

Identifikationskartensysteme
Branchenübergreifende elektronische Geldbörse
Teil 4: Datenelemente
Deutsche Fassung EN 1546-4:1999

DIN
EN 1546-4

ICS 35.240.15

Identification card systems – Inter-sector electronic purse – Part 4: Data objects;
German version EN 1546-4:1999

Systèmes de cartes d'identification – Porte-monnaie électronique intersectoriel –
Partie 4: Objets de données;
Version allemande EN 1546-4:1999

Die Europäische Norm EN 1546-4:1999 hat den Status einer Deutschen Norm.

Nationales Vorwort

Diese Norm wurde von der Arbeitsgruppe 10 „Branchenübergreifende elektronische Geldbörse“ des Technischen Komitees CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet. Sie wird von Deutschland geleitet.

Das nationale Spiegelgremium für diese Arbeitsgruppe war der NI-Arbeitskreis NI-17.10 „Branchenübergreifende elektronische Geldbörse“.

Fortsetzung 25 Seiten EN

Normenausschuss Informationstechnik (NI) im DIN Deutsches Institut für Normung e.V.

– Leerseite –

Deutsche Fassung

Identifikationskartensysteme
Branchenübergreifende elektronische Geldbörse
Teil 4: Datenelemente

Identification card systems – Inter-sector electronic purse –
Part 4: Data objects

Systèmes de cartes d'identification – Porte-monnaie élec-
tronique intersectoriel – Partie 4: Objets de données

Diese Europäische Norm wurde vom CEN am 29. Juli 1999 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 Zentralsekretariat 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 Zentralsekretariat mitgeteilt worden ist, hat den gleichen Status wie die offiziellen Fassungen.

CEN-Mitglieder sind die nationalen Normungsinstitute von Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, der Tschechischen Republik und dem Vereinigten Königreich.



EUROPÄISCHES KOMITEE FÜR NORMUNG
European Committee for Standardization
Comité Européen de Normalisation

Zentralsekretariat: rue de Stassart 36, B-1050 Brüssel

Inhalt

	Seite
Vorwort	2
1 Anwendungsbereich	2
2 Normative Verweisungen	2
3 Definitionen, Symbole und Abkürzungen	3
3.1 In EN 1546-1 definierte Benennungen	3
3.2 Symbole und Abkürzungen	3
4 Beschreibung des Verzeichnismechanismus	4
4.1 Einleitung	4
4.2 Angabe der Verwendung der TLV-Codierung	4
4.3 Struktur der Kopfliste	4
4.4 Codierung des Identifizierungskennzeichensfeldes	5
4.5 Codierung des Längensfeldes	8
4.6 Codierung der Datenelemente	8
4.7 Auslesen des Verzeichnisses einer IEP	8
4.8 Aufgliederung einer Kopfliste	9
4.9 Abbildung der Kopfliste	9
Anhang A (informativ) Beispiel für die Anwendung von Kopflisten	10
Anhang B (informativ) Beispiele für benutzerbestimmte Daten	25

Vorwort

Diese Europäische Norm wurde vom Technischen Komitee CEN/TC 224 „Maschinenlesbare Karten und zugehörige Geräteschnittstellen und Verfahren“ erarbeitet, dessen Sekretariat von AFNOR gehalten wird.

Diese Europäische Norm muss den Status einer nationalen Norm erhalten, entweder durch Veröffentlichung eines identischen Textes oder durch Anerkennung bis Februar 2000, und etwaige entgegenstehende nationale Normen müssen bis Februar 2000 zurückgezogen werden.

Entsprechend der CEN/CENELEC-Geschäftsordnung sind die nationalen Normungsinstitute der folgenden Länder gehalten, diese Europäische Norm zu übernehmen: Belgien, Dänemark, Deutschland, Finnland, Frankreich, Griechenland, Irland, Island, Italien, Luxemburg, Niederlande, Norwegen, Österreich, Portugal, Schweden, Schweiz, Spanien, die Tschechische Republik und das Vereinigte Königreich.

