

DIN EN 15320

ICS 35.240.15

**Identifikationskartensysteme –
Landgebundene Transportanwendungen –
Interoperable Anwendungen für den öffentlichen Verkehr –
Rahmenwerk;
Deutsche Fassung EN 15320:2007**

Identification card systems –
Surface transport applications –
Interoperable Public Transport Applications – Framework;
German version EN 15320:2007

Systèmes de cartes d'identification –
Applications pour le transport terrestre –
Applications de transport public interoperables;
Version allemande EN 15320:2007

Gesamtumfang 135 Seiten

Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN

Nationales Vorwort

Dieses Dokument (EN 15320:2007) geht auf Arbeiten der WG 11 „Transportanwendungen“ von CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen“ zurück, dessen Sekretariat vom AFNOR (Frankreich) gehalten wird. Das zuständige deutsche Gremium ist der NA 043-01-17-11 AK „Transportanwendungen“ im Normenausschuss Informationstechnik und Anwendungen (NIA) im DIN.

Für die Anwendung dieser Norm gibt der NA 043-01-17-11 AK „Transportanwendungen“ folgende Hinweise:

Bei der Erarbeitung der Deutschen Fassung wurden nur die allgemein gehaltenen Inhalte übersetzt, die es dem Leser ermöglichen sollen – über den Anwendungsbereich hinaus – die Zusammenhänge beim Aufbau eines Systems zur Nutzung der interoperablen Transportanwendung besser zu verstehen und eine Übersicht zu erhalten, welche technischen und kommerziellen Voraussetzungen zu berücksichtigen sind. Es werden jene Komponenten der Anwendung beschrieben, die zur Unterstützung einer interoperablen Umgebung notwendig sind (z. B. Zugriffsbedingungen, Daten, Datenstruktur und -darstellung, Sicherheit, Umgang mit Legacy-Systemen).

Zum besseren Verständnis wurden in einigen Fällen englische Formulierungen umschrieben oder auch zusätzlich durch englische Begriffe ergänzt. Dadurch sollen Fehlinterpretationen vermieden werden.

Die Umsetzung selbst ist den Experten vorbehalten, die die Voraussetzungen zur Implementierung der Anwendungen auf den maschinenlesbaren Karten und in den Terminals (Kartenlesegerät) unter Berücksichtigung von Sicherheitsaspekten schaffen.

Die Fachsprache der Umsetzenden dieser Europäischen Norm (z. B. Softwareingenieure, Programmierer usw.) ist Englisch. Aus diesem Grunde wurden Programmierabläufe, Datenelemente, Datentypen und Datengruppen überwiegend unverändert aus der Englischen Fassung übernommen.

Deutsche Fassung

**Identifikationskartensysteme —
Landgebundene Transportanwendungen —
Interoperable Anwendungen für den öffentlichen Verkehr —
Rahmenwerk**

Identification card systems —
Surface transport applications —
Interoperable Public Transport Applications —
Framework

Systèmes de cartes d'identification —
Applications pour le transport terrestre —
Applications de transport public interoperables

Diese Europäische Norm wurde vom CEN am 8. September 2007 angenommen.

Die CEN-Mitglieder sind gehalten, die CEN/CENELEC-Geschäftsordnung zu erfüllen, in der die Bedingungen festgelegt sind, unter denen dieser Europäischen Norm ohne jede Änderung der Status einer nationalen Norm zu geben ist. Auf dem letzten Stand befindliche Listen dieser nationalen Normen mit ihren bibliographischen Angaben sind beim Management-Zentrum des CEN oder bei jedem CEN-Mitglied auf Anfrage erhältlich.

Diese Europäische Norm besteht in drei offiziellen Fassungen (Deutsch, Englisch, Französisch). Eine Fassung in einer anderen Sprache, die von einem CEN-Mitglied in eigener Verantwortung durch Übersetzung in seine Landessprache gemacht und dem Management-Zentrum mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, den Niederlanden, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, der Schweiz, der Slowakei, Slowenien, Spanien, der Tschechischen Republik, Ungarn, dem Vereinigten Königreich und Zypern.



EUROPÄISCHES KOMITEE FÜR NORMUNG
EUROPEAN COMMITTEE FOR STANDARDIZATION
COMITÉ EUROPÉEN DE NORMALISATION

Management-Zentrum: rue de Stassart, 36 B-1050 Brüssel

Inhalt

	Seite
Vorwort	4
Einleitung.....	5
1 Anwendungsbereich	7
2 Normative Verweisungen.....	8
3 Begriffe	8
4 Symbole und Abkürzungen	12
5 Grundstruktur von Anwendungskomponenten.....	13
6 Datengruppen.....	15
7 Die abstrakte Schnittstelle (en: abstract interface).....	23
8 Anwendungssicherheit	32
9 Profile	39
Anhang A (normativ) Definitionen von Datengruppen.....	43
Anhang B (normativ) Bezeichnung und Abbildung von Datengruppen.....	46
Anhang C (normativ) Auflistung von Datenelementen nach EN 1545 zur Benutzung in der Anwendung	63
Anhang D (normativ) ASN.1-Tag-Zuweisungen	77
Anhang E (informativ) Allgemeine Anforderungen.....	86
Anhang F (informativ) Beispiele	93
Anhang G (informativ) Zugriff auf die interoperable Anwendung für den öffentlichen Verkehr.....	124
Anhang H (normativ) Zusammenhang zwischen Legacy-Systemen und der interoperablen Anwendung für den öffentlichen Verkehr	127
Anhang I (informativ) Unterstützung von Legacy-Systemen.....	130
Literaturhinweise	133
 Bilder	
Bild 1 — Interoperables Fahrgeldmanagementsystem.....	5
Bild 2 — Datenelement innerhalb eines Datenobjektes.....	14
Bild 3 — Datenstruktur	14
Bild 4 — Datengruppe	15
Bild 5 — Beziehungen zwischen den Datengruppen	16
Bild 6 — Datengruppeninhalte	21
Bild 7 — Produkt-Datengruppe mit festgeschriebenen und veränderlichen Teilen	21
Bild 8 — Die Anwendungsumgebung verknüpft die Datengruppen miteinander.....	22
Bild 9 — Abhängigkeiten zwischen logischen Schnittstellen, dem SSS, der Karte und dem Terminal	23
Bild 10 — Logische Schnittstelle 1: Kartendatenschnittstelle.....	25
Bild 11 — Logische Schnittstelle 2: Datengruppenschnittstelle	26
Bild 12 — Repräsentative Abfolge von Anwendungsbefehlen	31
Bild 13 — Anwendungszustände	32
Bild 14 — Kontrolldatenstruktur von Datengruppen	38
Bild 15 — Eintrag einer Kontrolldatenstruktur	38
Bild 16 — Struktur der Profil-ID	41
Bild 17 — Profilableitung	42
Bild E.1 — Interoperable Anwendung für den öffentlichen Verkehr	87
Bild E.2 — Produkte innerhalb der interoperablen Anwendung für den öffentlichen Verkehr	87
Bild E.3 — Nutzung der Produkte der interoperablen Anwendung für den öffentlichen Verkehr.....	88

Bild G.1 — Aktivierung der Karte und der Anwendung.....	124
Bild H.1 — Anwendungs-Wrapper	128
Bild H.2 — Einsatz in mehreren Umgebungen	128
Bild H.3 — Adapter für die interoperable Anwendung für den öffentlichen Verkehr	129
Bild H.4 — Zugriffshierarchie	129
Bild I.1 — Kompatible interoperable Anwendung für den öffentlichen Verkehr.....	132

Tabellen

Tabelle 1 — Funktionen der Kartendatenschnittstelle	25
Tabelle 2 — Funktionen der Datengruppenschnittstellen.....	26
Tabelle 3 — Aktivitäten und Nutzungsfälle der Anwendung	28
Tabelle 4 — Festlegung AM-Byte.....	39
Tabelle A.1 — Datengruppenbezeichnung	43
Tabelle A.2 — Datenstrukturen innerhalb von Datengruppen.....	44
Tabelle B.1 — Spezifische verbindliche Datenstrukturen — Anwendungsumgebung	46
Tabelle B.2 — Spezifische verbindliche Datenstrukturen — Ereignisprotokoll	47
Tabelle B.3 — Allgemeine verbindliche Datenstrukturen	48
Tabelle B.4 — Optionale Datenstrukturen — Typ A.....	51
Tabelle B.5 — Datenstrukturen — Typ L.....	57
Tabelle B.6 — Datenstruktur Cyclic Event Log	62
Tabelle C.1 — Ausführlich in EN 1545 beschriebene Anwendungsdatenelemente	63
Tabelle C.2 — Nicht ausführlich in EN 1545 beschriebene Anwendungsdatenelemente.....	67
Tabelle C.3 — Nicht in EN 1545 enthaltene Anwendungsdatenelemente	74
Tabelle F.1 — Beispiel für eine Kennung.....	93
Tabelle F.2 — Beispiel für einen Instanzbezeichner	93
Tabelle F.3 — Beispiel für ein Siegel.....	93
Tabelle F.4 — Fahrpreisermäßigung: Erzeugung von Inhaber-Id und Berechtigung	94
Tabelle F.5 — Fahrpreisermäßigung: Gültigkeitserstellung	95
Tabelle F.6 — Fahrpreisermäßigung: Nutzung der Ermäßigung.....	96
Tabelle F.7 — Mehrfahrtenkarte: Kunde erwirbt eine Mehrfahrtenkarte	97
Tabelle F.8 — Mehrfahrtenkarte: Eine Reise wird unternommen.....	98
Tabelle F.9 — Mehrfahrtenkarte: Eine weitere Reise wird unternommen	99
Tabelle F.10 — Mehrfahrtenkarte: Hinzufügen von Fahrten	100
Tabelle F.11 — Check-in, Check-out: Verfügbarkeit der gespeicherten Reiseberechtigungen (STR) ..	101
Tabelle F.12 — Check-in, Check-out: Check-in.....	101
Tabelle F.13 — Check-in, Check-out: Check-out.....	102
Tabelle F.14 — Check-in, Check-out: Nutzung der gespeicherten Reiseberechtigungen.....	103
Tabelle F.15 — Check-in, Check-out: Die Reise wird fortgesetzt.....	104
Tabelle F.16 — Check-in, Check-out: Weitere Nutzung der gespeicherten Reiseberechtigungen	105
Tabelle F.17 — Be-in, Be-out: Anspruch auf eine Fahrt	106
Tabelle F.18 — Be-in, Be-out: Nach Betreten des Fahrzeuges.....	106
Tabelle F.19 — Be-in, Be-out: Die Reise wird fortgesetzt	107
Tabelle F.20 — Streifenkarte: Barzahlung	108
Tabelle F.21 — Streifenkarte: Betreten des Fahrzeuges	109
Tabelle F.22 — Streifenkarte: Weitere Reisen	110
Tabelle F.23 — Bahnfahrt: Reservierung	112
Tabelle F.24 — Bahnfahrt: Eine Reise wird unternommen	113
Tabelle F.25 — RET: Ein Fahrschein wird erworben	114
Tabelle F.26 — RET: Check-in.....	115
Tabelle F.27 — RET: Check-out	116
Tabelle F.28 — RET: Check-in des folgenden Reiseabschnitts	117
Tabelle F.29 — RET: Check-out des folgenden Reiseabschnitts	118
Tabelle F.30 — RET: Check-in Rückreise	119
Tabelle F.31 — RET: Check-out Rückreise	120
Tabelle F.32 — Flächenzonentarif: Ein Fahrschein wird erworben.....	122
Tabelle F.33 — Flächenzonentarif: Der Fahrschein wird genutzt.....	123
Tabelle G.1 — Antworten auf bekannte Kartentypen	125

Vorwort

Dieses Dokument (EN 15320:2007) wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen“ erarbeitet, dessen Sekretariat vom AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Juni 2008, und etwaige entgegenstehende nationale Normen müssen bis Juni 2008 zurückgezogen werden.

Bei der Definition einer interoperablen Anwendung für den Öffentlichen Verkehr stützt sich das vorliegende Dokument auf folgende Normen:

- EN 1545-1:2005, *Identifikationskartensysteme — Landgebundene Transportanwendungen — Teil 1: Elementare Datentypen, allgemeine Codelisten und generelle Datenelemente*;
- EN 1545-2:2005, *Identifikationskartensysteme — Landgebundene Transportanwendungen — Teil 2: Datenelemente und Codelisten für Zahlungsvorgänge in Transport- und Reiseanwendungen*.

Dieses Dokument beschreibt die Grundlage einer technologieutralen Umgebung für eine interoperable Anwendung für den öffentlichen Verkehr im Rahmen der für Identifikationskartensysteme geltenden Definition. Die Interoperabilität kann jedoch nicht aufrechterhalten werden, wenn die entsprechenden maschinenlesbaren Karten unterschiedliche Schnittstellentechnologien verwenden. Daher legt dieses Dokument die Einhaltung von ISO/IEC 14443, Teile 1 bis 3, als notwendige Voraussetzung für die Sicherstellung der Interoperabilität fest.

Von Zeit zu Zeit wird diese Europäische Norm geändert und verbessert, wobei die Ergebnisse auf der CEN-Website veröffentlicht werden.

Die Verfasser dieser Norm sind nach bestem Wissen davon überzeugt, dass die Norm keine kommerziellen Urheberrechte, geistigen Eigentumsrechte oder Patente verletzt. CEN kann dies jedoch nicht garantieren und ist nicht für derartige Verletzungen oder Ansprüche verantwortlich, die nach der CEN-Geschäftsordnung behandelt werden.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Bulgarien, Dänemark, Deutschland, Estland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Lettland, Litauen, Luxemburg, Malta, Niederlande, Norwegen, Österreich, Polen, Portugal, Rumänien, Schweden, Schweiz, Slowakei, Slowenien, Spanien, Tschechische Republik, Ungarn, Vereinigtes Königreich und Zypern.

Einleitung

Die interoperable Anwendung für den öffentlichen Verkehr definiert die Grundlage und die Grundstruktur einer Transportanwendung, hauptsächlich für das Erstellen von Fahrscheinen zur Anwendung auf einer maschinenlesbaren Karte unter Nutzung der in EN 1545 definierten Datenelemente, wobei die Karte je nach Handelsvereinbarung zwischen den Beteiligten und dem Austausch spezifischer Umsetzungsdetails interoperabel verwendet werden darf. Dadurch sind unterschiedliche Betreiber in der Lage, von Dritten hergestellte maschinenlesbare Karten mit der Anwendung zu lesen, zu interpretieren und zu handhaben. Darüber hinaus sollte es, wiederum je nach Handelsvereinbarung zwischen den Beteiligten, möglich sein, dass ein Transportbetrieb seine Fahrscheinprodukte auf von Dritten ausgestellte maschinenlesbare Karten, die die Anwendung enthalten, schreiben kann. In Anhang H wird erläutert, wie Legacy-Systeme so mit der Anwendung kombiniert werden können, dass ein gewisses Maß an Interoperabilität durch einen Migrationspfad zu der Anwendung erreicht werden kann.

Diese Europäische Norm beschreibt die Grundlage einer auf einer maschinenlesbaren Karte enthaltenen Anwendung für den öffentlichen Verkehr, die an der Schnittstelle zu einem geeigneten Terminal vorgelegt wird. Wenn die Karte einen Prozessor enthält, liegt diese Schnittstelle in vielen Fällen zwischen der Karte und dem kartenlesenden Gerät (Kartenterminal). In anderen Fällen wird zur notwendigen Unterstützung zusätzliche Logik in das Terminalsystem mit aufgenommen. Dies wird durch Festlegung einer logischen abstrakten Schnittstelle erreicht. Das eigentliche Format der auf der Karte enthaltenen Daten wird in dieser Europäischen Norm nicht beschrieben. Dieses Format darf durch Abbildung der in dieser Europäischen Norm beschriebenen Daten auf der Karte unter Anwendung einer ASN.1-Codierungsregel abgeleitet werden.

Diese Europäische Norm bildet einen Teil einer Reihe von Normen, die sich auf den öffentlichen Verkehr bezieht und das in Bild 1 dargestellte interoperable Fahrgeldmanagementsystem definiert.

