldaten
	6	'999912312359'	Verfallszeitpunkt für Record
	1	'00'	Kennung für einen Ausweis
Tag	1	'E6'	Tag für Anwendungsdaten
Length	1	'27'	Länge der Anwendungsdaten
Tag	1	'CC'	Tag für Gruppenkennung
Length	1	'03'	Länge der Gruppenkennung
	3	'XX XX XX'	Gruppenkennung des Jugendschutzmerkmals
Tag	1	'CE'	Tag für Speicherung verschlüsselter Daten
Length	1	'12'	Länge des Datenobjekts
	1	'XX'	KV' des K_{JUGEND}
	1	'10'	Länge der Klartextdaten
	16	'XX..XX'	verschlüsseltes Jugendschutzmerkmal
Tag	1	'C6'	Tag für benutzerdefinierte Daten
Length	1	'0C'	Länge
	12	'4A 75 67 65 6E 64 73 63 68 75 74 7A'	Informationen für Kunden am TKL "Jugendschutz" ASCII kodiert

Die folgende Tabelle enthält den zu personalisierenden Aufbau des Jugendschutzmerkmals mit Klartextdaten:

Position	Länge (in Byte)	Wert	Erläuterung
1	1	'CE'	Tag für Ablage verschlüsselter Daten
2	1	'12'	Länge des Datenobjektes
3	1	'XX'	Schlüssel-Version KV' des K_{JUGEND}
4	1	'10'	Länge der Klartextdaten
5	4	'JJJJMMTT'	Geburtsdatum
6	12	'00..00'	Bitfeld

C.3 Ablauf der Prüfung des Jugendschutzmerkmals

Das Jugendschutzmerkmal dient zur Feststellung der Nutzungsberechtigung der angeforderten Dienstleistung. Es steht per se nicht in Zusammenhang mit der in Abhängigkeit von der Prüfung des Kriteriums durchzuführenden Bezahltransaktion. Authentikation und Bezahlung sind getrennte Abläufe. Das Jugendschutzmerkmal ist auch unabhängig von dem vom Kunden gewählten bzw. vom Akzeptanten angebotenen Zahlungsverfahren. Das bedeutet, dass sich der Kunde mit der Karte und dem darauf gespeicherten Jugendschutzmerkmal zunächst als Nutzungsberechtigter authentisieren muss, um anschließend die Ware oder die Dienstleistung zu bezahlen. Die Bezahlung kann dann mit GeldKarte, bar oder mit anderen Zahlungsmitteln erfolgen. Nach Authentisierung und Bezahlung wird die Ware ausgegeben.

Für den **Ablauf einer Authentikationstransaktion** ergeben sich folgende Schritte

1. Das Terminal fordert zum Einstecken der Karte und damit zur Authentisierung auf. Dies kann mittels eines Displays oder durch Aufdruck erfolgen. Hierbei kann unmissverständlich klargestellt werden, dass ohne die Authentisierung über die Karte keine Ware bezogen werden kann.

2. Nach dem Einstecken der Karte wird zunächst DF_MARKTPLATZ_NEU auf der Kundenkarte selektiert, die Kartendaten gelesen und die von der Karte bereitgestellten Schlüssel-Versionen recherchiert und gespeichert. Das Terminal überprüft anhand der Kartendaten, ob die Karte nicht bereits verfallen ist.

3. Zur Überprüfung des Jugendschutzmerkmals wird der entsprechende Datensatz MAC-gesichert gelesen und dem Sicherheitsmodul mit den Kartenidentifikationsdaten und dem Vergleichsdatum (aktuelles Datum) zur Überprüfung und Auswertung übergeben. Das Sicherheitsmodul hat vorher eine Zufallszahl ausgegeben, die der Kundenkarte übergeben wird und in die Berechnung des MAC eingeht. Das Sicherheitsmodul überprüft damit zuerst die Authentizität der Daten und das Vorliegen einer echten Kundenkarte.

4. Das Sicherheitsmodul überprüft, ob eine Gruppenkennung im Datensatz der Karte mit dem Jugendschutzmerkmal vorhanden ist und ob diese identisch mit einer im Sicherheitsmodul gespeicherten Gruppenkennung ist.