Diese Europäische Norm „*Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse*“ besteht aus folgenden Teilen:

- Teil 1: Definitionen, Begriffe und Strukturen
- Teil 2: Sicherheitsarchitektur
- Teil 3: Datenelemente und Datenaustausch
- Teil 4: Datenelemente

1 Anwendungsbereich

In diesem Teil von EN 1546 werden die Werte der erforderlichen Identifizierungskennzeichen festgelegt und die für ihre Benutzung notwendigen Verzeichnismechanismen beschrieben, um die Fähigkeit zur Zusammenarbeit zwischen IEP-Systemen zu erreichen, in denen Datenelemente unterschiedliche Längen besitzen und/oder sich die Anordnung der Datenelemente in Befehlen und Rückmeldungen von der in EN 1546-3 definierten unterscheidet. Die Mechanismen beruhen auf TLV-(Identifizierungskennzeichen-Länge-Wert-)Definitionen für jedes Datenelement.

Es werden auch zusätzlich zu den in EN 1546-3 definierten Identifizierungskennzeichen und Mechanismen solche für die Bearbeitung benutzerbestimmter Datenelemente definiert. Die angewendeten TLV-Mechanismen entsprechen ASN.1.

Im informativen Anhang wird der Gebrauch von Verzeichnissen beschrieben.

2 Normative Verweisungen

Diese Europäische Norm enthält durch datierte oder undatierte Verweisungen Festlegungen aus anderen Publikationen. Diese normativen Verweisungen sind an den jeweiligen Stellen im Text zitiert, und die Publikationen sind nachstehend aufgeführt. Bei datierten Verweisungen gehören spätere Änderungen oder Überarbeitungen dieser Publikationen nur zu dieser Europäischen Norm, falls sie durch Änderung oder Überarbeitung eingearbeitet sind. Bei undatierten Verweisungen gilt die letzte Ausgabe der in Bezug genommenen Publikation.

EN 1546-1, *Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 1: Definitionen, Begriffe und Strukturen*.

EN 1546-2, *Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 2: Sicherheitsarchitektur*.

EN 1546-3:1995, *Identifikationskartensysteme – Branchenübergreifende elektronische Geldbörse – Teil 3: Datenelemente und Datenaustausch*.

EN ISO 3166-1:1997, *Codes for the representation of names of countries and their subdivisions – Part 1: Country codes (ISO 3166-1:1997)*.

EN ISO/IEC 7816-4:1996, *Informationstechnik – Identifikationskarten – Karten mit integrierten Schaltkreisen und Kontakten – Teil 4: Interindustrielle Befehle für den Datenaustausch (ISO/IEC 7816-4:1996)*.

EN ISO/IEC 7816-6:1997, *Identifikationskarten – Karten mit integrierten Schaltkreisen und Kontakten – Teil 6: Interindustrielle Datenelemente (ISO/IEC 7816-6:1996)*.

ISO/IEC 8825 (all parts), *Information technology – ASN.1 encoding rules*.

ISO 8859-1:1987, *Information processing – 8-bit single-byte coded graphic character sets – Part 1: Latin alphabet No. 1*.

3 Definitionen, Symbole und Abkürzungen

3.1 In EN 1546-1 definierte Benennungen

In diesem Teil von EN 1546 werden folgende in EN 1546-1 definierte Benennungen angewendet:

- a) annehmende Stelle;
- b) Kartenausgeber;
- c) Währungsumrechnung;
- d) Protokoll der Währungsumrechnung;
- e) Identität;
- f) branchenübergreifende elektronische Geldbörse (IEP);
- g) IEP-Saldo;
- h) IEP-Kontrollanzeige;
- i) IEP-System;
- j) Aufladeeinrichtung;
- k) Aufladeprotokoll;
- l) Auflade-SAM; LSAM;
- m) Zahlung;
- n) Zahlungseinrichtung;
- o) Zahlungsprotokoll;
- p) Zahlungs-SAM; PSAM;
- q) SAM des Geldbörsenanbieters; PPSAM.