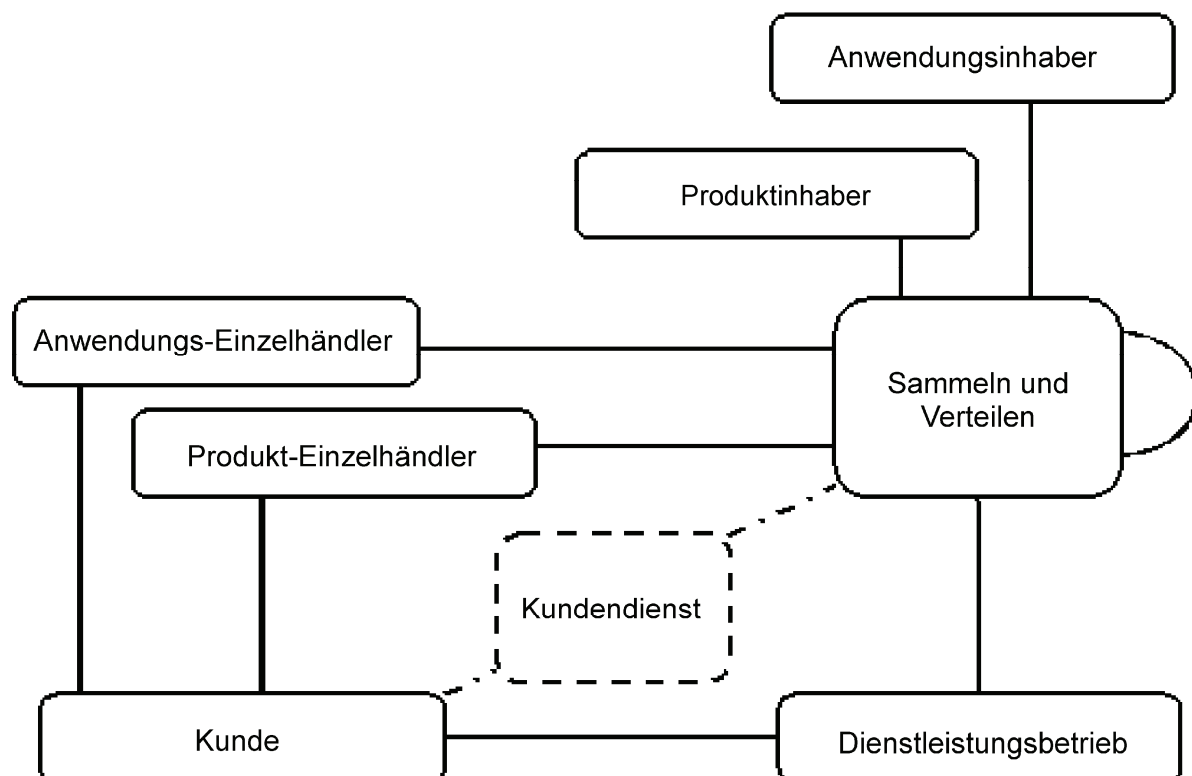


Bild 1 — Interoperables Fahrgeldmanagementsystem

Diese Europäische Norm beschreibt die Basis einer Umgebung, mit der folgende Ziele erreicht werden sollen:

- Schaffung einer Grundlage für das Anbieten maschinenlesbarer interoperabler Fahrscheine im öffentlichen Verkehrsnetz Europas;
- Erfüllung der Forderung nach Sicherstellung einer nahtlosen Reise für Fahrgäste, so dass diese mit einer einzigen Karte mit allen teilnehmenden Betreibern reisen können, möglicherweise in verschiedenen Netzen und Ländern, jedoch ohne dass dadurch der Wettbewerb eingeschränkt wird.

Diese Europäische Norm beschreibt die Bestandteile der Anwendung, die zur Unterstützung einer interoperablen Umgebung erforderlich sind, darunter:

- Zugriff auf die interoperable Anwendung für den öffentlichen Verkehr;
- Datenstruktur und -darstellung;
- Größe und Aufzählung von Daten;
- Verfahren für Datenzugriff;
- Überlegungen zu Sicherheit und Zugriff;
- Umgang mit Legacy-Systemen.

1 Anwendungsbereich

Diese Europäische Norm legt Datensätze, die an einer Schnittstelle, der Kartenuntersystem-Schnittstelle, in einer strukturierten Form vorgelegt werden, sowie die Regeln für den Umgang mit den Daten fest, so dass es möglich ist, Produkte, zum Beispiel Fahrscheine, so auf eine maschinenlesbare Karte zu schreiben, dass die Datenmenge auf der Karte minimiert wird, während die Daten für eine autorisierte Partei gleichzeitig leicht und effizient zugreifbar und interpretierbar sind.

Dies ist die Grundlage für eine anwendbare Interoperabilität. In diesem Sinne bildet diese Europäische Norm einen Grundstock für die Interoperabilität zwischen Systemen, deren Gegenstand die Geschäftsbeziehungen und der Austausch über Einzelheiten – wie diese Norm eigentlich auszulegen ist – sind. Als Teil dieser Fähigkeit erlaubt es die Gestaltung der Datenumgebung, zusätzliche neue Datensätze zur Darstellung neuer oder modifizierter Transportprodukte aufzunehmen, ohne bestehende Terminals bei der Handhabung aller auf der Karte vorhandenen Datensätze zu beeinträchtigen, unabhängig davon, ob diese interpretiert und möglicherweise genutzt werden sollen oder nicht.

Den Daten zugeordnet ist die Prozessgruppe, die für die Daten innerhalb der Anwendung gilt. Die Aufnahme der Prozesse in dieser Europäischen Norm bedeutet, dass ähnliche Daten von allen externen Dienstleistern und Terminals auf ähnliche Weise behandelt werden. Dies führt zu einer echten Interoperabilität, die durch diese Europäische Norm erreicht und aufrechterhalten werden kann. Zusätzlich bedeutet die Vereinbarung, dass die Anwendung sowohl Daten als auch Prozesse festlegt, dass sie Sicherheitsfragen auf der Ebene der Zugriffsrechte auf Daten sowie die Sicherheit der gesamten Umgebung, in der sie eingesetzt wird, berücksichtigen muss.

Die sicherheitsbezogenen Abschnitte dieser Europäischen Norm definieren die Anforderung an die Funktionalität, die mindestens erforderlich ist, um die Interoperabilität bei gleichzeitigem Schutz der in der Anwendung gespeicherten Informationen vor unberechtigtem Zugriff und versehentlicher oder absichtlicher Beschädigung zu unterstützen. Diese Europäische Norm definiert eine abstrakte Anwendungsschnittstelle zwischen Karte und Kartenterminal, die sich, je nach Fähigkeit der Karte, vollständig am Rand der Karte befindet oder eine Logik im Kartenterminal enthalten darf. Die Sicherheitsfrage wird ähnlich betrachtet wie bei einem externen System, das über die abstrakte Schnittstelle auf maschinenlesbare Karten zugreift, wobei es sich entweder nur um die Karte oder eine Kombination aus Karte und Kartenterminal handeln darf. Das bedeutet, dass Sicherheitskontrollen in der Karte, im Kartenterminal oder in beiden vorhanden sein dürfen. Zusätzliche Beschreibungen der Sicherheitsarchitektur und zu erwartende Umsetzungsfragen sind in den Abschnitten 7 und 8 beschrieben.

Diese Europäische Norm beschreibt die Mindestanforderungen an eine interoperable Transportanwendung, die auf einer maschinenlesbaren Karte vorhanden sein darf, entweder eigenständig oder zusammen mit anderen Anwendungen; sie umfasst daher eine Beschreibung der Datensätze und -formate auf logischer Ebene. Die abstrakte Schnittstelle muss viele verschiedene Arten von maschinenlesbaren Karten unterstützen, die einer kontaktlosen Schnittstelle nach ISO/IEC 14443 entsprechen. Dabei müssen die Teile 1 bis 3 von ISO/IEC 14443 unterstützt werden. Während diese Europäische Norm speziell für maschinenlesbare Karten gilt, kann andererseits auch der Wunsch bestehen, sie privat für andere Kundenmedien, wie etwa Key-Fobs, zu verwenden, vorausgesetzt, diese Kundenmedien sind in der Lage, bei geforderter Interoperabilität eine Schnittstelle mit Kartenterminals zu bilden, die mit dieser Europäischen Norm übereinstimmen.

Im Hinblick auf die Dateistrukturen sind die in dieser Europäischen Norm beschriebenen Datensätze und -formate hervorragend dafür geeignet, auf einer Karte nach ISO/IEC 7816-4 abgebildet zu werden. Diese Europäische Norm definiert jedoch nicht die Kartenarchitektur; die definierten Datenformate und -strukturen sind gleichermaßen in der Lage, auf einer reinen Speicherkarte oder einer komplexeren Karte mit mehreren Anwendungen, die einem anderen Dateiformat entspricht, umgesetzt zu werden, vorausgesetzt, das Kartenterminal unterstützt zur Erfüllung der Schnittstellenanforderungen nach dieser Europäischen Norm die geforderte Funktionalität, die die Karte nicht bietet.

Diese Europäische Norm beschreibt ein generisches logisches Modell im ASN.1-Format, das mit Hilfe der ASN.1-Codierungsregeln, zum Beispiel BER und PER, in einer realen Umgebung abgebildet werden kann. Es wird jedoch anerkannt, dass bestimmte übergeordnete Faktoren die Art und Weise beeinflussen können, in der Daten auf realen Karten abgebildet werden.

- Durch Transaktionszeit dargestellte Leistung ist in vielen Transportanwendungen ein kritischer Punkt. Durch die Anwendung externer Tag-Listen erlauben es die PER-Codierungsregeln, die physikalische Datenstruktur festzulegen und deren Größe zu verringern. Aus diesem Grund wird erwartet, dass in praktischen Umsetzungen PER oder eine ähnliche Codierungsregel verwendet wird;
- Einschränkungen im Hinblick auf den auf der Karte für die Daten zur Verfügung stehenden Raum beeinflussen ebenfalls die Entscheidung zu Gunsten der Verwendung von PER oder ähnlichen Codierungsregeln;
- Das Erfordernis der Aufrechterhaltung einer eingeschränkten oder vollständigen Kompatibilität mit bestehenden Legacy-Systemen und in der Entwicklung befindlichen Systemen bedeutet, dass speziell hergeleitete Codierungsregeln festgelegt werden dürfen, um die logischen Strukturen im erforderlichen Format abzubilden.

Als Grundlage der Interoperabilität stellt diese Norm die Basis für eine Interoperabilität zwischen Instanzen der Anwendung dar, die von unterschiedlichen Parteien je nach Handelsvereinbarungen und dem Austausch von Details zur physikalischen Auslegung der Norm bereitgestellt werden.

2 Normative Verweisungen

Die folgenden zitierten Dokumente sind für die Anwendung dieses Dokuments erforderlich. Bei datierten Verweisungen gilt nur die in Bezug genommene Ausgabe. Bei undatierten Verweisungen gilt die letzte Ausgabe des in Bezug genommenen Dokuments (einschließlich aller Änderungen).

EN 1545-1:2005, *Identifikationskartensysteme — Landgebundene Transportanwendungen — Teil 1: Elementare Datentypen, allgemeine Codelisten und generelle Datenelemente*

EN 1545-2:2005, *Identifikationskartensysteme — Landgebundene Transportanwendungen — Teil 2: Datenelemente und Codelisten für Zahlungsvorgänge in Transport- und Reiseanwendungen*

ISO/IEC 7816-4:2005, *Identification cards — Integrated circuit cards — Part 4: Organization, security and commands for interchange*

3 Begriffe

Für die Anwendung dieses Dokuments gelten die folgenden Begriffe.

3.1

Notation für darstellungsunabhängige Syntax

en: abstract syntax notation

Form der Notation, die verwendet wird, um Datenelemente und Prozesse zu beschreiben, Standard für CEN--Dokumentation

3.2

Konto

en: account

Protokoll über den aktuellen Wert und den (gebündelten) Transaktionsverlauf eines Produktes, das im Hintergrundsystem (en: back-office-system) des „Produktinhabers“ verwaltet wird

3.3

anonyme Karte

en: anonymous card

Karte, die nicht mit einem namentlich benannten Inhaber verbunden ist, die jedoch eine rückverfolgbare Seriennummer trägt

3.4

Anti-Tearing

en: anti-tear

beschreibt Maßnahmen, die sicherstellen, dass eine absichtliche Veränderung der Daten im Kundenmedium während des normalen Gebrauchs nicht zur Korruption des Kundenmediums führt

3.5

Anwendung

en: application

auf einer maschinenlesbaren Karte oder einem anderen Kundenmedium vorhandene Instanz der interoperablen Anwendung für den öffentlichen Verkehr

3.6

Anwendungsinhaber

en: application owner

Entität, die den Anwendungsvertrag zur Nutzung der Anwendung mit dem Kunden besitzt

3.7

Anwendungs-Einzelhändler

en: application retailer

Entität, die mit Genehmigung des Anwendungsinhabers Anwendungen an den Kunden ausgibt und beendet, Werte sammelt und diese rückerstattet

3.8

Kartenakzeptanzgerät

en: card accepting device

Gerät, das elektronisch mit einer Karte interagieren und Daten mit der Karte austauschen kann

3.9

Karteninhaber

en: card holder

Person, die die Nutzungsrechte an der Karte besitzt

3.10

Konto belasten

en: charge to account

Service/Prozess des nachträglichen Inrechnungstellens anstatt einer Vorauszahlung oder einer Zahlung zum Zeitpunkt des Erwerbs (Untertyp von Produkt)

3.11

Check-in, Check-out

en: check in – check out

Inhaber validieren die Karten aktiv beim Betreten und Verlassen definierter, vom Transportanbieter festgelegter Bereiche

3.12

Fahrpreisermäßigung

en: concession

Berechtigung zu einem verringerten (oder entfallenden) Fahrgeld auf Grundlage des Alters, Gesundheitszustands oder Status

3.13

Vertrag

en: contract

Vereinbarung zwischen zwei oder mehreren Parteien im Transportumfeld, die Bedingungen definiert, unter denen der Nutzer Dienstleistungen in Anspruch nehmen kann und die z. B. durch Produkte wie Fahrscheine oder Berechtigungen dargestellt werden können

3.14

Kundenmedium

en: customer media

Entität, die mindestens dieselbe Funktionalität unterstützt wie eine maschinenlesbare Karte, jedoch in einem anderen Formfaktor vorliegen kann

3.15

Datenelement

en: data element

Speicherelement für einen unzerlegbaren Datenwert

[siehe EN 1545-1 ^{N1)}]

3.16

Berechtigung

en: entitlement

Anspruch oder Qualifizierung für eine Dienstleistung, ausgedrückt als Produkt (eine Art von Produkttemplate)

3.17

Hotlist

en: hot list

Liste von Karten, Anwendungen, Produkten oder Teilen der Ausrüstung, für die eine Transaktion besonderer Aufmerksamkeit bedarf

3.18

interoperables Fahrgeldmanagement

en: interoperable fare management

umfasst alle Systeme zum Erwerb und zur Nutzung von Fahrgeldprodukten in einer interoperablen Umgebung des öffentlichen Verkehrs

3.19

Interoperabilität

en: interoperability

Fähigkeit von Systemen, anderen Systemen Dienstleistungen zur Verfügung zu stellen und von diesen zu übernehmen

3.20

Reise

en: journey

vollständige Folge von einem oder mehreren Fahrtabschnitten (Fahrten), der/die zum Erreichen eines bestimmten Zwecks an einem bestimmten Ziel erforderlich ist/sind, und die die Nutzung von mehr als einem Fahrzeug und mehr als einer Transportart umfassen kann

[siehe EN 1545-1 ^{N1)}]

N1) Gegenüber der Deutschen Fassung von EN 1545-1:2005 wurde die Definition fachlich präzisiert.