5. Die Datenobjekte mit Tag 'CE' werden im Datensatz gesucht und es wird geprüft, ob die im Sicherheitsmodul gespeicherte Schlüssel-Version KV' des KGK_{JUGEND} mit einer zur Verschlüsselung verwendeten Version dieses Schlüssels übereinstimmt.

6. Verlaufen alle Prüfungen positiv, leitet das Sicherheitsmodul mittels der Identifikationsdaten aus dem gespeicherten KGK_{JUGEND} den entsprechenden K_{JUGEND} ab und entschlüsselt das passende Kryptogramm mit dem abgeleiteten Schlüssel.

7. Der ordnungsgemäße Aufbau und die Kodierung des Kriteriums werden überprüft. Mittels der im Sicherheitsmodul gespeicherten Kennung des Anbieters und dessen Zuordnung zu einer Position im Bitfeld, überprüft das Sicherheitsmodul dann die Anwendbarkeit des Kriteriums. Ist diese nicht erfüllt, so gibt das Sicherheitsmodul eine negative Antwort an das Terminal zurück. Andernfalls wird mittels des aktuellen Datums überprüft, ob das im Sicherheitsmodul gespeicherte Zielalter mit dem übergebenen Jugendschutzmerkmal erfüllt ist. Dem Terminal wird lediglich das Ergebnis der Überprüfung mitgeteilt.

8. Das Sicherheitsmodul kann so konfiguriert werden, dass es die Transaktion protokolliert, indem die übergebenen Kommandonachrichten in einem internen Ringspeicher abgelegt werden. Das Terminal kann dann diese Daten auslesen und erhält auf Anfrage eine kryptographische Absicherung des Sicherheitsmoduls dieser protokollierten Daten. Zum späteren Nachweis der Zulässigkeit der Transaktion kann das Terminal die Kommandonachricht einschließlich des vom Sicherheitsmodul berechneten MAC speichern. Die Protokolldaten enthalten in keinem Fall das Jugendschutzmerkmal im Klartext.

9. Verläuft eine der Prüfungen negativ, wird die Transaktion abgebrochen. Eine Bezahltransaktion darf dann so lange nicht vom Terminal akzeptiert oder angestoßen werden, bis eine erfolgreiche Authentisierung stattgefunden hat.

Anhang D Parameter des FSAM

D.1 Einleitung

Um elektronische Fahrscheine in der ZKA-Chipkarte anzulegen, kommuniziert diese mit dem Sicherheitsmodul der Applikation Fahrschein (FSAM). Im sog. gekoppelten Modus gestattet das Sicherheitsmodul, dass ein Fahrschein in der ZKA-Chipkarte gespeichert werden konnte, nur wenn unmittelbar vorher eine Bezahltransaktion über den Wert des anzulegenden Fahrscheins mit der GeldKarte durchgeführt wurde. Die Funktionalität dieses Sicherheitsmoduls ist erweitert worden. Im sog. entkoppelten Modus ist es möglich, Fahrscheine in ZKA-Chipkarten abzulegen, ohne dass vorher eine Bezahltransaktion mit dieser GeldKarte durchgeführt wurde. Dadurch sollen sowohl höherpreisige Fahrscheine angelegt werden können, als auch die Wahl des Zahlungsmittel dem Kunden überlassen werden.

Über einstellbare Parameter kann das Sicherheitsmodul der Applikation Fahrschein sowohl mit einer strengen Kopplung zwischen Bezahl- und Anlegetransaktion betrieben werden, als auch in dem entkoppelten Modus einsetzbar sein. Die vielfältigen möglichen Werte dieser Parameter erlauben dabei einen fast stufenlosen Übergang in vielen Schritten zwischen einem fast komplett entkoppelten und einem streng gekoppelten Sicherheitsmodul. Dadurch kann das Sicherheitsmodul der Applikation Fahrschein an seinen geplanten Einsatzort und dessen Sicherheitsumgebung optimal angepasst werden.

Das Konzept zur Anpassung des Sicherheitsmoduls an seinen Einsatzort wird ergänzt um die Möglichkeit der Einschränkung des Funktionsumfangs des Sicherheitsmoduls. Dadurch können Sicherheitsmodule z.B. so konfiguriert werden, dass sie lediglich gesichert lesen können bzw. nur bestehende Fahrscheine entwerten, jedoch keine neuen Fahrscheine anlegen können.