Um die für ein allgemeines IEP-System speziellen Benennungen hervorzuheben, beginnen (im englischen Original) diese Benennungen in der gesamten Europäischen Norm mit großen Buchstaben, z. B. Purchase Log (Zahlungsprotokoll).

3.1.1 In EN 1546-2 definierte Benennungen

In diesem Teil von EN 1546 werden folgende in EN 1546-2 definierte Benennungen angewendet:

- a) Beendigungscode;
- b) Signatur.

Um die für ein allgemeines IEP-System speziellen Benennungen hervorzuheben, beginnen (im englischen Original) diese Benennungen in der gesamten Europäischen Norm mit großen Buchstaben, z. B. Completion Code (Beendigungscode).

3.1.2 In EN 1546-3 definierte Benennungen

In diesem Teil von EN 1546 werden folgende in EN 1546-3 definierte Benennungen angewendet:

- a) benutzerbestimmte Daten.

Um die für ein allgemeines IEP-System speziellen Benennungen hervorzuheben, beginnen (im englischen Original) diese Benennungen in der gesamten Europäischen Norm

mit großen Buchstaben, z. B. Discretionary Data (Benutzerbestimmte Daten).

3.1.3 Für diesen Teil von EN 1546 bestimmte Benennungen

Für die Anwendung dieser Norm gelten folgende Definitionen:

3.1.3.1

zusammengesetztes Datenobjekt

ein Datenobjekt, bei dem das Wertefeld selbst ein Datenobjekt ist (siehe EN ISO/IEC 7816-4:1996).

3.1.3.2

Datenelement

wie in EN 1546-3 definiert.

ANMERKUNG Es kann in einem Wertefeld eines Datenobjektes dargestellt werden (siehe EN ISO/IEC 7816-4:1996).

3.1.3.3

Datenobjekt

eine Verkettung folgender Byte-Ketten (siehe EN ISO/IEC 7816-4:1996):

- eines obligatorischen Identifizierungskennzeichnfeldes, bezeichnet als ein Identifizierungskennzeichen;
- eines obligatorischen Längnfeldes, das eine Länge L angibt;
- eines wahlfreien Wertefeldes mit L Bytes (wenn L ungleich '00' ist).

3.1.3.4

Verzeichnis

eine Menge von Kopflisten, die die festen Formate definieren, die von der IEP verwendet werden.

3.1.3.5

Kopfliste

ein Datenelement, das eine Verkettung von Identifizierungskennzeichen-Länge-Paaren ohne Begrenzer enthält.

3.1.3.6

einfaches Datenobjekt

ein Datenobjekt, bei dem das Wertefeld nicht als ein Datenobjekt betrachtet werden muss.

3.1.3.7

Identifizierungskennzeichen

ein Wert, der ein gegebenes Datenelement entweder eindeutig oder in Verbindung mit einem oder mehreren weiteren Identifizierungskennzeichen kennzeichnet.

Um die für ein allgemeines IEP-System speziellen Benennungen hervorzuheben, beginnen (im englischen Original) diese Benennungen in der gesamten Europäischen Norm mit großen Buchstaben, z. B. Data Object (Datenobjekt).

3.2 Symbole und Abkürzungen

A	Vektor (Bezeichner für eine geordnete Menge von Datenelementen)
n..m	der Bereich von n bis (einschließlich) m
'0'..'9' und 'A'..'F'	die sechzehn Hexadezimalziffern
Für die Beschreibung der Formate von Datenelementen werden folgende Vereinbarung angewendet:	
b	binär
n x	numerische (BCD-)Codierung mit x Stellen, z. B. n 6 bedeutet 6 numerische Stellen (codiert in 3 Bytes)
an x	alpha-numerische Codierung mit x Zeichen (nach ISO 8859-1)
ASN.1	abstract syntax notation one Notation Eins für darstellungsunabhängige Syntax
BCD	binary coded decimal Binär codierte Dezimalziffer