3.21

Schlüssel

en: key

binäre Zeichenfolge zur Überwachung des Zugriffs auf eine Anwendung oder ein Produkt oder als Grundlage für die Verschlüsselung oder während der Berechnung von Nachrichtenauthentisierungscode

3.22

Treuepunkte

en: loyalty

Bonus für die Nutzung von Transportdienstleistungen

3.23

Nachrichtenauthentisierungscode

en: message authentication code

berechnetes Feld, das auf Daten in zuvor angegebenen Feldern beruht, und mit dem eine Nachricht als authentisch bestätigt werden kann

3.24

maschinenlesbare Karte

en: machine readable card

Wertmarke oder Entität, konform zu ISO/IEC 14443, Teile 1 bis 3

3.25

Profil

en: profile

Mittel zum Erreichen der Interoperabilität zwischen unterschiedlichen Kartenplattformen

3.26

Produkt

en: product

ermöglicht einem Kunden, eine Transportdienstleistung zu nutzen. Dafür befindet sich auf einer Karte ein Produkttemplate. Das Produkt wird durch einen eindeutigen Bezeichner gekennzeichnet. Die interoperable Anwendung für den öffentlichen Verkehr unterscheidet zwischen vier Produktuntertypen: CTA, STR, Fahr-schein und Berechtigung

3.27

Produktinhaber

en: product owner

Entität, die die Funktionen ausführt, die mit dem Besitzen (Festlegen des Preises, der Nutzungsregeln und der kommerziellen Regeln), der Abrechnung und der Rechnungslegung verbunden sind

3.28

Produkt-Einzelhändler

en: product retailer

Entität, die dem Kunden mit Genehmigung des Produktinhabers Produkte verkauft und zurücknimmt, Werte sammelt und rückerstattet

3.29

Produktregeln

en: product rules

Anforderungen an den Produktinhaber (Nutzungs- und Preisregeln sowie kommerzielle Regeln)

3.30

Produktspezifikation

en: product specification

Spezifikation von Funktionen, Datenelementen und Sicherheitsschemata entsprechend den Produktregeln

3.31

Produkttemplate

en: product template

technische Vorlage der Produktspezifikation für die Implementierung, die vom Registrator mit einer eindeutigen, vom Produktinhaber vorgegebenen Bezeichnung (Produkttemplate-ID) versehen wird

3.32

Einzelhändler

en: retailer

siehe Produkt-Einzelhändler, Anwendungs-Einzelhändler

3.33

Fahrt

en: ride

Bestandteil einer Reise

3.34

Route

en: route

Verweis auf einen Weg durch ein Transportnetz

3.35

Siegel

en: seal

Authentizitätsgarantie

3.36

Dienstleistungsbetrieb

en: service operator

Entität, die dem Kunden bei Nutzung eines Produktes die entsprechende Dienstleistung erbringt

3.37

gespeicherte Reiseberechtigung

en: stored travel rights

spezialisierte Form der geschlossenen elektronischen Geldbörse (en: e-purse) für Reisen (Untertyp eines Produkttemplates, die anstelle einer Währung Transportwertseinheiten verwendet)

3.38

Fahrschein

en: ticket

Anspruch auf eine Reise (Untertyp von Produkt)

4 Symbole und Abkürzungen

3DES	Triple DES
AFI	Application Family Identifier (Bezeichner der Anwendungsfamilie)
AID	Application Identifier (Anwendungsbezeichner)
AM-DO	Access Mode Data Object (Datenobjekt Zugriffsart)
ASN.1	Abstract Syntax Notation One (Notation 1 für darstellungsunabhängige Syntax)
ATQ	Answer to Request (Antwort auf Anfrage)
ATS	Answer to Selection (Antwort auf Auswahl)
BER	Basic Encoding Rules (Basis-Cordierregeln)

CAD	Card Accepting Device (Kartenterminal)
CDS	Control Data Structure (Kontrolldatenstruktur)
CEN	European Committee for Standardization (Europäisches Komitee für Normung)
CICO	Check in – Check out (Check-in, Check-out)
CRC	Cyclic Redundancy Check (Zyklische Redundanzprüfung)
CTA	Charge to Account (Konto belasten)
DES	Data Encryption Standard (Datenverschlüsselungsnorm)
FCP	File Control (Dateisteuerung)
ID	Identity (Identität)
IEC	International Electrotechnical Commission (Internationale Elektrotechnische Kommission)
IFM	Interoperable Fare Management (Interoperables Fahrgeldmanagement)
ISO	International Organization for Standardization (Internationale Organisation für Normung)
MAC	Message Authentication Code (Meldungsberechtigungscode)
PER	Packed Encoding Rules (Komprimierte Codierregeln)
REQA	Request Type A (Anfrage Typ A)
REQB	Request Type B (Anfrage Typ B)
RSA	Rivat Shamir Adelman
SAK	Select Acknowledge (Auswahl anerkennen)
SC-DO	Security Condition Data Objekt (Datenobjekt Sicherheitsbedingung)
SSS	Security Sub-System (Sicherheitsuntersystem)
STR	Stored Travel Rights (Gespeicherte Reiseberechtigung)
TLV	Tag Length Value (Wert für die Tag-Länge)

5 Grundstruktur von Anwendungskomponenten¹⁾

5.1 Datenelement

Ein Datentyp im Sinne dieser Europäischen Norm ist eine der in EN 1545 beschriebenen Datenelemententitäten. Es ist die niedrigste hierarchische Entität der in dieser Europäischen Norm erläuterten Daten. Jedes Element muss einen Tag und einen Längendeskriptor enthalten, um ein den ASN.1-Konventionen entsprechendes TLV-Datenobjekt zu bilden.

1) Die folgenden Abschnitte beschreiben die in Bezug auf Daten in dieser Norm verwendete Terminologie.

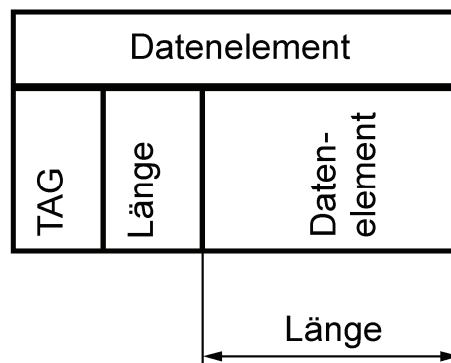


Bild 2 — Datenelement innerhalb eines Datenobjektes

Die meisten der in dieser Europäischen Norm verwendeten Datenelemente sind als einfache ASN.1-Datenelemente beschrieben und im Anhang C aufgelistet sowie original in EN 1545 festgelegt. In einigen speziellen Fällen handelt es sich bei den in dieser Europäischen Norm verwendeten Datenelementen um konstruierte Elemente entsprechend der Definition in EN 1545.

5.2 Datenstruktur

Ein in Datenobjekten enthaltener Satz von Datenelementen, der zweckmäßig als ASN.1-konstruiertes TLV-Objekt verknüpft wurde.

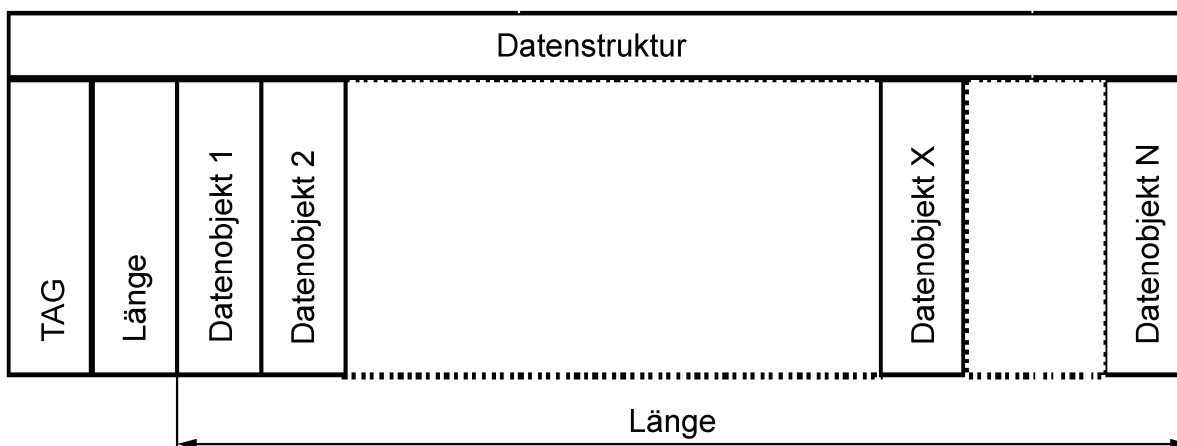


Bild 3 — Datenstruktur

Datenstrukturen sind aus praktischen Gründen wie folgt in Typen eingeteilt:

- M verbindlich (Datenstrukturen, die innerhalb einer spezifischen Datengruppe vorhanden sein müssen [siehe 5.3]);
- A zusätzlich (zusätzliche Datenstrukturen, die normalerweise zusammen mit der Datengruppe [siehe 5.3] oder dem Produkt erzeugt werden. Daten in diesen Strukturen werden während der Lebensdauer der Datengruppe normalerweise nicht verändert. Dies sollte sich in den Zugriffsrechten für das Sicherheitsuntersystem widerspiegeln, welche für die Datenstruktur innerhalb der die Datenstruktur enthaltenden Datengruppe gelten);
- L protokollierend (zusätzliche Datenstrukturen, die normalerweise während der Lebensdauer der Datengruppe [siehe 5.3] oder des Produktes erzeugt werden. Daten in diesen Strukturen dürfen nach der Erzeugung festgelegt und unveränderbar oder von Zeit zu Zeit aktualisierbar sein, je nach Erfordernis und den vom Sicherheitsuntersystem gesteuerten für die Zugriffsstruktur geltenden Zugriffsrechten).

5.3 Datengruppe

Eine Gruppierung auf höchster Ebene von Datenstrukturen, die als ein ASN.1-konstruiertes TLV-Objekt verknüpft sind, um große Gruppierungen von Daten zu identifizieren, die als kohärenter Satz durch den Tag zugänglich sind.

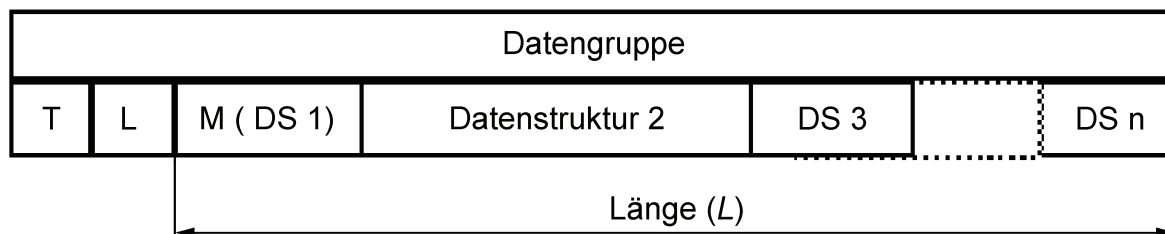


Bild 4 — Datengruppe

Die M-Datenstrukturen erscheinen in einer Datengruppe stets zuerst, wohingegen die Datenstrukturen des Typs A und des Typs L in jeder beliebigen Reihenfolge auftreten dürfen; A-Strukturen werden jedoch normalerweise zusammen mit der Datengruppe erzeugt, während L-Strukturen üblicherweise (jedoch nicht immer) nach der Erzeugung der Datengruppe hinzugefügt werden. Daher ist es üblich, aber nicht verbindlich, dass die Datengruppe in der Reihenfolge M, A..., L... konstruiert ist.

Einmal erzeugt und an eine Datengruppe angehängt, dürfen Datenstrukturen nicht gelöscht werden, bis die Datengruppe von der Anwendung in der Karte entfernt wurde, zum Beispiel, wenn ein Fahrschein benutzt wurde.

6 Datengruppen

6.1 Allgemeines

Die Konstruktion von und der Zugriff auf Datengruppen ist hier auf logische Weise entsprechend der Darstellung an der Schnittstelle definiert; die Umsetzung auf einer Karte darf in vielerlei Formen erfolgen, je nach Architektur und Codierung der Karte. Es besteht keine Abhängigkeit von und kein Zusammenhang mit der Definition einer Kartendateistruktur nach ISO 7816-4, obwohl die Datengruppenkonstruktion praktischerweise in dieser Architektur abgebildet werden kann, besonders, um die abweichenden Sicherheits- und Zugriffsanforderungen der die Datengruppe umfassenden Datenstrukturen zu reflektieren.

Folgende Datengruppen sind ausführlich in Anhang A definiert:

- Anwendungsumgebung (en: application environment);
- Produkt (en: products);
- Inhaber (en: holder);
- Ereignisprotokoll (en: event log);
- Wrapper.

Die Datengruppen sind miteinander verknüpft wie in Bild 5 dargestellt und in 6.2 beschrieben:

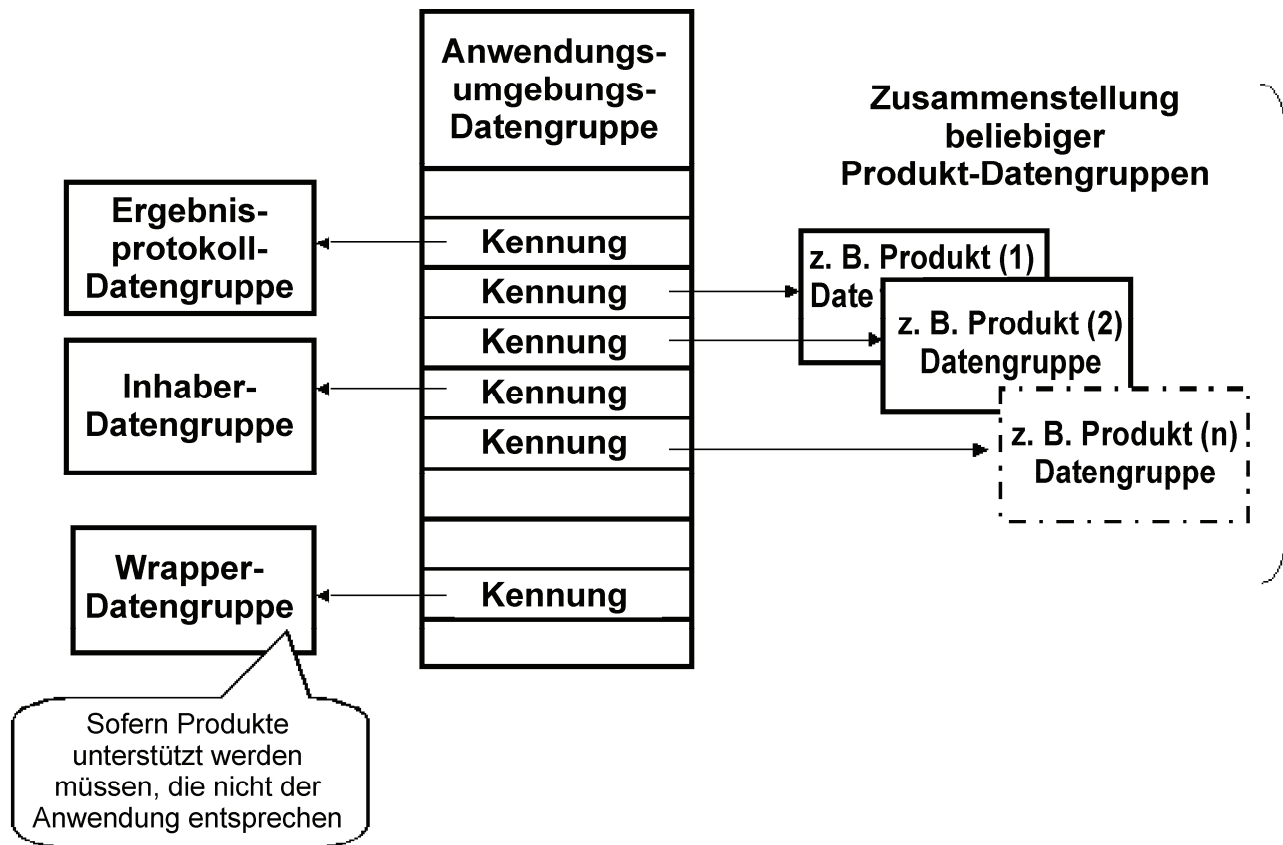


Bild 5 — Beziehungen zwischen den Datengruppen

6.2 Anwendungsumgebungs-Datengruppe (en: application environment data group)

Die Anwendungsumgebungs-Datengruppe erfüllt zwei Funktionen:

- Herstellen der Verknüpfung mit allen weiteren Datengruppen innerhalb der Anwendung (das heißt, sie stellt das Anwendungsprodukt-Verzeichnis dar);
- Bereitstellen von Informationen zur Anwendung (speziell zu dieser Instanz der Anwendung) auf der Karte, so, wie an der Schnittstelle interpretiert.