Zusätzlich kann in jede ausgestellte Berechtigung die Kennung des ausstellenden Sicherheitsmoduls aufgenommen werden. Das Sicherheitsmodul erhält zusätzliche Felder zur Protokollierung der übergebenen Datumsangabe und der ausgeführten Kommandos.

D.2 Parameter

Die Kopplung an die Bezahltransaktion wurde in Abstimmung mit dem VDV eingeführt, damit kein Anreiz zum Diebstahl eines FSAM geschaffen wird. Die Entkopplung der Bezahl- und der Anlegetransaktion soll nicht dazu führen, dass bei Diebstahl dieses Sicherheitsmoduls unbeschränkt Fahrscheine über eine beliebige Höhe ausgestellt werden können. Deshalb kann das Sicherheitsmodul so konfiguriert werden, dass die Höhe des Einzelbetrages, der Gesamtbetrag der entkoppelt ausgestellten Fahrscheine und die Anzahl der ausgestellten Fahrscheine unabhängig voneinander limitiert werden können. Dazu pflegt das Sicherheitsmodul 3 Felder mit Grenzwerten und Zähler für die Anzahl und den aktuellen Gesamtbetrag der entkoppelt ausgestellten Fahrscheine. Würde eine entkoppelt durchgeführte Anlegetransaktion zur Überschreitung auch nur eines der eingestellten Limits führen, so wird diese Transaktion nicht durchgeführt. Das Sicherheitsmodul kann

unabhängig von den eingestellten Limits immer Fahrscheine anlegen, die unmittelbar vorher mit dieser GeldKarte bezahlt wurden. Mittels einer kryptographisch abgesicherten Kommunikation mit einem Administrationssicherheitsmodul bzw. durch Datentelegramme, die durch den produzierenden Verlag bereitgestellt werden, können bei Bedarf die aktuellen Zählerstände zurückgesetzt und optional die eingestellten Limits verändert werden.

Wurde ein Bezahlvorgang vor dem Anlegen durchgeführt, so bleiben die Zähler unverändert und es findet keine Überprüfung der eingestellten Limits statt. Nur wenn kein Bezahlvorgang mit dieser GeldKarte durchgeführt wurde, werden die Zähler und der eingestellte maximale Einzelbetrag überprüft um festzustellen, ob der Vorgang durchgeführt werden darf. Dabei werden die folgenden Zähler bzw. Felder berücksichtigt:

Maximale Anzahl Fahrscheine (3 Byte binär kodiert)

In diesem Feld kann ein Wert zwischen 0 und 16.777.215 eingetragen werden. Ist hier der Wert ’00’ gespeichert, so darf kein Fahrschein (ohne vorherige Bezahltransaktion) angelegt werden. In einem zugeordneten Zähler (ebenfalls 3 Byte lang und binär kodiert) wird die Anzahl der bisher ohne vorherige Bezahltransaktion angelegten Fahrscheine gepflegt. Der im Zähler gespeicherte Wert wird mit jedem entkoppelten Anlegen eines Fahrscheins inkrementiert.

Maximaler Betrag des Fahrschein (3 Byte BCD-kodiert, ohne Nachkommastelle)