BER	basic encoding rules grundlegende Codierungsregeln
DD	discretionary Data benutzerbestimmte Daten
IC	integrated circuit integrierter Schaltkreis
IEP	inter-sector electronic purse branchenübergreifende elektronische Geld- börse
LDA	load device application Anwendung der Aufladeeinrichtung
LSAM	load SAM Auflade-SAM
PDA	purchase device application Anwendung der Zahlungseinrichtung
PSAM	purchase SAM Zahlungs-SAM
SAM	secure application module Anwendungssicherheitsmodul
TEHL	tag for an extended headerlist Identifizierungskennzeichen für eine er- weiterte Kopfliste
THL	tag for a headerlist Identifizierungskennzeichen für eine Kopfliste
TLV	tag-length-value Identifizierungskennzeichen-Länge-Wert
TOD	tag for operational data Identifizierungskennzeichen für Betriebsdaten

4 Beschreibung des Verzeichnismechanismus

Wenn nicht die vorgegebenen festen Nachrichtenformate nach EN 1546-3 verwendet werden, müssen die in diesem Teil von EN 1546 angegebenen Regeln angewendet werden.

4.1 Einleitung

Die in diesem Teil von EN 1546 definierte Anwendung von Verzeichnissen ist ein Verfahren für die Realisierung von Nachrichtenformaten in IEP-Systemen. Sie ermöglicht andere Längen für einige Datenelemente, eine unterschiedliche Anordnung von Datenelementen in Nachrichten und die Identifizierung der in den Nachrichten enthaltenen benutzerbestimmten Datenelemente (und ihre Längen). Der Mechanismus beruht auf der TLV-Codierung.

Die IEP zeigt an, ob entsprechend dem Wert des Anwendungsprofils der IEP (AP_{IEP}) die TLV-Codierung der Datenelemente erforderlich ist. Die genauen Einzelheiten der Codierung für AP_{IEP} werden in 4.2 angegeben.

Wenn die IEP die TLV-Codierung unterstützt, können die Datenelemente, die in den nach EN 1546-3 definierten Nachrichten gesendet werden, andere Längen und eine andere Anordnung besitzen, als in EN 1546-3 festgelegt. Für jede Transaktionsart und wahlweise für jede Protokoll-datei muss eine Kopfliste definiert werden, die in der IEP gespeichert werden darf.

Falls notwendig, können Endgeräte die Kopfliste der IEP mit dem Befehl Daten Erhalten nach 4.7 lesen.

Die Kopflisten geben alle die Informationen an, die zum Aufbau und zur Auswertung der Nachrichten zur bzw. von der IEP notwendig sind, da sie aus einer Anzahl von Identifizierungskennzeichen-Länge-Paaren bestehen, die das Vorhandensein und die Anordnung jedes Datenelementes in einer Nachricht/einem Protokoll Datensatz sowie ihre Länge definieren.

In anwendungsspezifischen Nachrichten übertragene Datenelemente werden nicht mit einem Identifizierungskennzeichen versehen, d. h., es werden keine Identifizierungskennzeichen- und Längfelder übertragen, sie müssen aber dem festen Format und der festen Reihenfolge entsprechen, die in der entsprechenden Kopfliste festgelegt sind.

4.2 Angabe der Verwendung der TLV-Codierung

Die IEP muss der Endeinrichtung angeben, ob feste Formate nach EN 1546-3 benutzt werden oder nicht. Für diesen Zweck werden die beiden Bits (b4-b3) im ersten Byte des Datenelementes $APIEP$ verwendet. Im Normalfall wird die Endeinrichtung dieses Datenelementes als Teil der Anwendungsauswahl empfangen.

Für die Codierung der Bits b3-b4 in AP_{IEP} bestehen folgende mögliche Kombinationen:

- b4-b3 = 00: ASN.1-BER wird nicht angewendet (es werden feste Formate nach EN 1546-3 verwendet);
- b4-b3 = 01: in der IEP sind Kopflisten für Befehle und Rückmeldungen vorhanden;
- b4-b3 = 10: in der IEP sind Kopflisten für das Layout von Protokolldateien vorhanden (feste Formate werden verwendet);
- b4-b3 = 11: in der IEP sind Kopflisten für Befehle, Rückmeldungen und für Layouts von Protokolldateien vorhanden.