6.3 Produkte

Eine Zusammenstellung von Produkt-Datengruppen (en: product data groups), die Produkte identifizieren, die während der Lebensdauer der Anwendung erzeugt und entfernt werden dürfen. Die Produkt-Datengruppen sind:

- gespeicherte Reiseberechtigung (en: Stored Travel Rights, STR);
- Konto belasten (en: charge to account);
- Kundenberechtigung (en: customer entitlement);
- Fahrschein (en: ticket).

Jede Produkt-Datengruppe besteht aus einer oder mehreren Datenstrukturen. Die Datenstrukturen setzen sich mindestens aus der relevanten Datenstruktur des Typs M sowie zusätzlichen Datenstrukturen des Typs A und/oder des Typs L zusammen, die je nach Erfordernis entweder bei der Definition der Datengruppe oder zu einem späteren Zeitpunkt erzeugt wurden.

Wenn ein Fahrscheintyp dergestalt ist, dass der Preis am Ende einer Reise auf der Grundlage der zurückgelegten Fahrtabschnitte zu berechnen ist, darf an jeder Umsteigestation eine zusätzliche Struktur des Typs L an die aktive Datengruppe der Fahrscheine angehängt werden. Diese Typ L-Datenstrukturen dürfen je nach Erfordernis hinzugefügt werden, wodurch die Länge der Produkt-Datengruppe vergrößert wird, oder die Größe darf durch Behandlung der hinzugefügten Typ L-Datenstrukturen auf zyklische Weise begrenzt werden, indem die älteste derartige Datenstruktur durch eine neue ersetzt wird, sobald die für die Größe vorgegebene Grenze erreicht wurde.

Wenn sich der Fahrscheinpreis allein nach der Zahl der zurückgelegten Fahrtabschnitte richtet, wird als Alternative zu Beginn des ersten Abschnitts eine Typ L-Datenstruktur in die aktive Datengruppe des Fahrscheines aufgenommen. Bei jeder Umsteigestation wird das Feld zur Zählung der Fahrtabschnitte in dieser Datenstruktur aktualisiert. In diesem Fall sollten die Zugriffsrechte der zusätzlichen Typ L-Struktur auf Lesen/Schreiben gesetzt sein.

6.4 Wrapper-Datengruppe (en: wrapper data group)

Die Wrapper-Datengruppe ist speziell für die Migration von Legacy-Systemen vorgesehen. Diese Datengruppe ermöglicht es, dass ein Legacy-Produkt, wie zum Beispiel ein Fahrschein, in eine Instanz der Anwendung aufgenommen wird und dieser entspricht, sodass es möglich ist, das Produkt zu erzeugen und zu erkennen, darauf zuzugreifen und es zu löschen. Jedoch liegt die Verarbeitung des Legacy-Produktes, nachdem auf dieses zugegriffen wurde, außerhalb des Anwendungsbereiches dieser Europäischen Norm und ist dem Anbieter des Legacy-Systems und den Betreibern, die dieses unterstützen, überlassen. Dieses Konzept ist ausführlicher in den Anhängen H und I beschrieben.

6.5 Inhaber-Datengruppe (en: holder data group)

Die Inhaber-Datengruppe ist optional, wobei ihr Nichtvorhandensein eine anonyme Anwendung erzeugt und ihr Vorhandensein eine personalisierte Anwendung definiert. Es sollte jedoch beachtet werden, dass eine Anwendung mit einer Inhaber-Datengruppe dennoch anonym wirken kann, indem einfach nicht auf die Inhaber-Datengruppe zugegriffen wird.

Die Inhaber-Datengruppe muss aus einer oder mehreren Datenstrukturen bestehen, die sich mindestens aus der Inhaber-Datenstruktur des Typs M sowie aus optionalen Datenstrukturen des Typs A und des Typs L zusammensetzen, die je nach Erfordernis entweder bei der Anlage der Datengruppe oder zu einem späteren Zeitpunkt erzeugt wurden.

6.6 Ereignisprotokoll-Datengruppe (en: event log data group)

Das Ereignisprotokoll ist ein zyklischer Satz von Datenstrukturen (Aufzeichnungen) eines Typs, der Ereignis-Datenstruktur. Die Anzahl der Einträge in das Ereignisprotokoll beträgt immer mindestens zwei, darf jedoch auch darüberliegen, je nach den Anforderungen des Umsetzenden und dem Raum, der auf der maschinenlesbaren Karte wahrscheinlich zur Verfügung stehen wird. Wenn keine Einträge mehr im Protokoll frei sind, wird der älteste Eintrag durch den neuesten ersetzt. Das bedeutet, dass:

- das Ereignisprotokoll ein Protokoll über die jeweils neuesten aufgezeichneten „n“ Ereignisse zeigt;
- das Ereignisprotokoll nicht zum Vorhalten von Daten verwendet werden kann, die für mehr als ein Ereignis zu speichern sind, da nicht bekannt ist, wann eine Aufzeichnung überschrieben wird. Daher kann dieser Mechanismus nicht dazu verwendet werden, die Zählung von Reisen vorzuhalten; er könnte jedoch eingesetzt werden, wenn der beim aktuellen Ereignis durchgeführte Vorgang vom vorherigen Ereignis abhängt;

- es wichtig ist, das Ereignisprotokoll nicht mit redundanten Aufzeichnungen zu „überladen“, um es mit größtmöglichem Nutzen zu verwenden. Aus diesem Grund sollte das Ereignisprotokoll nicht alle Ereignisse aufzeichnen, sondern nur diejenigen, die speziell als Ereignisprotokoll-Ereignisse festgelegt wurden;
- wenn es als erforderlich erachtet wird, ein allgemeines Ereignisprotokoll zu erzeugen, das sämtliche Ereignisse aufzeichnet, wird es sich dabei in Anbetracht der oben genannten Punkte um ein separat erzeugtes und verwaltetes Ereignisprotokoll außerhalb der Anwendung handeln. Gemeinhin würde ein derartiges Protokoll auf Kartenebene arbeiten.

Falls erforderlich und für unterschiedliche Zwecke dürfen Ereignisse sowohl im Ereignisprotokoll als auch in einer Typ L-Datenstruktur aufgezeichnet werden, die einer bestimmten Datengruppe, etwa einem Fahrschein, zugeordnet ist.

Das Verfahren zur Umsetzung auf der Karte hängt von den vorhandenen Einrichtungen ab, die diesen Datengruppentyp unterstützen. Um die Unterstützung in Situationen zu ermöglichen, in denen die Karte zyklische Dateien nicht unterstützt und in denen eine derartige Konstruktion durch die Anwendung unterstützt werden muss, enthält die Ereignisprotokoll-Datengruppe ein Datenelement, das von der Anwendung gepflegt werden muss und verwendet wird, um auf den letzten Eintrag im zyklischen Ereignisprotokoll zu zeigen. Wenn die Karte zyklische Dateien unterstützt, darf dieses Element ignoriert werden.

6.7 Verknüpfung zwischen Datengruppen

Es dürfen Anforderungen hinsichtlich der Bildung von Verknüpfungen zwischen Produkten bestehen. So darf zum Beispiel ein Produkt mit einem Kundenvertrag verknüpft sein, oder die Gültigkeit eines Produktes darf mit dem Vorhandensein eines weiteren Produktes innerhalb der Anwendung verknüpft sein. Das wird erreicht durch Verwendung eines Datenelementes „Abhängigkeitszeiger“ (en: dependency pointer), das in einer relevanten Datenstruktur innerhalb einer Gruppe erscheint.

Es muss jedoch beachtet werden, dass bei Entfernen der Datengruppe, auf die verwiesen wird, möglicherweise kein Mechanismus zur Annullierung dieses Abhängigkeitszeigers vorhanden ist. Der Abhängigkeitszeiger zeigt zwar niemals auf die falsche Datengruppe, er kann jedoch auf eine nicht vorhandene Datengruppe zeigen. Aus diesem Grund sollten bei der Verarbeitung von Datengruppen sämtliche Abhängigkeitszeiger im Hinblick auf die Gültigkeit überprüft werden, bevor versucht wird, sie für die Verweisung auf andere Datengruppen zu verwenden. Eine Möglichkeit ist die Aufnahme des Abhängigkeitszeigers in das logische Schema der Kennung, sodass bei Hinzufügen und Entfernen von Produkten die Auswirkung auf den Abhängigkeitszeiger überprüft und korrigiert werden kann, ohne sämtliche Produkt-Datengruppen lesen zu müssen.

Die Art des Abhängigkeitszeigers auf einer Karte hängt von der Umsetzung ab. Auf der in dieser Europäischen Norm beschriebenen logischen Ebene ist er jedoch auf der Datengruppenfolgennummer (en: data group sequence number) der Zieldatengruppe abzubilden. Die Interoperabilität zwischen Anwendungen wird durch Handelsbeziehungen und den Austausch der jeweiligen Herangehensweisen bei der Umsetzung aufrechterhalten.

6.8 Datengruppenlebensdauer (en: data group life cycle)

Die codierten Datengruppen werden auf einer Karte erzeugt und dort gespeichert, bis sie nicht länger benötigt werden und der Platz für andere Zwecke zur Verfügung gestellt werden muss, üblicherweise für die Erzeugung einer neuen Datengruppe. Die Verwaltung der Datengruppenlebensdauer ist eine Funktion der Verwaltung der Einträge der Anwendungsumgebungs-Datengruppe (im Verzeichnis) sowie der Platzverwaltung innerhalb des in der Anwendung verfügbaren Arbeitsplatzes.

Datengruppen können sich während ihrer Lebensdauer mit dem Anhängen neuer Datenstrukturen (Typen A und L) erweitern. Wie sich dies in der Praxis auf einer Karte widerspiegelt, hängt von der jeweiligen Karte ab und liegt nicht im Anwendungsbereich dieser Europäischen Norm.

Die Lebensdauer/Speicherung der unterschiedlichen Datengruppen wird wie folgt unterteilt:

application environment	—	Während der Lebensdauer der Anwendung auf der Karte
Holder	—	bis ausdrücklich freigegeben
Product		
Stored Travel Rights	—	bis nicht weiter erforderlich und ausdrücklich freigegeben
Charge to Account	—	bis nicht weiter erforderlich und ausdrücklich freigegeben
customer entitlement	—	bis nicht weiter erforderlich und der Platz benötigt wird
Ticket	—	bis nicht weiter erforderlich und der Platz benötigt wird
(wrapper	—	bis nicht weiter erforderlich und der Platz benötigt wird)
Event	—	während der Lebensdauer der Anwendung auf der Karte, Platz wieder- verwendet auf Basis zyklischer Aufzeichnungen

6.9 Verbindliche Strukturen von Datengruppen (en: data group mandatory structures)

6.9.1 Allgemeines

Anhang B beschreibt für die unterschiedlichen Datengruppentypen ausführlich die verbindlichen Datenelemente in den verbindlichen Datenstrukturen (Typ M). Während diese, wie in Anhang B dargestellt, einige Datenelemente enthalten, die für jeden einzelnen Datengruppentyp einzigartig sind, gibt es drei Unterstrukturen (zusammengesetzte Datenelemente innerhalb der Datengruppe), die allen gemeinsam sind und als administrativer Datenblock (en: administrative data block) bezeichnet werden. Sie unterstützen die Anforderungen an die eindeutige Bezeichnung, Sicherheitsversiegelung und das Binden von Datengruppen an die Anwendung. Dabei handelt es sich um:

- die Kennung;
- den Instanzbezeichner;
- das Siegel (optional).

6.9.2 Die Kennung (en: label)

6.9.2.1 Allgemeines

Die Kennung ist eine Datenstruktur, die eine Datengruppe eindeutig bezeichnet. Die Kennung umfasst auch das Ablaufdatum.

In jeder Anwendung gibt es zwei Arten von Kennungen:

- Anwendungskennung, definiert als die Kennung der Anwendungsumgebung (eine einzige Instanz je Anwendung);
- Produkt- oder Inhaberkennung.

6.9.2.2 Die Anwendungskennung (en: application label)

Die Anwendungskennung bezeichnet die Anwendung und ist an die maschinenlesbare Karte gebunden. Sie ermöglicht die Identifizierung der Anwendung aus einer Vielzahl von Anwendungen. Sie bietet Informationen zur Anwendung, deren Inhaber und deren Ablaufdatum. Die Kennung trägt ausreichend Informationen, damit eine Terminalanwendung feststellen kann, ob diese Instanz der Anwendung von der Terminalanwendung akzeptiert werden darf.

6.9.2.3 Die Produktkennung (en: product label)

Die Produktkennung ist Teil der verbindlichen Daten in einer Produkt-Datengruppe. Sie ist außerdem im veränderlichen Teil der Anwendungsumgebungs-Datengruppe enthalten, wo sie die Identifizierung einer Produktschablone aus einer Vielzahl von Produktschablonen in jeder beliebigen Anwendungsumgebung ermöglicht. Die Produktkennung trägt ausreichend Informationen, damit eine Terminalanwendung feststellen kann, ob die in dieser Instanz der Anwendung vorhandenen Produkte akzeptiert werden dürfen.

Die Kennungsdaten dürfen in der Produkt-Datengruppe und im veränderlichen Teil der Anwendungsumgebungs-Datengruppe kopiert werden, oder sie dürfen an nur einer Stelle vorgehalten und an einer anderen abgebildet werden, wie in 6.9.5.2 dargestellt.

6.9.2.4 Die Inhaberkennung (en: holder label)

Die Inhaberkennung ist Teil der verbindlichen Daten in einer Inhaber-Datengruppe. Ihre Anordnung und Verwendung erfolgt entsprechend der in 6.9.2.3 für die Produktkennung angegebenen Beschreibung.

6.9.3 Der Instanzbezeichner (en: instance identifier)

Der Instanzbezeichner bezeichnet eine Datengruppe eindeutig, um so ein bestimmtes Produkt zu bezeichnen und um einen Prüfpfad zu ermöglichen, der die Vielzahl von Instanzen eines bestimmten Produktes unterscheidet.

6.9.4 Das Siegel (en: seal)

Die Verwendung eines Siegels ist nicht verbindlich; im Falle einer Verwendung gelten jedoch die folgenden Regeln.

Um unberechtigte Veränderungen von Datenelementen in der Datengruppe festzustellen, muss das Siegel die Gruppeninhalte abdecken. Das Siegelungskonzept deckt alle in einer Datengruppe enthaltenen Daten ab, einschließlich ASN.1-Tagfelder und -Längenfelder.

Das Siegel wird an der Schnittstelle vorgelegt und stellt eine Berechnung der tatsächlich geschriebenen Daten bzw. der an der Schnittstelle vorgelegten Daten dar. Die Form des Siegels und ob tatsächlich dieses Siegel auf die Karte geschrieben wird oder ein anderes Siegel, das auf einer anderen Berechnung basiert, oder ob gänzlich auf das Siegel verzichtet wird, hängt von der jeweiligen Umsetzung ab.

Gruppen von Datenstrukturen, die für die normale Lebensdauer einer Datengruppe festgeschrieben sind, dürfen getrennt von den Gruppen von Strukturen versiegelt werden, die während der normalen Verwendung variieren können. Da viele Datengruppen aus einer Vielzahl von Teilen bestehen, von denen einige festgeschriebene Daten und einige veränderliche Daten enthalten, darf für die festen und die veränderlichen Teile jeweils ein eigenes Siegel erzeugt werden. Das ermöglicht es dem Produktinhaber, die Integrität des Siegels für einen Teil einer Datengruppe zu wahren, während andere Daten von Dritten modifiziert und neu versiegelt werden können, ohne dabei Sicherheitsschlüssel gemeinsam nutzen zu müssen. Die Verwendung eines einzigen Siegels für einige oder alle Datengruppen ist nicht ausgeschlossen und darf in vielen Anwendungen die bevorzugte Option sein.

6.9.5 Layout von Datengruppen (en: data group layouts)

6.9.5.1 Produkt/Inhaber-Datengruppen (en: product/holder data groups)

Die Bilder 6 und 7 zeigen das angenommene Layout einer Produkt- oder Inhaber-Datengruppe, die aus verbindlichen Datenstrukturen und den optionalen Daten besteht, die das Produkt oder den Inhaber beschreiben, und zwar in den in Anhang B angegebenen Strukturen.