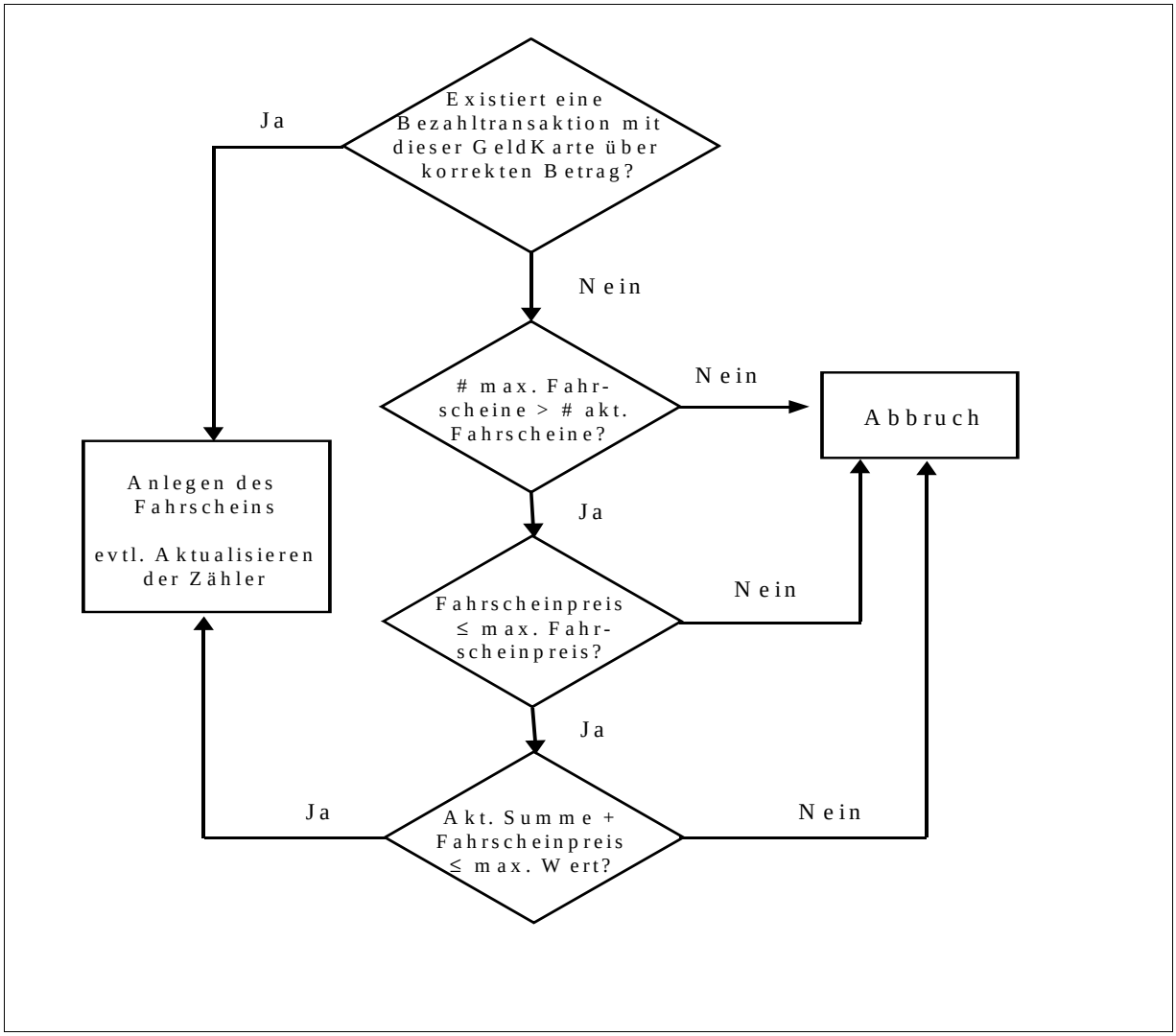
In diesem Feld kann ein Wert zwischen 0 und 999.999 hinterlegt werden. Übersteigt der Einzelpreis des entkoppelt anzulegenden Fahrscheins den gespeicherten Wert, so darf dieser Fahrschein nicht entkoppelt angelegt werden. Wird ein Fahrschein nicht entkoppelt angelegt, so wird dieser gespeicherte Wert nicht überprüft.

Maximaler Gesamtbetrag (3 Byte BCD-kodiert, ohne Nachkommastelle)

In diesem Feld kann ein Wert zwischen 0 und 999.999 hinterlegt werden. Dem Feld ist ein Zähler zugeordnet (4 Byte lang, BCD-kodiert mit 2 Nachkommastellen). Ist die Summe aus dem Wert dieses Zählers und dem Wert des aktuell entkoppelt anzulegenden Fahrscheins größer als der gespeicherte maximale Gesamtbetrag, so kann dieser Fahrschein nicht angelegt werden. Kann der Fahrschein entkoppelt angelegt, so wird der gespeicherte Wert des Zählers um den Preis des angelegten Fahrscheins erhöht.

Generell werden die Änderungen an den gespeicherten Werten erst gemacht, wenn der letzte Record einer Berechtigung geschrieben werden kann.