4.3 Struktur der Kopfliste

Eine Kopfliste definiert die Liste von Datenelementen, ihre Länge und in welcher Reihenfolge sie in einer Nachricht verkettet sind.

Eine Kopfliste ist entweder einfach oder erweitert.

Eine einfache Kopfliste umfasst:

- ein Identifizierungskennzeichen-Länge-Paar, TTL (Identifizierungskennzeichen für eine Kopfliste), das die Kopfliste und ihre Länge kennzeichnet;
- eine geordnete Menge von Identifizierungskennzeichen-Länge-Paaren, TODs (Identifizierungskennzeichen für Betriebsdaten), eine für jedes Datenelement der Nachricht.

Eine einfache Kopfliste ist ein einfaches Datenobjekt nach ISO/IEC 8825.

Eine erweiterte Kopfliste umfasst:

- ein Identifizierungskennzeichen-Länge-Paar, TEHL, das die Kopfliste und ihre Länge kennzeichnet;
- eine Kopfliste (einfach oder erweitert).

Eine erweiterte Kopfliste ist ein zusammengesetztes Datenobjekt nach ISO/IEC 8825.

Zum Beispiel legt die Kopfliste der Zahlungstransaktion die Identifizierungskennzeichen-Länge-Paare für alle Befehle/Rückmeldungen fest, die zu dieser Transaktion gehören. Das sind:

- a) die Identifizierungskennzeichen-Länge-Paare im Befehl und der Rückmeldung für IEP für Zahlung Initialisieren;
- b) die Identifizierungskennzeichen-Länge-Paare im Befehl und der Rückmeldung für IEP für Zahlung Abbuchen, erster Schritt;
- c) die Identifizierungskennzeichen-Länge-Paare im Befehl und der Rückmeldung für IEP für Zahlung Abbuchen, nachfolgender Schritt;
- d) die Identifizierungskennzeichen-Länge-Paare im Befehl und der Rückmeldung für IEP für Zahlungsquittung Abbuchen;

Kopflisten werden, wie in Bild 1 dargestellt, codiert.

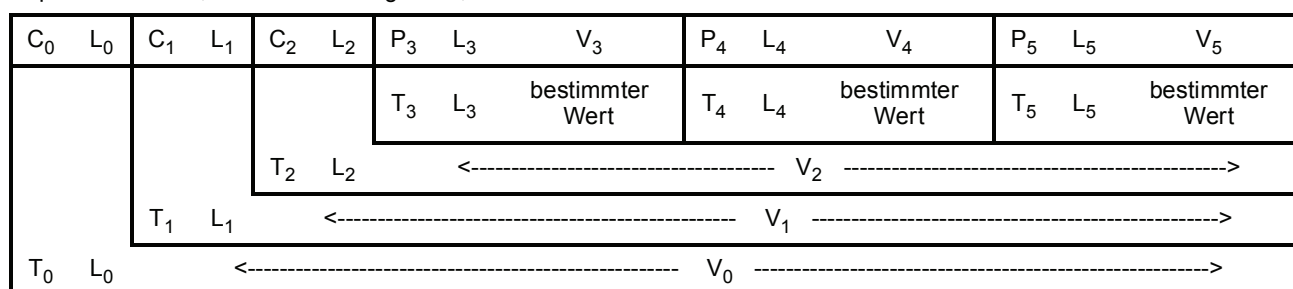


Bild 1 – Codierung einer Kopfliste

C₀, C₁, C₂ sind Identifizierungskennzeichen (T) von zusammengesetzten Datenobjekten mit den Längen L₀, L₁, L₂ bzw. den Werten V₀, V₁, V₂, die Teilmengen einer IEP-Kopfliste definieren, und sie entsprechen ASN.1.

C₀ könnte zum Beispiel das Identifizierungskennzeichen der vollständigen Kopfliste sein (in dieser Norm 'E5'), C₁ könnte das Identifizierungskennzeichen der Transaktionsart sein ('E7' für Zahlung) und C₂ könnte das Identifizierungskennzeichen der Rückmeldungsnachricht sein ('F1').