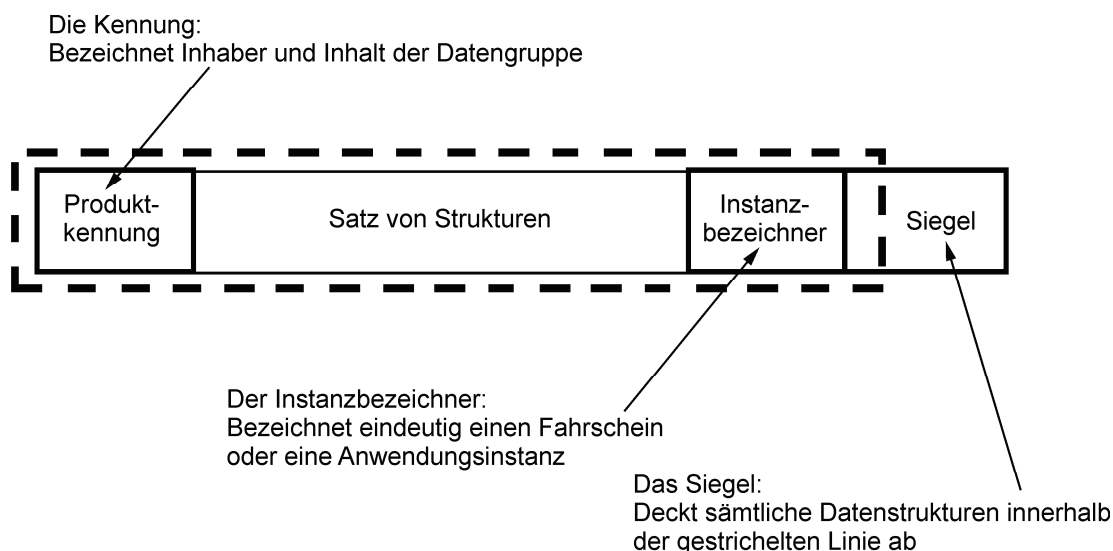


Bild 6 — Datengruppeninhalte

Wenn der Inhalt einer Datengruppe logisch in festgeschriebene und veränderliche Daten aufgeteilt ist und separat verwaltet wird, möglicherweise mit unterschiedlichen Zugriffsrechten für die festgeschriebenen und die veränderlichen Teile, darf die Datengruppe wie in Bild 7 dargestellt werden. In diesem Fall können die beiden Instanzbezeichner identisch sein oder nicht, während die beiden Siegel als Ergebnis der Daten erzeugt werden, die sie jeweils siegeln.

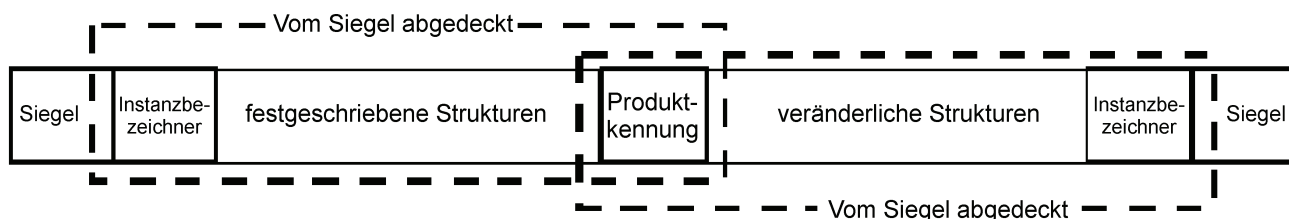


Bild 7 — Produkt-Datengruppe mit festgeschriebenen und veränderlichen Teilen

6.9.5.2 Anwendungsumgebungs-Datengruppe (en: application environment data group)

Die Anwendungsumgebungs-Datengruppe ist so aufgebaut wie die in 6.9.5.1 dargestellten Datengruppen. Die veränderlichen Daten in der Datengruppe sind jedoch logisch mit den Produkt- und Inhaber-Datengruppen verknüpft, die durch die in jeder Datengruppe vorhandenen Kennungsinformationen bezeichnet werden, wie in Bild 8 dargestellt.

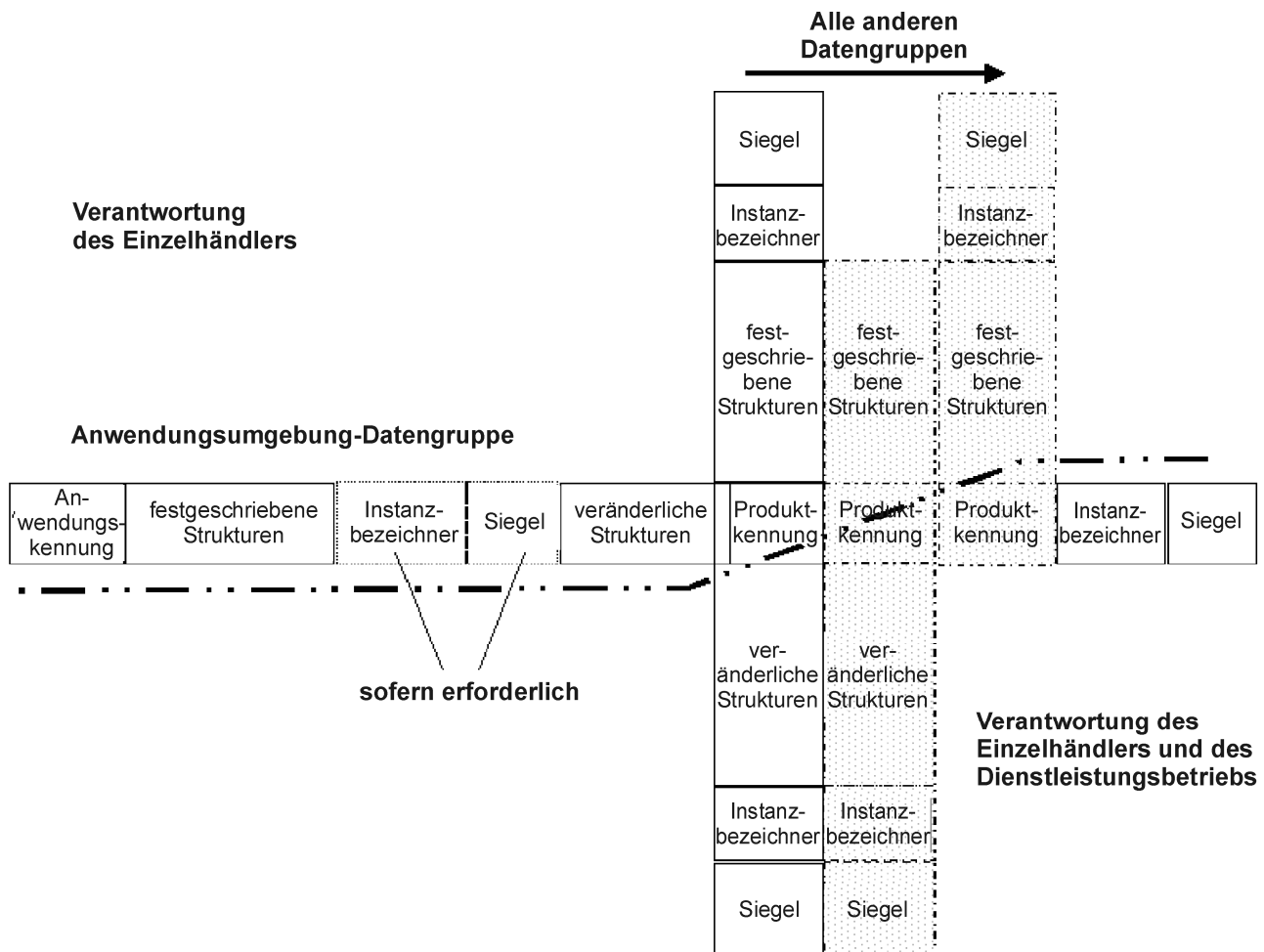


Bild 8 — Die Anwendungsumgebung verknüpft die Datengruppen miteinander

ANMERKUNG Wie dargestellt, duplizieren Kennungen die in der verbindlichen (M) Datenstruktur für jede Datengruppe definierten Daten. Für die praktische Umsetzung darf nur eine einzige Kopie dieser Daten in entweder dem veränderlichen Teil der Application Environment Data Group oder der Product Data Group gehalten und an der anderen erforderlich Stelle abgebildet werden oder sie darf dupliziert werden.

6.10 Priorität der Produkt-Datengruppen (en: product data group priority)

Das Prioritätsdatenelement (en: priority data element) ist ein optionales Datenelement im Instanzbezeichner einer Produkt-Datengruppe. Die Verwendung dieses Feldes, die darin eingestellten Werte, die Änderungsrechte und die ständige Verwaltung bleiben allein dem Umsetzenden überlassen.

Der Zugriff auf das Prioritätsdatenelement erfolgt durch Zugriff auf die Produkt-Datengruppe für jedes zu jedem beliebigen Zeitpunkt in einer Instanz der Anwendung vorhandene Produkt. Der Zugriff darf jedoch beschleunigt werden, wenn der Instanzbezeichner als logisches Schema neben der Kennung in der Anwendungsumgebungs-Datengruppe abgebildet wird. Dadurch wird das „Prioritätsfeld“ in das Produktverzeichnis der Instanz der Anwendung bewegt, das auf der maschinenlesbaren Karte vorhanden ist.

7 Die abstrakte Schnittstelle (en: abstract interface)

7.1 Allgemeines

Datengruppen bilden die Produkte und die dazugehörigen Einträge der Anwendungskennungen (Verzeichnis). Derartig codierte Datengruppen können auf einer Vielzahl von Plattformen für maschinenlesbare Karten und anderen Kundenmedien eingerichtet werden, die wiederum Schnittstellen zu einer Vielzahl von Terminalanwendungen bilden.

Eine solche abstrakte Schnittstelle stellt Standarddienstleistungen bereit, die nicht von den Fähigkeiten der Karte abhängig sind; sodass diese Europäische Norm die Grundlage für eine Interoperabilität mit vielen verschiedenen Kundenmedien bietet. Die Verteilung der Rollen zwischen der maschinenlesbaren Karte oder anderen Kundenmedien und der Terminalanwendung innerhalb der abstrakten Schnittstelle muss an die Fähigkeiten der Karte angepasst sein.

Um die unterschiedlichen Fähigkeiten der Vielzahl von Kartenplattformen und Produkten abzudecken, sind zwei logische Schnittstellen definiert:

- logische Schnittstelle 1: die Kartendatenschnittstelle;
- logische Schnittstelle 2: die Datengruppenschnittstelle.

Diese Schnittstellen definieren die Verbindung zwischen der Terminalanwendung und der maschinenlesbaren Karte und umfassen die Verwendung des Sicherheitsuntersystems. Die Verwendung dieser logischen Schnittstellen zwischen der Terminalanwendung und der maschinenlesbaren Karte ist für jede Anwendungs-umsetzung verbindlich.

Die Struktur der Abhängigkeiten zwischen der Terminalanwendung, der maschinenlesbaren Karte und dem Sicherheitsuntersystem ist in Bild 9 dargestellt.

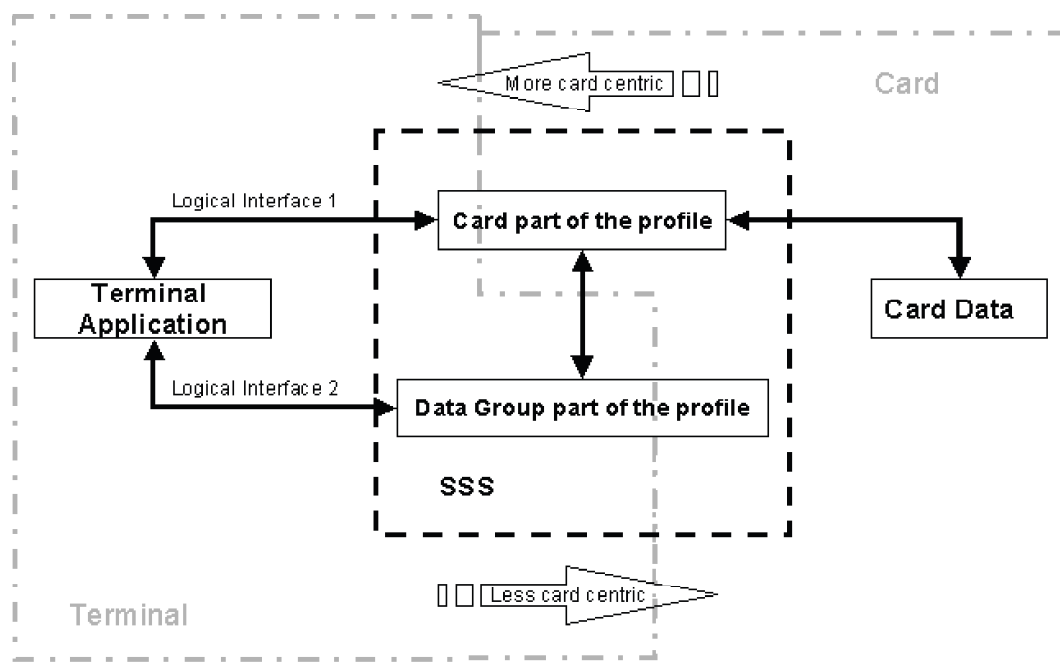


Bild 9 — Abhängigkeiten zwischen logischen Schnittstellen, dem SSS, der Karte und dem Terminal

7.2 Das Sicherheitsuntersystem (en: Security SubSystem, SSS)

Das Sicherheitsuntersystem (SSS) umfasst die sicheren Teile der Terminalanwendung und die sicheren Teile der Anwendung der maschinenlesbaren Karte. Es schließt die Funktionalität des Sicherheitsmanagementsystems der Karte und des Sicherheitsmanagementsystems der Datengruppen ein.

Das SSS ist so umzusetzen, dass die Funktionalität des Sicherheitsmanagements der Karte auf eine für die Fähigkeit der maschinenlesbaren Karte geeignete Weise dynamisch zwischen dem Terminal und der Karte aufgeteilt wird.

Jedes Ändern von Daten, bei der die Karte und das Terminal betroffen sind, muss ein SSS einbeziehen, das in der Lage ist, um:

- als unveränderbares sicheres Repositorium für die Anwendungs-, Produkt- und Transaktionsnummern-erzeugung zu dienen;
- Transaktionsprotokolle mit sicherer Nachrichtenübertragung (en: secure messaging) bereitzustellen;
- Datengruppen auf Authentizität zu prüfen;
- sicheren Zugriff auf Datengruppen zu bieten;
- sämtliche Schlüssel geheim zu halten;
- veränderte Datengruppeninhalte zu siegeln;
- eine sichere Speicherung und eine sichere Profilverwaltung zu bieten;
- eine sichere Nachrichtenübertragung zwischen dem Sicherheitsuntersystem und dem IFM-Manager zur Übernahme und Bestätigung von Aktualisierungen der Inhalte des Sicherheitsuntersystems umzusetzen.

Die erforderlichen Eigenschaften des Sicherheitsuntersystems für eine sichere Anwendung und einen sicheren Datenspeicher sind dergestalt, dass es die kryptografischen Schlüssel und Schema-Parameter speichern kann. Die sichere Anwendung muss Gegenmaßnahmen bieten, um zu verhindern, dass:

- Geheimschlüssel außerhalb der Anwendung preisgegeben werden;
- Sicherheitsfunktionen modifiziert werden;
- Schema-Parameter ohne Berechtigung verändert werden;
- Sequenzzähler zurückgesetzt werden.

Die Zulassung des SSS sollte nach formalen Sicherheitsbewertungskriterien erfolgen.

ANMERKUNG Es wird davon ausgegangen, dass diese Anforderungen durch die Verwendung eines sicheren Gerätes erfüllt werden, zum Beispiel in Form eines Chips auf der maschinenlesbaren Karte und einer Kartenanwendung, die leicht an jedes Kartenterminal angepasst werden können.

7.3 Logische Schnittstelle 1: Die Kartendatenschnittstelle

7.3.1 Allgemeines

Diese Schnittstelle wird durch einen Satz von allgemeinen Funktionsaufrufen zwischen der Terminalanwendung und der maschinenlesbaren Karte beschrieben. Der Umfang und die detaillierte Ausführung jeder Funktion sind durch die Sicherheitsanforderungen und das an der Schnittstelle präsentierte Profil der Kartenplattform festgelegt.