Das folgende Diagramm erläutert die Beschreibung des Ablaufs zum Anlegen eines Fahrscheins mit dem Sicherheitsmodul.



D.3 Konfigurationsbeispiele

Im folgenden Abschnitt werden zur Erläuterung der möglichen Konfigurationen des Sicherheitsmoduls einige Beispiele vorgestellt. Dabei wird der Wert 'XX' verwendet, falls der Wert beliebig sein kann. Die folgende Tabelle definiert einige Konfigurationen:

Typ	max. Anzahl Fahrscheine	max. Betrag eines Fahrscheins	max. Gesamtbetrag
1	0	'XX XX XX XX'	'XX XX XX XX'
2	100	'00 00 10 00'	'00 10 00 00'
3	100	'00 00 10 00'	'00 05 00 00'
4	16.777.215	'99 99 99 99'	'99 99 99 99'

Erläuterung:

Beim Typ 1 dürfen keine entkoppelten Fahrscheine angelegt werden, da als Limit für die maximal anzulegenden Fahrscheine der Wert 0 eingetragen ist,.

Die Konfiguration von Typ 2 erlaubt bis zu 100 Fahrscheine entkoppelt anzulegen, wobei der Wert der einzelnen Fahrscheine maximal 10 EUR betragen darf. Das Limit des maximalen Gesamtbetrages von 1000 EUR kann also niemals überschritten werden und ist damit in dieser Konfiguration eigentlich überflüssig.

Im Fall von Typ 3 kann das Limit des maximalen Gesamtbetrages relevant werden. Die Konfiguration erlaubt den maximalen Wert von 10 EUR pro Fahrschein, es können jedoch im Mittel nur Fahrscheine mit einen durchschnittlichen Wert von 5 EUR angelegt werden. In diesem Beispiel kann sowohl das Überschreiten der maximalen Anzahl der Fahrscheine als auch des maximalen Gesamtbetrages zu einer Sperrung des Sicherheitsmoduls führen.

Die Werte in Typ 4 sind die Maximalwerte der einzelnen Limits. Mit diesen Werten ist der prinzipiell endlose Betrieb des Sicherheitsmoduls möglich

D.4 Re-Initialisierung von Parametern und Limits

Haben sich die aktuellen Zählerstände so stark den jeweiligen Limits angenähert, dass ein Betrieb des Sicherheitsmoduls im entkoppelten Modus nicht mehr (lange) möglich ist, so können mittels eines Kommandos diese Zählerstände wieder auf den Wert '00' gesetzt werden. Außerdem können die Limitwerte des FSAM geändert werden. Dazu kommuniziert das Sicherheitsmodul der Applikation Fahrschein mit einer zentralen Stelle. Diese zentrale Stelle muss die zur Absicherung der Kommandos benötigten Schlüssel sicher verwalten und speichert in einer zentralen Datenbank pro FSAM die benötigten Daten (Sperrvermerke, (neue) Limitwerte, Sequenzzähler). Diese zentrale Stelle kann z.B. ein PC-System mit angeschlossenen Kryptomodul bei einem kreditwirtschaftlichen Verlag sein.

D.5 Transaktionsdatum

Sicherheitsmodule haben keine gesicherte Information über das aktuelle Datum. Sie erhalten diese Information vom Terminal. Um eine Möglichkeit zur Konsistenzprüfung zu haben, können im Sicherheitsmodul die Transaktionszeiten protokolliert werden. Dadurch wird die Liste der Transaktionszeiten auf aufsteigende Reihenfolge überprüft.

Das Feld EF_TRANS_DAT ermöglicht die Protokollierung des letzten dem Sicherheitsmodul übergebenen Transaktionsdatums und damit eine Konsistenzprüfung eines neuen Transaktionsdatums mit dem zuletzt gespeicherten Wert.

D.6 Protokollierung der Kommandos

Die Protokollierung der einzelnen ausgeführten Kommandos kann durch das FSAM abgesichert werden. Es kann jedem Kommando eine eindeutige Sequenznummer zugeordnet und vom Sicherheitsmodul eine kryptographisch abgesicherte Nachricht mit

dieser Zuordnung erstellt werden. Die Absicherung erfolgt dabei mit einem SAM-individuellen Schlüssel, der aus einem Betreiber-spezifischen Masterkey abgeleitet wird.