P₃, P₄, P₅ sind Identifizierungskennzeichen von einfachen Datenobjekten mit den Längen L₃, L₄, L₅ bzw. den Werten V₃, V₄ und V₅, die speziell zum Begriff der Kopfliste der IEP-Anwendung gehören. Diese einfachen Identifizierungskennzeichen definieren Datenelemente des IEP-Systems und ihren Ursprung ('D4' für Datenelemente, die aus der IEP stammen), und sie entsprechen ASN.1.

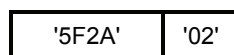
Die speziellen Werte (V₃, V₄, V₅) sind wie folgt strukturiert und sind keine Datenobjekte:

Jeder spezielle Wert definiert ein Datenelement, das mit einem Identifizierungskennzeichen und einer Länge bezeichnet wird:



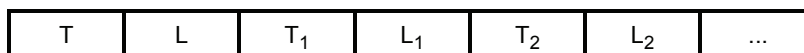
mit T = Identifizierungskennzeichen, L = Länge des Datenelementes.

Der Währungscode der IEP (CURR_{IEP}) kann beispielsweise wie folgt codiert werden:



Das Identifizierungskennzeichen dieses Datenelementes ist '5F2A' und die Länge beträgt 2 Bytes.

Ein spezieller Wert könnte auch eine Kette von Identifizierungskennzeichen-Länge-Paaren definieren, die zum selben Datenvektor gehören und wie folgt codiert werden könnte:



mit T = Identifizierungskennzeichen des Datenvektors, L = Länge der folgenden Identifizierungskennzeichen-Länge-Paare, T₁L₁ ... die Kette der einzelnen Identifizierungskennzeichen-Länge-Paare.

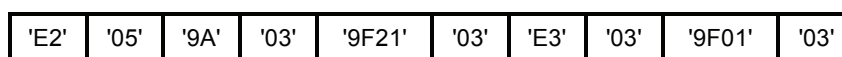
Der Vektor der Information für den (öffentlichen) Schlüssel der IEP könnte zum Beispiel wie folgt codiert werden:



'E0' ist das Identifizierungskennzeichen für den Vektor der Informationen für den IEP-Schlüssel mit einer Länge von 12 Bytes und 'E1' ist das Identifizierungskennzeichen für einen einzelnen Block eines öffentlichen Schlüssels, sein Zertifikat und zugehörige Daten (10 Bytes).

'CA', 'CE', '5F24', 'CF' sind die Identifizierungskennzeichen spezieller Datenelemente: Identität des Geldbörsenanbieters, Zertifikat des öffentlichen Schlüssels, Ablaufdatum des öffentlichen Schlüssels bzw. öffentlicher Schlüssel mit den Längen 3, 128, 3, 64 Bytes, d. h., ein öffentlicher Schlüssel mit 512 Bytes mit einem Zertifikat von 1024 Bits.

Der Vektor der benutzerbestimmten Datenelemente könnte zum Beispiel wie folgt codiert werden:



'E2' ist das Identifizierungskennzeichen für den Vektor der „nicht zu signierenden benutzerbestimmten Daten“ mit einer Länge von 6 Bytes und 'E3' ist das Identifizierungskennzeichen für den Vektor der „zu signierenden benutzerbestimmten Daten“ mit einer Länge von 3 Bytes, während '9A', '9F21', '9F01' die Identifizierungskennzeichen der speziellen Datenelemente sind: Transaktionsdatum, Transaktionszeit bzw. Identität der annehmenden Stelle, alle mit einer Länge von 3 Bytes. Spezielle Beispiele für die Anwendung der Kopflisten werden in Anhang A beschrieben.

4.4 Codierung des Identifizierungskennzeichenfeldes

In diesem Abschnitt werden die Regeln definiert, die zum Codieren des Identifizierungskennzeichenfeldes benötigt werden, und es werden spezielle Werte von Identifizierungskennzeichen aufgeführt, die den Datenobjekten zugewiesen wurden.