Die von dieser Schnittstelle verwendeten Funktionsaufrufe bestehen aus einer als Skript abgefassten Folge von plattformspezifischen Befehlen, die für eine bestimmte Kombination von Terminalanwendung und Kartenplattform festgelegt sind. Diese Unterschiede sind im entsprechenden Kartenprofil [en: Card Profile, CP(n)] quantifiziert, das im Karten-Sicherheitsmanagementsystem des Sicherheitsuntersystems gespeichert ist. Die Schnittstelle ist in Bild 10 dargestellt.

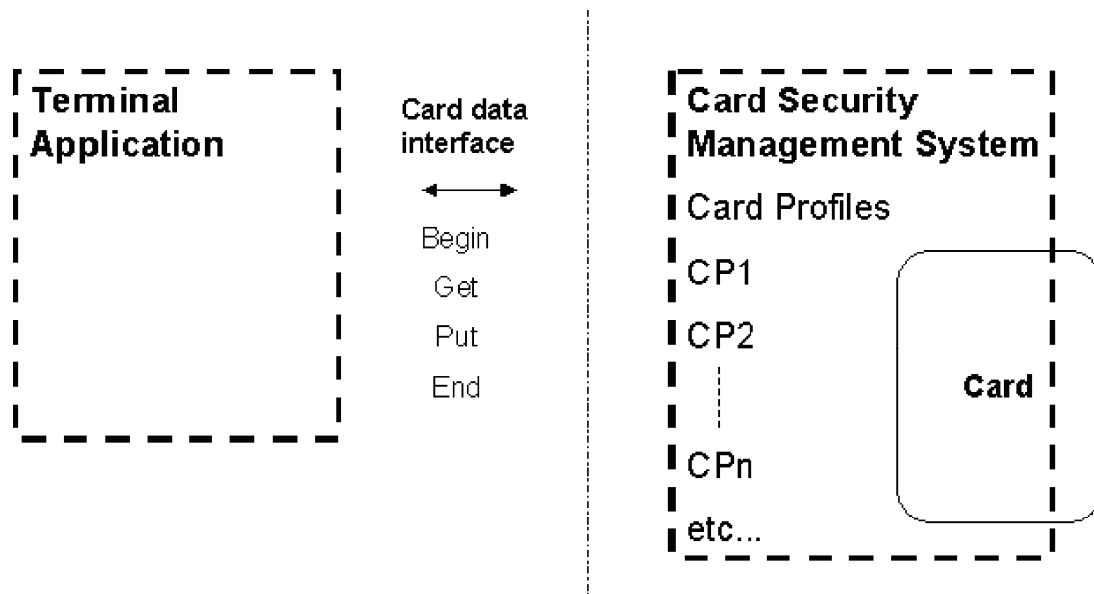


Bild 10 — Logische Schnittstelle 1: Kartendatenschnittstelle

7.3.2 Überblick über die Funktionen der Kartendatenschnittstelle

Jede Funktion muss durch eine Folge von Befehlen umgesetzt werden, die, in Abhängigkeit von der Kartentechnologie, vom Terminal an die Karte gesendet werden und bei Ausführung die in Tabelle 1 beschriebenen übergeordneten Funktionen durchführen.

Tabelle 1 — Funktionen der Kartendatenschnittstelle

Abstrakter Anwendungsbefehl ²⁾	Beschreibung
Begin	Selektion des Kartenprofils, Ausführen des Profils, Anwendung von Sicherheitsoperation (Authentifizierung, Diversifizierung, RND-Erzeugung, Architektur der Nachrichtenübermittlung ...) (d. h. eröffnet Kartensitzung)
Get	Sofern zulässig, Authentifizieren und Extrahieren der Nachricht, anschließend Übertragen von Clear-Daten an die Terminalanwendung
Put	Sofern zulässig, Erzeugen der Nachricht auf der Karte aus den Clear-Daten
End	Beenden des Anti-Tearing-Managements, Zurücksetzen aller Sicherheitszustände, Deaktivieren des Kartenprofils, z. B. durch Schließen der Kartensitzung

7.4 Logische Schnittstelle 2: Die Datengruppenschnittstelle

7.4.1 Allgemeines

Diese Schnittstelle wird durch einen Satz von allgemeinen Funktionsaufrufen zwischen der Terminalanwendung und der zu verarbeitenden Datengruppe beschrieben. Der Umfang und die detaillierte Ausführung jeder Funktion sind durch die Sicherheitsanforderungen und das Profil der zu verarbeitenden Datengruppe festgelegt.

2) Die Befehle umfassen sowohl die Kartenplattform als auch das Sicherheitsuntersystem.

Die von dieser Schnittstelle verwendeten Funktionsaufrufe bestehen aus einer als Skript abgefassten Folge von plattformspezifischen Befehlen, die für eine bestimmte Kombination von Terminalanwendung und Datengruppe festgelegt sind. Diese Unterschiede sind im entsprechenden Datengruppenprofil [en: Data Group Profile, DGP (n)] quantifiziert, das im Datengruppen-Sicherheitsmanagementsystem des Sicherheitsunter-systems gespeichert ist. Die Schnittstelle ist in Bild 11 dargestellt.

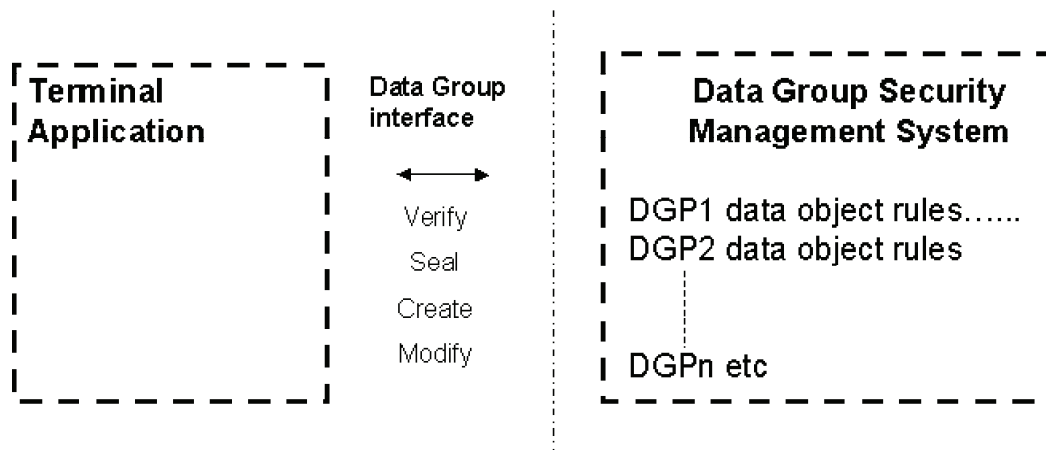


Bild 11 — Logische Schnittstelle 2: Datengruppenschnittstelle

7.4.2 Übersicht über die Funktionen der Datengruppenschnittstellen

Jede Funktion muss durch eine Folge von Befehlen umgesetzt werden, die, in Abhängigkeit von der Kartentechnologie, vom Terminal an das Sicherheitsuntersystem und/oder an die Karte gesendet werden und bei Ausführung die in Tabelle 2 beschriebenen übergeordneten Funktionen durchführen.

Tabelle 2 — Funktionen der Datengruppenschnittstellen

Abstrakter Anwendungsbefehl	Beschreibung
Verify	Sofern zulässig, Selektion der Schlüssel, Verifizieren des Siegels (Entschlüsseln des Datensatzes), Anwenden von Datenobjektregeln, ... Melden
Seal	Sofern zulässig, (Entschlüsseln des Datensatzes) Selektion der Schlüssel, Anwenden von Datenobjektregeln, Erzeugen des Siegels, ... Zurücksenden des Siegels
Create	Sofern zulässig, Erzeugen der Datengruppe, Hinzufügen eindeutiger Nummerierung, Anwenden von Datenobjektregeln
Modify	Sofern zulässig, Modifizieren des Inhalts, Hinzufügen eindeutiger Nummerierung, Anwenden von Datenobjektregeln

7.5 Anwendungsbezogene Befehle

7.5.1 Allgemeines

Die Anwendung muss für viele unterschiedliche Kartentypen gelten. Der Hauptunterschied zwischen diesen Typen besteht in der Fähigkeit der Technologie und in den Merkmalen des Zugriffs auf die Anwendung. Beispiele für Kartentypen reichen von kleinen Speicherkarten bis zu hoch entwickelten Mikrokontrollerkarten.

Mikrokontrollerkarten nutzen als Grundlage viele auf ISO/IEC 7816 basierende allgemeine Normen und Spezifikationen und bieten einen umfangreichen Satz von interoperablen Befehlen für das Lesen, Aktualisieren und Verwalten von Datenelementen und Datenstrukturen. Mechanismen für die Selektion von Anwendungen und Befehle für sicherheitsbezogene Funktionalität werden von diesen allgemeinen Normen und Spezifikationen ebenfalls bereitgestellt.

Auf der anderen Seite bietet eine kleine Speicherkarte im Allgemeinen nur untergeordnete Lese- und Schreibbefehle. Eine anwendungsbezogene Interpretation des Speicherinhalts muss außerhalb der Karte durchgeführt werden. Sicherheitsbezogene Funktionalität kann normalerweise nicht von der Karte bereitgestellt werden. In diesem Fall muss der überwiegende Teil der Sicherheitsanwendung im Terminal oder im Hintergrundsystem (en: back office) durchgeführt werden.

Diese Europäische Norm beschreibt nicht die Einzelheiten eines jeden Befehls, der mit maschinenlesbaren Karten verwendbar ist, sondern zeigt die höheren abstrakten Befehle.

Bei der Umsetzung abstrakter Befehle, die die Kartendatenschnittstelle betreffen, sind möglichst Befehlsfolgen zu verwenden, die in bestehenden ISO/IEC-Normen behandelt sind.

7.5.2 Abstrakte Befehle und Nutzungsfälle

Tabelle 3 identifiziert anwendungsbezogene Nutzungsfälle, die auf einer abstrakten Ebene in der maschinenlesbaren Karte vorhanden sein müssen. Einige dieser Nutzungsfälle dürfen aus mehreren Kartenbefehlen zusammengesetzt sein; einige dürfen mit einem einzigen Befehl durchgeführt werden oder dürfen auch ein anwendungsspezifisches Kartenkommando darstellen. Die aufgeführten Nutzungsfälle gelten nicht notwendigerweise für alle Arten von maschinenlesbaren Karten, die eine Instanz der Anwendung enthalten. Es darf auch Karten geben, die nur eine Teilmenge dieser Nutzungsfälle erfüllen.

Tabelle 3 — Aktivitäten und Nutzungsfälle der Anwendung

Aktivitäten	Beschreibung des Nutzungsfalls	Logische Schnittstelle 1/2	Abstrakte Anwendungs-befehle	Beispiele für genormte Befehle für Mikrokontroller	Beispiele für proprietäre Befehle für einfache Speicherkarten
Verwalten	Allgemeine Aktivität zum Ändern des Inhalts der Karte:	1	GET PUT VERIFY SEAL CREATE MODIFY	Create Application Create/Delete EF/DF Append/Update Record Read/Update Binary Get Data/Put Data Activate/Deactivate/Terminate	Write Sector Read Sector Authenticate (part) Present password None
Autorisieren	Gewährt Recht für Durchführung weiterer Aktivitäten:	1,2	VERIFY	Verify Card Holder External/Mutual Authentication Verify Signatures Secure Messaging (Trusted Channel), Derived Session Keys	Read Sector Authenticate (part) Present password None
Aktivieren	Befehl zum Aktivieren einer Instanz der Anwendung oder Datengruppe	1	PUT	Activate Application Activate File	Write Sector Authenticate (part) Present password None
Validieren	Überprüfen oder Stornieren eines Fahrscheines, Kundenvertrages	1	GET PUT	Read/Update Record Read/Update Binary Get Data/Put Data	Write Sector Read Sector Authenticate (part) Present password None
Erzeugen	Erzeugen einer neuen Instanz der Anwendung, Datengruppen, Datenstrukturen, Datenelemente	1,2	CREATE SEAL	Create Application Create EF/DF Append/Update Record Write Binary	Write Sector Authenticate (part) Present password None

Tabelle 3 (fortgesetzt)

Aktivitäten	Beschreibung des Nutzungsfalls	Logische Schnittstelle 1/2	Abstrakte Anwendungs-befehle	Beispiele für genormte Befehle für Mikrokontroller	Beispiele für proprietäre Befehle für einfache Speicherkarten
Löschen	Löschen einer Anwendung der Anwendung, Datengruppen, Datenstrukturen oder Datenelemente	1,2	MODIFY PUT	Delete Application Delete File Update record Write Binary	Write Sector Authenticate (part) Present password None
Erneuern	Eine Karte oder ein Produkt, bei der/dem der Kundenvertrag endet, wird erneuert	1,2	MODIFY PUT	Update Record Update Binary Create Application Create EF/DF Append/Update Record Write Binary	Write Sector Authenticate (part) Present password None
Ersetzen	Eine verloren gegangene Karte wird ersetzt	1,2	CREATE PUT	Update Record Update Binary Create Application Create EF/DF Append/Update Record Write Binary	Write Sector Authenticate (part) Present password None
Transaktion durchführen	Allgemeine Aktivitäten mit den Kartendaten, die nicht durch die übrigen Nutzungsfälle abgedeckt sind	1	PUT GET	Read/Update Record Read/Update Binary Get Data/Put Data	Write Sector Read Sector Authenticate (part) Present password None
Abbrechen	Stornieren eines Fahrscheines	1	MODIFY PUT	Read/Update Record Read/Update Binary Get Data/Put Data	Write Sector Authenticate (part) Present password None
Wiedereinsetzen	Ersetzen einer Datengruppe	1,2	CREATE MODIFY PUT	Update Record Update Binary Put Data	Write Sector Authenticate (part) Present password None

Tabelle 3 (fortgesetzt)

Aktivitäten	Beschreibung des Nutzungsfalls	Logische Schnittstelle 1/2	Abstrakte Anwendungs-befehle	Beispiele für genormte Befehle für Mikrokontroller	Beispiele für proprietäre Befehle für einfache Speicherkarten
Modifizieren	Aktivität zum Ändern des Inhalts eines bestehenden Daten-elementes	2	MODIFY PUT	Update Record Update Binary Put Data	Write Sector Authenticate (part) Present password None
Fahrschein erstellen	Aktivieren eines Fahrscheines zu Beginn einer Reise	1	MODIFY PUT	Read/Update Record Read/Update Binary Get Data/Put Data	Read Sector Write Sector Authenticate (part) Present password None
Beenden	Aktivität zum Beenden der Nutzung einer Anwendung oder Datengruppe ohne Löschen	1	MODIFY PUT	Update Record Update Binary Deactivate Put Data	Write Sector Authenticate (part) Present password None
Überprüfen	Aktivität zum Hinzufügen oder Ändern von Datenelementen bei Überprüfung	1	GET PUT	Read/Update Record Read/Update Binary Get Data/Put Data	Read Sector Write Sector Authenticate (part) Present password None
Produkt entnehmen	Auslesen des Kundenvertrages, Auslesen des Fahrscheines	1	GET	Read Record Read Binary Get Data	Read Sector Authenticate (part) Present password None
Beleg erstellen	Erhalten einer Bestätigung für eine Transaktion	1	GET	Read Record Read Binary Get Data	Read Sector Authenticate (part) Present password None

7.5.3 Eine repräsentative Kartentransaktion

Eine repräsentative Kartentransaktion muss den Beginn und das Ende einer Kartensitzung sowie die Umsetzung eines oder mehrerer dazwischen liegender Nutzungsfälle umfassen. Die Terminalanwendung muss die abstrakten Anwendungsbefehle unter Verwendung von Skripten mit plattformspezifischen Befehlen ausführen, die von der Kartenplattform und Nutzungsfällen abhängen.

In Bild 12 ist eine derartige Sitzung für repräsentative Mikroprozessor- und Speicherkarten dargestellt. Sitzungen beginnen und enden mit den Befehlen BEGIN bzw. END.