Das Feld für die Protokollierung der Daten wird EF_FLOG genannt.

D.7 Aussteller-Identifikation

Jedem Verkehrsunternehmen ist eine Betreiber_ID des VDV eindeutig zugeordnet. In alle Sicherheitsmodule dieses Betreibers wird dessen Kennung eingebracht. Die Abläufe zum Anlegen von elektronischen Fahrscheinen stellen sicher, dass diese Betreiber_ID in alle elektronischen Fahrscheine aufgenommen wird. Jeder Betreiber wird in der Regel mehrere Sicherheitsmodule haben. Eine eindeutige Identifizierung, mit welchen Sicherheitsmodul ein elektronischer Fahrschein geschrieben wurde, kann in jeden ausgestellten bzw. in jeden entkoppelt angelegten elektronischen Fahrschein aufgenommen werden. Die Daten werden im Tag 'C6' direkt hinter das Trennzeichen "@" eingefügt.

Anhand eines Konfigurationsbyte im FSAM kann festgelegt werden, ob und wie die Aussteller-Identifikation in einen anzulegenden Fahrschein aufzunehmen ist:

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
x	x							**Aussteller-Identifikation**
0	0							nicht aufnehmen
0	1							nur im entkoppelten Modus aufnehmen
1	1							generell aufnehmen
		x						**Aufbau der Aussteller-Identifikation**
		0						**Byte 5-9 des EF_ID des Sicherheitsmoduls (individuelle Kartennummer)**
		1						Byte 1-10 des EF_ID des Sicherheitsmoduls
			x	x	x	x	x	RFU (**R**eserved for **F**urther **U**se)

D.8 Weitere Zählerstände

Um z.B. mit den Vorverkaufsstellen abrechnen zu können, werden neben den Zählerständen zur Steuerung des entkoppelten Modus auch noch ein Zähler für die Anzahl der ausgestellten Tickets mit GeldKarte-Zahlung und die Summe der Fahrpreise der mit GeldKarte erworbenen Tickets gepflegt.

D.9 Konfiguration der Funktionalität

Die Ausführbarkeit einiger Varianten der Ergänzungskommandos **ANLEGEN, ÄNDERN, ADMIN** und **RESET** kann durch Einträge im EF_EXECUTION eingeschränkt werden. Jeder Variante der Ergänzungskommandos, die eingeschränkt werden kann, ist ein Record im EF_EXECUTION fest zugeordnet, der u.a. angibt, wie oft das Kommando noch ausgeführt

werden darf. Zwischen den Records im EF_EXECUTION und den Kommandos ist folgende Zuordnung festgelegt:

Record	Kommandozuordnung		
	INS	**P1**	**Bedeutung**
1	’50’	’20’	**ANLEGEN** Startrecord
2	’50’	’40’	**ANLEGEN** Einzelrecord
3	’50’	’A0’	**ANLEGEN** Überprüfen ohne ICV
4	'50'	'C0'	**ANLEGEN** Überprüfen mit ICV
5	'52'	'00'	**ÄNDERN** VZP erster Record
6	’52’	’20’	**ÄNDERN** VZP Nachfolgerrecord
7	’52’	’40’	**ÄNDERN** ZD_INFO
8	’52’	’80’	**ÄNDERN** Initialrecord
9	’5A’	’20’	**ADMIN** Check
10	’5C’	’20’	**RESET**

Ein Record von EF_EXECUTION ist 7 Byte lang und beinhaltet einen 3 Byte langen Zähler, dessen 3 Byte langen Initialwert und ein Steuerbyte. Die Ausführbarkeit eines Kommandos wird bei dessen Aufruf durch den Wert des Zählers in Byte 1-3 des zugeordneten Records im EF_EXECUTION wie folgt bestimmt:

- Hat der Zähler in Byte 1-3 den Wert 'FF FF FF', so ist das Kommando unbeschränkt ausführbar. Der Wert des Zählers bleibt unverändert.
- Hat der Zähler in Byte 1-3 den Wert '00 00 00', so ist eine Ausführung des Kommandos nicht zulässig.
- In allen anderen Fällen wird der 3 Byte lange Zähler durch ein internes Update des zugeordneten Records um 1 dekrementiert und die Kommandoausführung fortgesetzt.