4.4.1 Allgemeine Regeln

Allen in der vorliegenden Europäischen Norm verwendeten Datenelementen werden Identifizierungskennzeichenwerte zugewiesen. Diese Identifizierungskennzeichenwerte definieren entweder einfache oder zusammengesetzte Datenobjekte. Wenn zutreffend, werden durch ISO/IEC 7816-6 zugewiesene Datenelemente angewendet, alle weiteren für die IEP-Anwendung spezifischen Datenobjekte werden mit dieser Europäischen Norm definiert.

Der Wert eines Identifizierungskennzeichens gibt an, ob das entsprechende Datenobjekt einfach oder zusammengesetzt ist:

- wenn Bit b6 im ersten Byte des Identifizierungskennzeichens gleich 0 ist, ist es mit einem einfachen Datenobjekt verbunden;
- wenn Bit b6 im ersten Byte des Identifizierungskennzeichens gleich 1 ist, ist es mit einem zusammengesetzten Datenobjekt verbunden.

Ein Identifizierungskennzeichen kann entweder 1 Byte oder 2 Bytes lang sein:

- wenn die Bits b1-b5 des ersten Bytes des Identifizierungskennzeichens alle gleich 1 sind, beträgt die Länge 2 Bytes;
- in allen anderen Fällen beträgt die Länge 1 Byte.

Die Codierung des ersten Bytes des Identifizierungskennzeichens ist in Tabelle 1 dargestellt.

Tabelle 1 – Struktur des ersten Bytes eines Identifizierungskennzeichens

b8	b7	b6	b5	b4	b3	b2	b1	Bedeutung
0	1	-	-	-	-	-	-	Durch ISO/IEC 7816-6 zugewiesene Identifizierungskennzeichen
1	1	-	-	-	-	-	-	In diesem Teil von EN 1546 definierte weitere Identifizierungskennzeichen
-	-	0	-	-	-	-	-	Identifizierungskennzeichen für einfache Datenobjekte
-	-	1	-	-	-	-	-	Identifizierungskennzeichen für zusammengesetzte Datenobjekte
-	-	-	1	1	1	1	1	Das Identifizierungskennzeichen ist 2 Bytes lang. Der Wert im Bereich von 31..127 ist im zweiten Byte enthalten.
-	-	-	x	x	x	x	x	Das Identifizierungskennzeichen ist 1 Byte lang. Der Wert im Bereich von 0..30 ist in b1-b5 enthalten.

4.4.2 Einfache Datenobjekte

Die in Tabelle 2 aufgeführten einfachen Datenobjekte sind die in EN 1546-3 definierten Datenelemente. Das Format für diese Datenelemente ist in EN 1546-3 tiefergehend definiert.

Tabelle 2 – Einfache Datenobjekte

Identifizierungskennzeichen	Name	Beschreibung	Format	Länge
'4F'	AID	Anwendungsbezeichner	n 10-32	5-16 Bytes
'84'	(AID)	Dateiname, z. B. AID, in der Dateisteuerinformation	b	variabel
'C0'	ALG	Algorithmenbezeichner	b	1-5 Bytes
'C1'	AM	Authentisierungsmodus	Bitmap	1 Byte
'C2'	AP	Anwendungsprofil	Bitmap	2 Bytes
'C3'	BAL	Saldo	b	2-8 Bytes
'C4'	BALmax	Höchstsaldo	b	2-8 Bytes
'C5'	CC	Beendigungscode	b	2 Bytes
'5F2A'	CURRC	Währungscode	n 3	2 Bytes
'5F36'	CURRE	Währungsexponent	n 1	1 Byte
'CE'	$C_n K_n^P$	Zertifikat für einen öffentlichen Schlüssel	b	variabel
'5F25'	DACT	Aktivierungsdatum der Anwendung	n 6 YYMMDD	3 Bytes
'C6'	DDEA	Deaktivierungsdatum der Anwendung	n 6 YYMMDD	3 Bytes
'5F24'	DEXP	Ablaufdatum der Anwendung	n 6 YYMMDD	3 Bytes
'C7'	ID	Bezeichner der Komponente	b	2-8 Bytes
'CF'	K_n^P	Öffentlicher Schlüssel	b	variabel
'C8'	M	Transaktionsbetrag (vollständig oder Teil)	b	4-8 Bytes