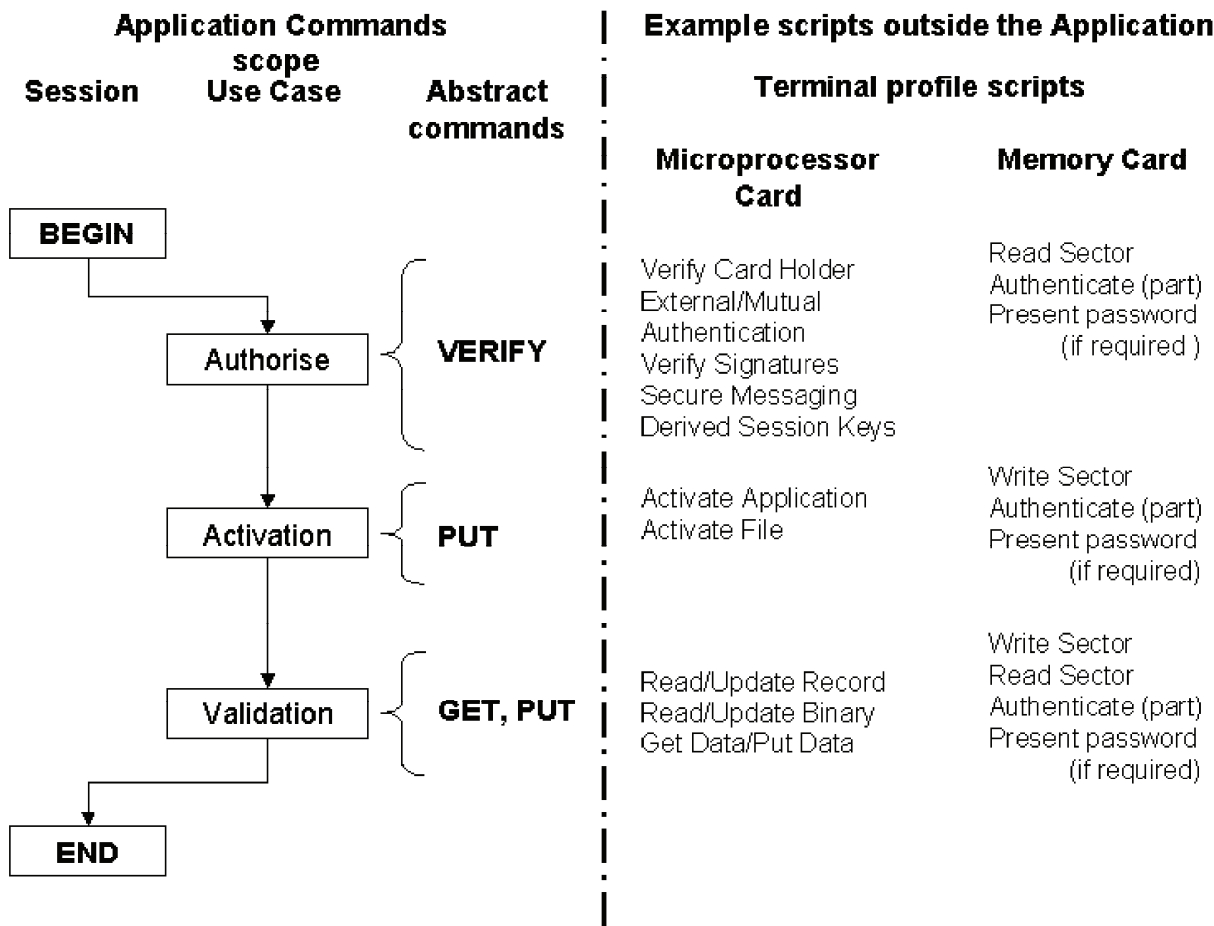


Bild 12 — Repräsentative Abfolge von Anwendungsbefehlen

7.5.4 Verhältnis zu den logischen Schnittstellen

Das Zustandsdiagramm in Bild 13 zeigt die Zustände 3, 4 und 5 der Terminalanwendung, die durch die Schnittstelle der abstrakten Befehle im normativen Teil dieser Europäischen Norm abgedeckt sind. Ausführlichere Angaben zu den Zuständen 1 und 2 sind im informativen Anhang G enthalten.

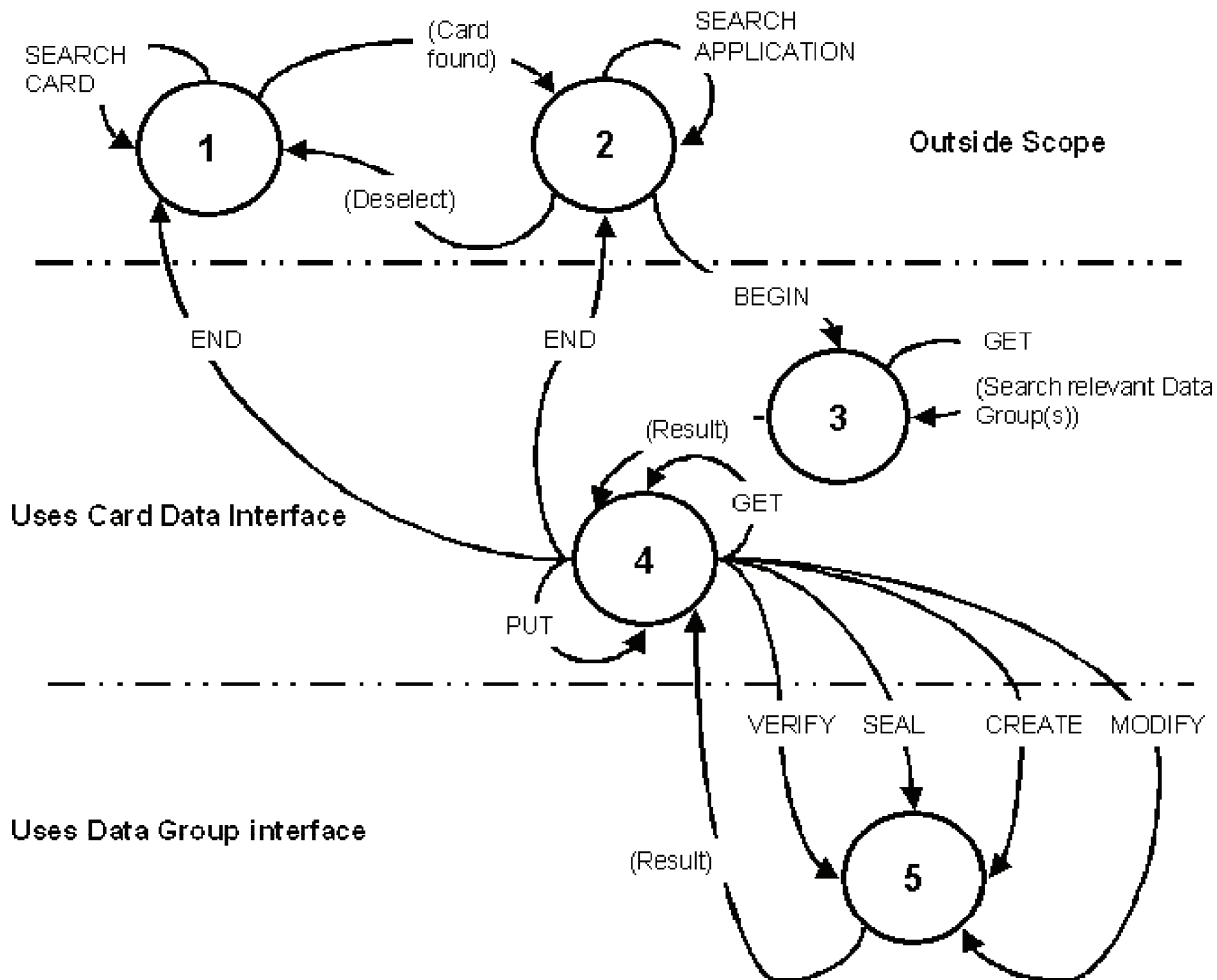


Bild 13 — Anwendungszustände

8 Anwendungssicherheit

8.1 Einführung in die Sicherheitsarchitektur

Dieser Abschnitt behandelt die Schnittstelle zwischen Karte und Kartenterminal und beschreibt eine Sicherheitsarchitektur, die es ermöglicht, Anwendungsprodukte auf Karten zu schreiben, die von reinem Speicher bis zu High-End-Mikroprozessoren reichen. In Verbindung mit dem Sicherheitsundersystem bildet sie einen Teilbereich einer End-to-End-Sicherheitsarchitektur für die Anwendung.

Die Vereinbarungen zwischen den verschiedenen Geschäftspartnern beeinflussen die für eine maschinenlesbare Karte erforderlichen Sicherheitsmerkmale. Es ist zu beachten, dass die Sicherheitsmerkmale die Anforderungen des Terminals, des Sicherheitsundersystems und möglicherweise des Hintergrundsystems bestimmen. Folglich ist es unmöglich, ein einziges Sicherheitssystem für eine Anwendung festzulegen, da unterschiedliche Schemata unterschiedliche Kartentechnologien mit unterschiedlichen Umsetzungen verwenden könnten. Dieser Abschnitt und die dazugehörigen Unterabschnitte beschreiben Sicherheitsmerkmale, die mit verschiedenen maschinenlesbaren Karten verwendet werden dürfen.

Die hier dargelegte Architektur trennt die logischen Sicherheitsanforderungen der Anwendungsprodukte von denen der maschinenlesbaren Karte und ermöglicht eine gegenseitige Festlegung zwischen Terminalanwendung und Karte für die Zugriffsrechte auf Datenstrukturen innerhalb der Datengruppen. Die Rolle des Terminals³⁾ und die Fähigkeit der Karte werden verwendet, um die Aufteilung der Funktionalität des Sicherheitsuntersystems zwischen Terminal und maschinenlesbarer Karte mit Hilfe einer Profilaushandlung festzulegen.

Die in Abschnitt 7 beschriebenen logischen Schnittstellen 1 und 2 spiegeln diese Funktionalitätsaufteilung wider, sodass der Zugriff auf die Datengruppen durch die Attribute der Kartenplattform (Zugangsschlüssel, gegenseitige Authentisierung usw.) gesteuert wird.

8.2 Anforderungen und Herangehensweisen an die Sicherheitsarchitektur

8.2.1 Allgemeines

Die Sicherheitsarchitektur der Anwendung muss Folgendes bieten:

- Vertraulichkeit;
- Integrität;
- Authentizität;
- Nachweisbarkeit;
- Anti-Cloning;
- Auditierbarkeit.

In den folgenden Unterabschnitten ist nacheinander jede Anforderung im Einzelnen beschrieben, von der eine Auswahl für eine übliche Kombination aus SSS und maschinenlesbarer Karte getroffen werden kann.

ANMERKUNG Viele Sicherheitsmerkmale von Mikroprozessorkarten sind ausführlich in ISO/IEC 7816-4 und ISO/IEC 7816-9 beschrieben.

8.2.2 Vertraulichkeit

Vertraulichkeit ist für ein System wichtig, um sicherzustellen, dass nur eine autorisierte Entität auf vertrauliche Informationen zugreifen kann. Dies kann durch unterschiedliche Mittel erreicht werden, von denen viele in bestehenden Normen zu maschinenlesbaren Karten ausführlich definiert sind; zu Referenzzwecken sind einige Verfahren im Folgenden kurz angegeben:

- Beschränkung des Zugriffs auf Datenelemente nur auf die Parteien, die eine entsprechende Erlaubnis besitzen; dieser Vorgang darf durch Nutzung eines Passwortes, gegenseitige Authentisierung oder andere Verfahren erreicht werden;
- Verschlüsselung sensibler Datenelemente, um Geschäftsgeheimnisse zu wahren oder, im Fall von persönlichen Daten, diese Daten zu schützen;
- Klassifizierung von Datenelementen als „nur lesbar“ für die karteninterne Anwendung. In diesem Fall dürfen diese Daten Voraussetzung für die erfolgreiche Ausführung einer Funktion sein.

3) Entwerter, Fahrkartenautomat, Guthabenanzeige usw.

8.2.3 Integrität

Integrität kann durch viele Verfahren erreicht werden, von denen einige im Folgenden kurz angegeben sind:

- die Anwendung einer Luhn-Prüfziffer ist ein grundlegendes Verfahren, das bei einigen ISO-Nummerierungs-Schemata angewendet wird, um eine Fehlübertragung von Zahlen festzustellen;
- die Verwendung einer Prüfsumme (ISO/IEC 14443). Dieses Verfahren wird angewendet, um Fehler auf Grund von Datenkorruption festzustellen. Es bietet jedoch keine Sicherheit in Bezug auf Authentizität.

Die kontaktlose Schnittstelle (beschrieben in ISO/IEC 14443) ist auf Grund ihrer Beschaffenheit anfällig für Unterbrechungen während der Nutzung, entweder durch benachbarte intermittierende Interferenzen oder, was häufiger der Fall ist, durch Entfernen einer maschinenlesbaren Karte aus dem Kartenterminal während einer Transaktion. Anti-Tearing-Verfahren sind anzuwenden, um dieses Problem zu vermeiden. In diesem Fall stellt entweder die Hardware in der Karte oder eine äquivalente Software in der Karte und im Terminal sicher, dass gültige Kartendaten erhalten bleiben, auch wenn die Karte während der Modifikation von Datenelementen ihre Stromversorgung verliert.

8.2.4 Authentizität

Zur Feststellung der Authentizität von Datenelementen dürfen unter anderem folgende Verfahren angewendet werden:

- das Siegeln einer Datengruppe stellt sicher, dass die Inhalte der Datengruppe nicht verändert wurden. Die Güte des Siegels hängt von den Algorithmen und Schlüsseln ab, die bei der Erstellung verwendet wurden;
- Anwendung von Nachrichtenauthentisierungs-codes (en: Message Authentication Codes, MAC) bei übertragenen Daten. Dies erhöht das Vertrauen, dass Meldungen weder unbeabsichtigt noch beabsichtigt verändert wurden.

Die Karte und das Terminal dürfen sich gegenseitig authentisieren. Dies darf auf vielerlei Arten erfolgen, zum Beispiel durch:

a) Mikroprozessorkarten:

- 1) Algorithmen zur internen, externen oder gegenseitigen Authentisierung, Authentisierung ohne Informationspreisgabe (en: zero knowledge proofs);

b) Speicherkarten:

- 1) dürfen proprietäre Algorithmen zur Authentisierung der gesamten Karte oder auf einer Sektor-für-Sektor-Basis anwenden.

8.2.5 Nachweisbarkeit (en: non-repudiation)

In jedem offenen System ist die Feststellung wesentlich, dass Transaktionen korrekt gemeldet und nicht entfernt oder ersetzt wurden. Verfahren für die Nachweisbarkeit von Daten, die in Verbindung mit Siegeln angewendet werden, dürfen Folgendes beinhalten:

- eindeutige Nummerierung von Produkt- und Anwendungsinstanzen in der gesamten Anwendung, um Möglichkeiten bereitstellen zu können, kopierte oder fehlende Instanzen von Datengruppen festzustellen;
- Verwendung von Sequenzzählern in Produkten, deren Dateninhalte sich im Laufe der Zeit ändern, um eine Verfolgung im Hinblick auf korrekte Durchführung zu ermöglichen, zum Beispiel Erhöhung der Anzahl von Fahrten auf einem für mehrere Fahrten geltenden Produkt außerhalb der Folge.

8.2.6 Anti-Cloning

Einer der simpelsten Kartenbetrugsarten ist das Kopieren der gesamten Karte auf eine leere Karte (Klonen). Maßnahmen zur Verhinderung von erfolgreichem Klonen dürfen Folgendes umfassen:

- Diversifikation von Kartenzugriffs- und/oder Authentisierungsschlüsseln. In diesem Fall besitzen keine zwei Karten dieselben Zugriffsschlüssel, wodurch das direkte Kopieren von Daten von einer Karte auf eine andere verhindert wird. Bei der Diversifikation sollten, sofern möglich, eindeutige Daten verwendet werden, die dauerhaft im Kartenspeicher gehalten werden, oder Daten, die bekanntermaßen eindeutig sind und in einen einmalig programmierbaren Speicher der Karte geschrieben werden;
- Diversifikation von Datengruppensiegeln. Durch die Sicherstellung, dass die Datengruppensiegel durch Daten von der physikalischen Kartenplattform diversifiziert sind, wird das Siegel wirksam an diese Plattform gebunden. Wenn daher die entsprechende Datengruppe auf eine andere Kartenplattform kopiert wird, versagt die Siegelverifizierung;
- die Ausgabe von „anwendungsbereiten“ (en: „application-ready“), jedoch unpersonalisierten Karten, sollte auf diejenigen beschränkt werden, die diese Karten tatsächlich benötigen. Außerdem sollte über jede defekte maschinenlesbare Karte Rechenschaft abgelegt werden.