Ein Steuerbyte hat den folgenden Aufbau:

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
x								**Steuerung der Protokollierung in EF_TRANS_DAT**
0								Transaktionsdatum des Kommandos nicht protokollieren
1								Transaktionsdatum des Kommandos protokollieren
	x	x	x	x	x	x		immer 0 0 0 0 0 0, sonst RFU
							x	**Steuerung der Protokollierung in EF_FLOG**
							0	Kommandoausführung nicht protokollieren
							1	Kommandoausführung protokollieren

Konfigurationsbeispiele für die Zählerwerte:

Kommando	Beispiel 1	Beispiel 2	Beispiel 3	Beispiel 4
ANLEGEN Startrecord	’00 00 00’	’00 00 00’	’00 00 00’	’FF FF FF’
ANLEGEN Einzelrecord	’00 00 00’	’FF FF FF’	’00 00 00’	’FF FF FF’
ANLEGEN Überprüfen ohne ICV	'XX XX XX'	'FF FF FF'	'FF FF FF'	'FF FF FF'
ANLEGEN Überprüfen mit ICV	'XX XX XX'	'00 00 00'	'00 00 00'	'FF FF FF'
ÄNDERN VZP erster Record	'00 00 00'	'00 00 00'	'00 00 00'	'FF FF FF'
ÄNDERN VZP Nachfolgerrecord	'00 00 00'	'00 00 00'	'00 00 00'	'FF FF FF'
ÄNDERN ZD_INFO	'00 00 00'	'00 00 00'	'FF FF FF'	'FF FF FF'
ÄNDERN Initialrecord	'00 00 00'	'00 00 00'	'00 00 00'	'FF FF FF'
ADMIN Check	'00 00 00'	'XX XX XX'	'00 00 00'	'FF FF FF'
RESET	'00 00 00'	'XX XX XX'	'00 00 00'	'FF FF FF'

Erläuterung:

In Beispiel 1 darf das Kommando ANLEGEN Startrecord und Einzelrecord nicht ausgeführt werden. Da damit jeder Anlegevorgang verboten ist, kann kein Fahrschein angelegt werden. Mit diesem Sicherheitsmodul kann nur überprüft werden, ob gesichert gelesene Daten der Kundenkarte authentisch sind. (Einsatz nur im Kontrollgerät)

In Beispiel 2 dürfen nur Berechtigungen angelegt werden, die in einem Record abgespeichert werden können. Verknüpfte Records können nicht angelegt werden. Das Sicherheitsmodul kann auch gelesene Records überprüfen.

Anmerkung: Ein Sicherheitsmodul, das Fahrscheine anlegen kann, muss auch immer überprüfen können, ob ein Schreibvorgang erfolgreich war. Deshalb muss das Kommando ANLEGEN Überprüfen immer möglich sein, wenn Fahrscheine elektronisch angelegt werden.

Die Konfiguration in Beispiel 3 erlaubt nur das Entwerten der Fahrscheine und das gesicherte Lesen der Fahrscheine.

Das Sicherheitsmodul in Beispiel 4 kann beliebige Fahrscheine anlegen. Neben der benötigten Funktionalität zum Überprüfen kann damit auch der Verfallzeitpunkt zurückgesetzt werden und Entwertungen von Mehrfachfahrscheinen vorgenommen werden. Mit dem Kommando ÄNDERN Initialrecord können noch nicht verfallene Fahrscheine auch komplett mit einem Initialrecord überschrieben werden, sofern die Anbieter_ID im Sicherheitsmodul mit der Anbieter_ID im betreffenden Fahrschein übereinstimmt.

Anhang E Abkürzungsverzeichnis

Abkürzung	Bedeutung
DFÜ	**D**aten**f**ern**ü**bertragung
FSAM	Sicherheitsmodul der Zusatzanwendung Fahrschein
MSAM	Sicherheitsmodul der Zusatzanwendung Marktplatz
ÖPV	**Ö**ffentlicher **P**ersonen**v**erkehr
RFU	**R**eserved for **F**urther **U**se
VDV	**V**erband **d**eutscher **V**erkehrsunternehmen
ZKA	**Z**entraler **K**redit**a**usschuss