Tabelle 2 (fortgesetzt)

Identifizierungskennzeichen	Name	Beschreibung	Format	Länge
'C9'	MTOT	Gesamttransaktionsbetrag (Zahlung)	b	4-8 Bytes
'5F32'	NT	Transaktionsnummer	b	2-8 Bytes
'CA'	PP	ID des Geldbörsenanbieters (oder der Instanz für die Schlüsselzertifizierung)	n 6	3 Bytes
'CB'	R	Zufallszahl	b	4-8 Bytes
'CC'	S _n	Signatur	b	variabel
'D2'	TRT	Transaktionsart und -status	Bitmap	1 Byte
'CD'	VK	Schlüsselversion	b	1-4 Bytes

4.4.3 Zusammengesetzte Datenelemente

Die in Tabelle 3 aufgeführten zusammengesetzten Datenelemente definieren die strukturellen Begrenzer, die beim Aufbau von Kopflisten angewendet werden können, um die genauen Formate für Nachrichten und Dateien in der IEP festzulegen, wie in 4.3 beschrieben. Um den Mehraufwand einzuschränken, entspricht der Anwendungsmechanismus für diese zusammengesetzten Datenobjekte bezogen auf die Kopflisten nicht genau ASN.1. Es ist nicht notwendig, Wertefelder aufzunehmen, da diese durch die Endeinrichtung selbst über ihre gespeicherten Verzeichnisse von den entsprechenden Daten in Befehlen und Rückmeldungen erhalten werden können.

Tabelle 3 – Zusammengesetzte Datenobjekte

Identifizierungskennzeichen	Name	Beschreibung
'D4'	IEP	Datenelemente von der IEP
'D5'	PSAM	Datenelemente vom PSAM
'D6'	PPSAM	Datenelemente vom PPSAM
'D7'	LSAM	Datenelemente vom LSAM
'D8'	xDA	Datenelemente von der Einrichtungsanwendung, z. B. LDA oder PDA
'D9'	xHOST	Datenelemente vom Hauptrechner, z. B. Hauptrechner des Geldbörsenanbieters oder Hauptrechner der annehmenden Stelle
'E0'	IK	Vektor der Schlüsselinformation
'E1'	CERT	Block, der einen öffentlichen Schlüssel, das Zertifikat und zugehörige Daten enthält
'E2'	DDU	nicht zu signierende benutzerbestimmte Daten
'E3'	DDS	zu signierende benutzerbestimmte Daten
'E4'	DDV	als Teil der Signatur zu überprüfende benutzerbestimmte Daten
'F0'	Befehl	im Befehl übertragene Datenelemente
'F1'	Rückmeldung	in der Rückmeldung übertragene Datenelemente
'F2'	TPARM	Identifizierungskennzeichen zur Angabe der Lage des zu aktualisierenden Parameters

Tabelle 4 – Für Kopflisten definierte Identifizierungskennzeichen

Identifizierungskennzeichen	Name	Beschreibung
'E5'	TGLALL	Kopfliste für alle Befehle und Rückmeldungen
'E6'	TGLL	Kopfliste für Befehle und Rückmeldungen, die sich auf das Aufladen beziehen
'E7'	TGLP	Kopfliste für Befehle und Rückmeldungen, die sich auf die Zahlung beziehen
'E8'	TGLC	Kopfliste für Befehle und Rückmeldungen, die sich auf den Zahlungsabbruch beziehen
'E9'	TGLE	Kopfliste für Befehle und Rückmeldungen, die sich auf die Währungsumrechnung beziehen
'EA'	TGLU	Kopfliste für Befehle und Rückmeldungen, die sich auf die Aktualisierung der IEP-Parameter beziehen