Das Klonen von Nachrichten, besonders das Abspielen von Nachrichten zwischen Karte und Terminal zu störenden oder betrügerischen Zwecken, kann durch die Anwendung von Verfahren, die als sichere Nachrichtenübertragung bekannt sind, verhindert werden. Hierbei wird eine sichere Sitzung zwischen der Karte und dem Terminal aufgebaut, sodass die Kommunikation in jede Richtung eine für diese Sitzung eindeutige Nachrichtenauthentikation trägt. Die sichere Nachrichtenübertragung darf in vielerlei Weise umgesetzt werden. Üblicherweise wird jedoch bei Nutzung eines Schlüssels jeder Nachricht ein MAC angehängt, der aus dem Prozess der gegenseitigen Authentisierung abgeleitet wurde. Andere Verfahren umfassen die Verschlüsselung/Entschlüsselung von Daten, die über die Kommunikationsschnittstelle gesendet werden.

8.2.7 Auditierbarkeit

Auditierbarkeit innerhalb einer Anwendungsumgebung darf durch die Anwendung der zuvor festgelegten Anforderungen erreicht werden und wo anwendbar das Führen von Protokollen zu Transaktionen und Ereignissen, die in einer Anwendungsumgebung erfolgen und auftreten. Dabei erfolgt eine eindeutige Nummerierung von:

- Anwendungen;
- Produkten;
- Transaktionen;
- Listen.

Hierfür ist sowohl eine Registrierungsstelle als auch eine anschließende Verwaltung erforderlich, was in den Bereich des IFM fällt und in die entsprechenden Teile der an anderer Stelle definierten IFM-Dokumentation aufzunehmen ist. Die Nummerierung von Produkten, die durch ein Verkaufsterminal im Offlinemodus erzeugt werden, muss sicher verwaltet und einem Teil der SSS-Funktionalität anvertraut werden.

8.3 Anforderung zur Unterstützung einer Reihe von Kartenplattformen

Die Sicherheitsarchitektur muss ausreichend flexibel sein, um das Hinzufügen von Anwendungsprodukten auf einer Vielzahl von maschinenlesbaren Karten zu unterstützen. Nachfolgend sind einige typische Beispiele aufgeführt:

a) kleine Speicherkarte/kontaktloser Fahrschein:

- 1) kein integrierter Sicherheitsschutz für Zugriffsüberwachung
- 2) keine Unterstützung von ISO/IEC 14443-4;
- 3) Unterstützung einer fest eingebauten Seriennummer;

b) gesicherte Speicherkarte:

- 1) Zugriffsüberwachung durch proprietäre Sicherheitsmethoden unter Verwendung von Short-Keys;
- 2) keine Unterstützung von ISO/IEC 14443-4;
- 3) Unterstützung einer fest eingebauten Seriennummer;

c) Mikroprozessorkarten:

- 1) Zugriffsüberwachung durch gegenseitige Authentisierung;
- 2) dürfen ISO/IEC 14443-4 unterstützen;
- 3) unterstützen üblicherweise öffentliche Sicherheitsalgorithmen (d. h. DES, 3DES, RSA usw.);
- 4) dürfen sichere Nachrichtenübertragung (Secure Messaging) unterstützen;
- 5) dürfen Zugriffsüberwachung auf Datenelementebene unterstützen.

Die im Sicherheitsmanagementsystem der Karte installierten Kartenprofile erlauben es der Terminalanwendung, ihre plattformspezifischen Kartentreiber so anzupassen, dass diese den Sicherheitsanforderungen der verwendeten Plattform entsprechen. Um Fälschungen entgegenzuwirken sind einige der Funktionen in das SSS einzubetten.

8.4 Anforderung der Unterstützung einer Reihe von Siegelungsverfahren für Datengruppen

Alle Datengruppen dürfen ein Siegel enthalten, das, durch anerkannte Verschlüsselungsverfahren erzeugt, die Authentizität des Datensatzes garantiert, aus dem es gebildet wurde. Diese Garantie gilt für die Datengruppe unabhängig von der Kartenplattform, auf der die Datengruppe vorhanden ist; sie darf jedoch mit dieser verknüpft sein. Siegel schützen alle Datenobjekte in der Datengruppe, einschließlich Datenobjekte, die die Datenelemente „Instanzbezeichner“ und „Kennung“ enthalten. Selbst wenn die von dem Kartenmedium transportierten Strukturen gesiegelt sind, erfolgt die Überprüfung der Gültigkeit der Siegel entsprechend dem festgelegten Sicherheitsschema im Netzwerk und darf nicht für alle Geräte verbindlich sein. Es gibt eine Vielzahl von möglichen Siegeln, zum Beispiel:

a) kein Siegel vorhanden:

- 1) weder die Datenintegrität noch die Berechtigung werden nachgewiesen;

b) CRC:

- 1) die Datenintegrität ist verifizierbar;
- 2) die Authentizität kann nicht verifiziert werden;

c) MAC oder digitale Unterschrift:

- 1) die Datenintegrität ist verifizierbar;
- 2) die Authentizität kann verifiziert werden;

d) MAC oder digitale Unterschrift, diversifiziert nach Kartenplattform

- 1) die Datenintegrität ist verifizierbar;
- 2) die Authentizität kann verifiziert werden;
- 3) Klonen wird wirksam verhindert.

8.5 Eindeutige Nummerierung

Eine eindeutige Nummerierung ist anzuwenden, um eine End-to-End-Sicherheit, die Verwaltung von Vorgangslisten und Hotlists und die Bereitstellung von Prüfpfaden für sämtliche Anwendungsvorgänge zu erleichtern. Jede Instanz eines jeden Produktes und die erzeugten Transaktionen müssen eindeutig in einer Anwendungsinstanz identifiziert werden. Das hierbei anzuwendende Verfahren ist ausführlich im entsprechenden IFM-Dokument beschrieben.

Um diese Anforderung zu erfüllen, muss jedes Produkt und jede Anwendung die Datenstruktur „Instanzbezeichner“ enthalten. Diese Struktur ist so codiert, dass sie eine individuelle Instanz eines Produktes oder einer Anwendung in einer Vielzahl von Anwendungsumgebungen eindeutig bezeichnet; sie ist von grundlegender Bedeutung für die Bereitstellung eines eindeutigen Prüfpfades im Produkt- und Anwendungsverkauf und in der Nutzung.

Auf Grund seiner bedeutenden Rolle bei der Umsetzung und Verwaltung von Anwendungsumgebungen muss der Instanzbezeichner einen Teil der Produkt- und Anwendungsumgebung bilden und durch das Siegel geschützt werden.

Die Anwendung kann unnötiges Duplizieren von Produkt-, Serien- und Iterationsnummern an anderer Stelle in der Datengruppe durch Verwendung der Datenstruktur Instanzbezeichner vermeiden.

ANMERKUNG Die Festlegung der Nummerierung von Inhabern, Transaktionsdaten und der eindeutigen Bezeichnung des Sicherheitsuntersystems ist Aufgabe des vollständig interoperablen Fahrgeldmanagementsystems (IFM), das den End-to-End-Betrieb einschließlich der maschinenlesbaren Karte definiert und von dem die Anwendung einen Teil bildet. Weitere relevante Normen behandeln die Festlegung der Nummerierung.

8.6 Sicherheitsbezogene Karteninformationen

8.6.1 Allgemeines

Die Anwendung besteht aus einer Anzahl von Datengruppen, die jeweils aus unterschiedlichen Datenstrukturen und Datenobjekten bestehen, welche die anwendungsspezifischen Datenelemente enthalten. Der Zugriff auf die einzelnen Datenstrukturen/Datenelemente ist zu schützen. Die erforderlichen Zugriffsbedingungen für eine einzelne Datenstruktur/ein einzelnes Datenelement werden aus den zwischen den verschiedenen Parteien vereinbarten Geschäftsregeln abgeleitet.

Im einfachsten Fall sind die Zugriffsbedingungen dem Terminal und der maschinenlesbaren Karte implizit bekannt, und es sind keine zusätzlichen auf der Karte gespeicherten Informationen erforderlich.

Aus einem oder mehreren der folgenden Gründe dürfen im Allgemeinen einige Steuerungsinformationen auf der maschinenlesbaren Karte vorhanden sein:

- die Karte ist in der Lage, den Zugriff und die Funktionalität zu kontrollieren;
- die Geschäftsregeln dürfen sich während der Lebensdauer einer Karte ändern;
- Karte und Terminal benötigen ein flexibles Verfahren, um mit Karten arbeiten zu können, die unterschiedliche Schemata nutzen;
- Profile von Terminals müssen im Feld erweitert werden;
- das Sicherheitssystem nutzt ein sich weiterentwickelndes Schlüsselmanagement und sich ändernde Schlüsselversionen.

Die folgenden Unterabschnitte beschreiben ein flexibles Mittel für den Zugriff von Karten oder Terminals auf Steuerungsinformationen, die optional umgesetzt werden dürfen.

8.6.2 Kontrolldatenstruktur (en: Control Data Structure)

Die Kontrolldatenstruktur (CDS) ist eine optionale logische Datenstruktur, die in jeder Datengruppe vorhanden sein darf und die Sicherheits- und Managementinformationen zu jeder Datenstruktur oder jedem Datenelement in dieser Datengruppe enthält. Wenn in einer Datengruppe keine CDS vorhanden ist, sind die Zugriffsbedingungen den Terminals implizit bekannt. Eine in der Karte vorhandene CDS sollte Vorrang vor jeder Information des Terminalprofils haben.

Eine CDS ist üblicherweise eine Datenstruktur des Typs A, die mit der Schaffung der Datengruppe festgelegt und während der Lebensdauer der Datengruppe nicht verändert wird.

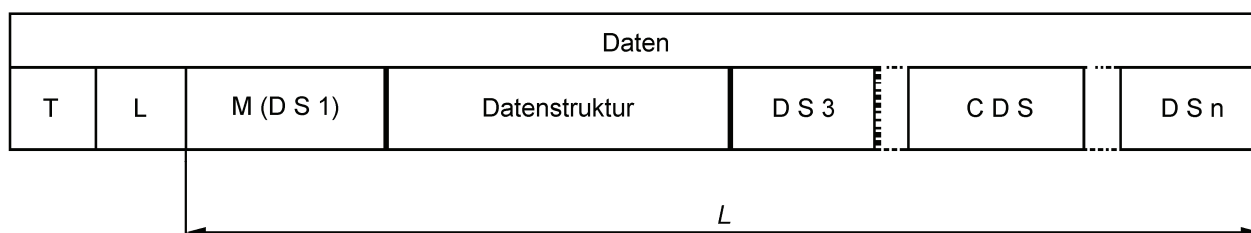


Bild 14 — Kontrolldatenstruktur von Datengruppen

8.6.3 Format der Kontrolldatenstruktur

Das Format einer CDS ist aus den in ISO/IEC 7816-4 definierten Zugriffsbedingungen abgeleitet. Eine verbindliche Zugriffsbedingung für eine Datenstruktur umfasst ein Datenobjekt zur Beschreibung der angewandten Funktionalität (ISO/IEC 7816-4 Zugriffsart-DO [en: Access Mode-DO, AM-BO] oder Zugriffsart-Byte [en: Access Mode Byte]) und ein Datenobjekt zur Beschreibung der Sicherheitsbedingung (ISO/IEC 7816-4 Zugriffsbedingung-DO [en: Security Condition-DO, SC-DO] oder Zugriffsbedingung-Byte [en: Security Condition Byte]). Es kann das kompakte oder das erweiterte Format gelten.

Ein Eintrag einer CDS ist ein Datenelement, bestehend aus:

- einem Verweis auf eine bestimmte Struktur/ein bestimmtes Element in der Datengruppe;
- der Zugriffsbedingung.

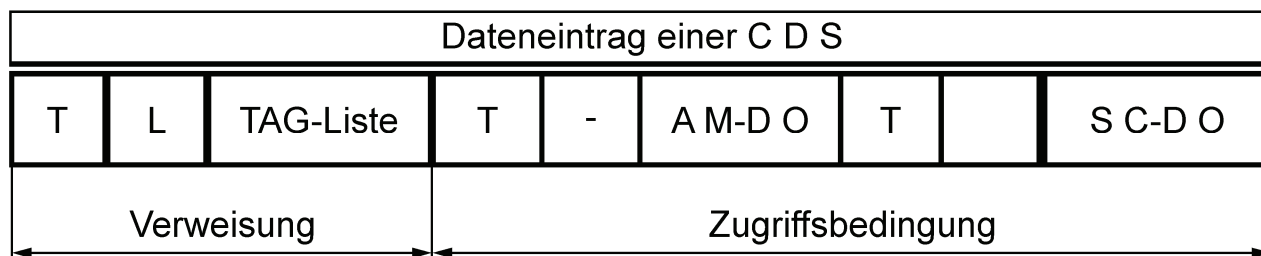


Bild 15 — Eintrag einer Kontrolldatenstruktur

Diese Beschreibung ist auch nützlich, um einen Eintrag in der CDS zu schützen.

ISO/IEC 7816-4 definiert die allgemeine Codierung eines AM-DO und eines SC-DO.

8.6.4 Erweiterung der Codierung von Zugriffsarten

Die Definition eines AM-DO kann auch verwendet werden, um die zulässige Funktionalität einer bestimmten Datenstruktur/eines bestimmten Datenelementes zu definieren, welche in Form eines Standardbefehls oder eines proprietären, auf die Instanz der Anwendung bezogenen Befehls erfolgen darf. Zum Beispiel sollte ein als Zähler verwendetes Datenelement nur durch den Befehl INCREASE/DECREASE geändert werden können. Andere Befehle sind unzulässig und für dieses Datenelement ungültig.

Die Definition des Zugriffsart-Byte in ISO/IEC 7816-4 kann entsprechend Tabelle 4 an die Erfordernisse der Anwendung angepasst werden:

Tabelle 4 — Festlegung Zugriffart-Byte

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
0	-	-	-	-	-	-	-	Befehle entsprechend der Definition in ISO/IEC 7816-4, Tabellen 16 bis 19
1	-	-	-	-	-	-	-	b7-b4 anwendungsspezifische Definitionen
-	1	-	-	-	-	-	-	Transportanwendungsspezifischer Befehl 1
-	-	1	-	-	-	-	-	Transportanwendungsspezifischer Befehl 2
-	-	-	1	-	-	-	-	Transportanwendungsspezifischer Befehl 3
-	-	-	-	1	-	-	-	Transportanwendungsspezifischer Befehl 4
-	-	-	-	-	1	-	-	Befehl entsprechend der Definition in ISO/IEC 7816-4, Tabellen 16 bis 19
-	-	-	-	-	-	1	-	Befehl entsprechend der Definition in ISO/IEC 7816-4, Tabellen 16 bis 19
-	-	-	-	-	-	-	1	Befehl entsprechend der Definition in ISO/IEC 7816-4, Tabellen 16 bis 19

Die Verwendung eines AM-DO mit APDU-Header-Definitionen (APDU – Application Protocol Data Unit) erweitert den Prozess für die Festlegung weiterer anwendungsspezifischer Befehle.

9 Profile

9.1 Allgemeines

Das Erstellen von Profilen ist ein Mittel, durch das Interoperabilität zwischen unterschiedlichen Kartenplattformen erreicht werden kann. Dieser Abschnitt beschreibt die unterschiedlichen Ansätze und Formate, die in der Anwendung zur Erstellung des Profils und deren Inhalte verwendet werden.

Je nach Fähigkeit der maschinenlesbaren Karte müssen das Terminal und dessen Sicherheitsuntersystem unterschiedliche Aufgaben erfüllen. Unterschiedliche Kartenplattformen erfordern unterschiedliche Verfahren, mit denen die Terminals das korrekte zu verwendende Profil erstellen können. Interoperabilität zwischen unterschiedlichen Instanzen der Anwendung darf durch Handelsvereinbarungen und den Austausch von Angaben zur Umsetzung erreicht werden.